KACE®システム管理アプライアンス13.0

管理者ガイド

目次

KACE システム管理アプライアンスについて

Quest® KACE® **システム管理アプライアンス** は、デバイスの管理、アプリケーションの展開、パッチ適用、資産管理、レポート作成、サービスデスクチケット管理などを自動化するための、仮想アプライアンスです。

KACE シリーズアプライアンスの詳細については、Quest の Web サイト（ https://www.quest.com/products/kace-systems-management-appliance/ ）を参照してください。

KACE システム管理アプライアンス は、エンドユーザーのチケットと資産を管理できる KACE システム管理アプライアンスの限定バージョンです。KACE エージェントを使用して、単一のデバイスノードと最大 250 のエージェント不要ノードを管理します。KACE システム管理アプライアンスとは異なり、パッチ適用機能やスクリプト作成機能、ソフトウェア資産管理機能は含まれていません。これらの機能については、このマニュアルで説明していますが、**KACE システム管理アプライアンス** では無効になっています。**KACE システム管理アプライアンス** を簡単に KACE システム管理アプライアンスにアップグレードして、エンドポイント管理機能の完全なセットを有効にできます。この製品、その技術仕様と参考資料の詳細については、https://support.quest.com/kace-systems-management-appliance/technical-documents のマニュアルのランディングページを参照してください。

アプライアンスコンポーネントについて

アプライアンスコンポーネントには、ソフトウェア、ハードウェア、Web ベースのインターフェイス、およびモバイルアプリケーションインターフェイスが含まれます。

アプライアンスコンポーネント

コンポーネント	説明
仮想アプライアンス	アプライアンスは、VMware® または Microsoft® Hyper-V® インフラストラクチャを使用する仮想環境で実行されます。管理対象デバイスの要件、および**管理者コンソール**にアクセスするためのブラウザの要件に関する最新情報については、製品ドキュメントページで利用できる技術仕様を参照してください。https://support.quest.com/kace-systems-management-appliance/technical-documents.
コマンドラインコンソール	**コマンドラインコンソール**は、アプライアンスへのターミナルウィンドウインターフェイスです。これは主にアプライアンスの設定とポリシーの適用のためのインターフェイスです。詳細については、「アプライアンスの電源投入と管理者コンソールへのログイン」を参照してください。
管理者コンソール	**管理者コンソール**は、アプライアンスを制御するために使用する Web ベースインターフェイスです。**管理者コンソール**にアクセスするには、http://**appliance_hostname**/admin に移動します。**appliance_hostname** はアプライアンスのホ

コンポーネント	説明
	スト名です。組織コンポーネントが有効になっている場合は、http://**appliance_hostname**/system から、**管理者コンソール**のシステムレベル設定にアクセスできます。**管理者コンソール**で URL の完全パスを表示すると、データベースの検索やリンクの共有に便利です。完全パスを表示するには、ログインで使用する URL に ui を追加します。例えば、次のようになります。http://**appliance_hostname**/adminui
ユーザーコンソール	**ユーザーコンソール**は、ユーザーがアプリケーションをセルフサービス方式で使用できるようにする Web ベースのインタフェースです。このインターフェイスから、サービスデスクのサポートチケットを提出して、ヘルプを要求したり問題をレポートしたりすることもできます。**ユーザーコンソール**にアクセスするには、http://**appliance_hostname**/user に移動します。**appliance_hostname** はアプライアンスのホスト名です。 **ユーザーコンソール**は次のものを提供します。 • ユーザーが必要に応じてダウンロードできるアプリケーションのリポジトリ。 • ユーザーがヘルプを依頼するチケットを送信および追跡するための手段。 • 日常的なタスクのサポート（ソフトウェアのインストールや、**Questサポート技術情報**、https://support.quest.com/kace-systems-management-appliance/kbへのアクセスなど）。 **ユーザーコンソール**をカスタマイズするには、次を参照してください。 • 組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定. • 組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定.
KACE エージェント	KACE エージェントは、デバイスにインストールして、アプライアンス経由でのデバイス管理を可能にするアプリケーションです。管理対象デバイスにインストールされたエージェントは、エージェントメッセージプロトコルを通じてアプライアンスと通信します。エージェントは、管理対象デバイスからのインベントリ情報の収集や、管理対象デバイスへのソフトウェアの配布などのスケジュール済みタスクを実行します。プリンタや、エージェントによるサポート対象以外のオペレーティングシステムを搭載したデバイスなど、エージェントソフトウェアをインストールできないデバイスでは、エージェント不要の管理も使用可能です。 詳細については、「KACE エージェントのプロビジョニング」を参照してください。

コンポーネント	説明
KACE GO	KACE GOは、管理者がスマートフォンやタブレットを使用して、サービスデスクチケット、インベントリ情報、およびアプリケーション導入機能にアクセスするためのアプリケーションです。このアプリケーションにより、管理者以外のユーザーもサービスデスクチケットの送信、提出されたチケットのステータスの表示、およびモバイルデバイスからのサポート技術情報記事の閲覧を行うことができるようになります。iOSデバイスの場合はApple® App Store℠から、Android™デバイスの場合はGoogle Play™ Storeからそれぞれ KACE GOをダウンロードできます。 詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。

管理者コンソールについて

管理者コンソールで使用可能なコンポーネントは、ライセンスキー、組織設定、アプライアンス設定、およびユーザーの役割に応じて異なる場合があります。

さらに、組織コンポーネントが有効化されている場合、管理者コンソールには2つのレベルが存在します。組織関連の機能を示す管理者レベルとアプライアンス関連の機能を示すシステムレベルです。

組織コンポーネントが有効化されている場合、管理レベルおよびシステムレベルの機能は管理レベルで利用可能になります。

注: ライセンスキーによって、組織コンポーネントが有効または無効のいずれであるかが決定されます。製品ライセンス情報の表示および組織についてを参照してください。

以下の3種類のログインモードがあります。

- **組織コンポーネントが有効化されていない場合の管理者モード**: アプライアンスで組織コンポーネントが有効化されていない場合は、http://**appliance_hostname**/admin（**appliance_hostname** はアプライアンスのホスト名）にアクセスして、このモードにログインします。このモードで使用可能なコンポーネントについては、組織コンポーネントが有効化されていない場合の管理者モードで使用可能なコンポーネントを参照してください。
- **組織コンポーネントが有効化されている場合の管理者モード**: アプライアンスで組織コンポーネントが有効化されている場合は、http://**appliance_hostname**/admin にアクセスして、デフォルトの組織にログインします。**appliance_hostname** はアプライアンスのホスト名です。管理者モードでは、選択した組織で使用可能なコンポーネントを管理できます。このモードで使用可能なコンポーネントについては、組織コンポーネントが有効化されている場合の管理者モードで使用可能なコンポーネントを参照してください。

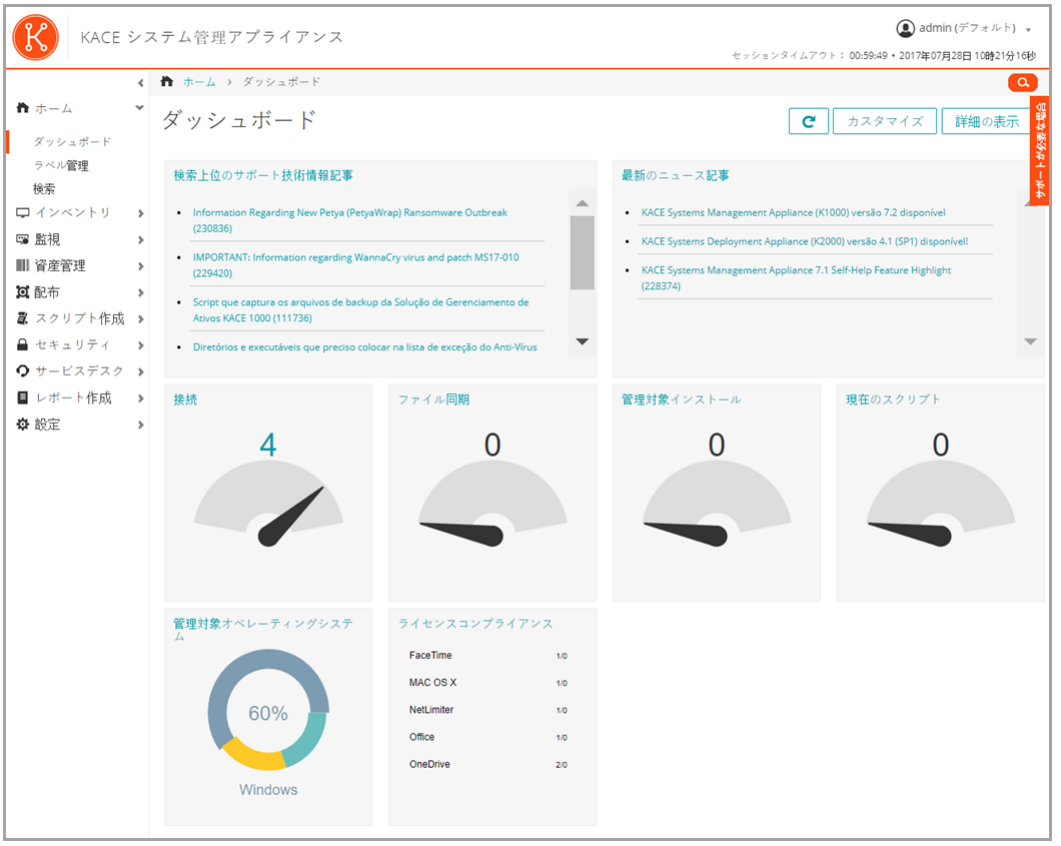
  アプライアンスの設定で ログインする組織 オプションが有効な場合は、組織 ボックスが表示されます。組織 ボックスに組織名を入力すると、その組織に直接ログインできます。

  組織が複数あり、高速切り替え オプションが有効化されている場合は、ページの右上隅でログイン情報の横にあるドロップダウンリストを使用して組織とシステムレベルを切り替えることができます。詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。
- **組織コンポーネントが有効化されている場合のシステムモード:** アプライアンスで組織コンポーネントが有効化されている場合は、http://**appliance_hostname**/system にアクセスして、システムモードにログインします。**appliance_hostname** はアプライアンスのホスト名ですこのモードでは、システムレベルで使用可能なコンポーネントを管理できます。このモードで使用可能なコンポーネントについては、組織コンポーネントが有効化されている場合のシステムモードで使用可能なコンポーネントを参照してください。

また、高速切り替え オプションが有効化されており、かつ複数ある組織のデフォルトの管理者アカウントのパスワードが同一の場合は、ページ右上隅にある 組織 ドロップダウンリストを使用して、組織を切り替えることもできます。詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。

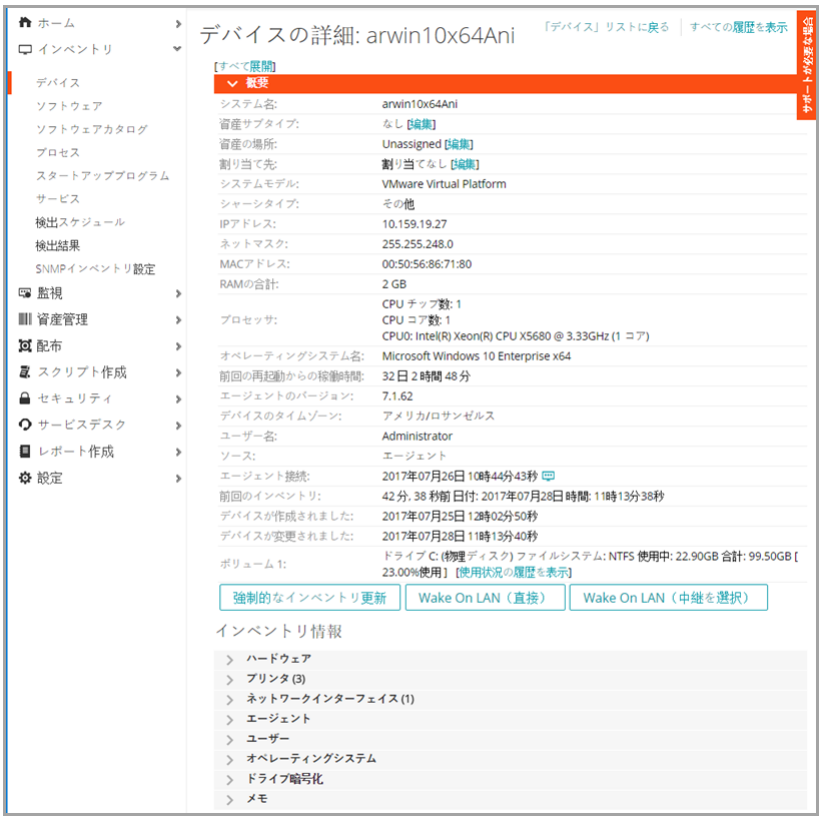
各モデルには次のタイプのページがあります。

- **ダッシュボード**: これらのページには、アプライアンスのステータス情報が表示されます。組織コンポーネントが有効化されている場合、ダッシュボードは組織およびアプライアンスレベルで利用可能になります。



- **リストページ**: これらのページでは、アプライアンス上の、または組織コンポーネントが有効化されている場合は選択された組織の使用可能なアイテムを表示できます。

- **詳細ページ**: これらのページでは、選択されたアイテムの詳細を表示および編集できます。

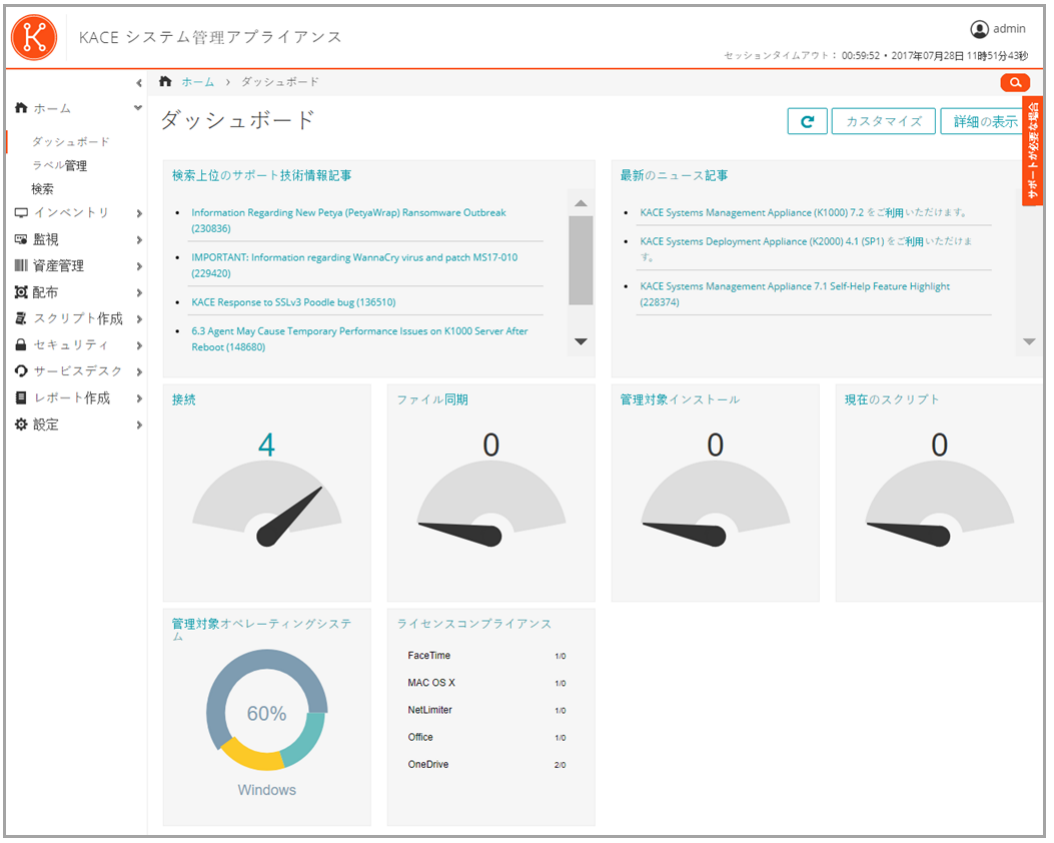


- **設定ページ**: これらのページでは、設定を行うことができます。

- **パネル**: これらのページでは、関連するコンポーネントと設定にアクセスできます。

組織コンポーネントが有効化されていない場合の管理者モードで使用可能なコンポーネント

組織コンポーネントが有効化されていない場合、管理者モードでは、管理者レベルのコンポーネントおよびシステムレベル（アプライアンスレベル）の設定がすべて表示されます。



組織コンポーネントが有効化されていない場合の管理者モードで使用可能なコンポーネント

コンポーネント	UIページ	用途...
ホーム	• ダッシュボード • ラベル管理 • 検索	アプライアンス統計の確認、ラベルの管理、履歴情報の表示、およびデータの検索を行います。詳細については、「「ホーム」コンポーネントの使用」を参照してください。
インベントリ	• デバイス • ソフトウェア • ソフトウェアカタログ • プロセス（複数） • スタートアッププログラム • サービス • 検出スケジュール • 検出結果 • SNMPインベントリ設定	ネットワーク上のデバイス、ソフトウェア、プロセス、サービス、スキャン、およびその他のアイ

コンポーネント	UIページ	用途...
		テムを管理します。詳細については、以下を参照してください。 • デバイスインベントリの管理 • ソフトウェア ページでのアプリケーション管理 • ソフトウェアカタログインベントリの管理 • プロセス、スタートアッププログラム、およびサービスインベントリの管理 • デバイス検出の使用 • インベントリに追加する特定の SNMP オブジェクトおよびコンピューター以外のデバイスを特定するための SNMP インベントリ設定の使用
監視	• デバイス • 警告 • プロファイル • メンテナンスウィンドウ • Log Enablement Packages	標準ライセンスがある 5 台のサーバーの基本イベント監視を管理して、コア Windows® イベントログ、シスログ、およびアプリケーションログからイベントデータを収集します。 監視モジュールライセンスによって、最大200台のサーバーのイベント監視を管理します。

コンポーネント	UIページ	用途...
		詳細については、次を参照してください。 サーバーの監視
資産	• 資産 • 資産タイプ • 契約 • ライセンス • ライセンスコンプライアンス • 場所 • 資産のインポート	物理資産（デバイス、ソフトウェア、プリンタなど）の追跡、および各資産とその設定の履歴の表示を行います。詳細については、以下を参照してください。 • インベントリの管理 • ライセンスコンプライアンスの管理
配布	• 管理対象インストール • ファイル同期 • Wake On LAN • レプリケーション • 警告	ソフトウェア（Questからの更新プログラムを含む）をリモートで配布および管理します。 詳細については、「管理対象デバイスへのパッケージの展開」を参照してください。
スクリプト	• スクリプト • 今すぐ実行 • 今すぐ実行のステータス • スクリプトログの検索 • 設定ポリシー • セキュリティポリシー • Mac プロファイル	管理対象デバイスで実行されるタスクを自動化します。 詳細については、「管理対象デバイスでのスクリプトの実行」を参照してください。
セキュリティ	• パッチ管理 • OVALスキャン • SCAPスキャン • Dellアップデート	マルウェア、スパイウェア、およびウイルスによるリスクを軽減します。OVAL（Open Vulnerability Assessment Language）は、管理対象デバイスのセキュリティの脆弱性を特定するために実行される一連のテストです。

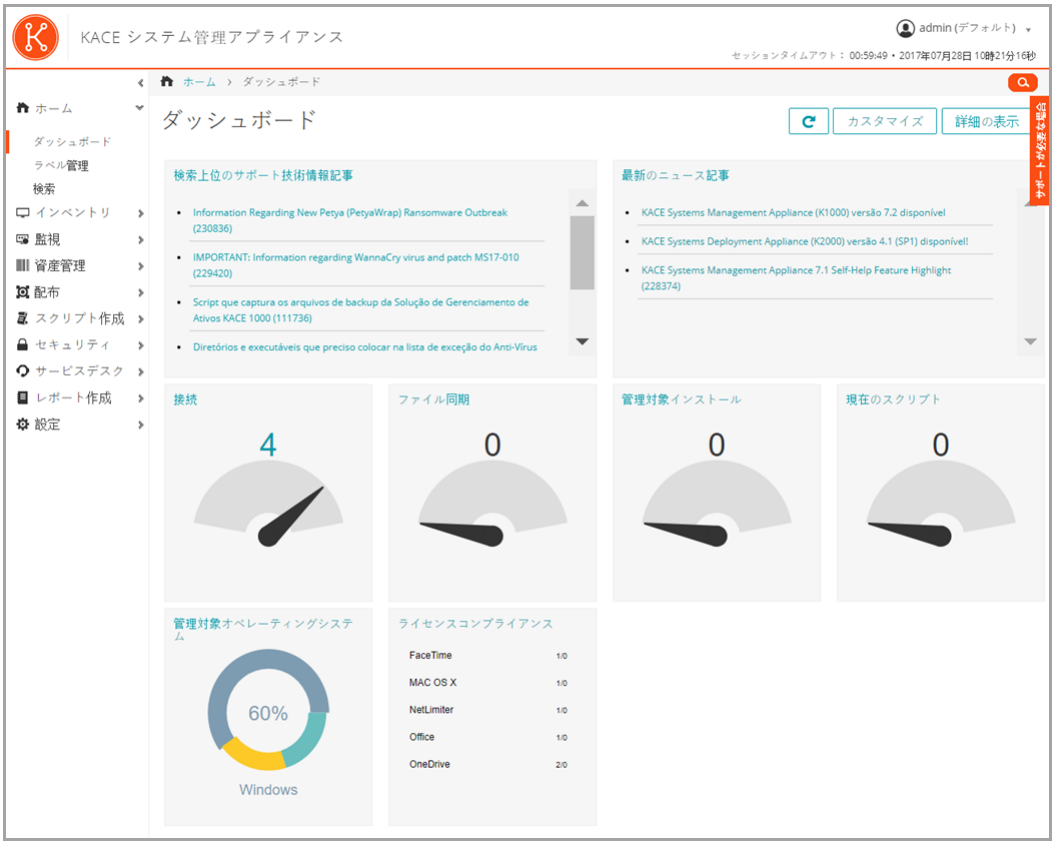
コンポーネント	UIページ	用途...
		詳細については、「デバイスのパッチ適用とセキュリティの維持」を参照してください。
サービスデスク（以前のバージョンからアップグレードされたアプライアンスではヘルプデスクと呼ばれる）	• チケット（複数） • ユーザーダウンロード • サポート技術情報 • 告知 • アーカイブ（チケットのアーカイブが有効化されている場合にのみ使用可能） • 設定	ユーザーがアクセスしてダウンロードするソフトウェアとドキュメントのリポジトリを提供します。チケットの作成および追跡を行うための豊富な機能を備えたサービスデスクが含まれています。 詳細については、「サービスデスクの使用」を参照してください。
レポート作成	• レポート • レポートスケジュール • 通知	パッケージ済みレポートとレポート作成ツールを実行してアプライアンスの実装を監視します。 詳細については、「レポートの使用と通知のスケジュール」を参照してください。
設定	• コントロールパネル • ユーザー • 資格情報 • 役割 • ログ • アプライアンスの更新 • プロビジョニング • リソース • 履歴 • サポート	アプライアンスとエージェントのプロビジョニングを管理します。詳細については、以下を参照してください。 • アプライアンスの設定 • ユーザーアカウント、LDAP認証、およびSSOの設定 • 資格情報の管理 • アプライアンスのメンテナンス • KACE エージェントのプロビジョニング • アプライアンスリソースのインポートとエクスポート • 設定履歴の管理 • トラブルシューティングツールの使用

組織コンポーネントが有効化されている場合の管理者モードで使用可能なコンポーネント

組織コンポーネントが有効化されている場合、管理者モードでは、現在の組織のみのコンポーネントおよび設定が表示されます。システムモードでは、アプライアンスレベルのコンポーネントが使用可能です。

アプライアンスで組織コンポーネントが有効化されており、http://**appliance_hostname**/admin にログインしている場合は、設定コンポーネントに選択した組織のみで使用可能な機能が表示されます。

その他のコンポーネントは、組織コンポーネントが有効化されているかどうかに関係なくすべて同じです。コンポーネントについては組織コンポーネントが有効化されていない場合の管理者モードで使用可能なコンポーネントを参照し、次の図を参照してください。



組織コンポーネントが有効化されている場合の管理者モードで使用可能なコンポーネント

コンポーネント	UIページ	用途...
設定	• コントロールパネル • ユーザー • 資格情報 • 役割 • プロビジョニング • リソース • 履歴 • サポート	ユーザー認証やエージェントのプロビジョニングなど、組織の一般設定を管理します。詳細については、以下を参照してください。 • アプライアンスの設定 • ユーザーアカウント、LDAP認証、およびSSOの設定 • 資格情報の管理 • KACE エージェントのプロビジョニング • アプライアンスリソースのインポートとエクスポート • 設定履歴の管理 • トラブルシューティングツールの使用

組織コンポーネントが有効化されている場合のシステムモードで使用可能なコンポーネント

組織コンポーネントが有効化されている場合、システムモードでは、アプライアンス設定に関連したコンポーネントが表示されます。管理者モードでは、組織レベルのコンポーネントが使用可能です。

アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインするか、**管理者コンソール**の右上隅にあるドロップダウンリストから **システム** を選択すると、次のコンポーネントを使用できます。

組織コンポーネントが有効化されている場合のシステムモードで使用可能なコンポーネント

コンポーネント	サブタブ	用途...
ホーム	• ダッシュボード	アプライアンスの統計の概要を確認します。 詳細については、「「ホーム」コンポーネントの使用」を参照してください。
設定	• コントロールパネル • 管理者 • ログ • アプライアンスの更新 • リソース • 履歴 • サポート	アプライアンスを管理し、**Quest サポート**などのリソースにアクセスします。詳細については、以下を参照してください。 • アプライアンスの設定 • アプライアンスのメンテナンス • アプライアンスリソースのインポートとエクスポート • 設定履歴の管理 • トラブルシューティングツールの使用
レポート作成	• レポート • レポートスケジュール	パッケージ済みレポートとレポート作成ツールを実行してアプライアンスの実装を監視します。 詳細については、「レポートの使用と通知のスケジュール」を参照してください。
組織	• 組織 • 役割 • フィルタ • デバイス	組織を追加し管理します（組織コンポーネントが必要です）。 詳細については、「組織の作成と管理」を参照してください。

「ホーム」コンポーネントの使用

「ホーム」コンポーネントには、ダッシュボード、ラベル管理、検索の機能が含まれます。

ダッシュボードについて

ダッシュボードは、組織やアプライアンスのアクティビティの概要を提供します。警告と、ニュース記事およびサポート技術情報記事へのリンクも提供します。

アプライアンスで組織コンポーネントが有効化されており、管理者コンソール（http://**appliance_hostname**/admin）にログインしている場合は、ダッシュボードに選択した組織の情報が表示されます。システム管理コンソール（http://**appliance_hostname**/system）にログインしている場合は、ダッシュボードにすべての組織を含めたアプライアンス情報が表示されます。

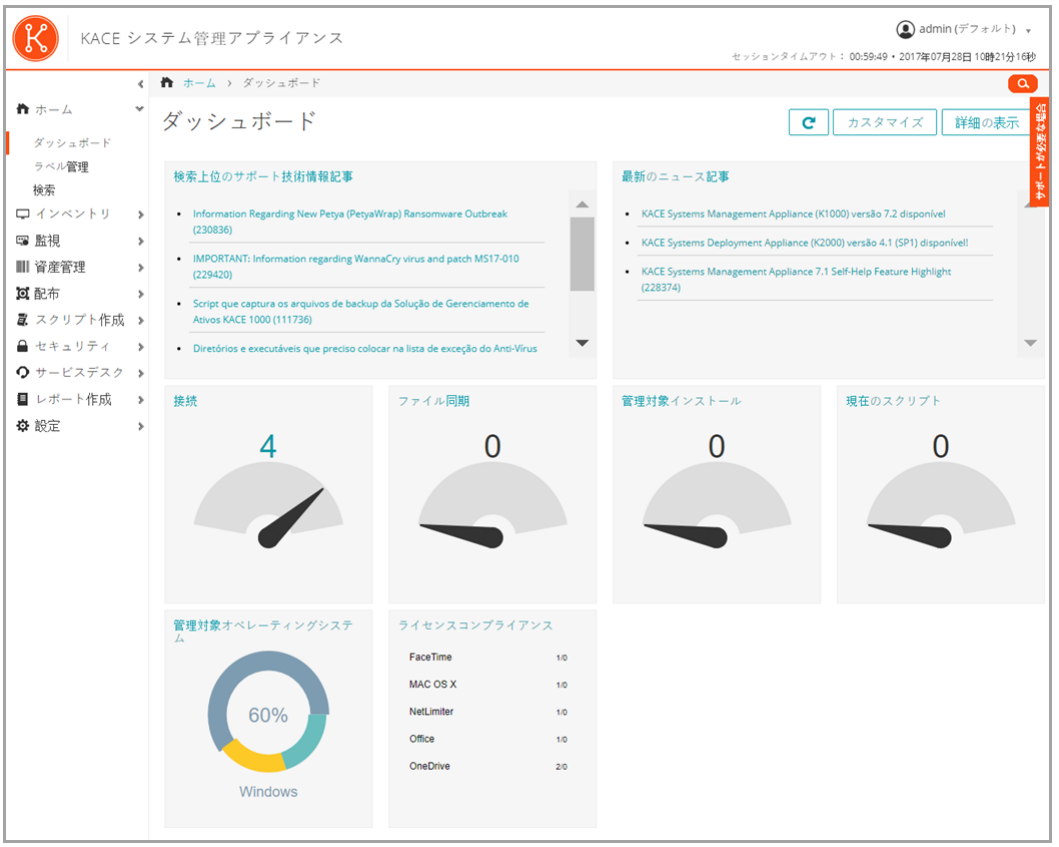
ヒント: アプライアンスは、概要ウィジェットを定期的に更新します。任意の時間にすべてのウィジェットを更新するには、ページの右上にある **更新** ボタンをクリックします: 。ウィジェットを個々に更新するには、ウィジェットの上にマウスを置き、ウィジェットの上の **更新** ボタンをクリックします。

管理者モードでのダッシュボードの表示

管理者モードのダッシュボードを表示して、アプライアンスの概要情報を検索するか、または組織コンポーネントが有効になっている場合は選択した組織の概要情報を検索します。

- 管理者コンソール（http://**appliance_hostname**/admin）にログインします。または、「管理ヘッダーに組織メニューを表示」が有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

Dashboard（ダッシュボード）ページが表示されます。



システムモードでのダッシュボードの表示

アプライアンスで組織コンポーネントが有効化されている場合は、システムダッシュボードを表示して、アプライアンスの概要情報を検索します。

- アプライアンスシステム管理コンソール（https://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。

システムダッシュボード ページが表示されます。

ダッシュボード ページのカスタマイズ

ダッシュボード ページをカスタマイズして、必要に応じて、ウィジェットを表示または非表示にできます。

1. 次のいずれかを実行します。
   - **アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または、管理ヘッダーに組織メニューを表示 がアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。**
   - **アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。**

   ダッシュボード ページまたは システム概要 ページが表示されます。
2. ウィジェットの上にマウスを置き、次のボタンのいずれかを使用します。
   - : ウィジェットの情報を更新します。
   - : ウィジェットに関する情報を表示します。
   - : ウィジェットを非表示にします。
   - : ウィジェットのサイズを変更します。
   - : ウィジェットをページ上の別の場所にドラッグできます。
3. 一部のウィジェットは編集可能で、表示する情報をフィルタリングできます。編集可能なウィジェットを編集するには、 をクリックし、表示されるダイアログボックスに必要な情報を入力します。場合によっては、必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。
4. ページの右上隅にある **カスタマイズ** ボタンをクリックすると、使用可能なウィジェットが表示されます。

5. インストールされているすべてのウィジェットを表示するには、**特定基準で表示 > すべてのアイテム**をクリックします。
6. サービスデスクウィジェットのみを表示するには、**特定基準で表示 > サービスデスク**をクリックします。
7. デバイスウィジェットのみを表示するには、**特定基準で表示 > デバイス** をクリックします。
8. 資産管理ウィジェットのみを表示するには、**特定基準で表示 > 資産管理** をクリックします。
9. セキュリティウィジェットのみを表示するには、**特定基準で表示 > セキュリティ** をクリックします。
10. 現在非表示のウィジェットを表示するには、**インストール** をクリックします。

ダッシュボードのウィジェットについて

ダッシュボードのウィジェットは、組織やアプライアンスのアクティビティの概要を提供します。

このセクションでは、ダッシュボードで使用可能なウィジェットについて説明します。アプライアンス上で組織コンポーネントが有効化されている場合は、ウィジェットに選択した組織の情報が管理者レベルで表示され、アプライアンスの情報がシステムレベルで表示されます。

ウィジェット	説明
一般ウィジェット	このセクションでは、アプライアンスのアクティビティの高レベルな概要を示します。これらのウィジェットに表示される情報では、潜在的な不具合を理解するために役立つ特定のインジケータに焦点が当てられます。
最新のニュース記事およびトップのサポート技術情報記事	この2つのウィジェットでは、Questからのニュースと情報へのリンクが提供されます。ニュース記事は日付順または重要度順に表示されます。サポート技術情報記事は、テクニカルサポートシステムでの優先度順に表示されます。
接続	このウィジェットには、アプライアンス Web サーバへの接続の数が表示されます。高い数値はサーバーに高い負荷がかかっていることを示し、これによってアプライアンスの応答速度が低下する場合があります。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ファイル同期	このウィジェットには、エージェント管理対象デバイスで進行中のファイル同期の数が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
管理対象インストール	このウィジェットには、エージェント管理対象デバイスで進行中の管理対象インストールの数が表示されます。アプライアンスで組織コンポーネントが有

ウィジェット	説明
	効になっている場合、ウィジェットには選択した組織の情報が表示されます。
現在のスクリプト	このウィジェットには、エージェント管理対象デバイスで実行可能なスクリプトの数が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ライセンスコンプライアンス	ソフトウェアのライセンス資産を作成済みの場合、このウィジェットにはライセンス認証された特定のソフトウェアがインストールされたエージェント管理対象デバイスの数と、使用可能なライセンスの数が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。 ライセンス資産は、ソフトウェア ページおよびソフトウェアカタログ ページにリストされたアプリケーションに対して作成できます。このウィジェットにライセンス情報が表示されるようにするには、アプリケーションのライセンスモードが Unit License（ユニットライセンス）または Enterprise（エンタープライズ）である必要があります。Shareware（シェアウェア）、Freeware（フリーウェア）、Not Specified（指定なし）など他のライセンスモードのアプリケーションは、このウィジェットに表示されません。 このウィジェットは情報提供のみを目的としており、アプライアンスは、ライセンスコンプライアンスを強制しません。例えば、ライセンスが期限切れであったり、コンプライアンスから外れていたとしても、エージェント管理対象デバイスへのソフトウェアのインストールがアプライアンスによって阻止されることはありません。 次のように、色によってしきい値レベルが示されます。 • **赤**: 使用率が緊急しきい値設定以上です。 • **オレンジ**: 使用率が警告しきい値設定以上になっていますが、緊急しきい値設定に対しては下回っています。 • **緑**: 使用率が警告しきい値設定を下回っています。 しきい値レベルを変更する方法については、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。 ライセンス資産の管理に関する情報については、インベントリの管理を参照してください。
プロビジョニング	このウィジェットには、KACE エージェントのプロビジョニングまたはインストールタスクのステータスが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。

ウィジェット	説明
プロビジョニングプラットフォーム	このウィジェットには、エージェント管理対象デバイスにインストールされているオペレーティングシステムの割合が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
進行中のタスク	このウィジェットには、アプライアンスで進行中のタスクの数が表示されます。この数には、スクリプト作成、インベントリ、メータリング、レプリケーション、パッチ適用、ブートストラップ、およびキャッシュクエリに関連するタスクが含まれます。アプライアンスで読み込み平均を表示し、必要に応じてタスクスループットを変更できます。詳細については、「エージェント通信とログ設定の定義」を参照してください。 アプライアンス上で組織コンポーネントが有効化されている場合、ウィジェットは System Dashboard（システムダッシュボード）ページで利用可能になります。
デバイスチェックイン率	このウィジェットには、過去 60 分間にアプライアンスに接続したデバイスの数が表示されます。アプライアンス上で組織コンポーネントが有効化されている場合、このウィジェットはシステムレベルで利用可能になります。
ソフトウェアライセンス設定	ソフトウェアのライセンス資産を設定し、ライセンスタイプ（サイト、サブスクリプション、ユニットなど）を指定した場合、その情報がこのウィジェットに表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ディスク容量	このウィジェットには、アプライアンスの空きディスク容量と使用中のディスク容量が表示されます。アプライアンス上で組織コンポーネントが有効化されている場合、このウィジェットはシステムレベルで利用可能になります。
ソフトウェア発行元	このウィジェットには、管理対象デバイスにインストールされているソフトウェアタイトルが最も多い、ソフトウェアカタログで定義済みの発行元が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ソフトウェアタイトル	このウィジェットには、管理対象デバイスでのインストール数が最も多い、ソフトウェアカタログで定義済みのソフトウェアタイトルが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。

ウィジェット	説明
有効期限が切れるデルの保証	このウィジェットはデルの保証情報を表示し、デルの保証レポートの レポート リストページへのリンクを提供します。 アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
監視アラートの概要	このウィジェットには、警告レベルごとにグループ化された未確認の警告数が表示されます。 次のように、アイコンによって警告レベルが示されます。 • : 緊急 • : エラー • : 警告 • : 情報 • : 復旧済み アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。 **リソース不足のアラート**。アプライアンスリソースが残り少なくなると、ダッシュボードに 重要アラート が表示され、サポートへの問い合わせなど、推奨される対応が提供されます。これらのアラートは、アプライアンスが多量のディスク、CPU、およびメモリリソースを使用することが検出されたとき、または多数のEメールを受信したときに生成されます。 重大なリソース不足のアラートは、過去10分以内に関連状態が検出され、表示される前に1時間持続した場合に表示されます。 これらのアラートの設定は、履歴設定で追跡されます。設定履歴の設定 ページでいずれかの リソース不足のアラート オプションをクリアすると無効にすることができます。詳細については、「組織コンポーネントが有効化されている場合のシステムレベルの設定履歴サブスクリプションの設定」を参照してください。
監視対象デバイス	このウィジェットには、監視が有効になっているデバイスのステータスが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
警告の監視	このウィジェットには、監視対象のデバイスに関する警告メッセージが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。

ウィジェット	説明
サービスデスクウィジェット	このセクションでは、サービスデスクチケットのパフォーマンスの高レベルな概要を示します。このウィジェットを使用すると、チケットの状態をすばやく確認し、カスタマエクスペリエンスを改善するためのインジケータを見つけられます。例えば、期限超過しているチケットの数を確認して、必要に応じて固有の不具合に注目できます。 **注:** サービスデスクウィジェットには、ログインユーザーに関連付けられたデフォルトキューのデータが表示されます。ユーザーに対するデフォルトが設定されていない、またはデフォルトとしてすべてのキューが設定されている場合、ウィジェットにはそのユーザーが所有しているすべてのキューのデータが表示されます。 **注:** ユーザーがキューを所有していない、またはデフォルトキューが有効ではない場合、ウィジェットにはデータが表示されません。
ショートカット	このウィジェットには、一般的なサービスデスクアクションへのリンクが含まれています。これらを使用して、新しい KB（サポート技術情報）記事の作成、レポートのスケジュール設定など、特定のタスクを迅速に開始します。
ビュー	このウィジェットには、作成したすべてのカスタムビューを含む、一般的なサービスデスクのページとウィザードへのリンクが含まれています。これらを使用して、自分の最近のチケット、未割り当てのすべてのチケット、本日期限のチケット など、特定のページにすばやく移動します。また、該当する場合は、カスタムビューへのリンクも表示されます。カスタムビューのリストはアルファベット順に並べられています。カスタムビューを特定の順序で表示する場合は、必要に応じて名前の前に数字を付けることができます。
レポート	このウィジェットには、一般的なサービスデスクレポートへのリンクが含まれています。これらを使用して、過去7日間の未解決チケット（所有者別）、停止済み/未解決のチケット（所有者別）など、特定のレポートをすばやく生成します。
本日開かれたチケット	このウィジェットには、本日開かれたサービスデスクチケットの数が含まれています。
所有者別のアクティブなチケット	これらのウィジェットには、アクティブ、クローズ、期限超過、本日期限超過、期限、本日期限、ま
カテゴリ別のアクティブなチケット	
優先度別のアクティブなチケット	
アクティブなチケット	

ウィジェット	説明
クローズチケット 期限超過チケット 所有者別の期限超過チケット 本日の期限超過チケット 本日期限のチケット 再度開かれたチケット	たは再度開かれたサービスデスクチケットが、次のカテゴリのいずれかにグループ化されます。 • カテゴリ • 優先度 • 所有者 • キュー • 範囲 結果のデータは、棒グラフ または ドーナツグラフで表示できます。 ウィジェットのタイトルを変更したり、チケットをグループ化する方法を選択したり、グラフのタイプを選択したりするには、ウィジェットで をクリックします。表示されたダイアログボックスで、編集を行い、**保存** をクリックします。
チケットの平均解決時間	このウィジェットには、過去 30 日間でチケット解決に要した平均日数が表示され、次のカテゴリにグループ化されています。 • カテゴリ • 優先度 • 所有者 • キュー • 月 結果のデータは、棒グラフ または ドーナツグラフで表示できます。 ウィジェットのタイトルを変更したり、チケットをグループ化する方法を選択したり、グラフのタイプを選択したりするには、ウィジェットで をクリックします。表示されたダイアログボックスで、編集を行い、**保存** をクリックします。
期限超過したチケット	このウィジェットには、現在期限が超過しているサービスデスクチケットの数が表示されます。
デバイスウィジェット	このセクションでは、管理対象デバイスの高レベルな概要を示します。このウィジェットを使用すると、デバイスの状態をすばやく確認し、パフォーマンスを改善するためのインジケータを見つけられます。例えば、使用可能なディスク容量の割合を確認して、必要な場合は固有の不具合に注目できます。
メモリごとのデバイス	このウィジェットには棒グラフが表示され、それぞれの棒はインストールされている RAM ごとのデバイスの数を表します。

ウィジェット	説明
プロセッサごとのデバイス	このウィジェットには棒グラフが表示され、それぞれの棒は固有のプロセッサ設定ごとのデバイスの数を表します。
ディスク容量ごとのデバイス	このウィジェットにはドーナツグラフが表示され、それぞれの部分は管理対象デバイスの空きディスク領域の割合を表します。ウィジェットのタイトルをクリックすると、関連付けられてたデバイスへのリンクを含むレポートが表示されます。円グラフのそれぞれの部分の上にマウスを置くと、選択した空きディスク領域の割合に対応する管理対象デバイスの割合が表示されます。例えば、円グラフの赤い部分の上にマウスを置くと、空きディスク領域が 25% 未満のデバイスの割合が表示されます。
管理対象オペレーティングシステム	このウィジェットには、各オペレーティングシステムを実行中の管理対象デバイスの割合が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、このウィジェットには、選択した組織のデバイスの割合が表示されます。
デバイス (製造元別)	このウィジェットには、デバイスインベントリに表示されている主なデバイスの製造元が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、このウィジェットには、選択した組織のデバイスの割合が表示されます。
デバイス (モデル別)	このウィジェットには、デバイスインベントリに表示されている主なデバイスのモデルが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、このウィジェットには、選択した組織のデバイスの割合が表示されます。
サブタイプごとのデバイス	このウィジェットにはドーナツグラフが表示され、それぞれの部分は管理対象デバイスのサブタイプ別デバイスの割合を表します。
VMware デバイス数	このウィジェットには、vCenter、ESXi ホスト、仮想マシン、プロビジョニングされた仮想マシンなど、各 VMware デバイスタイプの数が表示されます。ウィジェットのタイトルをクリックすると、デバイス リストページが表示されます。
VMware デバイスレポート	このウィジェットには、5 つの一般的な VMware インベントリレポートへのリンクが含まれます。ウィジェットのタイトルをクリックすると、仮想インフラストラクチャ フィルタが適用された レポート リストページが表示されます。
ステータス別の VMware ESXi デバイス	このウィジェットには、ESXi デバイスの現在のステータスを示すドーナツグラフが表示されます。可能な値には、次の 4 つがあります。OK、警告、エラー、および 不明。ウィジェットのタイトルをクリックすると、現在のステータス別にすべての

ウィジェット	説明
	ESXi デバイスを一覧表示する新しい VMware インベントリレポートが表示されます。
VMware ESXi バージョン数	このウィジェットには、上位 5 つの ESXi バージョンの数が表示されます。ウィジェットのタイトルをクリックすると、バージョン別にすべての ESXi デバイスを表示する新しい VMware インベントリレポートが表示されます。
資産管理ウィジェット	このセクションでは、資産の使用状況の大まかな概要を示します。このウィジェットを使用すると、資産の状態をすばやく確認し、資産構成を改善するためのインジケータを見つけられます。例えば、ソフトウェアライセンスがどのように使用されるかに焦点を当て、どのソフトウェアタイトルのライセンスを更新する必要があるかを特定できます。
タイプ別資産	このウィジェットにはドーナツグラフが表示され、それぞれの部分はデバイス、ソフトウェア、場所、ライセンス、およびその他の資産タイプごとの資産の割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択したタイプの資産の割合が表示されます。
ステータス別資産	このウィジェットにはドーナツグラフが表示され、それぞれの部分は アクティブ、廃棄、欠落、およびその他のステータスごとの資産の割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択したステータスの資産の割合が表示されます。
製品別未使用ライセンスのコスト（$）	このウィジェットには棒グラフが表示され、それぞれの棒は各製品の未使用ライセンスのコストを表します。この情報を使用して、未使用ライセンスを再割り当てまたはキャンセルし、最も必要なところにリソースをリダイレクトできます。
ライセンスコンプライアンス	ソフトウェアのライセンス資産を作成済みの場合、このウィジェットにはライセンス認証された特定のソフトウェアがインストールされたエージェント管理対象デバイスの数と、使用可能なライセンスの数が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。 ライセンス資産は、ソフトウェア ページおよびソフトウェアカタログ ページにリストされたアプリケーションに対して作成できます。このウィジェットにライセンス情報が表示されるようにするには、アプリケーションのライセンスモードが Unit License（ユニットライセンス）または Enterprise（エンタープライズ）である必要があります。Shareware（シェアウェア）、Freeware（フリーウェア）、Not Specified（指定なし）など他のライセンスモードのアプリケーションは、このウィジェットに表示されません。 このウィジェットは情報提供のみを目的としており、アプライアンスは、ライセンスコンプライア

ウィジェット	説明
	ンスを強制しません。例えば、ライセンスが期限切れであったり、コンプライアンスから外れていたとしても、エージェント管理対象デバイスへのソフトウェアのインストールがアプライアンスによって阻止されることはありません。 次のように、色によってしきい値レベルが示されます。 • 赤: 使用率が緊急しきい値設定以上です。 • オレンジ: 使用率が警告しきい値設定以上になっていますが、緊急しきい値設定に対しては下回っています。 • 緑: 使用率が警告しきい値設定を下回っています。 しきい値レベルを変更する方法については、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。 ライセンス資産の管理に関する情報については、インベントリの管理を参照してください。
ソフトウェアタイトル	このウィジェットには、管理対象デバイスでのインストール数が最も多い、ソフトウェアカタログで定義済みのソフトウェアタイトルが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ソフトウェア発行元	このウィジェットには、管理対象デバイスにインストールされているソフトウェアタイトルが最も多い、ソフトウェアカタログで定義済みの発行元が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
場所別資産	このウィジェットにはドーナツグラフが表示され、それぞれの部分は場所別の資産の割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択した場所の資産の割合が表示されます。
インストールされているが 60 日間使用されていないソフトウェア	このウィジェットには棒グラフが表示され、それぞれの棒は過去 60 日間使用されていないソフトウェアタイトルとその製品の対応するインスタンスの数を表します。この情報を使用して、これらのタイトルが必要かどうかをさらに調査し、未使用ライセンスを再割り当てまたはキャンセルし、最も必要なところにリソースをリダイレクトできます。
期限切れに近づいているソフトウェアライセンスのメンテナンス	このウィジェットには縦の棒グラフが表示され、それぞれの棒は一定時間経過後に期限が切れるソフトウェアライセンスの数を表します。
期限切れソフトウェアライセンスのメンテナンス	このウィジェットにはドーナツグラフが表示され、それぞれの部分は期限切れのライセンスと現在のライセンスの配分を表します。選択すると、グラフの

ウィジェット	説明
	それぞれの部分にカーソルを置いたときに、期限切れまたは現在のソフトウェアライセンスの割合が表示されます。
期限満了に近い契約	このウィジェットには縦の棒グラフが表示され、それぞれの棒は一定時間経過後に期限が切れる契約の数を表します。
期限切れの契約	このウィジェットにはドーナツグラフが表示され、それぞれの部分は期限切れの契約と現在の契約の配分を表します。選択すると、グラフのそれぞれの部分にカーソルを置いたときに、期限切れまたは現在の契約の割合が表示されます。
ソフトウェアライセンス設定	ソフトウェアのライセンス資産を設定し、ライセンスタイプ（サイト、サブスクリプション、ユニットなど）を指定した場合、その情報がこのウィジェットに表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
セキュリティウィジェット	このセクションには、環境内のパッチコンプライアンスの概要と、パッチプロセスに関する情報が表示されます。管理対象デバイスにインストールされたシステムパッチのレベルをすばやく確認し、システムセキュリティを改善するためのインジケータを探すために使用します。
緊急のパッチのコンプライアンス	このウィジェットには、「緊急」とマーク付けされたパッチの適用状況が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
Dellアップデート	このウィジェットは、管理対象デバイスに適用可能なDellアプリケーション、BIOS、およびファームウェアのアップデートを表示します。これらのアップデートは、その緊急度に応じて、中、重要、重大として分類されます。Dellアップデートスケジュールを作成すると、データがウィジェットに表示されます。詳細については、「Dell アップデートスケジュールの設定」を参照してください。 アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
マシン別のコンプライアンス	このウィジェットにはドーナツグラフが表示され、グラフのそれぞれの部分は各管理対象デバイスのパッチのコンプライアンスの割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択したデバイスのパッチのコンプライアンスの割合が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できま

ウィジェット	説明
	す。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
パッチ別のコンプライアンス	このウィジェットにはドーナツグラフが表示され、グラフのそれぞれの部分は該当する各パッチのコンプライアンスの割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択したパッチのコンプライアンスの割合が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
パッチインストールの進行状況	このウィジェットには、管理対象デバイスで現在実行中のパッチタスクの進行状況が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
パッチが展開されました	このウィジェットには、現在展開されているパッチの数が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
パッチが失敗しました	このウィジェットには、展開に失敗したパッチの数が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
パッチリリース済み	このウィジェットには、リリースされ、展開可能なパッチの数が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスご

ウィジェット	説明
	とに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
完了したパッチ適用タスク	このウィジェットには、管理対象デバイスでのパッチ適用タスク（タスクの検出、展開、およびロールバックなど）の進行状況が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
レポート	このウィジェットには、一般的なパッチ適用レポートへのリンクがあります。これらを使用して、緊急および最新の通知リスト、パッチ未対応のデバイスなどの特定のレポートをすばやく生成します。
SCAPの概要	このウィジェットは、デバイスで実行されたSCAPスキャンに関する情報を提供します。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ビュー	このウィジェットには、作成したすべてのカスタムビューを含む、一般的なパッチ適用のページとウィザードへのリンクが含まれています。パッチカタログ などの特定のページにすばやく移動するために使用します。カスタムビューがある場合は、それらはアルファベット順にソートされます。カスタムビューを特定の順序で表示する場合は、必要に応じて名前の前に数字を付けることができます。
Windows 10 リリース	このウィジェットには棒グラフが表示され、チャート内の各項目は特定の Windows 10 リリースとそのバージョンを実行している管理対象デバイスの数を表します。これにより、公開されている Windows 10 更新プログラムの対象となるデバイスの数を把握できます。

ダッシュボードの詳細の表示

ダッシュボードの詳細には、アプライアンスまたは選択した組織に関する統計が表示されます。

アプライアンスで組織コンポーネントが有効化されており、管理者コンソール（http://**appliance_hostname**/admin）にログインしている場合は、選択した組織の統計が表示されます。システム管理コンソール（http://**appliance_hostname**/system）にログインしている場合は、すべての組織を含めたアプライアンスの統計が表示されます。

管理対象デバイスを持たない新規のアプライアンスでは、ダッシュボードの詳細 ページには、ゼロが表示されるか、またはレコードが一切表示されません。

1. 次のいずれかを実行します。
   - **アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 がアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。**
   - **アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。**
2. **ホーム > ダッシュボード** をクリックします。

   ダッシュボード ページまたは システム概要 ページが表示されます。
3. ページの右上隅で **詳細の表示** をクリックします。

   ダッシュボードの詳細 ページが表示されます。次の情報が表示されます。

概要のセクション	説明
警告	インベントリの管理対象デバイスのライセンスの上限および使用率。
デバイス	使用中のオペレーティングシステムの内訳を含めた、管理対象デバイスに関する情報。 さらに、管理対象デバイスの数がライセンスキーによって許可される数を超えている場合は、ここで通知されます。
ソフトウェア	アプライアンスのインベントリ内の使用可能なアプリケーションの概要。これには、ソフトウェア ページと ソフトウェアカタログ ページにリストされたアプリケーションが含まれます。
配布	管理対象デバイスに配布されたアプリケーションが配布方法別に表示されます。このセクションには、有効化および無効化されているパッケージの数も表示されます。
警告の監視の概要	監視対象デバイスの警告レベルごとにグループ化された未確認のアラート数。 次のように、アイコンによって警告レベルが示されます。 •  : **緊急** •  : **エラー** •  : **警告** •  : **情報** •  : **復旧済み**
警告の概要	管理対象デバイスに配信された警告が警告タイプ別に表示されます。アクティブな警告と期限切れになった警告の数も表示されます。

概要のセクション	説明
	IT 勧告 には、**ユーザーコンソール**でのサポート技術情報記事の番号が示されます。
パッチ	Microsoft®やAppleなどのソフトウェアベンダーから受け取ったパッチ。この概要には、前回のパッチ（成功および試行済み）の日時、パッチの合計、およびダウンロードされたパッケージの合計が表示されます。
OVAL	Open Vulnerability Assessment Language（OVAL）（管理対象デバイスのセキュリティの脆弱性を特定するために実行される一連のテスト）に関する情報。OVAL情報には、以下が含まれます。 • 受け取った定義 • 前回のOVALダウンロード（試行済みと成功）の日時 • アプライアンスでのOVALテストの回数 • スキャンされたデバイスの数 • 管理対象デバイスで検出された脆弱性の数
検出（ネットワークスキャン）	ネットワークで実行された検出スキャンの結果。スキャンされたIPアドレスの数、検出されたサービスの数、および実行されたスキャンの回数が表示されます。

注: このページが更新されると、レコードカウントも更新されます。新しいアプライアンスインストールには、レコードはありません。

OVAL の詳細については、デバイスとアプライアンスのセキュリティの維持を参照してください。

タスクスケジュールの表示

タスクスケジュール ページには、マシン数とタスクのタイプに基づいた開始時間および推定期間を使用して、選択に従って現在の時間、日、または週に対してスケジュールされたタスクのリストが表示されます。スクリプトなどの詳細ページが関連付けられているタスクは、テーブルのタスク名をクリックしてアクセスすることができます。

管理者コンソールには、選択した組織に関連付けられたタスクと、バックアップウィンドウ などのシステムタスクが表示されます。**システム管理コンソール**でこのページを表示すると、すべての組織のすべてのタスクと（組織によって分離）、すべての利用可能なシステムタスクが表示されます。

ページに表示されるすべてのタスクチェーンは、接続線で表されます。タスクチェーンの詳細については、「タスクチェーンの使用」を参照してください。

複数のエージェントおよびデバイスに関連付けられたタスクは、グラデーションの線で表示され、線の長さは、タスクの期間または履歴データを反映していません。表示される単色の線は、期間が固定されているタスクを示しています。グラフの青い縦棒は、現在の日付と時刻を表します。

1. 次のいずれかを実行します。
   - **アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または、**管理ヘッダーに組織メニューを表示 **がアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。**
   - **アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。**

   ダッシュボード ページまたは システム概要 ページが表示されます。
2. 左側のナビゲーションバーの **ホーム** セクションで、**タスクスケジュール** をクリックします。

   タスクスケジュール ページが表示されます。
3. 異なるレベルの詳細を切り替えるには、必要に応じて **時間**、**日**、または **週** をクリックします。

アプライアンスバージョン、モデル、およびライセンス情報の表示

ヘルプ パネルの **アプライアンスについて** リンクには、アプライアンスバージョン、モデル、およびライセンス情報が表示されます。

1. ユーザーコンソール、管理者コンソール、またはシステムコンソールにログインします。
2. 管理者コンソールの右上で、**ヘルプ** をクリックします。

   右側に表示されるヘルプペインには、関連する**管理者コンソール**ページの概要が表示されます。ヘルプペインの下部には、以下のボタンがあります。
   - **アプライアンス管理者ガイド**（）：KACE システム管理アプライアンスヘルプコンテンツにアクセスできます。
   - **サポート技術情報**（）：関連する**管理者コンソール**ページに関連付けられたサポート技術情報記事を参照できます。

     注: このオプションは、**管理者コンソール**および**システムコンソール**でのみ利用できます。**ユーザーコンソール**には表示されません。
   - **サポート技術情報のビデオ再生**（）：関連する**管理者コンソール**ページに関連付けられた 1 つまたは複数のトレーニングビデオを参照できます。ヘルプペイン、選択したページ外の小さいウィンドウ、またはビデオをホストするターゲットのサポート技術情報ページでビデオを再生できます。

     注: このオプションは、関連するビデオがサポートポータルに存在する場合にのみ使用できます。さらに、**管理者コンソール**および**システムコンソール**にのみ表示されます。**ユーザーコンソール**には表示されません。
   - **ライブチャット**（）：KACEシステム管理アプライアンス製品スペシャリストとのチャットを開始します。

     注: このオプションは、**管理者コンソール**および**システムコンソール**でのみ利用できます。**ユーザーコンソール**には表示されません。
   - **未解決チケット**（）：サービスリクエストを作成できる サポート ページ（https://support.quest.com/create-service-request）にリンクします。

> **注:** このオプションは、**管理者コンソール**およびシステムコンソールでのみ利用できます。**ユーザーコンソール**には表示されません。

- **サポート**（ ）：**設定 > サポート** ページにリンクします。このページには、システム管理の問題をトラブルシューティングし、**Questサポート**に問い合わせるためのリソースが表示されます。

  > **注:** このオプションは、**管理者コンソール**およびシステムコンソールでのみ利用できます。**ユーザーコンソール**には表示されません。

- **KACE GOモバイルアプリ**（ ）：KACE GOモバイルアプリのダウンロードリンクを含むダイアログを表示します。このアプリは、iOSおよびAndroidプラットフォームで利用できます。

  > **注:** このオプションは、アプライアンスがK1 GOモバイルアプリと対話できるように構成済みの場合に利用できます。**管理者コンソール**およびシステムコンソールにのみ表示されます。**ユーザーコンソール**には表示されません。モバイルアクセスの有効化の詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。

- **バージョン情報**（ ）：KACEシステム管理アプライアンスのインストールに関する情報が表示されます。

  > **注:** このオプションは、**管理者コンソール**およびシステムコンソールでのみ利用できます。**ユーザーコンソール**には表示されません。

3. パネルの右下隅にある **バージョン情報** リンクをクリックします。

   アプライアンスライセンス情報が表示されます。

   - アプライアンスバージョン、モデル、およびシリアル番号。
   - ライセンスの有効期限（ 表示形式：月/日/年 ）。
   - ライセンスによって管理できる管理対象コンピューター、監視対象サーバーおよび資産の数。

     管理対象コンピュータとは、アプライアンスインベントリに含まれるデバイスで、1）Windows、Mac、Linux、または UNIX オペレーティングシステムが搭載され、2）PC またはサーバとして分類され、かつ 3）WSAPI またはモバイルデバイスの管理機能を使用してインベントリに手動で追加されていないデバイスを指します。
     監視対象サーバーとは、1）管理対象コンピューターの要件を満たし、かつ、2）監視が有効なサーバーを指します。
     ライセンスの上限の計算に含まれる**資産**とは、1）アプライアンスのインベントリに追加されているが、管理対象コンピュータまたは監視対象サーバの定義には適合しないデバイスで、かつ 2）WSAPI またはモバイルデバイスの管理機能を使用してインベントリに手動で追加されていないデバイスを指します。例えば、プリンタ、プロジェクタ、ネットワーク製品、ストレージデバイスなどは資産に該当します。資産管理コンポーネントを使用して作成、管理している資産は、ライセンスの上限の計算に含まれません。

     > **注:** 製品ライセンス契約に従い、デバイスを特定の数だけ管理できます。デバイスがMIA（ 未同期 ）となっている場合や既に使用されなくなった場合であっても、ライセンス数にカウントされます。手動で、またはAPIを通じてインベントリに追加されたデバイスは、ライセンス数にカウントされません。詳細については、「https://quest.com/docs/Product_Guide.pdf」を参照してください。
     >
     > **注:** ライセンスの上限を増やす方法については、次のQuestのウェブサイトを参照してください：https://quest.com/buy.

   - ライセンス条件。
   - サードパーティ製コードの帰属。

オプション：アプライアンスライセンス情報が、有効化されているコンポーネントとともに表示されます。詳細については、「製品ライセンス情報の表示」を参照してください。

製品ライセンス情報の表示

アプライアンスライセンス情報は、**管理者コンソール**の アプライアンスの更新 セクションに表示されます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **アプライアンスの更新** をクリックします。
3. ライセンス情報 セクションの **ヘルプ** ボタン。

   以下の情報が表示されます。

   - **管理対象コンピューター**：ライセンスによって管理できる管理対象コンピューターの数。**管理対象コンピュータ**とは、このインベントリに含まれるデバイスで、1）Windows、Mac、Linux、または UNIX オペレーティングシステムが搭載され、2）PC またはサーバとして分類され、かつ 3）WSAPI またはモバイルデバイスの管理機能を使用してインベントリに手動で追加されていないデバイスを指します。
   - **監視対象サーバー**：ライセンスによって管理できる監視対象サーバーの数。**監視対象サーバー**とは、1）管理対象コンピューターの要件を満たし、かつ、2）監視が有効なサーバーを指します。
   - **資産**: ライセンスの上限の計算に含まれる資産とは、1）このインベントリに追加されているが、管理対象コンピュータまたは監視対象サーバの定義には適合しないデバイスで、かつ 2）WSAPI またはモバイルデバイスの管理機能を使用してインベントリに手動で追加されていないデバイスを指します。例えば、プリンタ、プロジェクタ、ネットワーク製品、ストレージデバイスなどは資産に該当します。資産管理コンポーネントを使用して作成、管理している資産は、ライセンスの上限の計算に含まれません。

     注: 製品ライセンス契約に従い、デバイスを特定の数だけ管理できます。デバイスがMIA（ 未同期 ）となっている場合や既に使用されなくなった場合であっても、ライセンス数にカウントされます。手動で、またはAPIを通じてインベントリに追加されたデバイスは、ライセンス数にカウントされません。詳細については、「http://quest.com/docs/Product_Guide.pdf」を参照してください。

     注: ライセンスの上限を増やす方法については、次のQuestのウェブサイトを参照してください：https://quest.com/buy.
   - **期限**：ライセンスの有効期限（ 表示形式：月/日/年 ）。

     注: アプライアンスのメンテナンスの期限が切れると、パッチ適用サポートなどの一部の機能が使用できなくなります。これにより、ホームダッシュボードにエラーアラートが表示されます。ライセンスを更新するには、https://support.quest.com/contact-us/renewals にアクセスしてください。ダッシュボードの詳細については、「「ホーム」コンポーネントの使用」を参照してください。
   - **コンポーネント**：保有するライセンスで有効になっているコンポーネント。

オプション：製品シリアル番号、モデル番号、ライセンス条件、およびサードパーティ製コードの帰属を表示します。詳細については、「アプライアンスバージョン、モデル、およびライセンス情報の表示」を参照してください。

アプライアンスソフトウェアの更新プログラムについて

アプライアンスでは、ソフトウェア更新プログラムを確認するために、毎日 Quest のサーバへのチェックインが実行されます。これらの更新は通知更新と呼ばれます。

適用可能な更新プログラムがある場合は、次回管理者アカウント権限を使用してログインしたときに、**管理者コンソール**の ホーム ページに警告が表示されます。

関連トピック

手動による更新ファイルのアプライアンスへのアップロード.

ラベルについて

ラベルは、デバイスなどのアイテムをグループとして管理できるよう、整理および分類できるコンテナです。

例えば、オペレーティングシステムが同じデバイスや地理的に同じ場所にあるデバイスを、ラベルを使用して識別することができます。その後、そのラベルが割り当てられているすべてのデバイス上で、ソフトウェアの配布やパッチの展開などのアクションを開始できます。ラベルは、特定のアイテムに手動で割り当てることもできれば、SQLやLDAPクエリなどの基準に関連するアイテムに自動で割り当てることもできます。

ラベルは ラベル セクションのほか、デバイス ページなど、ラベルが使用されている**管理者コンソール**の他のセクションのものも追加できます。

使用可能なラベルは以下の通りです。

- **ラベル**: 手動で適用され、ユーザー、デバイス、ソフトウェア、管理対象インストールなどの整理に使用されるラベル。詳細については、「手動ラベルの管理」を参照してください。
- **Smart Label**: 指定した基準に基づいて自動的に適用および削除されるラベル。例えば、特定のオフィス（この例ではSan Franciscoのオフィス）にあるノートPCを追跡するには、まず「San Francisco Office」というラベルを使用します。次に、このオフィスにあるデバイスのIPアドレス範囲（サブネット）に基づいてSmart Labelを追加します。このIPアドレス範囲内にあるデバイスがインベントリに設定されるたびに、「San Francisco」というSmart Labelが自動的に適用されます。デバイスがIPアドレス範囲外になり、再度インベントリに設定されると、ラベルは自動的に削除されます。詳細については、「Smart Labelの管理」を参照してください。
- **LDAPラベル**: LDAPまたはActive Directory®クエリに基づいて、ユーザーおよびデバイスに自動的に適用されたり、ユーザーおよびデバイスから自動的に削除されたりするラベル。詳細については、「LDAPラベルの管理」を参照してください。

関連トピック

Smart Labelの管理

LDAPラベルの管理

情報の検索およびリストのフィルタリング

アプライアンスデータベースを検索して、リストページをフィルタリングし、アプライアンスに関する情報を見つけることができます。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のデータベースを個別に検索できます。一度にすべての組織のデータベースを検索したり、システムレベルで検索したりすることはできません。

adminレベルでの検索

管理者レベルのデータベースを検索して、アプライアンスに関する情報を見つけることができます。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のデータベースを個別に検索できます。一度にすべての組織のデータベースを検索したり、システムレベルで検索したりすることはできません。

1. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. 次のいずれかを実行します。
   - **ページの右上隅にある 検索 ボタンをクリックして、検索 フィールドを表示します。次に、4 文字以上を グローバル検索 フィールドに入力し、Enter または Return を押します。以下の図は、検索 フィールドの画面を示します。**

   - **ホーム > 検索 をクリックします。次に、右側のリストの上に表示される 検索 フィールドに 4 文字以上を入力し、Enter または Return を押します。以下の図は、検索 フィールドの画面を示します。**

ヒント: パーセント記号 (%) をワイルドカードとして使用できます。例えば、検索文字列でパーセント記号を使用すると、パーセント記号の前後の条件に一致するすべてのアイテムが検索されます。

ページレベルでの検索

ページレベル検索を使用すると、現在のページの情報を検索することができます。

1. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. リストページに移動します。例えば、左側のナビゲーションバーで、**インベントリ** をクリックします。デバイス ページが表示されます。
3. リストページのこの例では デバイス で、ページの右上隅の **検索** フィールドに検索文字列を入力します。**Enter**キーまたは**Return**キーを押して、ページレベル検索を開始します。

   以下は、ページレベル検索 フィールドの画面図です。

ヒント: パーセント記号 (%) をワイルドカードとして使用できます。例えば、検索文字列でパーセント記号を使用すると、パーセント記号の前後の条件に一致するすべてのアイテムが検索されます。

高度なオプションによるページレベルの検索

高度なページレベル検索を使用すると、さまざまな条件の組み合わせを使用して、現在のページの情報を検索することができます。高度なページレベル検索は、デバイス ページおよび ソフトウェア ページなど、ほとんどのリストページで使用できます。

例：高度な検索条件を使用した管理対象デバイスの検索

この例では、高度なページレベル検索を使用してディスク容量が少なくなっている Windows デバイスを検索する方法を示します。

範囲を限定したユーザーがデバイスで高度な検索を実行し、そのユーザー役割が Smart Label と関連付けられている場合、結果には Smart Label に関連付けられたデバイスのみが含まれます。追加のデバイスを確認するために、必要に応じて、Smart Label の範囲を変更できます。ユーザーの役割に対してデバイス範囲を設定する方法の詳細については、「ユーザーの役割の追加または編集」を参照してください。Smart Label の詳細については、「Smart Labelの管理」を参照してください。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. 右側の デバイス リストの上にある **高度な検索** タブをクリックします。

    高度な検索 パネルが開きます。

3. 次のように、Windowsデバイスの検索に必要な条件を指定します。

    オペレーティングシステム: 名前 | 次の値を含む | Windows
4. 演算子ドロップダウンリストで **および** を選択した状態で、**行の追加** をクリックして、新しい行を追加します。次に、ディスク領域が少なくなっているデバイスを検出するために必要な条件を指定します。

    ドライブ情報: ディスク容量（ % ） | > | 95
5. **検索** をクリックします。

リストが更新されて、検索条件に一致するデバイスが表示されます。

高度な検索 の条件を使用したSmart Labelと通知の追加

高度な検索 パネルで選択した条件を使用して、Smart Labelや通知を追加できます。

範囲を限定したユーザーがデバイスで高度な検索を実行し、そのユーザー役割が Smart Label と関連付けられている場合、結果には Smart Label に関連付けられたデバイスのみが含まれます。追加のデバイスを確認するために、必要に応じて、Smart Label の範囲を変更できます。ユーザーの役割に対してデバイス範囲を設定する方

法の詳細については、「ユーザーの役割の追加または編集」を参照してください。Smart Label の詳細については、「Smart Labelの管理」を参照してください。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. リストページに移動します。例えば、左側のナビゲーションバーで、**インベントリ** をクリックして、デバイス ページを表示します。
3. 右側のリストの上にある 高度な検索 タブをクリックして、検索条件を入力します。

   詳細については、「例：高度な検索条件を使用した管理対象デバイスの検索」を参照してください。
4. 右側のリストの上にある **Smart Label** タブをクリックします。

   Smart Label パネルが表示され、選択した検索条件をそのまま使用できます。

5. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。
   - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

     注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。
   - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

   注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。
6. **Create** をクリックします。

   Smart Labelは以下の通り適用されます。
   - デバイスがアプライアンスにチェックインすると、指定された基準にそれらのデバイスが一致しているかどうかに基づき、Smart Labelが自動的にそれらのデバイスに適用されるか、またはそれらのデバイスから除去されます。
   - **ホーム > ラベル > Smart Label** を使用して、特定のアプリケーション Smart Label が編集されると、直ちにすべてのアプリケーションに適用されるか、または、すべてのアプリケーションから除去されます。
   - アイテムが インベントリ > ソフトウェア ページで更新されると、指定された条件にそれらのアイテムが一致しているかどうかに基づき、Smart Labelが自動的にアプリケーションに適用されるか、またはアプリケーションから除去されます。
7. 右側のリストの上にある **通知** タブをクリックします。

   通知 パネルが表示され、選択した検索条件をそのまま使用できます。

8. 次の情報を入力します。

フィールド	説明
タイトル	Eメールの 件名 行に表示する情報。
受信者	対象とする受信者のEメールアドレス (複数可) 。Eメールアドレスは、完全修飾Eメールアドレスでなくてはなりません。複数のアドレスにEメールを送信するには、コンマを使用して各アドレスを区切るか、またはEメール配布リストを使用します。
頻度	選択した条件とインベントリのアイテムを比較するクエリがアプライアンスによって実行される間隔。条件に一致した場合、通知が送信されます。

9. **オプション**：条件を検証するには、**通知のテスト** をクリックします。

   リストが更新されて、検索条件に一致するアイテムが表示されます。テスト中は、Eメール通知は送信されません。
10. **通知の作成** をクリックします。

通知が追加され、Eメール通知 ページに表示されます。

通知の頻度のスケジュールの詳細については、通知スケジュールの編集を参照してください。

関連トピック

例：高度な検索条件を使用した管理対象デバイスの検索

高度な検索 タブからのSmart Labelの読み込み

高度な検索 タブが使用可能なリストページからSmart Labelを読み込むことができます。

範囲を限定したユーザーがデバイスで高度な検索を実行し、そのユーザー役割が Smart Label と関連付けられている場合、結果には Smart Label に関連付けられたデバイスのみが含まれます。追加のデバイスを確認するために、必要に応じて、Smart Label の範囲を変更できます。ユーザーの役割に対してデバイス範囲を設定する方法の詳細については、「ユーザーの役割の追加または編集」を参照してください。Smart Label の詳細については、「Smart Labelの管理」を参照してください。

1. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. リストページに移動します。例えば、**インベントリ** をクリックして、デバイス リストを表示します。
3. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
4. 高度な検索 パネルの上部にある Smart Label ドロップダウンリストから、読み込むSmart Labelを選択します。

   ドロップダウンリストには、表示しているリストページに適合するSmart Labelが表示されます。例えば、デバイス ページでは、ドロップダウンリストにデバイス Smart Label が表示されます。また、ラベルは、基となるSQLがSmart Labelウィザード以外で編集されていない場合にのみ表示されます。これは、ウィザードではカスタムSQLを表示できないためです。
5. **読み込む** をクリックします。

高度な検索 パネルに、選択したSmart Labelの条件が表示されます。

「高度な検索」の条件を使用したカスタムビューの作成

「高度な検索」の条件を使用してカスタムビューを作成できます。カスタムビューは、定義済みの「高度な検索」の条件を使用してアイテムのリストを表示します。カスタムビューは、ソフトウェアカタログ ページ、資産 ページ、サービスデスクチケット ページなどのリストページで利用できます。

カスタムビューはユーザーに固有です。ユーザーは、他のユーザーによって作成されたカスタムビューにアクセスすることはできません。

1. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. ソフトウェアカタログ ページや 資産 ページなど、カスタムビューのオプションがあるページに移動します。
3. ページの右上隅にある **高度な検索** タブをクリックして、検索条件を入力します。
4. ページの右上隅にある **カスタムビュー** タブをクリックして、カスタムビュー パネルを表示します。
5. カスタムビューの条件を選択します。例えば、「インフラストラクチャアプリケーション」のカテゴリのアプリケーションをメータリングしたすべてのWindowsデバイスを表示するビューを、ソフトウェアカタログページ上に作成するには、次の手順を実行します。
    a. 「インフラストラクチャアプリケーション」として分類されたアプリケーションを検出するために必要な条件を以下のように指定します。

    カテゴリ | = | インフラストラクチャアプリケーション

    b. 演算子ドロップダウンリストで **および** を選択した状態で、**行の追加** をクリックして、新しい行を追加します。
    c. メータリングされたアプリケーションを検出するために必要な条件を以下のように指定します。

    メータリング | は | True

    d. 演算子ドロップダウンリストで **および** を選択した状態で、**行の追加** をクリックして、新しい行を追加します。
    e. 次のように、Windowsデバイスの検索に必要な条件を指定します。

    プラットフォーム | = | Windows

6. **オプション**：**テスト** をクリックして、リストを更新し、検索条件に一致するアイテムを表示します。
7. ビュー名 フィールドにカスタムビューの名前を入力し、**作成** をクリックします。

特定基準で表示 ドロップダウンリストにカスタムビューが表示されます。

関連トピック

例：高度な検索条件を使用した管理対象デバイスの検索

製品ドキュメントへのアクセス

管理者コンソールでは、ヘルプコンテンツおよびドキュメント検索が可能です。関連サポート技術情報記事の参照や必要な場合は製品のスペシャリストとチャットすることもできます。

1. ユーザーコンソール、管理者コンソール、またはシステムコンソールにログインします。
2. 管理者コンソールの右上で、**ヘルプ** をクリックします。

    右側に表示されるヘルプペインには、関連する**管理者コンソール**ページの概要が表示されます。ヘルプペインの下部には、以下のボタンがあります。

    - **アプライアンス管理者ガイド**（）：KACE システム管理アプライアンスヘルプコンテンツにアクセスできます。
    - **サポート技術情報**（）：関連する**管理者コンソール**ページに関連付けられたサポート技術情報記事を参照できます。

注: このオプションは、**管理者コンソール**およびシステムコンソールでのみ利用できます。**ユーザーコンソール**には表示されません。

- **サポート技術情報のビデオ再生**（ ）：関連する**管理者コンソール**ページに関連付けられた 1 つまたは複数のトレーニングビデオを参照できます。ヘルプペイン、選択したページ外の小さいウィンドウ、またはビデオをホストするターゲットのサポート技術情報ページでビデオを再生できます。

  注: このオプションは、関連するビデオがサポートポータルに存在する場合にのみ使用できます。さらに、**管理者コンソール**およびシステムコンソールにのみ表示されます。**ユーザーコンソール**には表示されません。

- **ライブチャット**（ ）：KACEシステム管理アプライアンス製品スペシャリストとのチャットを開始します。

  注: このオプションは、**管理者コンソール**およびシステムコンソールでのみ利用できます。**ユーザーコンソール**には表示されません。

- **未解決チケット**（ ）：サービスリクエストを作成できる サポート ページ（ https://support.quest.com/create-service-request ）にリンクします。

  注: このオプションは、**管理者コンソール**およびシステムコンソールでのみ利用できます。**ユーザーコンソール**には表示されません。

- **サポート**（ ）：**設定 > サポート** ページにリンクします。このページには、システム管理の問題をトラブルシューティングし、**Questサポート**に問い合わせるためのリソースが表示されます。

  注: このオプションは、**管理者コンソール**およびシステムコンソールでのみ利用できます。**ユーザーコンソール**には表示されません。

- **KACE GOモバイルアプリ**（ ）：KACE GOモバイルアプリのダウンロードリンクを含むダイアログを表示します。このアプリは、iOSおよびAndroidプラットフォームで利用できます。

  注: このオプションは、アプライアンスがK1 GOモバイルアプリと対話できるように構成済みの場合に利用できます。**管理者コンソール**およびシステムコンソールにのみ表示されます。**ユーザーコンソール**には表示されません。モバイルアクセスの有効化の詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。

- **バージョン情報**（ ）：KACEシステム管理アプライアンスのインストールに関する情報が表示されます。

  注: このオプションは、**管理者コンソール**およびシステムコンソールでのみ利用できます。**ユーザーコンソール**には表示されません。

3. ページレベルのヘルプトピックのリンクをクリックします。

   メインの ヘルプ システムが表示され、選択したトピックが表示されます。
4. ヘルプシステムの左のペインで、**検索** タブをクリックします。

   検索キーワードはすべて、暗黙のブール型ANDステートメントを使用します。例えば、**Windowsプロビジョニング**で検索すると、このキーワードが2つとも含まれる検索結果が表示されます。

   ヒント: ヘルプシステムのPDFバージョンの場合、ヘルプシステムのメインナビゲーションバー（ ）の右側の Acrobat ボタンをクリックします。
5. **管理者またはシステムコンソール専用**です。関連する管理者コンソールに関連付けられているサポート技術情報記事または システムコンソール ページを検索します。
   a. ヘルプペイン下部の をクリックします。

      ヘルプペインには、関連するサポート技術情報記事のリストが表示されます。

      注: サポート技術情報記事は現在のところ英語でのみ利用できます。

b. 特定の記事を検索するには、ナビゲーションボタンを使用します。
c. 必要に応じて、特定のキーワードでリストされている記事を検索します。
d. 目的の記事を見つけたら、ヘルプペインでリンクをクリックします。

選択したサポート技術情報記事がブラウザの新しいタブに表示されます。

重要: 記事のコンテンツを見るには、Questユーザー名およびパスワードを使用してQuestサポートサイトにログインする必要があります。

6. **管理者またはシステムコンソール専用**です。関連する管理者コンソールに関連付けられているサポート技術情報記事または システムコンソール ページを検索します。
   a. ヘルプペイン下部の をクリックします。

   ヘルプペインには、関連するトレーニングビデオのリストが表示されます。

   注: ビデオにアクセスするには、Quest ユーザー名およびパスワードを使用して Quest サポートサイトにログインする必要があります。トレーニングビデオは現在、英語でのみ視聴できます。

   b. 必要に応じて、特定のビデオを検索するには、ナビゲーションボタンを使用します。
   c. ビデオを再生するには、Play Video（ビデオの再生）ボタンをクリックします。

   選択したビデオがヘルプペインで再生を開始します。

   d. ヘルプペインでビデオを再生し続けるか、Picture-In-Picture（ピクチャインピクチャ）、Fullscreen（全画面表示）、または Popout player（ポップアウトプレーヤー）などの別の表示オプションを使用して、選択したページの外側でビデオを表示します。これらのコントロールはビデオの下部にあります。
7. **管理者またはシステムコンソール専用**です。製品スペシャリストとチャットします。
   a. をクリックします。

   サポートとのチャット ダイアログボックスが表示されます。

   b. 必要に応じて、氏名、E メールアドレス、チャットの目的 を入力し、**チャットの開始** をクリックします。

   サポートとのチャット ダイアログボックスが更新され、指定したトピックに関する情報が含まれている可能性のある既存のナレッジベース（KB）記事のリストが表示されます。トピックのリストは、要求された情報のタイプに応じて、複数のページに表示される場合があります。

   c. KB 記事のリストを確認します。必要に応じて、リストの下部にあるページナビゲーションコントロールを使用します。KB 記事を読むには、リスト内のタイトルをクリックします。
   d. 表示されている KB 記事のいずれにも必要な情報が記載されていない場合は、**上記の解決策のどれも問題を解決しませんでした。チャットを続行します** をクリックします。

   注: この機能は、質問に答えられる製品スペシャリストが対応できるときにのみ利用できます。ライブチャットが利用できない場合は、ダイアログボックスに示されます。

   ライブチャット ダイアログボックスが表示されます。サポートとのチャット ダイアログボックスで指定した情報を使用して、氏名、E メールアドレス、製品、チャットの目的 の各ボックスに値が入力されます。

   e. **チャットの開始** をクリックします。

   ライブチャット ダイアログボックスが更新されます。

   f. ライブチャット ダイアログボックスに質問を入力し、**送信** をクリックして製品スペシャリストとのチャットを開始します。
8. **管理者またはシステムコンソール専用**です。サポートチケットを開きます。
   a. をクリックします。

   ブラウザの新しいタブまたはウィンドウに サービスリクエストの送信 ページ（https://support.quest.com/create-service-request）が表示されます。

b. このページを使用し、必要に応じてサービスチケットを開きます。

9. **管理者またはシステムコンソール専用**です。 をクリックします。

   設定 > サポート ページが表示されます。このページには、システム管理の問題をトラブルシューティングし、**Questサポート**に問い合わせるためのリソースが表示されます。

10. **アプライアンスでモバイルアクセスが有効にされているとき、管理者またはシステムコンソール専用です。**

    注: モバイルアクセスの有効化についての詳細は、モバイルデバイスによるアクセスの設定を参照してください。

    a. をクリックします。

       KACE GOのダウンロードを許可するダイアログボックスが表示されます。このアプリケーションは、iOSとAndroidでのプラットフォームごとのアプリケーションストアにて入手可能です。

    b. 必要に応じて、お使いのモバイルデバイスOS用のリンクをクリックして、アプリケーションをダウンロードします。

    KACE GOのダウンロードおよび設定についての詳細は、KACE GOのダウンロードおよび使用を参照してください。

11. **管理者またはシステムコンソール専用**です。KACE システム管理アプライアンスのインストールに関する情報を確認します。

    a. をクリックします。

       製品情報が記載されているダイアログボックスが表示されます。

    b. このダイアログボックスを閉じるには、**閉じる** をクリックします。

12. ヘルプペインを閉じるには、**サポートが必要な場合** をクリックします。

管理者コンソールへのログイン: 初めてネットワークを構成した後の最初のログイン

ネットワーク設定の構成後、アプライアンスが再起動されたら、LAN（ローカルエリアネットワーク）上の任意のコンピューターからアプライアンスの**管理者コンソール**にログインできます。

初めてネットワークを構成した後の最初のログイン時に、アプライアンスライセンスキーを指定し、**admin**アカウントのパスワードを設定します。

注: 使用しているブラウザの設定に基づいて、初回ログイン時に**管理者コンソール**に表示される言語が決定されます。この設定をログイン後に変更する方法については、「ロケール設定の構成」を参照してください。

1. Webブラウザを開き、次の管理者コンソールの URL を入力します。

   （http://**appliance_hostname**/admin）にログインします。例：http://kace_sma/admin。

2. 次の情報を入力します。

オプション	説明
ライセンスキー	Questからのご案内のEメールに記載されているライセンスキーを入力します。ダッシュも含めてください。ライセンスキーがない場合は、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。
パスワード	デフォルトの **admin** アカウントのパスワードを入力します。これは、アプライアンスの**管理者コンソール**にログインするために使用するアカウントで

オプション	説明
	す。この時点でデフォルトの **admin** アカウントがアプライアンス上で唯一のアカウントになります。このアカウントのパスワードを忘れると、システムを出荷時のデフォルト状態にリセットすることが必要になる場合があり、データロスが発生します。 **注:** 複数のタイプの KACE アプライアンスを使用する場合、Quest では、すべてのアプライアンスの **admin** アカウントに同じパスワードを使用することをお勧めします。共通のパスワードを使用することにより、後でアプライアンス同士をリンクすることが可能になります。
会社名	会社またはグループの名前を入力します。
タイムゾーン	アプライアンスが設置されている地域のタイムゾーンを選択します。

3. **設定適用と再起動** をクリックします。

   アプライアンスが再起動します。
4. アプライアンスが再起動したら、ブラウザページを更新します。
5. エンドユーザー使用許諾契約（EULA）に同意し、次に、ログインID adminとパスワード（初期セットアップページで選択したもの）を使用してログインします。
6. 通知フィールドの横のチェックボックスをオンまたはオフにして、管理者アカウントのEメール通知を有効または無効にします。この設定は必要に応じて後で変更できます。詳細については、「アプライアンス管理者のEメール通知の管理」を参照してください。

オプション	説明
Questセキュリティ通知を有効にする	Quest 管理者のEメールアドレスにセキュリティ通知を送信できるようにします。この機能は、システムレベルの管理者アカウントでのみ使用可能です。管理者レベルの管理者アカウントまたは管理者以外のユーザーアカウントでは使用できません。
Quest販売およびマーケティング通知を有効にする	Questがこの管理者のEメールアドレスに販売およびマーケティング通知を送信できるようにします。この機能は、システムレベルの管理者アカウントでのみ使用可能です。管理者レベルの管理者アカウントまたは管理者以外のユーザーアカウントでは使用できません。

管理者コンソールが表示され、アプライアンスが使用可能になります。

はじめに

アプライアンスを使用するには、ネットワーク設定に一致するようにアプライアンスを設定する必要があります。

また、ラベル、ユーザー認証、レプリケーション共有、資格情報管理、資産、ライセンスコンプライアンス、サービスデスクの各機能を環境のニーズに合わせてセットアップできます。アプライアンスで組織コンポーネントが有効化されている場合は、必要に応じて組織および組織設定を追加または編集できます。

アプライアンスの設定

アプライアンスの設定は、アプライアンスのネットワーク、セキュリティ、ロケール、およびその他の設定項目のセットアップで構成されています。

要件と仕様

アプライアンスの技術仕様には、デバイスを管理するためのアプライアンスの容量上限および要件が記載されています。

アプライアンスハードウェアに関する最新情報、管理対象デバイスの要件、および**管理者コンソール**にアクセスするためのブラウザの要件の詳細については、製品ドキュメントページで利用できる技術仕様を参照してください。https://support.quest.com/kace-systems-management-appliance/technical-documents.

アプライアンスの電源投入と管理者コンソールへのログイン

最初にアプライアンスの電源をオンにするとき、LAN 上の任意のコンピュータからアプライアンス**管理者コンソール**にログインできます。ただし、アプライアンスに IP アドレスを割り当てるための DHCP サーバが必要です。それによって、セットアップウィザードを使用して、初期ネットワーク設定を構成できます。

- 仮想アプライアンスの仮想バージョンを所有している場合、アプライアンスソフトウェアをダウンロードして、仮想インフラストラクチャを設定します。詳細については、仮想アプライアンス用の設定ガイドを参照してください。https://support.quest.com/kace-systems-management-appliance/release-notes-guides に移動します。
- アプライアンスの物理バージョンをインストールしている場合は、「**Dell PowerEdge R430 Getting Started With Your System**」文書および本アプライアンスに付属する、安全にお使いいただくための注意をお読みいただき、その指示に従ってください。Questアプライアンスは特別に構成されたプラットフォームですので、内部コンポーネントのインストール/削除、ファームウェアのアップデート、BIOS設定の変更などを行う必要はありません。アプライアンスのセットアップについては、本書記載の手順にのみ従ってください。
- 社内のDNS（ドメインネームシステム）サーバーのAレコードに、アプライアンスのホスト名を入力します。「A」レコードは「MX」レコードのホスト名を定義します。これにより、ユーザーはサービスデスクにEメールチケットを送信できるようになります。アプライアンスのホスト名は、デフォルトでは k1000 ですが、初期セットアップ中に変更可能です。
- スプリットDNSを使用するかどうか決定します。リバースプロキシを使用してアプライアンスをインターネットに接続する場合、またはアプライアンスを周辺ネットワークやスクリーンサブネットに配置する場

合には、スプリット DNS を使用すると便利です。DMZでは、LAN（ローカルエリアネットワーク）に新たなセキュリティレイヤが追加されます。

- （オプション）アプライアンスの静的IPアドレスを取得します。

DHCP サーバーがない場合は、**コマンドラインコンソール**を使用して、ネットワーク設定を構成できます。詳細については、「コマンドラインコンソールへのアクセス」を参照してください。

注: サービスとしての KACE にログインする方法については、『**KACE as a Service Setup Guide**』（サービスとしての KACE セットアップガイド）を参照してください。https://support.quest.com/kace-systems-management-appliance/release-notes-guides に移動します。

1. 物理バージョンのアプライアンスを設定する場合:
   a. アプライアンスをラックに取り付け、モニタを直接アプライアンスに接続します。
   b. ネットワークケーブルを以下のポートに接続します。

   c. アプライアンスの電源をオンにします。

      コマンドラインコンソールのログイン画面が、アプライアンスに接続されたモニタに表示されます。ログイン画面に、アプライアンスのDHCPネットワーク設定が表示されます。
2. アプライアンスの仮想バージョンを設定する場合、仮想マシンの電源をオンにして、アプライアンスを起動します。

   初回のスタートアップは5〜10分かかります。

   コマンドラインコンソール ログイン画面に、アプライアンスの DHCP ネットワーク設定が表示されます。
3. LANに接続されている任意のコンピューター上でブラウザを開き、コマンドラインコンソールのログイン画面に表示されているURLにアクセスします。例：http://kace_sma.local/admin。

   ソフトウェア取引契約書 ページが表示されます。
4. 契約書に同意します。

   初期セットアップ ウィザードが表示されます。
5. アプライアンスの設定に必要な情報がすべてそろっていることを確認したら、**次へ** をクリックします。
6. 指示に従って、表示される 診断サポートコンソール ページの情報を確認し、シークレットキーとオフライントークンを安全な場所に記録します。
7. ライセンスと管理者の設定 ページで、以下の情報を入力します。

オプション	説明
ライセンスキー	Questからの**案内**のEメールに記載されているライセンスキーです。ダッシュも含めてください。ライセンスキーがない場合は、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。
会社名	会社またはグループの名前です。
管理者Eメール	Questからの連絡の宛先となるEメールアドレスです。
パスワード	デフォルトの **admin** アカウントのパスワードです。このアカウントは、アプライアンスの**管理者コンソール**にログインするために使用します。この時点でデフォルトの **admin** アカウントがアプライアンス上で唯一のアカウントになります。このアカウ

オプション	説明
	ントのパスワードを忘れると、システムを出荷時のデフォルト状態にリセットすることが必要になる場合があり、データロスが発生します。 **注:** 複数のタイプの KACE アプライアンスを使用する場合、Quest では、すべてのアプライアンスの **admin** アカウントに同じパスワードを使用することをお勧めします。同じ admin アカウントのパスワードを使用することで、後でアプライアンス同士をリンクすることが可能になります。詳細については、「Quest KACEアプライアンスのリンク」を参照してください。
2 要素認証	アプライアンスにログインしているユーザーのセキュリティをより強力にするには、この設定を 有効 にします。この機能では、ログインプロセスにステップが 1 つ追加されます。これは、Google Authenticator アプリケーションに依存して検証コードを生成します。このアプリは、定期的に新しい 6 桁のコードを生成します。有効にすると、エンドユーザーはログインするたびに現在の検証コードを要求されます。 **注:** この機能を有効にする場合は、アプライアンスサーバのクロック、および Google Authenticator を実行しているデバイスが正確であることを確認してください。Google Authenticator は、現在の時刻に依存してトークンを作成します。サーバーのクロックが Google Authenticator を実行しているデバイスのクロックと同期されていない場合、トークンの検証が失敗し、アカウントのロックアウトが発生する可能性があります。

8. 画面の指示に従って、初期セットアップを完了します。

   初期セットアップが完了すると、アプライアンスが再起動し、**管理者コンソール**のログインページが表示されます。

   注: アプライアンスの IP アドレスを変更した場合は、新しいアドレスにアクセスして、ログインページを表示します。

9. ログイン ID「admin」と、初期セットアップ中に選択したパスワードを使用して、管理者コンソールにログインします。

   ライセンスと管理者の設定 ページで 2 要素認証が有効になっている場合は、2 要素認証の設定 ページが表示されます。

10. **2 要素認証のみ。**2 要素認証の設定 ページの指示に従い、スマートフォンを使用して Google Authenticator の検証コードを生成します。検証コード フィールドに、Google Authenticator のコードを入力し、**設定を完了** をクリックします。その後はログインのたびに新しい検証コードが要求されます。

    この手順をスキップするには、**設定をスキップ** をクリックします。このステップは、設定されている移行ウィンドウでのみバイパスできます。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。

管理者コンソールが表示され、アプライアンスが使用可能になります。使用しているブラウザの設定に基づいて、初回ログイン時に **管理者コンソール** に表示される日時情報のロケール形式が決定されます。言語設定の変更に関する詳細は、「ロケール設定の構成」を参照してください。

コマンドラインコンソールへのアクセス

コマンドラインコンソールは、アプライアンスへのターミナルウィンドウインターフェイスです。このインターフェイスを使用して、**管理者コンソール**アプライアンスの場合と同じように、アプライアンス設定を設定できます。これは、DHCP サーバーが利用できず、**管理者コンソール**にログインできない場合に便利です。

コマンドラインコンソールは、サービスとしての K1 とは併用されません。

1. 物理バージョンのアプライアンスがある場合：
    a. アプライアンスにモニタとキーボードを直接接続します。
    b. ネットワークケーブルを以下のポートに接続します。

    c. アプライアンスの電源をオンにします。

    コマンドラインコンソールのログイン画面が、アプライアンスに接続されたモニタに表示されます。
2. 仮想バージョンのアプライアンスがある場合は、仮想マシンの電源をオンにして、アプライアンスを起動します。

    コマンドラインコンソールのログイン画面が表示されます。
3. プロンプトで、次のように入力します。

    ログイン：konfig

    パスワード：konfig
4. コマンドラインコンソールで使用する言語を選択します。上矢印キーと下矢印キーを使用してフィールド間を移動します。
5. ネットワーク設定を構成します。詳細については、「アプライアンスのネットワーク設定の変更」を参照してください。

    ヒント: フィールド内のオプションを選択するには、右矢印キーと左矢印キーを使用します。フィールド間を移動するには、上矢印キーと下矢印キーを使用します。
6. 下矢印キーを使用してカーソルを 保存 に移動し、**Enter**キーまたは**Return**キーを押します。

    アプライアンスが再起動します。

設定の変更追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。

関連トピック

履歴設定について

システムレベルおよび管理者レベルの一般設定項目の設定

アプライアンス上で組織コンポーネントが有効化されている場合、一般設定項目はシステムレベルおよび管理者レベルで利用可能になります。アプライアンス上で組織コンポーネントが有効化されていない場合、すべての一般設定項目は管理者レベルで利用可能になります。

アプライアンスで組織コンポーネントが有効化されている場合は、以下を参照してください。

- 組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定.
- 管理者レベルまたは組織固有の一般設定項目の設定.

組織コンポーネントが有効化されていない場合は、以下を参照してください。

- 組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定.

組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定

アプライアンス上で組織コンポーネントが有効化されている場合、アプライアンス一般設定項目の設定はシステムレベルで行います。

アプライアンスで組織コンポーネントが有効化されていない場合は、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。

1. システムレベルの 一般設定 ページに移動します。
    a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
    b. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。
    c. コントロールパネル で **一般設定** をクリックします。
2. 一番上のセクションで、次の情報を入力します。

オプション	説明
会社名	会社の名前を入力します。
デフォルトのロケール	**コマンドラインコンソール**で使用する言語を選択します。これには、konfig ユーザーアカウントを使用します。
企業Eメールサフィックス	ユーザーのEメール送信元のドメインを入力します。例：quest.com。
アプライアンス管理者Eメール	アプライアンス管理者のEメールアドレスを入力します。システム関連のメッセージ（ 重大な警告を含む ）はこのアドレスに送信されます。
セッションタイムアウト	ユーザーセッションを終了し、ユーザーに再ログインを要求するまでの、非アクティブ状態を保持できる時間を設定します。デフォルトは「1」です。**ユーザーコンソール**と**管理者コンソール**には、この期限をユーザーに警告するためのタイムアウトセッションカウンタがあります。非アクティブ状態の期間のみがカウントされます。カウンタは、ユー

オプション	説明
	ザーがコンソールとアプライアンスサーバーの通信を発生させるアクション（ウィンドウの更新、変更の保存、ウィンドウの変更など）を実行すると再開されます。カウンタが上限に達すると、ユーザーはログアウトされ、ログイン画面が表示されます。この際、未保存の変更は失われます。タイムアウトセッションカウンタは、各コンソールの右上に表示されます。
モバイルデバイスによるアクセスを有効にする	アプライアンスに対するモバイルデバイスによるアクセスを有効または無効にします。モバイルデバイスによるアクセスにより、iOS または Android のスマートフォンまたはタブレットで KACE GO アプリケーションを使用してアプライアンスと対話できるようになります。管理者はこのアプリケーションを使用して、サービスデスク、インベントリ、およびアプリケーション展開機能にアクセスできます。詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。
ログイン時に組織の選択が必要	組織 ドロップダウンリストを**管理者コンソール**のログインページ（http://**appliance_hostname**/admin）に表示します。ここで、**appliance_hostname** はアプライアンスのホスト名です。これによって、ログイン時に組織を選択できるようになります。このオプションを無効にすると、ログインページに 組織 ドロップダウンリストが表示されないため、http://**appliance_hostname**/admin から、デフォルト組織にしかログインできなくなります。ただし、組織の高速切り替えを有効にすると、「Default」組織へのログイン後に組織間の切り替えが可能になります。
管理ヘッダーに組織メニューを表示	**管理者コンソール** の右上隅、ログイン情報の隣にある 高速切り替え ドロップダウンリストを表示します。このドロップダウンリストを使用すると、組織間の切り替え時にログインページを省略できます。ドロップダウンリストに表示する組織は、同じ **admin** アカウントのパスワードを使用している必要があります。**admin** アカウントのパスワードが一致する組織のみがリストに表示されます。ドロップダウンリストへの変更は、いったんログアウトし、再度ログインすることによって初めて反映されます。

3. （**オプション**）ベータ通知 セクションで、ベータプログラムに参加するかどうかを指定します。

   ベータプログラムの参加者は、ベータ版のアプライアンスが利用可能になったときに通知を受け取ります。これらの通知は、ホームダッシュボードにアラートとして表示されます。

   これらの通知は、特定の設定を対象とする場合があります。これらを有効にしても、ベータ版への自動アップグレードはトリガされず、また、このアプライアンスはベータプログラムに自動的に登録されません。ベータ版の登録には引き続き参加する必要があり、詳細は通知に記載されています。

   ホームダッシュボードの詳細については、「「ホーム」コンポーネントの使用」を参照してください。

   a. **KACE からベータ通知を有効化** を選択します。
   b. これらの通知をシステム管理コンソールにのみ表示する場合は、**ベータ通知をシステム UI に制限** を選択します。

このオプションをクリアしたままにすると、**管理者コンソール**と**システム管理コンソール**の両方にベータ通知が表示されます。

4. エージェントタスク セクションで、KACE エージェントのタスクスループットを表示または設定できます。

オプション	説明
前回のタスクスループットの更新	この値は、アプライアンスのタスクスループットが最後に更新された日付と時刻を示します。
現在の読み込み平均	このフィールドの値は、任意の時点のアプライアンスに対する負荷を示します。アプライアンスが正常に動作するには、このフィールドの値が0.0と10.0の間になければなりません。
タスクスループット	スケジュール済みタスク（インベントリの収集、スクリプト作成、パッチの更新など）のアプライアンスでの調整方法を制御する値。 **注:** この値は、「現在の読み込み平均」の値が10.0以下で、かつ「前回のタスクスループットの更新」の時間が15分を超える場合にのみ増やすことができます。

5. 重複したマシン検出設定（高度）セクションで、重複するデバイスレコードを防止するために以下のオプションを設定します

   アプライアンスは、既存のインベントリレコード（新規/不明の KUID の使用によって決定される）がないデバイスからインベントリを受信すると、このセクションで選択したデバイスのプロパティをスキャンして、新しいデバイスか既存のデバイスかを判断します。デバイスが既存のインベントリレコードに属していると判断された場合、新しいデバイスレコードは既存のレコードとマージされます。

オプション	説明
既存のマシンレコードを照合する必要がある	次のチェックボックスの 1 つまたは複数を選択して、アプライアンスが重複する可能性のあるデバイスを識別するために使用するデバイスプロパティを指定します。 • **マシン名** • **BIOSのシリアルナンバー** • **製造元** • **オペレーティングシステムのファミリ**
MAC アドレス	既存のデバイスレコードと照合するマシンレコードに関連付けられている MAC アドレスの番号を指定します。

6. ユーザーコンソール セクションで、必要に応じてテキストを変更します。

オプション	説明
タイトル	**ユーザーコンソール**のログインページに表示される見出し。

オプション	説明
ようこそメッセージ	**ユーザーコンソール**のようこそメッセージまたは説明。このテキストは、**ユーザーコンソール** ログインページのタイトルの下に表示されます。

7. 使用可能な使用ポリシー セクションで、ポリシー設定を選択します。

オプション	説明
有効	ユーザーが、**管理者コンソール**、**ユーザーコンソール**、または**コマンドラインコンソール** にアクセスする場合、または SSH や FTP を使用してログインする場合に、アプライアンスがポリシーを表示して、ユーザーにポリシーの条件に同意するよう要求できるようにします。
タイトル	**ユーザーコンソール**のログインページに表示されるポリシーの見出し。
メッセージ	ポリシーの詳細（ログインページの Title（タイトル）の下に表示されます）。ユーザーは、**ユーザーコンソール**にログインする前にポリシーの条件に同意する必要があります。

8. レポート作成 セクションで、レポート作成システムのパスワードを指定します。

オプション	説明
ユーザー名	（読み取り専用）レポートの生成に使用されるユーザー名。ユーザー名のレポートを使用すると、書き込み権限を与えることなく、データベースへのアクセスを可能にできます（追加のレポート作成ツールを提供）。
ユーザーパスワード	レポートユーザーのパスワード。このパスワードは、レポート作成システムおよびMySQL™のみによって使用されます。

9. ログの保持 セクションで、ログ情報を保持する日数を選択します。選択した日数より古いログエントリは、ログから自動的に削除されます。詳細については、「アプライアンスログの表示」を参照してください。
10. ユーザー通知の保持 セクションで、ユーザー通知を保持する日数を選択します。選択した日数より古いユーザー通知は、通知ペインをから自動的に削除されます。詳細については、「ユーザー通知を設定する」を参照してください。
11. 共有先 セクションで、データ共有オプションを選択します。

    このセクションで選択したデータ共有オプションにかかわらず、Quest は、ご使用の製品ライセンスを検証するための最小限のライセンス関連情報を収集します。この情報には、アプライアンスの MAC アドレス、アプライアンスソフトウェアのバージョン、ライセンスキー、管理対象デバイスの数などが含まれます。

オプション	説明
ハードウェア、ソフトウェア、およびアプライアンスの使用率サマリデータをデルと共有する	（推奨）概要情報をQuestと共有します。この情報には、アプライアンスによって管理されているデバイスの数、管理対象インストール、およびアプリケーションに加えて、アプライアンスのステータス、稼働時間、および読み込み平均が含まれます。

オプション	説明
	サポートが必要な場合に**Questサポート**に追加情報が提供されるよう、このオプションを使用することをお勧めします。Questと共有されたデータは、製品の改善計画で使用されます。
使用率の詳細データとクラッシュレポート（ITNinjaコミュニティの機能を使用するために必要）を共有する	（推奨）詳細情報をQuestと共有し、匿名情報をITNinja.comと共有します。この情報には、エージェントとアプライアンスのクラッシュレポート、ユーザーインターフェイスの使用状況の統計、およびアプリケーションタイトルなどのインベントリ情報が含まれます。Quest はこの情報を使用して、ソフトウェアカタログの改善を促進しています。また、ITNinja は匿名データを使用して、http://www.itninja.com 上の関連コンテンツを識別し、アプライアンス**管理者コンソール**に動的フィードを提供します。 ITNinja.comは、ITプロフェッショナルが情報を共有したり、システムの管理や導入に関するさまざまなトピックについて調査したりできるコミュニティWebサイトです。ITNinja フィードは、ソフトウェアの展開に関するヒントおよびその他のコンテキスト情報を、アプライアンス**管理者コンソール**内の関連ページに動的に表示する機能です。ITNinja フィードを有効にするには、**使用率の詳細データと共有 ...** を選択する必要があります。この設定により、ITNinjaとの情報共有が匿名で行われます。ITNinja フィードは、**使用率のサマリデータを共有** を選択した場合にのみ使用できます。また、ソフトウェア、管理対象インストール、およびファイル同期の詳細ページなど、ソフトウェアまたは展開に関連するページでのみ使用できます。フィードは、ソフトウェアカタログ の詳細ページでは利用できません。 このオプションをオフにすると、アプライアンスとITNinjaコミュニティの間でインベントリデータが共有されなくなります。ただし、このオプションをオフにしても、既に共有されている情報は削除されません。詳細については、**Questサポート**にお問い合わせください。
拡張パッチ診断の共有	（推奨）詳細なパッチ診断を Quest と共有します。

12. カスタム管理者コンソール、ユーザーコンソール、またはレポートロゴと背景色を使用するには、ログイン画面オプション セクションに次の情報を入力します。

オプション	説明
システムコンソールログインの背景色 **管理者コンソールログインの背景色** **ユーザーコンソールログインの背景色**	アプライアンスには、次のレベルからアクセスできます。 • **管理者コンソール**は、組織関連の機能を表示します。 • **システム管理コンソール**は、アプライアンス関連機能へのアクセスを提供します。 • **ユーザーコンソール**は、ユーザーがセルフサービスでアプリケーションを使用で

オプション	説明
	きるようにします。このインターフェイスから、サービスデスクのサポートチケットを提出して、ヘルプを要求したり問題をレポートしたりすることもできます。**ユーザーコンソール**にアクセスするには、http://<appliance_hostname>/user に移動します。<appliance_hostname> はアプライアンスのホスト名です。 これらの Web ベースのインターフェイスごとに、ログイン画面の異なる背景色を指定できます。組織レベルで指定された色は、システムレベル設定よりも優先されます。 色選択機能をクリックして使用し、ログイン画面の背景に表示する色を指定します。必要に応じて、マウスを使用して色を選択するか、RGB 値を指定できます。色選択機能を閉じると、右側の HTML カラーコード フィールドに、選択した色の HTML コードが表示されます。選択を元に戻すには、**リセット** をクリックして最初からやり直します。 **注:** 色選択機能は、Internet Explorer 11 ではサポートされていません。
システムコンソールのロゴ **管理者コンソールのロゴ** **ユーザーコンソールロゴ** **レポートのロゴ**	該当する各セクションで、**ファイルの選択** をクリックし、使用可能な Web インターフェイスおよびシステム生成レポートでカスタムロゴとして使用するグラフィックファイルを指定します。 サポートされているグラフィックファイル形式は、.bmp、.gif、.jpg、および .png です。組織レベルで設定されたロゴは、システムレベル設定よりも優先されます。 デフォルトのロゴとカスタマイズバージョンのサンプルを確認するには、次の図を参照してください。

デフォルトのユーザーコンソールのロゴ

カスタムのユーザーコンソールのロゴ

レポートのデフォルトロゴ

カスタムレポートのロゴ

13. Hewlett-Packard（HP）または Lenovo のデバイスを管理する場合は、その保証情報を取得することができます。そのためには、製造元の保証 API キー セクションで、HP および / または Lenovo の API キーを入力して、保証データを取得します。Lenovo ではキーのみが要求されますが、HP ではキーとシークレットの両方が要求されます。これらの値は、暗号化されてデータベースに保存されます。

   重要: 保証情報を取得するには、製造元の保証 API キーを設定する必要があります。詳細については、「https://go.kace.com/to/k1000-help-warranty」にアクセスしてください。

   設定されている場合、デバイスの保証情報は、HP または Lenovo のデバイスを選択したとき、インベントリ情報 グループの デバイスの詳細 ページに表示されます。詳細については、「デバイス詳細のアイテムのグループおよびセクション」を参照してください。

オプション	説明
Hewlett-Packard	管理対象の HP デバイスの保証情報を取得する場合は、このオプションを選択します。このオプションを選択してからクリアした場合、HP API キーとシークレットがデータベースから削除されます。

オプション	説明
キー	管理対象の HP デバイスの保証情報を取得するための API キー。
シークレット	管理対象の HP デバイスの保証情報を取得するためのシークレット。
Lenovo	管理対象の Lenovo デバイスの保証情報を取得する場合は、このオプションを選択します。このオプションを選択してからクリアした場合、Lenovo キーがデータベースから削除されます。
キー	管理対象の Lenovo デバイスの保証情報を取得するための API キー。

14. **保存してサービスを再起動** をクリックします。

関連トピック

ロケール設定の構成

モバイルデバイスによるアクセスの設定

組織の作成と管理

管理者レベルまたは組織固有の一般設定項目の設定

アプライアンス上で組織コンポーネントが有効化されている場合、組織固有の一般設定項目を管理者レベルで設定します。各組織の一般設定項目は別個に設定します。

詳細については、「組織の追加、編集、および削除」を参照してください。

アプライアンスで組織コンポーネントが有効化されていない場合は、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。

1. 管理者レベルの 一般設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**一般設定** をクリックします。
2. General Options（ 一般的なオプション ）セクションで、次の情報を表示または入力します。

オプション	説明
Last Updated（ 前回更新日 ）と **Organization Name**（ 組織名 ）	（ 読み取り専用 ）情報が変更された日付、および組織の名前。「組織名」はシステムレベルで編集できます。詳細については、「組織の追加または編集」を参照してください。
会社名	会社の名前を入力します。
管理者Eメール	アプライアンス管理者のEメールアドレスを入力します。システム関連のメッセージ（ 重大な警告を含む ）はこのアドレスに送信されます。

オプション	説明
企業Eメールサフィックス	ユーザーのEメール送信元のドメインを入力します。例：example.com。

3. オプション：ロケール設定 セクションで、ロケール設定を指定します。詳細については、「ロケール設定の構成」を参照してください。

オプション	説明
組織のロケール	選択した組織の**管理者コンソール**と**ユーザーコンソール**で使用するロケールを選択します。組織が複数ある場合、それぞれの組織に異なるロケールを選択することができます。詳細については、以下を参照してください。 • 組織の追加、編集、および削除 • ロケール設定の構成

4. オプション：SAMBA共有設定 セクションで、ファイル共有オプションを選択し、**SAMBA設定の保存** をクリックします。ファイル共有が無効になっている場合は、システムレベルで有効にしてから組織で有効にする必要があります。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。

オプション	説明
ファイル共有を有効にする	アプライアンスのクライアント共有を使用して、ファイル（管理対象デバイスにアプリケーションをインストールする際に使用するファイルなど）を保存します。 アプライアンスのクライアント共有は、プロビジョニングサービスで利用可能な組み込みのWindowsファイルサーバーで、ネットワーク上でSambaクライアントを配布するのに役立ちます。Questでは、管理対象デバイス上でアプリケーションのインストールを実行しているときにのみ、このファイルサーバーを有効にすることをお勧めします。
ファイル共有ユーザーの「admin」パスワード	ファイル共有ディレクトリへのアクセスに使用するadminアカウントのパスワードを入力します。

5. Ignore Client IP Address Settings（クライアントの IP アドレス設定を無視）セクションで、無視する IP アドレスを 1 つ以上入力します。複数ある場合は、アドレスをコンマで区切ります。IPアドレスの無視は、プロキシアドレスのように、複数のデバイスが同じIPアドレスをレポートする可能性がある場合に役立ちます。
6. License Usage Warning Configurations（ライセンス使用率の警告設定）セクションで、ソフトウェアライセンス使用率の警告しきい値と緊急しきい値に使用するパーセンテージを選択します。ソフトウェアライセンス資産を設定している場合、しきい値情報はDashboard（ダッシュボード）のライセンス関連ウィジェットに表示されます。
7. データの保持 セクションで、アプライアンスデータベースにデータを保持するためのオプションを選択します。

オプション	説明
デバイス稼働時間データの保持	デバイス稼働時間情報がアプライアンスデータベースに保持される月数。 デバイス稼働時間とは、管理対象デバイスが 1 日に稼働する時間数を指します。このデータを指定した

オプション	説明
	月数の間保持するか、「**無制限**」に保持するか、または保持しない（「**無効**」）こともできます。
メータリング情報の保持	メータリング情報がアプライアンスデータベースに保持される月数。 メータリング情報は、管理している Windows デバイスおよび Mac デバイス上のアプリケーションのインストールや使用に関する情報です。選択した月数よりも古いメータリング情報は、毎月初日に削除されます。詳細については、「メータリング情報について」を参照してください。
ソフトウェアカタログへのカタログ未登録データの保持	カタログ未登録のアプリケーションに関する情報をアプライアンスデータベースに保持するかどうか。 カタログ未登録のアプリケーションはアプライアンスインベントリに存在するものの、ソフトウェアカタログに掲載されていない実行可能ファイルで、アプライアンスはデフォルトではそのようなアプリケーションに関する情報を保持します。ただし、多数の管理対象デバイスを抱える組織の場合、このデータを保持すると、データベースのサイズが大幅に増える場合があります。このサイズが増えると、**管理者コンソール** にページをロードするためにかかる時間と、データベースバックアップを実行するためにかかる時間が長くなることがあります。 カタログ未登録のソフトウェアのデータをアプライアンスデータベースに保持するには、このチェックボックスをオンにします。データの保持を無効にするには、このチェックボックスをオフにします。 カタログ未登録のソフトウェアのデータの保持が無効になっている場合： • 管理対象デバイス上のエージェントが完全なインベントリ情報を引き続きアップロードし、アプリケーションに関連する raw データのフィンガープリントが採取されます。データ共有が有効である場合、データはQuest KACEソフトウェアカタログにもアップロードされます。詳細については、「データ共有の基本設定の構成」を参照してください。 • アプライアンスは、カタログ登録済みのアプリケーションおよびローカルカタログ登録済みのアプリケーションに関連する情報を組織データベースに引き続き保存します。 • カタログ未登録のアプリケーションに関連する情報は組織データベースに保存されず、**管理者コンソール**のカタログ未登録のアプリケーションリストは空になります。 • カタログ登録済みのアプリケーションのレポートは、引き続き想定どおりに機能します。ただし、カタログ未登録のアプリケーションに関連するレポートには、カタログ登録済みのソフトウェアタイトルに含まれるアプリケーションのみが記載されます。

オプション	説明
Microsoft Defender の脅威データの保持	Microsoft Defender の脅威データがアプライアンス データベースに保持される月数。

8. 資産アーカイブ セクションで、アーカイブ用にマークを付けた資産が実際にアーカイブされるまでの保持日数を入力します。デフォルト値は3日です。
9. ユーザーアーカイブセクションでは、必要に応じてユーザーのアーカイブを有効にするかどうかを示します。
    a. ユーザーアカウントをアーカイブできるようにするには、**ユーザーのアーカイブの有効化**チェックボックスをオンにします。

    注: ユーザーのアーカイブが有効になると、削除できるユーザーアカウントはアーカイブ済みとしてマークされているものだけになります。

    b. アーカイブタグフィールドに、アーカイブされたユーザーの状態に関連付けるラベルを入力します。例えば、アーカイブ済みや非アクティブです。
    c. サービスデスクチケットおよびアーカイブされたユーザーに関連する資産を保守するかどうかを示します。チケット関連付けフィールドと資産関連付けフィールドのそれぞれに対して、次のいずれかのオプションを設定します。

    - **ユーザーの維持**：アーカイブされたユーザーとチケットまたは資産の関連付けを継続する場合、このオプションを選択します。このオプションを選択するとアーカイブされたユーザー名の横に表示される構成済みのアーカイブタグは、そのユーザーがアクティブではなくなっていることを示します。
    - **ユーザーの削除**：アーカイブされたユーザーとすべてのチケットや資産の関連付けを削除する場合、このオプションを選択します。

    ユーザーアカウントのアーカイブ方法の詳細については、ユーザーアカウントのアーカイブを参照してください。
10. デバイス割り当て セクションで、ユーザーとデバイスを照合する方法を、**ワンタイム同期**、**継続的な同期**、または **無効** から指定します。
11. Device Actions（デバイスのアクション）セクションで、**新しいアクションの追加** をクリックし、有効化するスクリプト形式のアクションを選択します。

    「デバイスのアクション」は、管理対象デバイス上で実行可能なスクリプト形式のアクションです。事前にプログラムされた複数のアクションがあります。独自のアクションを追加するには、アクション メニューで **カスタムアクション** を選択し、コマンドライン テキストボックスにコマンドを入力します。

    デバイスのアクション用に使用できる変数は次の通りです。

    KACE_HOST_IP

    KACE_HOST_NAME

    KACE_CUSTOM_INVENTORY_*

    デバイスのアクションの実行時に、変数がアプライアンスによって適切な値に置き換えられます。

    KACE_CUSTOM_INVENTORY_*のアスタリスク（*）は、カスタムインベントリルールに関連付けられているソフトウェアアプリケーションの名前で置き換えます。デバイスのアクションの実行時に、その名前がデバイスのカスタムインベントリルールの値で置き換えられます。ソフトウェアアプリケーションの名前は大文字で入力します。使用できる文字は次の通りです。「A〜Z」、「0〜9」、「.」、「-」。

    注: アクション ドロップダウンリストのほとんどのアクションを機能させるために、追加のアプリケーションをインストールするよう求められます。例えば、DameWareを使用するには、自分のデバイスに加え、アクセスするデバイスにTightVNCをインストールする必要があります。

    この機能は、Windows デバイスでのみサポートされます。デバイスアクションを実行している Windows デバイスに KACE エージェントバージョン 9.0 以降のエージェントがインストールされ、接続されている必要があります。

エージェントを介してデバイスを開始する場合、アクションの実行可能ファイルは %PATH% に配置する必要があります。エージェントは 32 ビットであるため、64 ビットの Windows デバイスでは、%windir%/Wow64 ディレクトリのエイリアスとして %windir%/System32 を使用します。64 ビット Windows システムの %windir%/System32 ディレクトリにあるプログラムを実行する必要がある場合は、%windir%/SysNative 仮想ディレクトリを使用する必要があります。マシンアクションを定義するときは、%windir%/SysNative を %PATH% 環境変数に追加するか、実行可能ファイルの前に %windir%/SysNative を追加して、完全修飾パスを提供することができます。

12. 管理者がすべてのデバイスにパッチを適用できないようにする場合は、パッチスケジュール セクションで、**すべてのデバイス を非表示** チェックボックスを選択します。

    注: この設定は、設定されているパッチスケジュールがすべてのデバイスに存在しない場合にのみ適用できます。それ以外のケースに適用しようとすると、警告が表示されます。

13. 許可された一括アクション セクションで、KACE Cloud Mobile Device Manager（MDM）と VMware 仮想マシンデバイスに対して一括アクションを有効にするかどうかを指定します。一括アクションが有効になっている場合、関連付けられている KACE Cloud MDM および VMware 仮想マシンコマンドが デバイス リストページの **アクションを選択** メニューから使用可能になります。

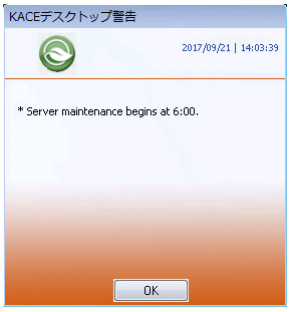
オプション	説明
KACE Cloud MDM の一括アクションを有効にする	デバイス リストページで複数の KACE Cloud MDM デバイスに対してコマンドを有効にするには、このチェックボックスをオンにします。
仮想マシンの一括アクションを有効にする	デバイス リストページで複数の VMware または Hyper-V 仮想マシンデバイスに対してコマンドを有効にするには、このチェックボックスをオンにします。
Chrome OS の一括アクションを有効にする	デバイス リストページで複数の Chrome OS デバイスに対してコマンドを有効にするには、このチェックボックスをオンにします。
デバイスの一括再起動コマンドを有効にする	デバイス リストページで複数のデバイスに対して再起動コマンドを有効にするには、このチェックボックスをオンにします。
Microsoft Defender の一括アクションを有効にする	デバイス リストページで複数のデバイスに対して Microsoft Defender コマンドを有効にするには、このチェックボックスをオンにします。

14. カスタム管理者コンソール、ユーザーコンソール、レポート、および KACE エージェントアラートのロゴと背景色を使用するには、ログイン画面オプション セクションで次の情報を入力します。

オプション	説明
管理者コンソールログインの背景色 **ユーザーコンソールログインの背景色**	アプライアンスには、次のレベルからアクセスできます。 • **管理者コンソール**は、組織関連の機能を表示します。 • **システム管理コンソール**は、アプライアンス関連機能へのアクセスを提供します。 • **ユーザーコンソール**は、ユーザーがセルフサービスでアプリケーションを使用できるようにします。このインターフェイスから、サービスデスクのサポートチケットを提出して、ヘルプを要求したり問題を

オプション	説明
	レポートしたりすることもできます。**ユーザーコンソール**にアクセスするには、http://<appliance_hostname>/user に移動します。<appliance_hostname> はアプライアンスのホスト名です。 **管理者コンソール**で組織を選択した場合、**管理者コンソール**および**ユーザーコンソール**ログイン画面の別の背景色を指定できます。組織レベルで指定された色は、システムレベル設定よりも優先されます。システムレベル設定を行う方法の詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。 色選択機能をクリックして使用し、ログイン画面の背景に表示する色を指定します。必要に応じて、マウスを使用して色を選択するか、RGB 値を指定できます。色選択機能を閉じると、右側の HTML カラーコード フィールドに、選択した色の HTML コードが表示されます。選択を元に戻すには、**リセット** をクリックして最初からやり直します。 **注:** 色選択機能は、Internet Explorer 11 ではサポートされていません。
管理者コンソールのロゴ **ユーザーコンソールロゴ** **レポートのロゴ** **エージェント警告のロゴ**	該当する各セクションで、**ファイルの選択** をクリックし、**管理者コンソール**、**ユーザーコンソール**、システム生成レポート、および管理対象デバイスに表示される KACE エージェントアラートでカスタムロゴとして使用するグラフィックファイルを指定します。 サポートされているグラフィックファイル形式は、.bmp、.gif、.jpg、および .png です (.bmp ファイルのみをサポートする KACE エージェントアラートは除く) 。組織レベルで設定されたロゴは、システムレベル設定よりも優先されます。 デフォルトの KACE エージェントアラートとカスタマイズバージョンのサンプルを確認するには、次の図を参照してください。**管理者コンソール**、**ユーザーコンソール**、およびシステムレベルのレポートでのデフォルトのロゴとカスタムロゴの例については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。
警告のデフォルトロゴ	

警告のカスタムロゴ



15. **保存してサービスを再起動** をクリックします。
16. 複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定

アプライアンス上で組織コンポーネントが有効化されていない場合、すべてのアプライアンス一般設定項目は管理者レベルで利用可能になります。

アプライアンスで組織コンポーネントが有効化されている場合は、管理者レベルまたは組織固有の一般設定項目の設定を参照してください。

1. 管理者レベルの 一般設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**一般設定** をクリックします。
2. 一般的なオプション セクションで、次の情報を入力します。

オプション	説明
前回更新日	読み取り専用：情報が変更された日付、および組織の名前。
会社名	会社の名前を入力します。
管理者Eメール	アプライアンス管理者のEメールアドレスを入力します。システム関連のメッセージ（ 重大な警告を含む ）はこのアドレスに送信されます。
企業Eメールサフィックス	ユーザーのEメール送信元のドメインを入力します。例：example.com。

オプション	説明
モバイルデバイスによるアクセスを有効にする	アプライアンスに対するモバイルデバイスによるアクセスを有効または無効にします。モバイルデバイスによるアクセスにより、iOS または Android のスマートフォンまたはタブレットで KACE GO アプリケーションを使用してアプライアンスと対話できるようになります。管理者はこのアプリケーションを使用して、サービスデスク、インベントリ、およびアプリケーション展開機能にアクセスできます。 詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。
セッションタイムアウト	ユーザーセッションを終了し、ユーザーに再ログインを要求するまでの、非アクティブ状態を保持できる時間を設定します。デフォルトは「1」です。**ユーザーコンソール**と**管理者コンソール**には、この期限をユーザーに警告するためのタイムアウトセッションカウンタがあります。非アクティブ状態の期間のみがカウントされます。カウンタは、ユーザーがコンソールとアプライアンスサーバーの通信を発生させるアクション（ウィンドウの更新、変更の保存、ウィンドウの変更など）を実行すると再開されます。カウンタが上限に達すると、ユーザーはログアウトされ、ログイン画面が表示されます。この際、未保存の変更は失われます。タイムアウトセッションカウンタは、各コンソールの右上に表示されます。

3. クライアントドロップファイルサイズフィルタ セクションで、ファイルサイズを指定します。

オプション	説明
クライアントドロップファイルサイズフィルタ	組織のクライアントドロップの場所のファイルサイズフィルタ。 クライアントドロップの場所は、アプライアンス上にある組織のストレージエリア（SAMBA 共有）です。このストレージエリアは、アプリケーションインストーラーやアプライアンスバックアップファイルなどの大規模ファイルをアプライアンスにアップロードするために使用されます。クライアントドロップの場所へのファイルのアップロードは、大規模ファイルではブラウザがタイムアウトする可能性がある、**管理者コンソール**でデフォルトの HTTP メカニズムを使用してファイルをアップロードする方法の代わりになります。 Client Drop Size（クライアントドロップサイズ）フィルタにより、組織のクライアントドロップの場所にアップロードされるファイルを Software Detail（ソフトウェア詳細）ページの Upload and Associate Client Drop File（クライアントドロップファイルのアップロードと関連付け）リストに表示するかどうかを決定します。例えば、Client Drop Size（クライアントドロップサイズ）フィルタを 1 GB に設定すると、Upload and Associate Client Drop File（クライアントドロップファイルのアップロードと関連付け）リストにはサイズが 1 GB 以上

オプション	説明
	のファイルが表示されます。サイズが 1 GB 未満のファイルは、リストに表示されません。 Software Detail（ソフトウェア詳細）ページでアプリケーションファイルを選択して保存すると、そのファイルは組織のクライアントドロップの場所から適切なエリアに移動します。 クライアントドロップの場所に配置されるアプライアンスバックアップファイルは、アプライアンスバックアップファイルとして自動的に識別され、5 分以内に バックアップ設定 ページで選択できるようになります。詳細については、「アプライアンスクライアントドロップの場所へのファイルのコピー」を参照してください。

4. ユーザーコンソール セクションで、ユーザーコンソール のテキストのカスタマイズを指定します。

オプション	説明
タイトル	**ユーザーコンソール**のログインページに表示される見出し。**ユーザーコンソール**は、ユーザーがアプリケーションをセルフサービス方式で使用できるようにする Web ベースのインタフェースです。このインターフェイスから、サービスデスクのサポートチケットを提出して、ヘルプを要求したり問題をレポートしたりすることもできます。**ユーザーコンソール**にアクセスするには、http://<appliance_hostname>/user に移動します。<appliance_hostname> はアプライアンスのホスト名です。
ようこそメッセージ	**ユーザーコンソール**のようこそメッセージまたは説明。このテキストは、**ユーザーコンソール** ログインページのタイトルの下に表示されます。

5. 使用可能な使用ポリシー セクションで、ポリシー設定を選択します。

オプション	説明
有効	ユーザーが、**管理者コンソール**、**ユーザーコンソール**、または**コマンドラインコンソール** にアクセスする場合、または SSH や FTP を使用してログインする場合に、アプライアンスがポリシーを表示して、ユーザーにポリシーの条件に同意するよう要求できるようにします。
タイトル	**ユーザーコンソール**のログインページに表示されるポリシーの見出し。
メッセージ	ポリシーの詳細（ログインページの Title（タイトル）の下に表示されます）。ユーザーは、**ユーザー**

オプション	説明
	コンソールにログインする前にポリシーの条件に同意する必要があります。

6. ログの保持 セクションで、ログ情報を保持する日数を選択します。選択した日数より古いログエントリは、ログから自動的に削除されます。詳細については、「アプライアンスログにアクセスしてMicrosoft Exchange Serverサーバーエラーを表示する」を参照してください。
7. ユーザー通知の保持 セクションで、ユーザー通知を保持する日数を選択します。選択した日数より古いユーザー通知は、通知ペインをから自動的に削除されます。詳細については、「ユーザー通知を設定する」を参照してください。
8. 共有先 セクションで、データ共有オプションを指定します。

注: このセクションで選択したデータ共有オプションにかかわらず、Quest は、ご使用の製品ライセンスを検証するための最小限のライセンス関連情報を収集します。この情報には、アプライアンスの MAC アドレス、アプライアンスソフトウェアのバージョン、ライセンスキー、管理対象デバイスの数などが含まれます。

オプション	説明
ハードウェア、ソフトウェア、およびアプライアンスの使用率サマリデータをデルと共有する	（推奨）概要情報をQuestと共有します。この情報には、アプライアンスによって管理されているデバイスの数、管理対象インストール、およびアプリケーションに加えて、アプライアンスのステータス、稼働時間、および読み込み平均が含まれます。サポートが必要な場合に**Questサポート**に追加情報が提供されるよう、このオプションを使用することをお勧めします。Questと共有されたデータは、製品の改善計画で使用されます。
使用率の詳細データとクラッシュレポート（ITNinjaコミュニティの機能を使用するために必要）を共有する	（推奨）詳細情報をQuestと共有し、匿名情報をITNinja.comと共有します。この情報には、エージェントとアプライアンスのクラッシュレポート、ユーザーインターフェイスの使用状況の統計、およびアプリケーションタイトルなどのインベントリ情報が含まれます。Quest はこの情報を使用して、ソフトウェアカタログの改善を促進しています。また、ITNinja は匿名データを使用して、http://www.itninja.com 上の関連コンテンツを識別し、アプライアンス**管理者コンソール**に動的フィードを提供します。 ITNinja.comは、ITプロフェッショナルが情報を共有したり、システムの管理や導入に関するさまざまなトピックについて調査したりできるコミュニティWebサイトです。ITNinja フィードは、ソフトウェアの展開に関するヒントおよびその他のコンテキスト情報を、アプライアンス**管理者コンソール**内の関連ページに動的に表示する機能です。ITNinja フィードを有効にするには、**使用率の詳細データと共有 ...** を選択する必要があります。この設定により、ITNinjaとの情報共有が匿名で行われます。ITNinjaフィードは、**使用率のサマリデータを...と共有** を選択した場合にのみ使用できます。また、ソフトウェア、管理対象インストール、およびファイル同期の詳細ページなど、ソフトウェア展開に関連するページでのみ使用できます。フィードは、ソフトウェアカタログ の詳細ページでは利用できません。

オプション	説明
	このオプションをオフにすると、アプライアンスとITNinjaコミュニティの間でインベントリデータが共有されなくなります。ただし、このオプションをオフにしても、既に共有されている情報は削除されません。詳細については、**Questサポート**にお問い合わせください。
拡張パッチ診断の共有	（推奨）詳細なパッチ診断を Quest と共有します。

9. Locale Settings（ロケール設定）セクションで、次のロケール設定を指定します。これらの基本設定によって、管理者コンソールに表示される日時の情報の形式が決まります。

オプション	説明
組織のロケール	組織の**管理者コンソール**と**ユーザーコンソール**とで使用する言語。
コマンドラインコンソールロケール	**コマンドラインコンソール**で使用するロケール。これには、konfig ユーザーアカウントを使用します。

10. Ignore Client IP Address Settings（クライアントの IP アドレス設定を無視）セクションで、無視する IP アドレスを 1 つ以上入力します。複数ある場合は、アドレスをコンマで区切ります。IPアドレスの無視は、プロキシアドレスのように、複数のデバイスが同じIPアドレスをレポートする可能性がある場合に役立ちます。
11. License Usage Warning Configurations（ライセンス使用率の警告設定）セクションで、ソフトウェアライセンス使用率の警告しきい値と緊急しきい値に使用するパーセンテージを選択します。ソフトウェアライセンス資産を設定している場合、しきい値情報は Dashboard（ダッシュボード）のライセンス関連ウィジェットに表示されます。
12. Update Reporting User Password（ユーザーパスワードレポートの更新）セクションで、組織でレポートを実行するために必要なアカウントのパスワードを指定します。Database Name（データベース名）または Report Username（レポートユーザー名）を変更することはできません。
13. Data Retention（データの保持）セクションで、アプライアンスにデータを保持するためのオプションを選択します。このデータを指定した月数の間保持するか、「**無制限**」に保持するか、または保持しない（「**無効**」）こともできます。

オプション	説明
デバイス稼働時間データの保持	デバイスの稼働時間データを保存する期間。デバイスの稼働時間データとは、管理対象デバイスが1日に稼働する時間数を指します。このデータを指定した月数の間保持するか、「**無制限**」に保持するか、または保持しない（「**無効**」）こともできます。
メータリング情報の保持	メータリング情報がアプライアンスデータベースに保持される月数。 メータリング情報は、管理している Windows デバイスおよび Mac デバイス上のアプリケーションのインストールや使用に関する情報です。選択した月数よりも古いメータリング情報は、毎月初日に削除されます。詳細については、「メータリング情報について」を参照してください。
ソフトウェアカタログへのカタログ未登録データの保持	カタログ未登録のアプリケーションに関する情報をアプライアンスデータベースに保持するかどうか。 カタログ未登録のアプリケーションはアプライアンスインベントリに存在するものの、ソフトウェアカ

オプション	説明
	タログに掲載されていない実行可能ファイルで、アプライアンスはデフォルトではそのようなアプリケーションに関する情報を保持します。ただし、多数の管理対象デバイスを抱える組織の場合、このデータを保持すると、データベースのサイズが大幅に増える場合があります。この場合、**管理者コンソール**にページをロードするためにかかる時間と、データベースバックアップを実行するためにかかる時間が長くなることがあります。 カタログ未登録のソフトウェアのデータをアプライアンスデータベースに保持するには、このチェックボックスをオンにします。データの保持を無効にするには、このチェックボックスをオフにします。 カタログ未登録のソフトウェアのデータの保持が無効になっている場合： • 管理対象デバイス上のエージェントが完全なインベントリ情報を引き続きアップロードし、アプリケーションに関連する raw データのフィンガープリントが採取されます。データ共有が有効である場合、データはQuest KACEソフトウェアカタログにもアップロードされます。詳細については、「データ共有の基本設定の構成」を参照してください。 • アプライアンスは、カタログ登録済みのアプリケーションおよびローカルカタログ登録済みのアプリケーションに関連する情報を組織データベースに引き続き保存します。 • カタログ未登録のアプリケーションに関連する情報は組織データベースに保存されず、**管理者コンソール**のカタログ未登録のアプリケーションリストは空になります。 • カタログ登録済みのアプリケーションのレポートは、引き続き想定どおりに機能します。ただし、カタログ未登録のアプリケーションに関連するレポートには、カタログ登録済みのソフトウェアタイトルに含まれるアプリケーションのみが記載されます。

14. Device Actions（デバイスのアクション）セクションで、**新しいアクションの追加** をクリックし、有効化するスクリプト形式のアクションを選択します。

    「デバイスのアクション」は、管理対象デバイス上で実行可能なスクリプト形式のアクションです。事前にプログラムされた複数のアクションがあります。独自のアクションを追加するには、アクション メニューで **カスタムアクション** を選択し、コマンドライン テキストボックスにコマンドを入力します。

    デバイスのアクション用に使用できる変数は次の通りです。

    KACE_HOST_IP

    KACE_HOST_NAME

    KACE_CUSTOM_INVENTORY_*

    デバイスのアクションの実行時に、変数がアプライアンスによって適切な値に置き換えられます。

    KACE_CUSTOM_INVENTORY_*のアスタリスク（*）は、カスタムインベントリルールに関連付けられているソフトウェアアプリケーションの名前で置き換えます。デバイスのアクションの実行時に、その名前

がデバイスのカスタムインベントリルールの値で置き換えられます。ソフトウェアアプリケーションの名前は大文字で入力します。使用できる文字は次の通りです。「A〜Z」、「0〜9」、「.」、「-」。

注: アクション ドロップダウンリストのほとんどのアクションを機能させるために、追加のアプリケーションをインストールするよう求められます。例えば、DameWareを使用するには、自分のデバイスに加え、アクセスするデバイスにTightVNCをインストールする必要があります。

この機能は、Windows デバイスでのみサポートされます。デバイスアクションを実行している Windows デバイスに KACE エージェントバージョン 9.0 以降のエージェントがインストールされ、接続されている必要があります。

エージェントを介してデバイスを開始する場合、アクションの実行可能ファイルは %PATH% に配置する必要があります。エージェントは 32 ビットであるため、64 ビットの Windows デバイスでは、%windir%/Wow64 ディレクトリのエイリアスとして %windir%/System32 を使用します。64 ビット Windows システムの %windir%/System32 ディレクトリにあるプログラムを実行する必要がある場合は、%windir%/SysNative 仮想ディレクトリを使用する必要があります。マシンアクションを定義するときは、%windir%/SysNative を %PATH% 環境変数に追加するか、実行可能ファイルの前に %windir%/SysNative を追加して、完全修飾パスを提供することができます。

15. カスタム管理者コンソール、ユーザーコンソール、レポート、および KACE エージェントアラートのロゴと背景色を使用するには、ログイン画面オプション セクションで次の情報を入力します。

オプション	説明
管理者コンソールログインの背景色 **ユーザーコンソールログインの背景色**	アプライアンスには、次のレベルからアクセスできます。 • **管理者コンソール**は、組織関連の機能を表示します。 • **システム管理コンソール**は、アプライアンス関連機能へのアクセスを提供します。 • **ユーザーコンソール**は、ユーザーがセルフサービスでアプリケーションを使用できるようにします。このインターフェイスから、サービスデスクのサポートチケットを提出して、ヘルプを要求したり問題をレポートしたりすることもできます。**ユーザーコンソール**にアクセスするには、http://<appliance_hostname>/user に移動します。<appliance_hostname> はアプライアンスのホスト名です。 **管理者コンソール**で組織を選択した場合、**管理者コンソール**および**ユーザーコンソール**ログイン画面の別の背景色を指定できます。組織レベルで指定された色は、システムレベル設定よりも優先されます。システムレベル設定を行う方法の詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。 色選択機能をクリックして使用し、ログイン画面の背景に表示する色を指定します。必要に応じて、マウスを使用して色を選択するか、RGB 値を指定できます。色選択機能を閉じると、右側の HTML カラーコード フィールドに、選択した色の HTML コードが表示されます。選択を元に戻すには、**リセット** をクリックして最初からやり直します。 **注:** 色選択機能は、Internet Explorer 11 ではサポートされていません。

オプション	説明
管理者コンソールのロゴ **ユーザーコンソールロゴ** **レポートのロゴ** **エージェント警告のロゴ**	該当する各セクションで、**ファイルの選択** をクリックし、**管理者コンソール**、**ユーザーコンソール**、システム生成レポート、および管理対象デバイスに表示される KACE エージェントアラートでカスタムロゴとして使用するグラフィックファイルを指定します。 サポートされているグラフィックファイル形式は、.bmp、.gif、.jpg、および .png です（.bmp ファイルのみをサポートする KACE エージェントアラートは除く）。組織レベルで設定されたロゴは、システムレベル設定よりも優先されます。 デフォルトの KACE エージェントアラートとカスタマイズバージョンのサンプルを確認するには、次の図を参照してください。**管理者コンソール**、**ユーザーコンソール**、およびシステムレベルのレポートでのデフォルトのロゴとカスタムロゴの例については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。

警告のデフォルトロゴ

警告のカスタムロゴ

16. Hewlett-Packard（HP）または Lenovo のデバイスを管理する場合は、その保証情報を取得することができます。そのためには、製造元の保証 API キー セクションで、HP および / または Lenovo の API キーを入力して、保証データを取得します。Lenovo ではキーのみが要求されますが、HP ではキーとシークレットの両方が要求されます。これらの値は、暗号化されてデータベースに保存されます。

重要: 保証情報を取得するには、製造元の保証 API キーを設定する必要があります。詳細については、「https://go.kace.com/to/k1000-help-warranty」にアクセスしてください。

設定されている場合、デバイスの保証情報は、HP または Lenovo のデバイスを選択したとき、インベントリ情報 グループの デバイスの詳細 ページに表示されます。詳細については、「デバイス詳細のアイテムのグループおよびセクション」を参照してください。

オプション	説明
Hewlett-Packard	管理対象の HP デバイスの保証情報を取得する場合は、このオプションを選択します。このオプションを選択してからクリアした場合、HP API キーとシークレットがデータベースから削除されます。
キー	管理対象の HP デバイスの保証情報を取得するための API キー。
シークレット	管理対象の HP デバイスの保証情報を取得するためのシークレット。
Lenovo	管理対象の Lenovo デバイスの保証情報を取得する場合は、このオプションを選択します。このオプションを選択してからクリアした場合、Lenovo キーがデータベースから削除されます。
キー	管理対象の Lenovo デバイスの保証情報を取得するための API キー。

17. **保存してサービスを再起動** をクリックします。

    アプライアンスが再起動します。

アプライアンスの日付と時刻の設定

管理者コンソールの 設定 セクションで、アプライアンスの日付と時刻の設定を行います。アプライアンス上で組織コンポーネントが有効化されている場合、日付と時刻の設定はシステムレベルで利用可能になります。

計算の多くは日付と時刻の設定に基づいて行われるため、アプライアンスのこれらの設定を正確に保つことが重要です。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **日付と時刻の設定** をクリックします。

   日付と時刻の設定 ページが表示されます。
3. 次の設定を指定します。

オプション	説明
タイムゾーン	ドロップダウンリストでタイムゾーンを選択します。
時刻設定	オプションを選択します。 • **「ネットワークタイムプロトコルを設定します」**。インターネットタイムサーバーを使用します。このオプションを選択した場

オプション	説明
	合、サーバー フィールドにサーバーのWebアドレスを入力します。 • 「**日付と時刻の手動設定**」。アプライアンスのクロックを手動で設定します。ドロップダウンリストで時間と日付を指定します。時間ドロップダウンリストでは、24時間制が使用されています。
サーバー	インターネットタイムサーバーを使用して、アプライアンスの時間を設定します。テキストボックスにタイムサーバーのWebアドレスを入力します。例：time.example.com。

4. **保存して再起動** をクリックします。

   Webサーバーが再起動し、設定が適用されます。

   注: アクティブな接続は、再起動中にドロップされる場合があります。変更を保存すると、15秒後にページが自動的に更新されます。アプライアンス Web サーバーの再起動後、更新された日付と時刻が**管理者コンソール**の右下に表示されます。

ユーザー通知の管理

アプライアンスのユーザー通知は、注意が必要な特定のイベントについて警告します。

これらのアラートは通知パネルに表示され、画面の右上隅にあるベルアイコンをクリックするとアクセスできます。管理者は、必要に応じて通知設定を確認または編集できます。

ユーザー通知アラートを確認する

アプライアンスでは、事前定義された特定の条件が検出されると、管理者コンソールにユーザー通知アラートが表示されます。

トリガされたユーザー通知のリストには、画面の右上隅にあるベルアイコンを使用してアクセスできます。このアイコンを使用して、必要に応じて通知ペインを表示または非表示にします。新しい通知が報告されると、ベルアイコンにオレンジ色のインジケータが表示されます。新しい通知をすべて確認すると、インジケータが消えます。

リストに表示されるそれぞれの通知アラートは、関連する通知設定によってトリガされます。詳細については、「ユーザー通知を設定する」を参照してください。

アラートの背景色は、情報（青）、警告（黄）、警告（赤）で、アラートの重大度を示します。これは通知設定でも決定されます。

通知項目には常にタイムスタンプがあり、アラートがいつ発生したかを示します。アプライアンスが再起動しても、設定された期間リストに残ります。必要に応じて、一般設定 ページで通知保持期間を編集できます。詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。

一部の通知には、通知に関連付けられたオブジェクトにドリルダウンするために使用できるリンクが含まれています。例えば、ライセンスの有効期限通知が表示された場合、通知のリンクをクリックすると、期限が迫っているライセンスインスタンスに直接移動します。

通知が複数の項目（デバイスまたはライセンス）に適用される場合は、該当する項目ごとに 1 つずつ、複数の通知アラートが表示されます。

また、通知設定が 1 人または複数のユーザーに関連付けられている場合、結果の通知アラートは **管理者コンソール** 内のそれらのユーザーにのみ表示されます。通知設定がどのユーザーにもこのようにリンクされていない場合、**管理者コンソール** にログインした管理者権限を持つすべてのユーザーが関連する通知を表示できます。この

メカニズムは、すべてのユーザーへのすべての通知が常に表示される **システム管理コンソール** には適用されません。

リスト内の各エントリの右上隅にある削除アイコンをクリックすると、個々の通知を削除できます。通知のリストをクリアするには、**すべて削除** をクリックします。

1. 次のいずれかを実行します。
   - **アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または**、管理ヘッダーに組織メニューを表示 **がアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。**
   - **アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。**

   ダッシュボード ページまたは システム概要 ページが表示されます。
2. 画面の右上隅で、ベルアイコンをクリックして通知ペインを表示します。
3. 通知のリストを確認します。
4. （**オプション**）必要に応じて、個々の通知またはすべての通知を削除できます。
   - 通知を削除するには、通知アラートの右上隅にある削除アイコンをクリックします。
   - すべての通知を削除し、リスト全体をクリアするには、通知ペインの右上隅にある **すべて削除** をクリックします。

ユーザー通知を設定する

アプライアンスには、事前定義されたさまざまな通知設定が含まれています。

管理者は、ユーザー通知 ページでこれらの設定を確認できます。各設定の詳細は、リストで選択した後に ユーザー通知の詳細 ページに表示されます。一部の設定は有効または無効にできますが、その他の設定は読み取り専用です。

1 つまたは複数のラベルを使用して、通知設定を特定のユーザーに関連付けることができます。これにより、結果として発生する通知アラートは、これらのラベルで指定されたユーザーに対してのみ **管理者コンソール** に表示されます。通知設定がこのようにどのユーザーにもリンクされていない場合、管理レベルの権限を持つすべてのユーザーは、通知がトリガされたときに、**管理者コンソール** で関連する通知アラートを表示できます。これらの設定は **システム管理コンソール** には適用されず、すべてのユーザーへのすべての通知が常に表示されます。

1. ユーザー通知 リストページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**設定** をクリックして、**ユーザー通知** をクリックします。
2. ユーザー通知 ページで、通知のリストを確認します。

   各項目について、リストには、その名前、説明、通知が有効かどうか、カテゴリ、および関連付けられているラベルが表示されます。使用可能なカテゴリがいくつかあり、それぞれが環境の特定の面に重点を置いています。例えば、カテゴリ別にリストを並べ替えたり、セキュリティ や パッチ適用 など、特定のセグメントのすべての通知を確認したりできます。
3. 特定の通知設定を確認または編集するには、次の手順を実行します。
   a. ユーザー通知の名前をクリックします。
   b. ユーザー通知の詳細 ページの内容を確認します。

   名前、説明、および カテゴリ の設定は読み取り専用です。一部の通知設定では、**有効** チェックボックスを使用して有効または無効にできます。このボックスが淡色表示されている場合、通知設定は常に有効です。

   c. ユーザー通知ラベル 領域を確認し、必要に応じてラベルのコレクションを編集します。

   通知設定にラベルを追加すると、そのラベルで指定されたユーザーだけが、トリガされた通知アラートを表示できます。通知設定がこの方法を使用する特定のユーザーを指していない場合、**管理者コン**

ソール の管理レベルの権限を持つすべてのユーザーに通知を表示できます。ただし、**システム管理コンソール** には、これらの設定に関係なく、すべてのログインユーザーへのすべての通知が表示されます。

通知設定に関連付けられているラベルを表示、追加、または編集するには、次の手順を実行します。

a. **関連ラベルの管理** をクリックします。
b. 表示される ラベルを選択 ダイアログボックスで、ユーザー通知に関連付けるラベルのリストを確認または編集します。各通知設定に複数のラベルを追加できます。
c. 完了したら、**OK** をクリックして、ユーザー通知の詳細 ページに戻ります。
d. ユーザー通知の詳細 ページで、**保存** をクリックします。

すべてのユーザーに対して 2 要素認証を有効にする

2 要素認証 (2FA) は、ログインプロセスにさらにステップを追加することで、ユーザーがアプライアンスにログインするためのセキュリティを強化します。これは、Google Authenticator アプリケーションに依存して検証コードを生成します。このアプリは、定期的に新しい 6 桁のコードを生成します。有効にすると、エンドユーザーはログインするたびに現在の検証コードを要求されます。

Google Authenticator アプリケーションをダウンロードするには、必要に応じて、次のいずれかのサイトをご覧ください。

- **Android デバイス**： https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- **iOS デバイス**： https://itunes.apple.com/ca/app/google-authenticator/id388497605?mt=8

以下で説明しているように、**管理者コンソール**の 2 要素認証 ページを使用して、選択した組織内のすべてのユーザーに **管理者コンソール** と **ユーザーコンソール** への 2FA アクセスを有効にすることができます。また、**システム管理コンソール** を使用して、**管理者コンソール** と **ユーザーコンソール** への 2FA アクセスを有効または無効にすることができます。詳細については、「組織のための 2 要素認証の設定」を参照してください。

1. 管理者レベルの 2 要素認証 ページに移動します。
    a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**2 要素認証** をクリックします。
2. 管理者コンソールのすべてのユーザーに対して 2FA を有効にするには、admin ポータルの 2 要素認証 の下で **すべてのユーザーに必須** を選択します。

    このオプションは、ユーザー詳細 ページの 2FA 設定を上書きします。このページですべてのユーザーに対し 2FA が有効になっている場合、選択した組織 (該当する場合) に関連付けられているすべてのユーザーの ユーザーの詳細 ページで、個々のユーザーに対して無効にすることはできません。
3. ユーザーコンソールのすべてのユーザーに対して 2FA を有効にするには、ユーザーポータルの 2 要素認証 の下で **すべてのユーザーに必須** を選択します。

ポート設定、NTPサービス、およびWebサイトアクセスの検証

エージェント通信、ソフトウェアカタログの更新、パッチダウンロードなどの機能を有効にするには、ポート設定、NTPサービス、およびWebサイトアクセスを適切に設定する必要があります。

ポート設定の検証

デバイス管理およびデータベースまたはファイルアクセスを有効にするには、アプライアンスのポートを適切に設定する必要があります。

- アプライアンスの次の該当するポートがファイアウォール設定によってブロックされていないことを確認します。

ポート	用途	方向
20および21	（オプションおよび非推奨）ファイアウォールの外部からFTP経由でアプライアンス上のバックアップファイルにアクセスするために使用。	アプライアンスへの受信方向
22	（推奨）quest.comへのSSHトンネルを作成するために使用。	アプライアンスからの送信方向
25	（オプション）アプライアンスのEメール用SMTPサーバーが使用（SSL不使用）。SMTP Eメールを設定する場合にのみ必要です。詳細については、「SMTP Eメールサーバーの設定」を参照してください。	アプライアンスからの送信方向
80	（SSL が有効化されていない場合は必須）**管理者コンソール**および**ユーザーコンソール**への標準HTTP（Web）アクセスに使用。	アプライアンスへの受信方向
110	（オプション）POP3 Eメール用に使用（SSL不使用）。	アプライアンスへの受信方向
161	（オプション）SNMP監視に使用。詳細については、「ネットワーク上のデバイスの検出」を参照してください。	アプライアンスからの送信方向
199	（オプション）SNMP 多重化プロトコルである SMUX 経由で、ネットワーク上の管理対象デバイスへの単方向（読み取り専用）SNMP アクセスに使用します。詳細については、次を参照してください。 アプライアンスのセキュリティ設定の構成	アプライアンスからの送信方向
443	（必須）SSL アクセスおよびエージェントのメッセージプロトコル通信に使用されます。 デバイスがHTTPSを使用してアプライアンスにチェックインする際にこのポートを使用します。	アプライアンスへの受信方向

ポート	用途	方向
	アプライアンスは、KACE エージェントがインストールされているデバイスからの通信をこのポートでリッスンします。	
587	（オプション）アプライアンスのセキュアなEメール用SMTPサーバーが使用（SSLが有効）。セキュアなSMTP Eメールを設定する場合にのみ必要です。詳細については、「SMTP Eメールサーバーの設定」を参照してください。	アプライアンスからの送信方向
995	（オプション）POP3 Eメール用に使用（SSLが有効）。	アプライアンスへの受信方向
3306	（オプション）外部ツールによるアプライアンスデータベースへのアクセスに使用。例えば、Microsoft Access?? や Excel?? を使用してアプライアンスデータベース上でレポートを実行する際に、このポートが使用されます。	アプライアンスへの受信方向

- アプライアンスが次の該当するデバイスポートにアクセスできることを確認します。

ポート	用途
7	（オプション）Wake On LANに使用される、ネットワーク上のUDPトラフィック用にアプライアンスが使用。詳細については、「Wake On LANの使用」を参照してください。
139	（オプション）Windows デバイス上での KACE エージェントのプロビジョニング中に使用。
161	（オプション）SNMP監視に使用。このポートは開いており、SNMPにバインドされる必要があります。詳細については、「ネットワーク上のデバイスの検出」を参照してください。
445	（オプション）KACE エージェントのプロビジョニング中に使用。詳細については、「KACE エージェントのプロビジョニング」を参照してください。

- 認証にLDAPサーバーを使用するには、アプライアンスから次の該当するポートにアクセスできることを確認します。

ポート	用途
389	（オプション）LDAPアクセスに使用。

ポート	用途
636	（オプション）セキュアLDAPアクセスに使用。

NTPサービスのステータスの検証

HTTPS を使用してパッチをダウンロードするときに、アプライアンスで NTP（ネットワークタイムプロトコル）サービスが実行されている必要があります。証明書の有効性を確保するために、セキュアプロトコルによってアプライアンスのその時点の日付スタンプが使用されるため、NTPサービスが必要です。

NTPサービスが実行されていないと、証明書が無効であると示されて、パッチのダウンロードが失敗する場合があります。

アプライアンスから必要な Web サイトへのアクセスの許可

パッチのダウンロード、製品情報へのアクセス、および **Questサポート**との対話のためには、ファイアウォール、DNS サーバ、およびプロキシサーバの設定で、アプライアンスからドメインのポート 80 とポート 443 へのアクセスを許可する必要があります。

- アプライアンス管理者コンソールに次の Web サイトへのリンクがあることを確認します。

Webサイト	説明
https://twitter.com/quest	Twitter??
https://www.facebook.com/questsoftware	Facebook??
http://linkedin.com/	LinkedIn??
http://my.kace.com/inKpadsubscriptioncenter	Quest KACE Inkpad
https://www.quest.com/community/b/en/p/endpoint-management	Quest KACEブログ
https://kace.uservoice.com/forums/82699-k1000	Quest KACE Uservoice

ネットワーク設定とセキュリティ設定の構成

アプライアンスネットワーク設定には、ネットワークを介してアプライアンスにアクセスするために必要なホスト名、Webサーバー名、IPアドレスなどの情報が含まれます。

アプライアンスのネットワーク設定の変更

初期設定後、環境のニーズに合わせていつでもアプライアンスのネットワーク設定を変更できます。

アプライアンスの仮想/物理バージョンの場合、ネットワーク設定は管理者コンソールまたはコマンドラインコンソールへの初回ログイン時に構成されます。詳細については、「アプライアンスのネットワーク設定の変更」を参照してください。

サービスとしてのK1000の場合、アプライアンスは、静的なIPアドレス、サブネットマスク、およびデフォルトゲートウェイを使用して事前設定されています。設定情報については、『**KACE as a Service Setup Guide**』（サービスとしての KACE セットアップガイド）を参照してください。https://support.quest.com/k1000-as-a-service/release-notes-guides に移動します。

アプライアンスネットワーク設定の大部分を変更するには、アプライアンスを再起動する必要があります。変更後の設定が有効な場合は、合計の再起動ダウンタイムは1〜2分です。

ヒント: 外部 SMTP サーバーのテストにアプライアンスの再起動は必須でありません。変更を保存する前に SMTP 設定をテストできます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **ネットワーク設定** をクリックして、ネットワーク設定 ページを表示します。
3. ネットワーク設定 ページの アプライアンスネットワーク設定 セクションに次の情報を入力します。

オプション	説明
DNSホスト名	アプライアンスのホスト名を入力します。デフォルトはk1000です。
Webサーバー名	アプライアンスの完全修飾ドメイン名を入力します。完全修飾ドメイン名とは、**ホスト名とドメイン**を連結した値です。例えば、k1000.example.comです。デバイスは、この名前を使用してアプライアンスに接続します。Questでは、DNSサーバに、アプライアンスの静的IPアドレスのエントリを追加することをお勧めします。SSL証明書を使用する場合、証明書と同じ完全修飾ホスト名を使用する必要があります。
自動的に生成されたサーバ名	このチェックボックスをオンにすると、次のフォーマットを使用して、アプライアンス Web サーバ名をシステムで生成できます。Hostname.Domain。例えば、k1000.example.com です。このチェックボックスをオフにすると、カスタムのウェブサーバ名を入力できます。

4. IPv4 設定 セクションで、次の情報を入力します。

オプション	説明
DHCP を使用してネットワークを構成	DHCP（ 動的ホスト構成プロトコル ）を使用して、アプライアンスの IPv4 アドレスおよびその他のネットワーク設定情報を自動的に取得する場合は、このオプションを選択します。
Configure Network Manually（ ネットワークの手動構成 ）	アプライアンスの IPv4 アドレス、ドメイン、サブネットマスク、デフォルトゲートウェイ、および DNS 設定を手動で指定する場合は、このオプションを選択します。 • **IP アドレス**：アプライアンスの静的IPアドレスを入力します。

オプション	説明
	注意: IP アドレスが不正確な場合は、Web インターフェイス (管理者コンソールとユーザーコンソール) からアプライアンスにアクセスできません。この場合には、アプライアンスのコマンドラインコンソールを開き、konfig ログインを使用して正確な IP アドレスを入力します。 • **ドメイン**：アプライアンスが参加しているドメインを入力します。例：example.com。 • **サブネットマスク**：アプライアンスが参加しているサブネット (ネットワークセグメント) を入力します。デフォルトは、255.255.255.0です。 • **デフォルトゲートウェイ**：アプライアンスのネットワークゲートウェイを入力します。 • **プライマリ DNS**：アプライアンスがホスト名の解決に使用するプライマリDNSサーバーのIPアドレスを入力します。 • **セカンダリ DNS**：(オプション) アプライアンスがホスト名の解決に使用するセカンダリDNSサーバーのIPアドレスを入力します。

5. IPv6 設定 セクションで、次の情報を入力します。

オプション	説明
SLAAC を使用してネットワークを構成	アプライアンスのネットワーク設定を構成するために、IPv6 により提供される、SLAAC (ステートレスアドレス自動設定) を使用する場合は、このオプションを選択します。SLAAC では、デバイスは接続済みのインターフェイスから通知されたプレフィックスに基づいて独自の IPv6 アドレスを選択できます。
Configure Network Manually (ネットワークの手動構成)	アプライアンスの IPv6 アドレス、プレフィックス長、およびデフォルトゲートウェイを手動で指定する場合は、このオプションを選択します。 • **IPv6 アドレス**：アプライアンスの静的 IPv6 アドレスを入力します。 **注意: IP アドレスが不正確な場合は、Web インターフェイス (管理者コンソールとユーザーコンソール) からアプライアンスにアクセスできません。この場合には、アプライアンスのコマンドラインコンソールを開き、konfig ログインを使用して正確な IP アドレスを入力します。** • **プレフィックス長**：IPv6 アドレスプレフィックスにビット数を入力します。IPv6 プレ

オプション	説明
	フィックスは通常、64 ビットで構成されます。 • **デフォルトゲートウェイ**：アプライアンスのネットワークゲートウェイを入力します。
IPv6 を無効にする	アプライアンスの IPv6 アドレスを無効にする場合は、このオプションを選択します。これはデフォルトの設定です。

6. **オプション**：プロキシサーバーを設定するには、プロキシ設定 セクションで **プロキシサーバーを有効にする** を選択し、次のプロキシサーバー設定を指定します。

オプション	説明
タイプ	プロキシタイプ（HTTPまたはSOCKS5のいずれか）を入力します。
サーバー	プロキシサーバーの名前を入力します。
ポート	プロキシサーバーのポートを入力します。デフォルトのポートは8080です。
基本プロキシ認証を有効にする	プロキシサーバーへのアクセスにローカル資格情報を使用するには、このチェックボックスをクリックします。
ログイン	プロキシサーバーにアクセスするためのユーザー名を入力します。
パスワードおよびパスワードの確認入力	プロキシサーバーにアクセスするためのパスワードを入力します。

注: アプライアンスでは、ユーザー名とパスワードを要求する、基本的なレルムベースの認証を使用したプロキシサーバーをサポートしています。プロキシサーバーが他の種類の認証を使用する場合は、プロキシサーバーの例外リストにアプライアンスのIPアドレスを追加してください。

7. 外部 SMTP サーバーを使用するには、Email Configuration（E メール設定）セクションで **SMTP サーバーの有効化** を選択し、SMTP サーバーオプションを指定します。

オプション	説明
サーバー	外部 SMTP サーバーのホスト名（**smtp.gmail.com** など）または IP アドレスを指定します。外部 SMTP サーバでは、匿名（認証なし）のアウトバウンド E メール転送を許可する必要があります。ネットワークポリシーで、アプライアンスがSMTPサーバに直接問い合わせられることを確認します。また、メールサーバは、アプライアンスからのEメールのリレーを、認証なしで許可するように設定する必要があります。IP アドレスを指定する場合は、アドレスを括弧で囲みます。例えば、「[10.10.10.10]」と入力します。
ポート	外部 SMTP サーバーに使用するポート番号を入力します。標準的な SMTP にはポート 25 を使用しま

オプション	説明
	す。セキュアな SMTP にはポート 587 を使用します。
ログイン	外部 SMTP サーバーにアクセスするアカウントのユーザー名を入力します（「**your_account_name**@gmail.com」など）。
パスワードおよびパスワードの確認入力	指定したサーバーアカウントのパスワードを入力します。

8. SMTP 設定をテストします。
    a. **Test Connection**（テスト接続）をクリックします。
    b. 表示される 接続テスト SMTP ダイアログボックスに、新しく設定した SMTP サーバを使用してテスト E メールを送信する E メールアドレスを入力し、**テスト E メールを送信** をクリックします。

        接続テスト SMTP ダイアログボックスが更新され、テスト結果の E メール操作のステータスが表示されます。テストに失敗した場合は、設定を確認し、もう一度試してください。
9. **保存** をクリックします。

    アプライアンスが再起動します。変更後の設定が有効な場合は、合計の再起動ダウンタイムは1〜2分です。
10. アプライアンスの IP アドレスを変更した場合は、新しいアドレスにアクセスして、管理者コンソールログインページを表示します。

ローカルルーティングテーブルの設定

アプライアンスがネットワーク上の複数のゲートウェイ経由でトラフィックをルーティングできるように、ローカルルーティングテーブルを設定します。

ローカルルーティングテーブルは、1つのオフィスに物理アプライアンスがあり、管理対象デバイスが別の場所に配置されている場合に役立ちます。例えば、アプライアンスがテキサスにあり、管理対象デバイスがカリフォルニアに配置されている場合、アプライアンスはテキサスのサブネット上のデバイスに対してサービスを提供します。ローカルルーティングテーブルを使用すると、アプライアンスがカリフォルニアのネットワークを参照して、テキサスのデバイスに加えてカリフォルニアのデバイスもホストできるようになります。

1. アプライアンスの コントロールパネル に移動します。
    - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
    - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **ローカルルーティングテーブル** をクリックして、ローカルルーティングテーブル設定 ページを表示します。
3. **追加** ボタンをクリックして、エントリを追加します。
4. 次の設定を指定します。

オプション	説明
名前	ルートの名前を入力します。

オプション	説明
ターゲット	アプライアンスの通信相手となるターゲットの IP アドレスまたはネットワークを入力します。
サブネットマスクまたはCIDR	指定したネットワークのサブネットマスクを入力します。例：24, 255.255.240.0.これはホストに適用されます。
ゲートウェイ	アプライアンスとターゲットネットワーク間でトラフィックをルーティングするルーターの IP アドレスを入力します。

5. 行の最後で **保存** をクリックし、エントリを保存します。
6. ページの一番下で **保存して再起動** をクリックして、すべての変更を保存します。

   Apache™ サービスの再起動が必要であることを示す警告が表示されます。
7. **OK** をクリックして続行します。

ローカル Web サーバの設定の構成とホストへのアクセスの許可

ローカル Web サーバの設定を構成し、**管理者コンソール**、**システム管理コンソール**、および**ユーザーコンソール**へのアクセスを許可するホストの許可リストを指定します。許可リストを作成すると、アクセスが許可リストにあるホストに制限されます。

注: IP アドレスまたはドメイン名の 許可リスト への追加を行うと、その IP アドレスまたはドメインのみがアクセスできるようになります。それ以外はブロックされます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **アクセス制御リスト** をクリックして、アクセス制御リストの詳細 ページを表示します。
3. 次のオプションを指定します。

オプション	説明
アクセス制限なし	このオプションを選択すると、あらゆるWebアドレスからのアクセスが許可されます。
以下の指定に従ってアクセスを制限する	このオプションを選択すると、許可リストにあるWebアドレスへのアクセスが制限されます。指定したターゲットに加え、アプライアンスのサブネット上の IP アドレスにアクセスできるようにするには、**アプライアンスと同じサブネット上のすべての IP アドレスを許可する** を選択します。

4. 許可リスト セクションで **追加** ボタンをクリックして、エントリを追加します。
5. 次のオプションを指定します。

オプション	説明
ターゲット	ターゲットを指定します。 • **adminui**：これは管理者レベルの**管理者コンソール**です。http://**appliance_hostname**/admin にログインできる IP アドレスおよび / またはホスト名の許可リスト。 • **userui**：これは**ユーザーコンソール**です。http://**appliance_hostname**/user にログインできる IP アドレスおよび / またはホスト名の許可リスト。 • **systemui**: これは**システム管理コンソール**です（アプライアンス上で組織コンポーネントが有効化されている場合にのみ利用可能）。http://**appliance_hostname**/system にログインできる IP アドレスおよび / またはホスト名の許可リスト。 • **api**：これはアプライアンス API です。KACE GO アプリケーションを含む API を使用してアプライアンスにアクセスできる IP アドレスおよび / またはホスト名の許可リスト。
IPアドレス/ドメイン名	許可するアドレスを入力します。次のどちらかになります。 • ドメインまたはサブドメイン名（全部または一部） • IPアドレス（全部または一部）
サブネットマスク/CIDR	許可するサブネットマスク/CIDR（Classless Inter-Domain Routing）を入力します。これを使用することで、より詳細にサブネットを制御できます。

6. 行の最後で **保存** をクリックし、エントリを保存します。
7. ページの一番下で **保存** をクリックし、すべての変更を保存します。

   Apacheサービスの再起動が必要であることを示す警告が表示されます。
8. **OK** をクリックして続行します。

注: IPアドレスまたはドメイン名を「許可リスト」に追加すると、そのIPアドレスまたはドメインのみがそのページにアクセスできるようになります。それ以外はブロックされます。

アプライアンスのセキュリティ設定の構成

アプライアンスのセキュリティ設定を構成して、SAMBA共有、SSL、SNMP、SSH、データベースアクセス、FTPアクセスなどの特定の機能を有効にする必要があります。

SSL を有効にするには、正しい SSL プライベートキーファイルと署名された SSL 証明書が必要です。プライベートキーにパスワードが設定されている場合、アプライアンスを自動的に再起動できません。この問題がある場合は、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。

- セキュリティ設定に対する変更を保存すると、アプライアンスが再起動されます。
- ポート 443 へのアクセスを有効にしてアプライアンスを再起動した後で、**管理者コンソール**のログインページが Firefox® ブラウザで正しく表示されないことがあります。この問題が発生した場合は、Firefoxブラウザのキャッシュとcookieを削除して、もう一度やり直してください。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **セキュリティ設定** をクリックして、セキュリティ設定 ページを表示します。
3. 一番上のセクションで、各設定を次のように指定します。

オプション	説明
SSHを有効にする	アプライアンスへのSSHログインを許可します。SSHが有効化されていると、ポート22を経由するSSH暗号化通信が許可されます。
Webサーバーの圧縮を有効にする	アプライアンスがWebページを圧縮できるようにします。圧縮することで、ブラウザでの **ユーザーコンソール** および **管理者コンソール** ページの読み込み時間を短縮できます。
SNMP読み込みアクセスを有効にする	SNMP 多重化プロトコルである SMUX を使用して、ポート 199 経由でネットワーク上の管理対象デバイスへの単方向（読み取り専用）SNMP アクセスを有効にします。詳細については、「ポート設定の検証」を参照してください。
SNMPコミュニティ文字列	読み取り専用SNMPアクセスを有効にするSNMPコミュニティ文字列。デフォルト値はpublicです。
SNMPトラップ監視を有効にする	ネットワーク上の管理対象デバイスを監視するためのプロトコルであるSNMP（Simple Network Management Protocol）を有効化します。SNMPは、Dell Open Manageおよび多くのサードパーティ製品でサポートされています。ネットワークデバイスからのSNMPトラップを受信したくない場合は、このオプションをクリアします。 アプライアンスでこの機能を有効にし、関連するデバイスの監視も有効にした場合、アプライアンスはプリンタ、プロジェクタ、ルーターなどの監視対象ネットワークデバイスからのSNMPトラップを受信できます。この機能は、SNMP接続を使用するエージェント不要デバイスなどのSNMP管理対象デバイスを介して管理されるネットワークデバイスにのみ適用されます。

オプション	説明
	デバイスの監視を有効にする方法の詳細については、1つ、または複数のデバイスの監視の有効化を参照してください。 SNMPトラップはネットワークデバイスから開始するメッセージであり、アプライアンス上のトラップレシーバに送信されます。例えば、ルーターの電源装置に障害が発生したときにルーターからメッセージを送信できます。また、プリンタで用紙切れが起こったときに、プリンタからメッセージを開始します。アプライアンスでは、これらのトラップを受信し、特定の事前定義のしきい値に到達するとアラートを生成します。 • **SNMPバージョン1または2**：このバージョンには、有効なコミュニティ文字列のみが必要です。コミュニティ文字列は、監視対象ネットワークデバイスからのSNMPトラップメッセージをアプライアンスで受信できるようにするために必要です。アプライアンスは複数のコミュニティ文字列をサポートします。コミュニティ文字列を追加するには、**v1/v2** タブを開き、＋をクリックし、コミュニティ文字列を入力し、**保存** をクリックします。 • **SNMPバージョン3**：このバージョンには、拡張セキュリティ機能およびリモート設定機能が実装されており、有効なユーザー名と暗号化情報が必要です。セキュリティ名を追加

オプション	説明
	するには、**v3** タブを開き、＋をクリックして、次の情報を入力します。 ◦ **セキュリティ名**：SNMPトラップを送信するユーザーベースのセキュリティモデル（USM）アカウントの名前。 ◦ **エンジンID**：SNMPトラップを送信するSNMPアプリケーションエンジンのID。 ◦ **認証パスワード**：セキュリティ名に関連付けられたパスワード。 ◦ **認証プロトコル**：ユーザーの認証に使用するプロトコル。MD5またはSHAです。 ◦ **プライバシーパスワード**：データパケットの暗号化キー。 ◦ **プライバシープロトコル**：暗号化プロトコル。AESまたはDESです。 ◦ **セキュリティレベル**：セキュリティのレベルを指定します。 ▪ 「**authPriv**」：送信者のIDが検証され、情報が暗号化されます。 ▪ 「**authNoPriv**」：送信者のIDが検証されますが、情報は検証されません。 ▪ 「**noAuthNoPriv**」：送信者のIDは検証されず、情報は暗号化されません。
MIBファイル	ベンダー固有のMIB（管理情報ベース）ファイルをアップロードします。MIBファイルを使用すると、アプライアンス上のトラップレシーバでSNMPトラップを人間が読めるメッセージに変換できます。これらのファイルはオプションです。 • MIBファイルをアップロードするには、セキュリティ設定 ページの MIBファイル の下の MIBをアップロード 領域で、**参照** を選択します。 • MIBファイルは、一定の標準を満たしている必要があります。アプライアンスでは、アップロードしたMIBファイルごとに検証が行われます。標準を満たさないMIBファイルをアップロードした場合は、エラーメッセージが セキュリティの設定 ページの上部に表示されます。MIBファイルの内容を検証しない場合は、**MIB検証をスキップ** チェックボックスを選択します。
バックアップファイルのセキュリティを有効にする	アプライアンスのバックアップファイルへのアクセスに、ユーザー名とパスワードを要求します。バックアップファイルは、ブラウザに URL を入力することで利用できます。

オプション	説明
	ユーザー名とパスワードの認証なしで、URLによるバックアップファイルへのアクセスを有効にするには、このオプションをオフにします。アクセスを必要とする外部プロセスに役立ちます。詳細については、「アプライアンスバックアップについて」を参照してください。
FTP経由のバックアップを有効にする	読み取り専用のFTPサーバーを経由したデータベースバックアップファイルへのアクセスを有効にします。これにより、別のサーバー上でプロセスを作成し、バックアップファイルにアクセスすることができます。 このアクセスが不要な場合は、このオプションをオフにします。
FTPを書き込み可能にする	FTPによるバックアップファイルのアップロードを有効にします。FTPは、バックアップファイルがデフォルトHTTPメカニズムに対して大きすぎて、ブラウザのタイムアウトが生じる場合に役立ちます。
新しいFTPユーザーパスワード	バックアップファイルへのFTPアクセスにパスワードを要求します。
mDNSを有効にする	アプライアンスがマルチキャストドメインネームシステム（mDNS）とDNS Service Discovery（DNS-SD）要求に応答できるようにします。このオプションにより、ユーザーおよび管理者は、より簡単に**ユーザーコンソール**と**管理者コンソール**を見つけることができます。アプライアンスがこれらの要求に応答する必要がない場合は、このオプションをオフにします。
Munin のアクセスを有効にする	アプライアンスでサーバーの時間経過に伴う使用状況とメトリックを表示できるようにします。 **注:** これにより、/munin に対して無制限にアクセス (非認証) できます。
データベースアクセスを有効にする	ユーザーがポート 3306 経由で、外部ツール（Microsoft Access や Excel など）を使用してアプライアンスデータベース上でレポートを実行できるようにします。この方法でデータベースを公開する必要がない場合は、このオプションをオフにします。

オプション	説明
	注:（32 ビット）MySQL ODBC ドライバをインストールしている場合、このアプライアンスデータベースには任意の ODBC 準拠のサードパーティツールからアクセスできます。この機能を使用するには、このチェックボックスをオンにする必要があります。また、MySQL ODBC ドライバのデータソースを設定し、アプライアンスの接続情報を入力する必要があります。詳細については、MySQL ODBC ドライバのドキュメントを参照してください。
セキュアデータベースアクセス（SSL）を有効にする	データベースへのSSLアクセスを有効にして、その他のSSLオプションにアクセスします。
リモート syslog を有効にする	アプライアンスがリモートの syslog サーバーに限定的なサーバーログデータを送信できるようにします。 **注:** この方法で送信されたログデータは暗号化されず、UDP（ユーザーデータグラムプロトコル）を使用します。このオプションを選択する前に、組織が設定している、セキュリティとネットワークの飽和状態に関するガイドラインを確認してください。
リモート Syslog サーバー	リモート Syslog サーバーの完全修飾ドメイン名（FQDN）または IP アドレスとポート番号を指定します。IPv4 および IPv6 アドレスがサポートされています。ポート番号を指定しない場合、アプライアンスは Syslog トラフィック用のデフォルトポート番号 514（UDP）を使用します。

4. 2 要素認証 セクションで、2 要素認証（2FA）機能を設定します。2FA は、ログインプロセスにさらにステップを追加することで、ユーザーがアプライアンスにログインするためのセキュリティを強化します。これは、Google Authenticator アプリケーションに依存して検証コードを生成します。このアプリは、定期的に新しい 6 桁のコードを生成します。有効にすると、エンドユーザーはログインするたびに現在の検証コードを要求されます。

   注: この機能を有効にする場合は、アプライアンスサーバのクロック、および Google Authenticator を実行しているデバイスが正確であることを確認してください。Google Authenticator は、現在の時刻に依存してトークンを作成します。サーバーのクロックが Google Authenticator を実行しているデバイスのクロックと同期されていない場合、トークンの検証が失敗し、アカウントのロックアウトが発生する可能性があります。

   a. 次のオプションを指定します。有効にすると、これらは優先順位の順に、上から下へと表示されます。例えば、以前管理者コンソールに 2FA を設定している場合、2FAはユーザーコンソールに対してのみ有効にすることができます。

   - **システムポータルで 2 要素認証を有効にする**：**システム管理コンソール**に 2FA を使用する場合は、このチェックボックスをオンにします。すべてのユーザーに対して 2FA を有効にするには、**すべてのユーザーに必須** を選択します。

     注: このオプションは、複数の組織が設定されているアプライアンスでのみ使用できます。

   - **admin ポータルで 2 要素認証を有効にする**：このオプションは、**システム管理コンソール**に 2FA を有効にした場合、またはアプライアンスに設定されている組織が 1 つだけの場合にのみ表示されます。**管理者コンソール**に 2FA を使用する場合は、このチェックボックスをオンに

します。次に、以下のオプションのいずれかを選択して、ログイン時に 2FA を必要とするユーザーを指定します。

- **すべてのユーザーに必須**：**1 つの組織が設定されているアプライアンスのみ。**すべてのユーザーに対して 2FA を有効にするには、このオプションを選択します。
- **組織によって定義**：**複数の組織が設定されているアプライアンスのみ。**必要に応じて、**管理者コンソール**で各組織のすべてのユーザーに同じ 2FA の設定を適用します。
- **すべてのユーザーに必須**：**複数の組織が設定されているアプライアンスのみ。管理者コンソール**のすべてのユーザーに対して 2FA を有効にします。
- **必須でありません**：**複数の組織が設定されているアプライアンスのみ。管理者コンソール**のすべてのユーザーに対して 2FA を無効にします。

- **ユーザーポータルで 2 要素認証を有効にする**：このオプションは、**管理者コンソール**で 2FA を有効にした場合にのみ表示されます。**ユーザーコンソール**に 2FA を使用する場合は、このチェックボックスをオンにします。次に、以下のオプションのいずれかを選択して、ログイン時に 2FA を必要とするユーザーを指定します。
  - **組織によって定義**：必要に応じて、**ユーザーコンソール**で各組織のすべてのユーザーに同じ 2FA の設定を適用します。
  - **すべてのユーザーに必須**：**ユーザーコンソール**のすべてのユーザーに対して 2FA を有効にします。
  - **必須でありません**：**ユーザーコンソール**のすべてのユーザーに対して 2FA を無効にします。

b. **移行ウィンドウ** の下で、2FA を必要とするユーザーが 2FA の設定手順をバイパスできる時間を指定します。

例えば、、ユーザーが自宅に携帯電話を忘れてきて、新しいコードを生成できない場合、ここで指定された期間にポータルにアクセスすることができます。

5. ブルートフォース防止 領域の設定を使用すると、複数回の連続した攻撃で偽の資格情報を使用してアプライアンスへのアクセスを取得することを防止できます。指定された期間内での認証試行の失敗回数を設定でき、この回数を超えると、アプライアンスはそのユーザーがログインできないようにします。

   デフォルト設定は、5 分間に 3 回の試行回数です。これらの値は必要に応じて後で変更できます。

   アプライアンスでユーザーアカウントのログインが無効になった場合でも、他のユーザーは影響を受けず、有効な資格情報を使用してアプライアンスにログインできます。

6. **オプション**：アプライアンスの暗号化キー セクションで、**キーの生成** をクリックして新しい暗号化キーを生成します。このキーを使用して、Questサポートがテザリングを使用してトラブルシューティングのためにアプライアンスにアクセスできるようにします。現在のキーが侵害されたと考えられる場合以外は、新しいキーを生成する必要はありません。詳細については、「Quest KACE サポートへの tether を有効にする」を参照してください。

   タイムスタンプで、キーが生成された時刻が示されます。

7. シングルサインオン セクションで、認証設定を指定します。

オプション	説明
無効	アプライアンスでシングルサインオンを使用できないようにします。シングルサインオンを使用すると、ドメインにログオンしているユーザーが、アプライアンスのログインページに資格情報を再入力する必要なく、アプライアンス**管理者コンソール**と**ユーザーコンソール**にアクセスできるようになります。
Active Directory	認証にActive Directoryを使用します。Active Directoryでは、ドメインを使用して、ネットワーク上のユーザーを認証します。詳細については、

オプション	説明
	「Active Directory を使用したシングルサインオン」を参照してください。

8. **SAMBA** セクションで、各設定を次のように指定します。

オプション	説明
組織コンポーネントが有効になっているアプライアンスの場合： **組織のファイル共有を有効にする** 組織コンポーネントがないアプライアンスの場合: **ファイル共有を有効にする**	アプライアンスのクライアント共有を使用して、ファイル（管理対象デバイスにアプリケーションをインストールする際に使用するファイルなど）を保存します。 アプライアンスのクライアント共有は、プロビジョニングサービスで利用可能な組み込みのWindowsファイルサーバーで、ネットワーク上でSambaクライアントを配布するのに役立ちます。Questでは、管理対象デバイス上でアプリケーションのインストールを実行しているときにのみ、このファイルサーバーを有効にすることをお勧めします。 **注:** 組織コンポーネントがアプライアンスで有効になっていない場合は、各組織に対して他のファイル共有オプションを選択できます。詳細については、「システムレベルでのファイル共有の有効化」を参照してください。
Samba 最小プロトコル、Samba 最大プロトコル	必要に応じて、最小と最大の Samba プロトコルを選択します。各設定では、次のオプションを使用できます。 • 「**SMB2**」: SMB プロトコルの再実装。Windows Vista およびそれ以降のバージョンの Windows で使用されます。SMB2 にはサブプロトコルがあります。デフォルトで、SMB2 は SMB2_10 バリアントを選択します。 • 「**SMB2_02**」: 最も古い SMB2 バージョン。 • 「**SMB2_10**」: Windows 7 SMB2 バージョン。 • 「**SMB2_22**」: 初期の Windows 8 SMB2 バージョン。 • 「**SMB2_24**」: Windows 8 ベータ版 SMB2 バージョン。 • 「**SMB3**」: SMB2 プロトコルの再実装。Windows 8 で使用されます。SMB3 にはサブプロトコルがあります。デフォルト

オプション	説明
	で、SMB3 は SMB3_11 バリアントを使用します。 • 「**SMB3_00**」: Windows 8 SMB3 バージョン（SMB2_24 と同様）。 • 「**SMB3_02**」: Windows 8.1 SMB3 バージョン。 • 「**SMB3_10**」: 初期の Windows 10 テクニカルプレビューバージョン。 • 「**SMB3_11**」: Windows 10 テクニカルプレビューバージョン。
サインインが必要	Samba プロトコルへのサインインを有効にします。
ゲストアクセスを無効にする	Samba のゲストアクセスを無効にします。
アプライアンスのファイル共有にNTLMv2を要求する	アプライアンスファイル共有に対する NTLMv2 認証を有効にします。このオプションを有効にした場合は、アプライアンスファイル共有に接続する管理対象デバイスは NTLMv2 をサポートし、NTLMv2 を使用してアプライアンスに対する認証を受ける必要があります。NTLMv2は、NTLMやLANMANよりも安全ですが、非NTLMv2設定の方がより一般的なため、通常、このオプションはオフになっています。このオプションを有効にすると、Samba サーバーで **lanman auth** と **ntlm auth** が無効になります。NTLMv2レベル1〜4がサポートされています。NTLM v2 レベル 5 が必要な場合は、KACE エージェントの手動プロビジョニングを検討してください。詳細については、「KACE エージェントを手動展開する」を参照してください。
オフボードファイル共有にNTLMv2を要求する	エージェントのプロビジョニングなど、Samba クライアントを介してサポートされるアプライアンスの特定の機能が、NTLMv2 を使用して強制的にオフボードネットワークファイル共有に対する認証を受けるようにします。NTLMv2は、NTLMやLANMANよりも安全ですが、非NTLMv2設定の方がより一般的なため、通常、このオプションは無効になっています。このオプションを有効にすると、SAMBAクライアント機能の **client ntlmv2 auth** オプションが有効になります。

9. **オプション**：SSL セクションで、次の SSL 設定を指定します。

重要: SSLを有効にすると、管理対象デバイスでは片方向に、自動的に変換されます。SSLを無効にする場合、デバイスを手動で再設定する必要があります。

オプション	説明
ポート80接続を有効にする	アプライアンスに対するポート80経由のアクセスを有効にします。

オプション	説明
	ポート 80 接続を無効にする場合は、**Questサポート**に問い合わせて、SSL を処理するエージェント展開スクリプトを調整してください。
ポート 80 からポート 443 への転送の有効化	SSL が期待どおりに動作していることを確認すると、ポート 80 からポート 443 へのすべての通信の転送を有効にできます。この転送を有効にする場合は、このチェックボックスをオンにします。
SSLを有効にする	管理対象デバイスが、SSL（HTTPS）を使用してアプライアンスに接続できるようにします。 この設定は、非SSLモードのLANにアプライアンスを適切に展開した後で有効にする必要があります。 SSL を有効にするには、手順 10 の説明に従って SSL 証明書をロードする必要があります。

10. SSL 証明書をロードするには、次のいずれかを行います。
    - SSL 証明書とプライベートキーが、Apache ベースの Web サーバで使用されるものと同様、Privacy Enhance Mail（PEM）形式である場合：
        1. **PEM SSL 証明書のアップロード** を選択します。
        2. SSLプライベートキーファイル フィールドと SSL 証明書ファイル フィールドで、プライベートキーと証明書ファイルを選択します。
        3. SSL 中間証明書（PEM 形式も含む）を有効にしてアップロードする場合は、**SSL 中間証明書を有効にする** を選択します。SSL 中間証明書は、証明書発行者がルート証明書のプロキシとして提供する署名付き証明書です。
    - 証明書が PKCS-12 形式の場合：
        1. **PKCS-12 SSL 証明書のアップロード** を選択します。
        2. PKCS-12 ファイル フィールドで、ファイルを選択します。
        3. PPKCS-12 ファイルのパスワード フィールドに、PKCS-12 ファイルのパスワードを入力します。
    - SSL 証明書に Let's Encrypt サービスを使用するには、次の手順を実行します。
        1. **Let's Encrypt SSL 証明書の適用** をクリックします。Let’s Encrypt は、無料の、自動化された、オープンな認証局（CA）です。Let's Encrypt から証明書を取得すると、チャレンジを使用してその証明書のドメイン名が制御されていることが証明書のサーバによって検証されます。

            注: HTTP-01 チャレンジは、ポート 80 でのみ実行できます。任意のポートを指定すると、チャレンジのセキュリティが低下するため、自動証明書管理環境（ACME）標準では許可されません。そのため、アプライアンスは、着信通信用にポート 80 を開いたパブリック側のボックスと、パブリックに解決可能な DNS で実行する必要があります。詳細については、https://letsencrypt.org/docs/challenge-types/を参照してください。
        2. E メールアドレス フィールドに、E メールアドレスを入力します。Let's Encrypt 証明書は、定期的に有効期限が切れますが、アプライアンスは自動プロセスを使用して、有効期限が切れる前に証明書を更新します。このアドレスは、証明書の有効期限が切れた場合に、Let's Encrypt との通信に使用されます。この E メールアドレスを使用して登録された Let's Encrypt アカウントが必要です。
        3. チェックボックスをオンにして、サービス利用規約に同意します。
    - 証明書要求を生成するか、自己署名証明書をロードするには、次の手順を実行します。
        1. **CSR（証明書署名要求）または自己署名 SSL 証明書を生成します** をクリックします。

2. 表示される領域で、**SSL 証明書フォーム** をクリックします。SSL証明書の生成 の指示に従います。

11. Secure Attachments in Service Desk（サービスデスクの添付ファイルの保護）セクションで、サービスデスクチケットに添付されたファイルについてセキュリティを追加するかどうかを選択します。
    - チケットに添付されたファイルについてセキュリティを有効にする場合は、チェックボックスをオンにします。このオプションを選択した場合、ユーザーはアプライアンス**管理者コンソール**または**ユーザーコンソール**内からのみ、チケットに添付されたファイルにアクセスできます。
    - ユーザーが**ユーザーコンソール**または**管理者コンソール**の外部からチケットリンクをクリックしてファイルにアクセスできるようにする場合は、チェックボックスをオフにします。
12. **保存してサービスを再起動** をクリックして変更を保存し、アプライアンスを再起動します。

> **注:** ポート 443 へのアクセスを有効にしてアプライアンスを再起動した後で、**管理者コンソール**のログインページが Firefox ブラウザで正しく表示されないことがあります。この問題が発生した場合は、Firefoxブラウザのキャッシュとcookieを削除して、もう一度やり直してください。

シングルサインオン方法としてのActive Directoryの設定

Active Directory シングルサインオンを使用すると、ドメインにログオンしているユーザーが、ログオン資格情報を毎回再入力する必要なく、アプライアンス**管理者コンソール**と**ユーザーコンソール**にアクセスできるようになります。

アプライアンスを Active Directory サーバに接続する前に、次の点を確認します。

- アプライアンスが Active Directory サーバにアクセスできるように、ネットワークと DNS の設定が構成されている。詳細については、「アプライアンスのネットワーク設定の変更」を参照してください。
- Active Directory サーバの時刻設定がアプライアンスの時刻設定と一致している。アプライアンスの時刻設定に関する情報については、「アプライアンスの日付と時刻の設定」を参照してください。

1. アプライアンスの コントロールパネル に移動します。
    - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
    - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. セキュリティ設定 ページの シングルサインオン セクションで、**Active Directory** を選択し、次の情報を入力します。

オプション	説明
ドメイン	Active Directory® サーバーのドメインのホスト名。例：example.com。
ユーザー名	Active Directory サーバーの管理者アカウントのユーザー名。例:「username@example.com」。
パスワード	Active Directoryサーバーの管理者アカウントのパスワード。
コンピュータオブジェクトコンテナ	Active Directory サーバーでの管理者アカウントのコンピュータオブジェクトコンテナの名前。
コンピュータオブジェクト名	Active Directory サーバーでの管理者アカウントのコンピュータオブジェクトコンテナの名前。

オプション	説明
サービスアカウントコンテナ	Active Directory サーバーでの管理者アカウントのサービスアカウントコンテナの名前。

3. **参加** をクリックします。

   アプライアンスは、読み取り専用の権限が必要な次のテストを実行し、アプライアンスのドメインへの参加が許可されるよう正確にドメインが設定されているかどうかを確認します。

   - サポートされているオペレーティングシステムと正しいオペレーティングシステムパッチがあることを確認する
   - QASをインストールするための十分なディスク領域があることを確認する
   - システムのホスト名が「localhost」でないことを確認する
   - ネームサービスがDNSを使用するように設定されているかどうかを確認する
   - resolv.confにネームサービスエントリの適切なフォーマットがあること、およびホストが解決できることを確認する
   - Active Directory用の適切なDNS SRVレコードを持つネームサーバーがあることを確認する
   - UDPポート389が開いている書き込み可能なドメインコントローラーを検出する
   - Active Directoryサイトを検出する（使用可能な場合）
   - TCPポート464がKerberos kpasswdに対して開いているかどうかを確認する
   - UDPポート88およびTCPポート88が、Kerberosトラフィックに対して開いているかどうかを確認する
   - TCPポート389がLDAPに対して開いているかどうかを確認する
   - グローバルカタログサーバーがあること、およびTCPポート3268がグローバルカタログサーバーとの通信用に開かれているかどうかを確認する
   - Active Directoryに対して有効な時間差があることを確認する
   - Active DirectoryでQASアプリケーション設定を確認する
   - TCPポート445が、Microsoft CIFSトラフィックに対して開いているかどうかを確認する

   これらのテストは書き込み権限を必要としないため、ディレクトリへの書き込み権限の有無を確認しません。また、これらのテストでは、ユーザー名とパスワードの資格情報も確認しません。資格情報が不正確な場合は、テストに成功しても、アプライアンスはドメインに参加できない場合があります。

   テストの結果を示すメッセージが表示されます。エラーがある場合、**ログ** をクリックし、ログ ドロップダウンリストで **サーバーエラー** を選択して、エラーを表示することができます。
4. **オプション**：**強制的に参加** を選択し、サーバーを参加させてエラーを無視し、ドメインに参加します。
5. **保存してサービスを再起動** をクリックします。

ユーザーが Active Directory ドメインに参加したデバイスにログインすると、資格情報を再入力する必要なく、アプライアンス**ユーザーコンソール**にアクセスできます。Active Directory ドメインに参加していないデバイスのユーザーにはログインウィンドウが表示され、ローカルのアプライアンスユーザーアカウントを使用してログインすることができます。詳細については、「システムレベルのユーザーアカウントの追加または編集」を参照してください。

注: Microsoft Edge および Firefox のブラウザでシングルサインオンを使用する場合は、ユーザーがブラウザの設定を行い、適切な認証が使用されるようにする必要があります。詳細については、「シングルサインオンを使用するためのブラウザの設定」を参照してください。

SSL証明書の生成

管理者コンソールを使用して、自己署名 SSL 証明書を生成、またはサードパーティ証明書の証明書署名要求を生成できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **セキュリティ設定** をクリックして、セキュリティ設定 ページを表示します。
3. SSL セクションで、**SSL を有効にする** をクリックします。

   その他の SSL オプションが表示されます。
4. **CSR（ 証明書署名要求 ）または自己署名 SSL 証明書を生成します** をクリックしてから、**SSL 証明書フォーム** をクリックして SSL 証明書フォーム ページを表示します。

   注: 証明書署名要求を以前に生成したことがある場合は、それがページに表示されます。新しい要求を生成するには、Configure（ 設定 ）セクションの情報を更新し、**保存** をクリックしてから **自己署名証明書の作成** をクリックする必要があります。
5. 設定 セクションで、次の情報を入力します。

オプション	説明
会社名	会社の名前。
組織名	組織のユニットまたはビジネスグループの名前。
共通名	SSL証明書を作成するアプライアンスの共通名。
Eメール	Eメールアドレス。
市区町村名	地域の名前。
都道府県名	都道府県の名前。
国名	国の名前。

6. **保存** をクリックします。

   SSL 証明書フォーム を初めて保存した場合は、Certificate Signing Request（ 証明書署名要求 ）セクションが表示されます。フォームを以前に保存したことがある場合は、Certificate Signing Request（ 証明書署名要求 ）セクションが更新されます。
7. 次のいずれかを実行します。
   - **サードパーティ証明書発行者を使用して証明書を生成するには、次の手順を実行します。**
     1. 「-----BEGIN CERTIFICATE REQUEST-----」 と 「-----END CERTIFICATE REQUEST-----」 の間の行を含め、Certificate Signing Request（ 証明書署名要求 ）セクションのすべてのテキストをコピーして、証明書発行者か、または会社にウェブサーバー証明書を提供する担当者に送信します。
     2. サードパーティから証明書を受信したら、セキュリティ設定 ページに戻り、証明書をアップロードします。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。
   - **自己署名証明書を生成するには、次の手順を実行します。**

1. **自己署名証明書の作成** をクリックして、証明書を生成し、Certificate Signing Request（証明書署名要求）セクションの下に表示します。
2. **自己署名証明書の作成** をクリックし、**はい** をクリックします。
3. セキュリティ設定 ページで、**保存してサービスを再起動** をクリックします。

自己署名証明書は kbox.pem という名前の **PEM** ファイルに変換され、KACE エージェントのデータフォルダに配置されます。

注: プライベートキーは、Private Key（プライベートキー）フィールドに表示されます。有効な証明書を展開すると、アプライアンスに展開されます。他の人にプライベートキーを送信してはなりません。プライベートキーは、別のWebサーバーにこの証明書を展開する場合に備えて、ここに表示されます。

注: SSLの証明書とプライベートキーは、セキュリティ上の理由から、アプライアンスの日ベースのバックアップに含まれません。これらの2ファイルを、自分用として保存しておいてください。

エージェント設定の構成

KACE エージェントで使用されるポートとセキュリティの設定は、エージェント設定で行います。これらの設定は、エージェントインフラストラクチャ固有であり、他のアプライアンス設定や実行時の処理には影響しません。

注: エージェント設定を変更すると、アプライアンスと管理対象デバイスにインストールされているエージェント間の通信が一時的に中断されるため、注意が必要です。詳細については、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。

Koneaについて

Konea は、エージェント管理対象デバイスにインストールされている KACE エージェントとアプライアンス間の通信を可能にするコンポーネントです。

Koneaは、システム管理操作のために最適化されたリアルタイム通信を可能にします。

エージェント設定の構成

KACE エージェントの設定は、アプライアンスで行うことができます。この設定は、システムレベルの設定です。アプライアンスで組織コンポーネントが有効化されている場合、エージェント設定はすべての組織に適用されます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **エージェント設定** をクリックして、エージェント設定 ページを表示します。
3. 次の設定を指定します。

オプション	説明
レガシーエージェントを許可（11.0 以前）	このオプションは、既存のアプライアンスをバージョン 11.0 にアップグレードする場合にのみ表示されます。このオプションは、アプライアンスの全体的なセキュリティを低下させるセキュアな接続なしでレガシーエージェントを引き続き使用する場合

オプション	説明
	にのみ有効のままにします。すべてのレガシーエージェントを最新バージョンにアップグレードすることをお勧めします。このオプションを無効にすると、11.0 より前のすべてのエージェントが非アクティブになり、セキュア接続が設定されるまでアプライアンスに接続できなくなります。このオプションは、無効にすると有効にできなくなります。 セキュアな接続を使用するようにエージェントを設定する方法の詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。

注: KACE エージェントバージョン 11.0 以降では、すべての通信が Konea トンネルを介して伝送されるため、次の設定は必要ありません。Konea の詳細については、「Koneaについて」を参照してください。

ファイル転送に SSL が必要	セキュア接続を使用する KACE エージェントを設定します。SSL（Secure Sockets Layer）接続を使用すると、エージェントは暗号化されたリンクを確立でき、すべてのデータをプライベートで完全な状態を確実に維持しながらエージェントと送受信できます。 **重要: この設定を変更した後、設定内容がクライアントマシンに反映されるように、AMPTools restartコマンドを使用してエージェントを手動で再スタートする必要があります。**
SSL証明書の検証	接続を確立する前に、SSL証明書を検証します。SSL証明書には、暗号化に使用する公開キーおよび所有者IDに関する情報が含まれます。 **重要: この設定を変更した後、設定内容がクライアントマシンに反映されるように、AMPTools restartコマンドを使用してエージェントを手動で再スタートする必要があります。**
CA 証明書バンドルファイル	一部の環境では、エージェントサーバーとの通信中にカスタム cURL（クライアント URL）CA（証明機関）証明書を使用します。これは、デフォルトのエージェントバンドルで参照されていない権限によって署名された SSL 証明書を確認するために使用できます。 • カスタム cURL CA バンドルをアップロードするには、**ファイルを選択** をクリックします。証明書バンドルファイルは .PEM 形式である必要があります。アプライアンスがファイルの内容を検証します。ファイルが有効な場合は、既存のバンドルまたはデフォルトのバンドル（cacert.pem ）を適宜置き換え

オプション	説明
	ます。ファイルが無効な場合は、エラーメッセージが表示されます。 • デフォルトの証明書に戻すには、**デフォルトにリセット** をクリックします。 **注:** このオプションは、有効なカスタム CA バンドルをアップロードした後でのみ使用できます。

4. **保存してサービスを再起動** をクリックして設定を保存し、メッセージプロトコルプロセッサを再起動します。

関連トピック

アプライアンスのセキュリティ設定の構成

アプライアンスの問題のトラブルシューティング

オプション：エージェント通信の設定を構成します。これにより、エージェントがアプライアンスと通信する頻度が決まります。詳細については、「エージェント通信の管理」を参照してください。

セッションタイムアウトと自動更新設定の構成

セッションタイムアウトはシステムレベルの設定で、ユーザーが**管理者コンソール**または**ユーザーコンソール**から自動的にログアウトされるまでに非アクティブ状態を保持できる時間を指定します。自動更新設定はユーザーレベルの設定です。この設定により、コンソールページの更新頻度が決まります。

セッションタイムアウトの設定

セッションタイムアウトは、セキュリティ要件を満たすように設定できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **一般設定** をクリックして、一般設定 ページを表示します。
3. 一番上のセクションで、セッションタイムアウトを設定します。

オプション	説明
セッションタイムアウト	ユーザーセッションを終了し、ユーザーに再ログインを要求するまでの、非アクティブ状態を保持できる時間を設定します。デフォルトは「1」です。**ユーザーコンソール**と**管理者コンソール**には、この期限をユーザーに警告するためのタイムアウトセッションカウンタがあります。非アクティブ状態の期間のみがカウントされます。カウンタは、ユーザーがコンソールとアプライアンスサーバーの通信を発生させるアクション（ウィンドウの更新、変更の保存、ウィンドウの変更など）を実行すると再開されます。セッションがタイムアウトの 60 秒前に到達すると、メッセージボックスが表示され、セッションを延長するか、ログオフできます。カウンタ

オプション	説明
	が上限に達すると、ユーザーはログアウトされ、ログイン画面が表示されます。この際、未保存の変更は失われます。 タイムアウトセッションカウンタは、各コンソールの右上に表示されます。

4. **保存してサービスを再起動** をクリックします。

自動更新プロパティの設定

自動更新を設定すると、リストページに最新の結果を表示できます。また、自動更新をオフにすると、ブラウザでページが再読み込みされたときにのみページが更新されます。

プロビジョニング結果 ページや デバイス ページなどのステータスを表示するページでは、更新頻度を30秒以下に設定することをお勧めします。ソフトウェアカタログ ページなどのその他のページでは、更新により時間がかかるため、更新間隔を長くしたり、自動更新をオフにしたりする方が適している場合があります。

自動更新設定は、ページおよびユーザー固有の設定です。ページごとおよびユーザーアカウントごとに、個別に設定します。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. 更新する情報があるページに移動します（ **インベントリ** > **デバイス**など ）。

   デバイス ページが表示されます。
3. **自動更新** ドロップダウンリストの右上で、頻度を選択します。

   選択した頻度に従ってリストが更新されます。
4. ページの右上隅にある **更新** ボタンをクリックすると、ページがすぐに更新されます。
5. **オプション**：**自動更新** ドロップダウンリストの右上で、**オフ** を選択して、自動更新をオフにします。

   自動更新が無効化されます。ページ上の情報が自動更新されなくなります。

ロケール設定の構成

ロケール設定によって、コマンドラインコンソール、管理者コンソール、およびユーザーコンソールのテキストに使用される言語が決まります。ロケール設定では、**管理者コンソール**および**ユーザーコンソール**に表示される日時の情報の形式が決まります。インタフェース内では、ロケール設定に関係なく、すべてのテキストが英語で表示されます。

ライセンス契約により利用できるロケールオプション。詳細については、「アプライアンスバージョン、モデル、およびライセンス情報の表示」を参照してください。

ロケール設定を適用する方法

ロケール設定は、特定の順序で適用されます。

コマンドラインコンソール、**管理者コンソール**、および**ユーザーコンソール**内のテキストのロケールを選択するとき、アプライアンスでは次の優先順位が使用されます。

1. **ユーザー**: ユーザーロケールが設定されている場合は、それを使用します。
2. **組織**：ユーザーロケールが設定されていない場合は、組織設定を使用します（ アプライアンス上で組織コンポーネントが有効化されている場合にのみ使用可能 ）。
3. **ブラウザ**：ユーザーロケールも組織ロケールも設定されていない場合は、ブラウザ設定を使用します。
4. **システム（ コマンドラインコンソール ）**：ユーザー、組織、ブラウザのロケールが設定されていない場合は、システム設定を使用します。

5. **デフォルト**：上記のオプションのいずれも設定されていない場合は、デフォルトのロケール（英語）を使用します。

管理者コンソールおよびコマンドラインコンソールのロケール設定の構成

システムレベルの**管理者コンソール**のロケール設定を構成できます。konfig ユーザーアカウントでアクセスする**コマンドラインコンソール**のロケールもこの設定で制御します。

ロケール設定によって、管理者コンソールに表示される日時の情報の形式が決まります。インタフェース内では、ロケール設定に関係なく、すべてのテキストが英語で表示されます。サービスデスクから送信される E メールに使用される日時の形式も、ロケール設定で決まります。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **一般設定** をクリックして、一般設定 ページを表示します。
3. アプライアンスで組織コンポーネントが有効化されている場合、次のことを行います。
   a. 一番上のセクションの デフォルトのロケール ドロップダウンリストからロケールを選択します。
   b. ページの一番下で **保存してサービスを再起動** をクリックします。
4. アプライアンスで組織コンポーネントが有効化されていない場合、次のことを行います。
   a. Locale Settings（ロケール設定）セクションで、Organization Locale（組織のロケール）ドロップダウンリストから使用するロケールを選択します。
   b. ロケール設定 セクションで、コマンドラインコンソール ドロップダウンリストから使用するロケールを選択します。
   c. **保存してサービスを再起動** をクリックします。

選択したロケールは、**管理者コンソール**および**コマンドラインコンソール**に使用されます。

ユーザーコンソールでのロケール設定の構成

アプライアンスは複数のロケールをサポートしています。**管理者コンソール**、**システム管理コンソール**、およびオンラインヘルプは、英語、フランス語、ドイツ語、日本語、ポルトガル語（ブラジル）、スペイン語で表示できます。

これらの言語に加えて、必要に応じて**ユーザーコンソール**をアフリカーンス語（南アフリカ）などの他のサポートされないロケールに翻訳することができます。**ユーザーコンソール**をサポートされない言語に翻訳する場合、ヘルプコンテンツは英語で表示されますが、**管理者コンソール**、**システム管理コンソール**、関連するオンラインヘルプなどの、アプライアンスのその他の要素は選択した言語で表示されます。

デフォルトでは、ブラウザのロケールによって**ユーザーコンソール**に表示される言語が決まります。**ユーザーコンソール**が他の言語に翻訳されており、プロパティが構成されている場合（下に示すように）、そのロケールをブラウザで使用するユーザーの**ユーザーコンソール**は翻訳された言語になります。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **ローカライゼーション** をクリックして、ユーザーコンソールのローカライゼーション設定 ページを表示します。
3. 翻訳前のロケールに関連付けられたテキスト文字列を、ポータブルオブジェクトテンプレート（POT）と共に翻訳用として Gettext ポータルオブジェクト（PO）ファイルにエクスポートします。Gettext POファイルについては、https://www.gnu.org/software/gettext/manual/html_node/PO-Files.htmlを参照してください。
   a. ユーザーコンソールのローカライゼーション設定 ページでは、Gettext Po（ポータブルオブジェクト）ファイルのエクスポート で **ロケールのエクスポート** をクリックして、翻訳前のロケールを選択します。表示されるリストにはサポート対象の言語がすべて含まれており、以前翻訳したユーザーコンソールの言語もすべて含まれます。
   b. **エクスポート** をクリックします。

   しばらくすると、次のコンテンツを含むZIPファイルがダウンロード可能になります。
   - PO（ポータブルオブジェクト）ファイルには、選択したロケール内に存在する**ユーザーコンソール**のテキスト文字列がすべて含まれます。
   - POT（ポータブルオブジェクトテンプレート）ファイルに含まれるテンプレートファイルは、GetTextユーティリティ（オプション）を使用して空のPOファイルを生成するために使用されます。
4. 必要に応じて、ユーザーコンソールのテキスト文字列を翻訳して PO ファイルを作成します。
5. 翻訳済みのユーザーコンソールの文字列をインポートします。

   POファイル内の文字列を翻訳するには、POファイルエディタを使用できます。詳細については、次を参照してください。
   - **GNU gettextユーティリティに関する文書**： https://www.gnu.org/software/gettext/manual/html_node/index.html
   - **GNU Web翻訳者マニュアル**： https://www.gnu.org/software/trans-coord/manual/web-trans/html_node/index.html#SEC_Contents https://www.gnu.org/software/gettext/manual/html_node/PO-Files.html
   - **POファイル形式**： https://www.gnu.org/software/trans-coord/manual/web-trans/html_node/PO-Editors.html
   - **エディタによる提案を使用したPO（ポータブルオブジェクト）ファイルの編集についての追加の情報**： https://www.gnu.org/software/trans-coord/manual/web-trans/html_node/PO-Editors.html

     a. Gettext Po（ポータブルオブジェクト）ファイルのインポート の **ロケールのインポート** をクリックして、インポートしているPOファイルに関連付けるロケールを選択します。これは、ブラウザのロケールが一致した場合にユーザーコンソールが翻訳されるロケールであり、その翻訳ではインポートした PO ファイルを翻訳したものを使用します。
     b. 翻訳されたPO（ポータブルオブジェクト）ファイル の **ファイルの選択** をクリックし、翻訳されたPOファイルに移動します。
     c. **インポート** をクリックします。
6. 以前インポートしたロケールをすべて削除する場合、アップロードされたロケールの削除 の ロケールの削除 をクリックして、削除するロケールを選択します。**削除** をクリックします。

組織のロケール設定の構成

アプライアンス上で組織コンポーネントが有効化されている場合は、組織ごとにロケール設定を個別に構成します。

ロケール設定によって、管理者コンソール と ユーザーコンソール に表示される日時の情報の形式が決まります。インタフェース内では、ロケール設定に関係なく、すべてのテキストが英語で表示されます。サービスデスクから送信される E メールに使用される日時の形式も、ロケール設定で決まります。

1. 一般設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**一般設定** をクリックします。
2. アプライアンスで組織コンポーネントが有効化されている場合、次のことを行います。
    a. Locale Settings（ ロケール設定 ）セクションで、Organization Locale（ 組織のロケール ） ドロップダウンリストから使用するロケールを選択します。
    b. ページの一番下で **保存してサービスを再起動** をクリックします。
    c. 複数の組織がある場合、それぞれの組織について前の手順を繰り返します。
3. アプライアンスで組織コンポーネントが有効化されていない場合、次のことを行います。
    a. Locale Settings（ ロケール設定 ）セクションで、Organization Locale（ 組織のロケール ） ドロップダウンリストから使用するロケールを選択します。
    b. ロケール設定 セクションで、コマンドラインコンソール ドロップダウンリストから使用するロケールを選択します。
    c. **保存してサービスを再起動** をクリックします。

選択したロケールが適用されます。組織ユーザーが **管理者コンソール** および **ユーザーコンソール** にログインすると、このロケールの形式が表示されます。ただし、ブラウザ設定もロケールを表示するように設定されている場合に限ります。ただし、組織のロケール設定よりもユーザーのロケール設定が優先されます。

ユーザーのロケール設定の構成

各ユーザーのロケール設定を構成できます。ユーザーのロケール設定は、組織およびシステムレベルのロケール設定よりも優先されます。

ロケール設定によって、**管理者コンソール** と **ユーザーコンソール** に表示される日時の情報の形式が決まります。インタフェース内では、ロケール設定に関係なく、すべてのテキストが英語で表示されます。

1. ユーザー詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
    c. ユーザーの名前をクリックします。
2. ロケール ドロップダウンリストでロケールを選択します。
3. **保存** をクリックします。

ユーザーが **管理者コンソール** または **ユーザーコンソール** にログインすると、選択したロケールが使用されます。ただし、ブラウザ設定も同じロケールを表示するよう設定されている場合に限ります。ユーザーの組織のロケール設定よりも、ユーザーのロケール設定が優先されます。

デフォルトテーマの設定

デフォルトのインストールでは、管理コンソールがすべての新規ユーザーに対してデフォルトの ライト テーマで表示されます。さらに、ダークテーマとハイブリッドテーマという 2 つのテーマが利用できます。アプライアンスのデフォルトのテーマを変更することができます。アプライアンステーマが用途に適していない場合は、プロファイルに合わせて別のテーマを選択してください。

例えば、ライトテーマがシステムレベルでデフォルトでアプライアンスに設定されていて、ダークテーマをユーザープロファイルに関連付けた場合、ログインするたびにダークテーマが適用されます。

アプライアンスのデフォルトテーマの設定

デフォルトのインストールでは、アプライアンスは ライト テーマを使用するように設定されています。必要に応じて、デフォルトのアプライアンステーマとして別のテーマを選択することができます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **一般設定** をクリックして、一般設定 ページを表示します。
3. 表示される 一般設定 ページの テーマ で **デフォルトのアプライアンステーマ** をクリックし、次のオプションのいずれかを選択します。**ライト**、**ハイブリッド**、または **ダーク**。

   デフォルトのアプライアンステーマとして **ライト** または **ハイブリッド** テーマを選択すると、ログインページは白色の背景で表示されます。デフォルトのアプライアンステーマとして **ダーク** テーマを適用すると、暗色背景が適用されます。ログイン画面の色は、ユーザーアカウントに関連付けられたテーマではなく、設定されたアプライアンスのテーマが常に反映されます。例えば、**管理者コンソール**で ダーク テーマを選択した場合、このテーマはユーザーアカウントに関連付けられ、ログインするたびに適用されます。ただし、アプライアンスがデフォルトで ライト テーマを使用している場合、ログイン画面は常に白色の背景で表示されます。ログインに成功すると、ダーク テーマが適用されます。

   注: どのテーマを選択したかにかかわらず、レポートは常に白色の背景で表示されます。

   注: 新しく作成したユーザーの場合、**管理者コンソール**にはデフォルトのテーマが使用されます。これは、次回ログイン時に変更できます。詳細については、「ユーザーに対するデフォルトテーマの設定」を参照してください。

ユーザーに対するデフォルトテーマの設定

デフォルトのインストールでは、ライト テーマが各ユーザープロファイルに適用されます。必要に応じて、ユーザープロファイルに別のテーマを選択することができます。例えば、ライトテーマがシステムレベルでデフォルトでアプライアンスに設定されていて、ダークテーマをユーザープロファイルに関連付けた場合、ログインするたびにダークテーマが適用されます。

1. 次のいずれかを実行します。
   - **アプライアンス 管理者コンソール（ https://appliance_hostname/admin。ここで、appliance_hostname はお使いのアプライアンスのホスト名 ）にログインします。または、管理**

ヘッダーに組織メニューを表示 がアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

- アプライアンス システム管理コンソール（ https://appliance_hostname/system。ここで、appliance_hostname はお使いのアプライアンスのホスト名 ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。
- アプライアンス ユーザーコンソール（ https://appliance_hostname/user。ここで、appliance_hostname はお使いのアプライアンスのホスト名 ）にログインします。または、ページの右上隅にあるドロップダウンリストから ユーザーコンソール を選択します。

2. ページの右上隅にあるドロップダウンリストから、**マイプロファイル** を選択します。

   ユーザープロファイル ダイアログボックスが表示されます。

3. ユーザープロファイル ダイアログボックスの プロファイル タブで **テーマ** をクリックし、ユーザーアカウントに関連付けるテーマを選択します。**ライト**、**ダーク**、または **ハイブリッド**。

   ここで選択したテーマはユーザーアカウントに関連付けられ、ログインするたびに適用されます。アプライアンスのデフォルトテーマを設定することもできます。詳細については、「アプライアンスのデフォルトテーマの設定」を参照してください。

データ共有の基本設定の構成

システムレベルでデータ共有の基本設定を構成します。データ共有の基本設定により、アプライアンスの情報がどれくらい Quest と共有されるかが決まります。また、データ共有の基本設定により、ITNinja からの情報が 管理者コンソール に表示されるかどうかが決まります。

このセクションで選択したデータ共有オプションにかかわらず、Quest は、ご使用の製品ライセンスを検証するための最小限のライセンス関連情報を収集します。この情報には、アプライアンスの MAC アドレス、アプライアンスソフトウェアのバージョン、ライセンスキー、管理対象デバイスの数などが含まれます。

1. アプライアンスの コントロールパネル に移動します。
   - アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。
   - アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。
2. **一般設定** をクリックして、一般設定 ページを表示します。
3. Questとのデータの共有 セクションで、次のいずれかのオプションを選択します。

オプション	説明
ハードウェア、ソフトウェア、およびアプライアンスの使用率サマリデータをデルと共有する	（ 推奨 ）概要情報をQuestと共有します。この情報には、アプライアンスによって管理されているデバイスの数、管理対象インストール、およびアプリケーションに加えて、アプライアンスのステータス、稼働時間、および読み込み平均が含まれます。サポートが必要な場合に**Questサポート**に追加情報が提供されるよう、このオプションを使用することをお勧めします。Questと共有されたデータは、製品の改善計画で使用されます。
使用率の詳細データとクラッシュレポート（ ITNinja コミュニティの機能を使用するために必要 ）を共有する	（ 推奨 ）詳細情報をQuestと共有し、匿名情報をITNinja.comと共有します。この情報には、エージェントとアプライアンスのクラッシュレポート、ユーザーインターフェイスの使用状況の統計、およびアプリケーションタイトルなどのインベントリ情報が含まれます。Quest はこの情報を使用し

オプション	説明
	て、ソフトウェアカタログの改善を促進しています。また、ITNinja は匿名データを使用して、http://www.itninja.com 上の関連コンテンツを識別し、アプライアンス**管理者コンソール**に動的フィードを提供します。 ITNinja.comは、ITプロフェッショナルが情報を共有したり、システムの管理や導入に関するさまざまなトピックについて調査したりできるコミュニティWebサイトです。ITNinja フィードは、ソフトウェアの展開に関するヒントおよびその他のコンテキスト情報を、アプライアンス**管理者コンソール**内の関連ページに動的に表示する機能です。ITNinja フィードを有効にするには、**使用率の詳細データと共有 ...** を選択する必要があります。この設定により、ITNinjaとの情報共有が匿名で行われます。ITNinja フィードは、**使用率のサマリデータを共有** を選択した場合にのみ使用できます。また、ソフトウェア、管理対象インストール、およびファイル同期の詳細ページなど、ソフトウェアまたは展開に関連するページでのみ使用できます。フィードはソフトウェアカタログ の詳細ページでは利用できません。 このオプションをオフにすると、アプライアンスとITNinjaコミュニティの間でインベントリデータが共有されなくなります。ただし、このオプションをオフにしても、既に共有されている情報は削除されません。詳細については、**Questサポート**にお問い合わせください。

4. **保存してサービスを再起動** をクリックします。

DIACAPコンプライアンス要件について

DIACAP（Department of Defense Information Assurance Certification and Accreditation Process）などの規則をサポートするように、アプライアンスを設定できます。

DIACAP に準拠するために、管理者は次のタスクを実行します。

- 「使用可能な使用ポリシー」を有効にします。詳細については、「使用可能な使用ポリシーの有効化または無効化」を参照してください。
- SSHおよびデータベースアクセスを無効にします。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。
- SAMBAによるファイル共有を無効にします。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。

使用可能な使用ポリシーの有効化または無効化

DIACAP（Department of Defense Information Assurance Certification and Accreditation Process）などの規則に準拠するために、ユーザーは、**管理者コンソール**、**ユーザーコンソール**、または**コマンドラインコンソール**にアクセスする場合、あるいは SSH または FTP を使用してログインする場合に、ユーザーに対して使用可能な使用ポリシーを表示できます。

使用可能な使用ポリシーは、システムレベルの設定です。アプライアンス上で組織コンポーネントが有効化されている場合は、すべての組織のシステムレベルで使用可能な使用ポリシーを有効化または無効化します。個別の組織のこのポリシーを有効化または無効化することはできません。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **一般設定** をクリックして、一般設定 ページを表示します。
3. 使用可能な使用ポリシー セクションで、ポリシー設定を選択します。

オプション	説明
有効	ユーザーが、**管理者コンソール**、**ユーザーコンソール**、または**コマンドラインコンソール** にアクセスする場合、または SSH や FTP を使用してログインする場合に、アプライアンスがポリシーを表示して、ユーザーにポリシーの条件に同意するよう要求できるようにします。
タイトル	**ユーザーコンソール**のログインページに表示されるポリシーの見出し。
メッセージ	ポリシーの詳細（ログインページの Title（タイトル）の下に表示されます）。ユーザーは、**ユーザーコンソール**にログインする前にポリシーの条件に同意する必要があります。

4. **保存してサービスを再起動** をクリックします。

   ユーザーは、**管理者コンソール**、**ユーザーコンソール**、または**コマンドラインコンソール**に移動する場合、あるいは SSH または FTP を使用してログインする場合、最初に使用可能な使用ポリシーに合意してからログインする必要があります。

注: シングルサインオンが有効化されている場合は、ログインページが表示されないため、ユーザーが自動的にログインされる前に使用可能な使用ポリシーが表示されません。詳細については、「シングルサインオン（ SSO ）について」を参照してください。

モバイルデバイスによるアクセスの設定

モバイルデバイスによるアクセスを使用すると、KACE GO アプリケーションでアプライアンスを対話操作できます。

KACE GOは、管理者がスマートフォンやタブレットを使用して、サービスデスクチケット、インベントリ情報、およびアプリケーション導入機能にアクセスするためのアプリケーションです。このアプリケーションにより、管理者以外のユーザーもサービスデスクチケットの送信、提出されたチケットのステータスの表示、およびモバイルデバイスからのサポート技術情報記事の閲覧を行うことができるようになります。iOSデバイスの場合はApple App Storeから、Androidデバイスの場合はGoogle Playストアからそれぞれ KACE GOをダウンロードできます。

注: KACE GOは英語でのみ利用可能です。

モバイルデバイスによるアクセスを使用するには、アプライアンスおよびユーザーのモバイルデバイスによるアクセスを有効にし、モバイルデバイスにKACE GOをダウンロードして、インストールする必要があります。

アプライアンスに対するモバイルデバイスによるアクセスの有効化

デフォルトでは、モバイルデバイスによるアクセスは無効になっています。KACE GO アプリケーションを使用してユーザーがアプライアンスにアクセスできるようにするには、最初にアプライアンスのモバイルデバイスによるアクセスを有効化する必要があります。

モバイルデバイスによるアクセスは、システムレベルで有効化されます。アプライアンス上で組織コンポーネントが有効化されているときにモバイルデバイスによるアクセスを有効化すると、この機能が組織全体で有効化されます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **一般設定** をクリックして、一般設定 ページを表示します。
3. 一番上のセクションで、モバイルデバイスによるアクセスを有効にする チェックボックスをオンにします。
4. KACE GOアプリケーションをダウンロードします。
   a. **モバイルアプリの取得** をクリックします。

      KACE GOのダウンロードを許可するダイアログボックスが表示されます。このアプリケーションは、iOSとAndroidでのプラットフォームごとのアプリケーションストアにて入手可能です。

      ヒント: このダイアログボックスは、ヘルプペインからも表示できます。詳細については、「製品ドキュメントへのアクセス」を参照してください。

   b. 必要に応じて、お使いのモバイルデバイスOS用のリンクをクリックして、アプリケーションをダウンロードします。

   KACE GOのダウンロードおよび設定についての詳細は、KACE GOのダウンロードおよび使用を参照してください。
5. **保存してサービスを再起動** をクリックします。

   アプライアンスでモバイルデバイスによるアクセスが有効になります。ただし、KACE GO アプリケーションを使用してユーザーがアプライアンスにアクセスできるようにするには、ユーザーのアカウントに対してモバイルデバイスによるアクセスを有効化する必要があります。詳細については、「ユーザーに対するモバイルデバイスによるアクセスの有効化」を参照してください。

   アプライアンス上で組織コンポーネントが有効化されている場合は、組織レベルまたは管理者レベルでユーザーアカウントに対してモバイルデバイスによるアクセスを有効化します。モバイルデバイスによるアクセスは、ユーザーアカウントに対してシステムレベルで有効または無効にすることはできません。

ユーザーに対するモバイルデバイスによるアクセスの有効化

アプライアンスでモバイルデバイスによるアクセスを有効化した後は、ユーザーに対してアクセスを有効化する必要があります。アプライアンスで組織コンポーネントが有効化されている場合は、各組織のユーザーのアクセスを個別に有効化できます。

1. ユーザー詳細 ページに移動します。

a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
c. ユーザーの名前をクリックします。

2. **モバイルデバイスによるアクセス** チェックボックスをオンにします。

ヒント: モバイルデバイスによるアクセス チェックボックスが表示されていない場合は、アプライアンスのモバイルデバイスによるアクセスが有効化されていることを確認してください。

3. **保存** をクリックします。
4. 複数のユーザーに対してモバイルデバイスによるアクセスを有効化するには:
a. ユーザー ページで該当するユーザーのチェックボックスを選択します。
b. **アクションの選択 > モバイルデバイスによるアクセス > 有効にする** を選択します。

モバイルデバイスによるアクセスが有効になります。

関連トピック

アプライアンスに対するモバイルデバイスによるアクセスの有効化

選択したユーザーは、Apple App StoreまたはGoogle PlayからKACE GOアプリケーションをダウンロードできます。

KACE GOのダウンロードおよび使用

iOSデバイスの場合はApple App Storeから、Androidデバイスの場合はGoogle Play Storeからそれぞれ KACE GOをスマートフォンまたはタブレットにダウンロードできます。

1. モバイルデバイス上でApple App StoreまたはGoogle Playにアクセスし、「**KACEGO**」を検索します。
2. アプリケーションをダウンロードして起動します。
3. プロンプトが表示されたら、プッシュ通知を有効化するかどうかを選択します。

プッシュ通知を有効化すると、アプリケーションによってサービスデスクチケットの通知がモバイルデバイスに送信されます。これらの通知は、サービスデスクの「**イベント発生時にEメールを送信**」の設定に基づいて送信されます。

4. 次の情報を入力し、初期設定を選択します。

オプション	説明
アプライアンスの URL	アプライアンスのIPアドレスまたは完全修飾ドメイン名。
ユーザー名およびパスワード	モバイルデバイスによるアクセスが有効化されているアカウントのユーザー名およびパスワード。
パスワードの保存	デバイス上で、アプリケーションがパスワードを記憶できるようになります。このオプションを選択した場合は、セキュリティ保護のため、QuestからPIN（ 個人識別番号 ）を作成するように求められます。**パスワードの保存** を選択していない場合は、KACE GOによってユーザーデータがキャッシュされたり、保存されたりすることはありません。
SSLを使用	デバイスとアプライアンスの間の SSL 通信を有効化します。この設定を使用するには、アプライアンスで SSL が有効化されている必要がありま

オプション	説明
	す。アプライアンスでSSLが有効化されていない場合、**SSLを使用** を選択すると、ログインに失敗します。

詳細については、KACE GOアプリケーションのヘルプセンターを参照するか、https://quest.com/products/kace-systems-management-appliance/にアクセスしてください。

関連トピック

Eメールトリガの設定

アプライアンスのセキュリティ設定の構成

アプライアンスでのモバイルデバイスによるアクセスの無効化

すべてのユーザーがKACE GOによるアプライアンスへのアクセスを行えないようにするには、アプライアンスレベルまたはシステムレベルでモバイルデバイスによるアクセスを無効化します。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **一般設定** をクリックして、一般設定 ページを表示します。
3. 一番上のセクションで、モバイルデバイスによるアクセスを有効にする チェックボックスをオフにします。
4. **保存してサービスを再起動** をクリックします。

   KACE GOによるアクセスがすべてのユーザーに対して無効になります。現在KACE GOを使用してアプライアンスにログインしているユーザーは切断されます。

ただし、個々のユーザー設定は保持され、この機能がその後アプライアンスで再度有効化された場合は使用できるようになります。例えば、モバイルデバイスによるアクセスがアカウントに対して有効化されており、アプライアンスでモバイルデバイスによるアクセスを再度有効化した場合は、そのアカウントのモバイルデバイスによるアクセスも再度有効になります。

ユーザーに対するモバイルデバイスによるアクセスの無効化

選択したユーザーがKACE GOによるアプライアンスへのアクセスを行えないようにするには、ユーザーレベルでのモバイルデバイスによるアクセスを無効化します。

1. ユーザー リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
2. 1人または複数のユーザーの隣のチェックボックスをオンにします。
3. **アクションの選択 > モバイルデバイスによるアクセス > 無効にする** を選択します。

選択したユーザーのモバイルデバイスによるアクセスが無効になります。選択したユーザーが現在KACE GOを使用してアプライアンスにログインしている場合、そのユーザーは切断されます。

組織およびリンク先アプライアンスの高速切り替えの有効化

高速切り替えにより、各アイテムに個別にログインせずに、インタフェース間の切り替えを行えるようになります。組織コンポーネントが有効になっているアプライアンスの場合、これらのインターフェイスには**管理者レベルおよびシステムレベルの管理者コンソール**、**ユーザーコンソール**、およびリンクされている K シリーズアプライアンスが含まれています。

組織コンポーネントが有効になっていないアプライアンスでは、デフォルトで高速切り替えが有効になっています。また、デフォルトで**ユーザーコンソール**へのリンクが表示されます。ただし、ログインユーザーが**管理者コンソール**と**ユーザーコンソール**の両方にアクセスする権限を持っている場合に限ります。

高速切り替え用のドロップダウンリストに表示する組織は、同じ **admin** アカウントのパスワードを使用している必要があります。**admin** アカウントのパスワードが一致する組織のみがリストに表示されます。リンク先アプライアンス同士では、要件はほぼ同じです。

1. 一般設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**一般設定** をクリックします。
2. 管理ヘッダーに組織メニューを表示 チェックボックスをオンにします。

    注: この設定は、アプライアンス上で組織コンポーネントが有効化されている場合にのみ使用可能です。
3. **オプション**：ユーザーがログイン時に組織を選択する必要があるようにするには、Require organization selection at login（ ログイン時に組織の選択が必要 ）チェックボックスをオンにします。

    注: この設定は、アプライアンス上で組織コンポーネントが有効化されている場合にのみ使用可能です。
4. **保存してサービスを再起動** をクリックします。

    変更は、いったんログアウトし、再度ログインすることによって、ログインページと**管理者コンソール**の一番上のセクションに反映されます。使用可能なオプションがドロップダウンリストに表示されます。

関連トピック

Quest KACEアプライアンスのリンク

Quest KACEアプライアンスのリンク

アプライアンスのリンクによって、1 つの Quest KACE アプライアンスにログインして、**管理者コンソール**からすべてのリンク先アプライアンスにアクセスできます。

アプライアンスをリンクすると、各アプライアンスに個別にログインしなくても、1 つのアプライアンスにログインするだけで、**管理者コンソール**の右上隅にあるドロップダウンリストからすべてのリンク先アプライアンスにアクセスできるようになります。管理対象のすべてのQuest KACE Kシリーズアプライアンスをリンクできます。

アプライアンスをリンクするには、次の操作を行う必要があります。

- 組織コンポーネントが有効化されている各アプライアンスで高速切り替えを有効にします。詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。
- 各Kシリーズアプライアンス上でリンクを有効にします。詳細については、「アプライアンスリンクの有効化」を参照してください。

リンクを有効にすると、各アプライアンスの名前とキーが作成されます。名前とキーをコピーして、各アプライアンスの リンク先アプライアンスの詳細 ページに貼り付けます。

同じ**管理者コンソール**から複数の Quest KACE アプライアンスにアクセスできますが、リンクすることで、アプライアンス間でのリソースや情報の転送ができなくなります。詳細については、「アプライアンスリソースのインポートとエクスポート」を参照してください。

注: 異なるタイプの Quest KACE アプライアンスがあり、それらをリンクすることを計画している場合は、各アプライアンスの **admin** ユーザーアカウントのパスワードを同じにする必要があります。

アプライアンスリンクの有効化

アプライアンスまたはシステムレベルの一般設定でアプライアンスリンクを有効化できます。KACE SDA での方法については、そのアプライアンスのヘルプを参照してください。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール (https://appliance_hostname/admin) にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール (https://appliance_hostname/system) にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **リンク設定** をクリックして、リンク先アプライアンスの有効化 ページを表示します。
3. **アプライアンスリンクを有効にします** チェックボックスをオンにします。
4. 次の情報を入力します。

オプション	説明
名前	このアプライアンス固有のロジカルネーム。アプライアンスがリンクされている場合、この名前がページの右上隅にあるドロップダウンリスト (ログイン情報の隣) に表示されます。
ログインの有効期限	リンクを開いたままにしておく時間 (分単位)。この期間が終了すると、リンク先アプライアンスに切り替えるときに、ログイン資格情報を提供する必要があります。デフォルトは120分です。
タイムアウト	リモートアプライアンスがリンク要求に応答するまで、アプライアンスが待機する時間 (分単位)。デフォルトは10秒です。

5. **Federation API アクセス設定** チェックボックスを選択します。

   注: このオプションを有効にすると、リンク先アプライアンスのフェデレーションAPI設定を構成できます。詳細については、「フェデレーションAPI設定のアクセスの有効化」を参照してください。
6. **保存** をクリックして、アプライアンスリンク情報を表示します。
7. 名前 フィールドのテキストと キー フィールドのテキストをコピーして、メモ帳ファイルなどの中央的な場所に貼り付けます。
8. リンク先の各アプライアンスで、上記の手順を繰り返します。

すべてのアプライアンスでリンクを有効にしたら、リンクを設定します。詳細については、「名前とキーのアプライアンスへの追加」を参照してください。

名前とキーのアプライアンスへの追加

Quest KACE アプライアンスをリンクするには、**管理者コンソール**にアプライアンス名とキーを追加します。

これらの手順は、KACE SMA のリンク方法を示しています。KACE SDA での方法については、そのアプライアンスのヘルプを参照してください。

アプライアンスをリンクできるようにする前に、各アプライアンスのリンクを有効にして、各アプライアンスの名前とキーを中央サイトにコピーする必要があります。詳細については、「アプライアンスリンクの有効化」を参照してください。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **リンク先アプライアンス** をクリックして、リンク先アプライアンス ページを表示します。

   注: アプライアンスリンクが有効になっていない場合、Linked Appliance Enablement（ リンク先アプライアンスの有効化 ）ページにリダイレクトされます。
3. **アクションの選択 > 新規作成** を選択して、リンク先アプライアンスの詳細 ページを表示します。
4. リンクするアプライアンスの名前を ホスト名 フィールドに貼り付けます。

   これは、アプライアンスリンクの有効化の手順に従ってコピーした名前です。
5. **ポート80接続を無効にする** を選択して、ポート443をセキュアな通信用に使用します。ポート80と443を使用する両方の通信が暗号化されます。
6. リンクするアプライアンスのキーを キー フィールドに貼り付けます。

   これは、アプライアンスリンクの有効化の手順に従ってコピーしたキーです。
7. **保存** をクリックすると、接続のテスト ボタンが表示されます。
8. **接続のテスト** をクリックし、2つのリンク先アプライアンスの間の接続を確認します。

   設定が正しく構成されると、Connection Successful（ 正常に接続されました ）メッセージが表示されます。
9. 2 番目のアプライアンスにログインし、上記の手順を繰り返して、1 番目のアプライアンスの名前とキーを 2 番目のアプライアンスに追加します。
10. **保存** をクリックすると、**接続のテスト** ボタンが表示されます。
11. **接続のテスト** をクリックし、2つのリンク先アプライアンスの間の接続を確認します。

    設定が正しく構成されると、Connection Successful（ 正常に接続されました ）メッセージが表示されます。

アプライアンスに再ログインすると、ページの右上隅にあるドロップダウンリスト（ ログイン情報の隣 ）に他のリンク先アプライアンスが表示されます。アプライアンスを切り替えるには、切り替えるアプライアンスの名前をドロップダウンリストで選択してください。

フェデレーションAPI設定のアクセスの有効化

お使いの環境で統合 KACE SMA を使用している場合、フェデレーション API 設定 ページでは、リンク先アプライアンスの API アクセスを有効にすることができます。

次のオプションは、リンク先アプライアンスの有効化 ページで選択する必要があります。

- **アプライアンスリンクを有効にする**
- **フェデレーションAPIアクセス設定を有効にする**

詳細については、「アプライアンスリンクの有効化」を参照してください。

1. アプライアンス監理者コンソール（ http://**appliance_hostname**/admin ）にログインして、**設定** をクリックします。
2. アプライアンスの コントロールパネル で、**フェデレーションAPI設定** をクリックし、フェデレーション API設定 ページを表示します。
3. フェデレーションAPI設定 ページで、**アクセスの有効化** チェックボックスをオンにします。
4. 表示される リモートシステム で、必要に応じて各リンク先アプライアンスのアクセスレベルを指定します。
   a. 役割を設定するアプライアンスを含む行で、役割 列をクリックし、次のいずれかのオプションを選択します。**管理者**、**読み取り専用の管理者**、または **ユーザーコンソール**。
   b. **保存** をクリックします。
5. **保存** をクリックして、アプライアンスリンク情報を表示します。

アプライアンスリンクの無効化

Quest KACEアプライアンスがリンクされている場合は、必要に応じてリンクを無効にできます。アプライアンスリンクを無効にした後でも、ログオフするまでは、他のアプライアンスに切り替えたり、制御したりできます。

注: このセクションでは、アプライアンスでリンクを無効化する方法について説明します。KACE SDA での方法については、そのアプライアンスのヘルプを参照してください。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **リンク設定** をクリックして、リンク先アプライアンスの有効化 ページを表示します。
3. Enable Appliance Linking（ アプライアンスリンクを有効にします ） チェックボックスをオフにします。
4. **保存** をクリックします。

履歴設定の定義

アプライアンスの設定、資産、およびオブジェクトに加えられた変更の履歴を設定（ サブスクライブ ）および表示することができます。

履歴設定について

アプライアンスでは、設定、資産、およびオブジェクトの変更履歴を設定（サブスクライブ）および表示できます。

- **設定**：追跡対象のアイテムは、一般設定と、MIAデバイス、パッチのサブスクリプション、ユーザー認証などの設定です。詳細については、「設定履歴の管理」を参照してください。
- **資産**: 追跡対象のアイテムは、デバイス、コストセンター、部門、ライセンス、場所、アプリケーション、ベンダー、およびユーザーによって作成された資産タイプです。詳細については、「資産履歴の管理」を参照してください。
- **オブジェクト**：追跡対象のアイテムは、警告、ラベル、パッチスケジュール、レプリケーション共有、レポート、スクリプト、およびアプリケーションなどです。詳細については、「オブジェクト履歴の管理」を参照してください。

この履歴には、変更が加えられた日付、変更が加えられたときにログインしていたユーザー、および変更のタイプが示されます。この情報は、システム管理に伴う問題をトラブルシューティングする際に役立ち、CSV（コンマ区切り値）またはカスタムレポートの形式でエクスポートできます。

履歴リストは情報提供のみを目的としています。履歴リストを使用して以前の状態に戻したり、変更を元に戻したりすることはできません。

設定履歴の管理

設定に加えられた変更の履歴を設定（サブスクライブ）および表示することができます。設定オプションは、アプライアンスで組織コンポーネントが有効化されているかどうかによって異なります。

- 組織コンポーネントが有効化されていない場合：**設定** > **履歴** ですべての履歴リストおよび設定を表示します。手順については、組織の設定履歴サブスクリプションの設定を参照してください。
- 組織コンポーネントが有効化されている場合: 各組織およびシステムレベルの履歴リストと設定を個別に表示します。手順については、組織コンポーネントが有効化されている場合のシステムレベルの設定履歴サブスクリプションの設定を参照してください。

組織の設定履歴サブスクリプションの設定

アプライアンスの設定履歴、または組織コンポーネントが有効化されている場合は選択された組織の設定履歴サブスクリプションを設定できます。

1. 設定履歴の設定 ページに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左のナビゲーションバーで **設定**、**履歴** の順にクリックします。
   c. サブスクリプション セクションで、**設定** をクリックします。

   このページに表示されるオプションは、アプライアンスで組織コンポーネントが有効化されているかどうかによって異なります。組織コンポーネントが有効化されているアプライアンスの場合は、システムレベルで追加のオプションを使用できます。
2. 履歴の保持 ドロップダウンリストでは、変更がアプライアンスに保持され、履歴リストに表示される期間を選択します。**無制限** を選択すると、すべての変更が保持されます。**無効**を選択すると、既存の履歴リストが消去され、アプライアンスは変更をリストに追加しなくなります。

   重要: 履歴の保持を非常に長い期間（数ヶ月や 無制限 など）に設定すると、インベントリ **セクションでアイテムのページ読み込みが遅くなる可能性があります。**
3. カテゴリとフィールドの選択 セクションで、追跡する設定の隣にあるチェックボックスをオンにします。追跡しない設定については、隣のチェックボックスをオフにします。
4. 以下の操作を実行して、設定に関するフィールドを選択します。

a. 設定の隣の **編集** アイコンをクリックします（このアイコンは、設定のチェックボックスがオンの場合に表示されます）。

フィールドの選択ダイアログが表示されます。

b. 追跡対象の履歴が示されているフィールドを選択して、**OK** をクリックします。

5. **保存** をクリックします。
6. **オプション**：複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

関連トピック

組織コンポーネントが有効化されている場合のシステムレベルの設定履歴サブスクリプションの設定

組織コンポーネントが有効化されている場合のシステムレベルの設定履歴サブスクリプションの設定

アプライアンス上で組織コンポーネントが有効化されている場合、システムレベルで設定履歴サブスクリプションを設定できます。

組織レベルの履歴設定の詳細については、設定履歴の管理を参照してください。

1. 設定履歴の設定 ページに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左のナビゲーションバーで **設定**、**履歴** の順にクリックします。
   c. 履歴パネルの サブスクリプション セクションで、**設定** をクリックします。
2. カテゴリとフィールドの選択 セクションで、追跡する設定の隣にあるチェックボックスをオンにします。追跡しない設定については、隣のチェックボックスをオフにします。
3. 以下の操作を実行して、設定に関するフィールドを選択します。
   a. 設定の隣の **編集** アイコンをクリックします（このアイコンは、設定のチェックボックスがオンの場合に表示されます）。

   フィールドの選択ダイアログが表示されます。

   b. 追跡対象の履歴が示されているフィールドを選択して、**OK** をクリックします。
4. **保存** をクリックします。

設定履歴の表示

履歴のサブスクリプションが、情報を保持するように設定されている場合、設定に対して行われた変更の履歴を表示することができます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 履歴 をクリックします。
3. レポート作成 セクションで、**設定** をクリックして、設定履歴 ページを表示します。
4. リストをフィルタリングするには、右側のテーブルの上に表示される特定基準で表示 ドロップダウンリストから**タイプ** または **ユーザー別に表示** を選択します。

   リストが再表示され、選択したタイプ または ユーザー に一致するアイテムのみが示されます。

資産履歴の管理

資産情報（デバイス、コストセンター、部門、ライセンス、場所、アプリケーション、ベンダー、ユーザーが作成した資産タイプなど）の変更履歴を設定（サブスクライブ）および表示することができます。

資産履歴サブスクリプションの設定

アプライアンスの資産履歴サブスクリプション、または組織コンポーネントが有効化されている場合は選択された組織の資産履歴サブスクリプションを設定できます。

1. 資産履歴の設定 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**履歴** の順にクリックします。
    c. 履歴パネル の サブスクリプション セクションで、**資産** をクリックします。
2. 履歴の保持 ドロップダウンリストでは、変更がアプライアンスに保持され、履歴リストに表示される期間を選択します。**無制限** を選択すると、すべての変更が保持されます。**無効**を選択すると、既存の履歴リストが消去され、アプライアンスは変更をリストに追加しなくなります。

    重要: 履歴の保持を非常に長い期間（数ヶ月や 無制限 **など）に設定すると、**インベントリ **セクションでアイテムのページ読み込みが遅くなる可能性があります。**

3. Asset Type and Field Selection（資産タイプとフィールドの選択）セクションで、追跡する資産タイプの隣にあるチェックボックスをオンにします。追跡しない資産タイプは、隣のチェックボックスをオフにします。
4. 資産タイプに関するフィールドを選択するには、次の手順を実行します。
    a. 資産タイプの隣の **編集** アイコンをクリックします（このアイコンは、資産タイプのチェックボックスがオンの場合に表示されます）。
    フィールドの選択ダイアログが表示されます。
    b. 追跡対象の履歴が示されているフィールドを選択して、**OK** をクリックします。
5. **保存** をクリックします。
6. **オプション**：複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

資産履歴の表示

履歴のサブスクリプションが、情報を保持するように設定されている場合、資産に対して行われた変更の履歴を表示することができます。

1. 資産履歴 リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**履歴** の順にクリックします。
    c. 履歴パネル の レポート セクションで、**資産** をクリックします。
2. リストをフィルタリングするには、右側のテーブルの上に表示される特定基準で表示 ドロップダウンリストから**タイプ** または **ユーザー別に表示** を選択します。

リストが再表示され、選択したタイプ または ユーザー に一致するアイテムのみが示されます。

オブジェクト履歴の管理

ラベル、パッチスケジュール、レプリケーション共有、ユーザーといったオブジェクトの変更履歴を設定（サブスクライブ）および表示できます。

オブジェクト履歴の設定

アプライアンスのオブジェクト履歴サブスクリプション、または組織コンポーネントが有効化されている場合は選択された組織の資産履歴サブスクリプションを設定できます。

1. オブジェクト履歴の設定 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**履歴** の順にクリックします。
    c. 履歴パネルの サブスクリプション セクションで、**オブジェクト** をクリックします。
2. 履歴の保持 ドロップダウンリストでは、変更がアプライアンスに保持され、履歴リストに表示される期間を選択します。**無制限** を選択すると、すべての変更が保持されます。**無効**を選択すると、既存の履歴リストが消去され、アプライアンスは変更をリストに追加しなくなります。

    重要: 履歴の保持を非常に長い期間（数ヶ月や 無制限 など）に設定すると、インベントリ セクションでアイテムのページ読み込みが遅くなる可能性があります。
3. Object Type and Field Selection（オブジェクトタイプとフィールドの選択） セクションで、追跡するオブジェクトタイプの隣にあるチェックボックスをオンにします。追跡しないオブジェクトタイプは、隣のチェックボックスをオフにします。
4. 以下の操作を実行して、オブジェクトタイプに関するフィールドを選択します。
    a. オブジェクトタイプの隣の **編集** アイコンをクリックします（このアイコンは、オブジェクトタイプのチェックボックスがオンの場合に表示されます）。

    フィールドの選択ダイアログが表示されます。
    b. 追跡対象の履歴が示されているフィールドを選択して、**OK** をクリックします。
5. **保存** をクリックします。
6. **オプション**：複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

オブジェクト履歴の表示

履歴のサブスクリプションが、情報を保持するように設定されている場合、オブジェクトに対して行われた変更の履歴を表示することができます。

1. オブジェクト ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**履歴** の順にクリックします。
    c. 履歴パネル の レポート セクションで、**オブジェクト** をクリックします。
2. リストをフィルタリングするには、右側のテーブルの上に表示される特定基準で表示 ドロップダウンリストから**タイプ** または **ユーザー別に表示** を選択します。

リストが再表示され、選択したタイプ または ユーザー に一致するアイテムのみが示されます。

変更履歴情報の使用

アイテムの変更履歴の参照、変更履歴リストのアイテムの検索、履歴レコードの削除、履歴レコードのエクスポート、履歴レコードからのレポートの作成を行うことができます。

アイテムの変更履歴の表示

アイテムに関する詳細を表示しているときに、アイテムの変更履歴を表示できます。

1. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. アイテムの 詳細 ページに移動します。例えば、**スクリプト作成** をクリックして、スクリプトの名前をクリックします。
3. ページ上部の **すべての履歴の表示** リンクをクリックします。

   変更のリストが表示されます。変更が加えられていない場合、または変更履歴が有効になっていない場合、このページには何も表示されません。

変更履歴リスト内でのアイテムの検索

変更履歴リスト内のアイテムを検索できます。

1. 設定、資産、またはオブジェクトの履歴リストに移動します。
   - 設定履歴の表示
   - 資産履歴の表示
   - オブジェクト履歴の表示
2. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
3. 検索プロパティを選択し、**検索** をクリックします。

   検索結果が表示されます。

履歴レコードの削除

履歴リストから履歴レコードを削除できます。

1. 設定、資産、またはオブジェクトの履歴リストに移動します。
   - 設定履歴の表示
   - 資産履歴の表示
   - オブジェクト履歴の表示
2. 1つ以上のエントリの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

履歴レコードのエクスポート

履歴レコードをCSV、Excel、およびTSV形式にエクスポートします。

1. 設定、資産、またはオブジェクトの履歴リストに移動します。
   - 設定履歴の表示
   - 資産履歴の表示
   - オブジェクト履歴の表示
2. **オプション**：特定のタイプ（「**追加**」など）のアイテムをエクスポートする場合は、特定基準で表示 ドロップダウンリストからアイテムタイプを選択します。

リストをフィルタリングしない場合、すべてのリストアイテムがエクスポートされます。アイテムのチェックボックスを選択しても、アイテムはエクスポート対象として選択されません。

3. **アクションの選択** > **エクスポート** > **format** を選択します。

アイテムのグループを管理するためのラベルのセットアップおよび使用

手動ラベル、Smart Label、LDAPラベル、およびラベルグループをセットアップして、デバイスなどのアイテムのグループを管理できます。

ラベルについて

ラベルは、デバイスなどのアイテムをグループとして管理できるよう、整理および分類できるコンテナです。

例えば、オペレーティングシステムが同じデバイスや地理的に同じ場所にあるデバイスを、ラベルを使用して識別することができます。その後、そのラベルが割り当てられているすべてのデバイス上で、ソフトウェアの配布やパッチの導入などのアクションを開始できます。ラベルは、特定のアイテムに手動で割り当てることもできれば、SQLやLDAPクエリなどの基準に関連するアイテムに自動で割り当てることもできます。次のタイプのアイテムにラベルを適用できます。

- デバイス、アプリケーション、プロセス、スタートアップアイテム、サービスなどのインベントリアイテム
- 場所、ライセンス、ベンダーなどの資産アイテム
- 検出結果
- パッチ
- Dellアップデートパッケージ
- ユーザー

手動ラベルは手動で適用および除去されますが、Smart LabelとLDAPラベルは自動で適用および除去されます。詳細については、以下を参照してください。

- Smart Labelについて
- LDAPラベルについて

Smart Labelについて

Smart Label は、指定した基準に基づいて自動的に適用および削除されるラベルです。

例えば、San Francisco オフィスなど特定の場所にあるラップトップを追跡または管理するには、その場所にあるデバイスの IP アドレス範囲またはサブネットに基づいて、**San Francisco Office** という名前の Smart Label を作成できます。デバイスをインベントリに設定すると、その IP アドレス範囲内のデバイスに Smart Label（**San Francisco Office**）が自動的に適用されます。デバイスが IP アドレス範囲外になり、再度インベントリに設定されると、ラベルは自動的に削除されます。

Smart Labelは、アプライアンスがデバイスインベントリを処理するときに、管理対象デバイスに対して適用または削除されます。そのため、デバイスでメータリングを有効化するSmart Labelを作成しても、Smart Labelがデバイスに対して適用されるまでに時間がかかることがあります。また、デバイスがメータリング情報をレポートするまでにも時間がかかる場合があります。アプライアンスによってデバイスインベントリが処理され、Smart Labelが適用された後にのみ、Smart Labelの基準に一致するデバイスでメータリングが有効化されます。

関連トピック

Smart Labelの管理

LDAPラベルについて

LDAPラベルは、LDAPサーバーと対話するラベルです。これらのラベルは、LDAPクエリまたは検索フィルタを使用して、デバイスとユーザーレコードに自動的に割り当てられます。

次の2つのタイプのLDAPラベルがあります。

- **デバイス**: デバイスレコードに適用されるラベル。これは、名前、説明、およびその他のLDAP条件によってデバイスを自動的にグループ化する場合に役立ちます。デバイスがインベントリ設定されるたびに、このクエリがLDAPサーバーに対して実行されます。検索フィルタ フィールドのadmin値は、デバイスに ログインしているユーザーの名前に置き換えられます。結果が返された場合、デバイスに Associated Label Name（ 関連するラベル名 ）フィールドで指定されたラベルが割り当てられます。
- **ユーザー**: ユーザーレコードに適用されるラベル。これは、ドメイン、場所、予算コード、またはその他のLDAP条件によってユーザーを自動的にグループ化する場合に役立ちます。ユーザーが手動またはスケジュールに従ってアプライアンスにインポートされると、LDAPラベルがユーザーレコードに適用されるか、ユーザーレコードから除去されます。

関連トピック

LDAPラベルの管理

ラベルグループについて

ラベルグループのラベルを割り当てることによって、ラベルを編成できます。ラベルグループに含まれるラベルは、互いにタイプを共有しています。

ラベルグループに複数のラベルを含めることができるだけではなく、ラベルに対して複数のラベルグループを関連付けることもできます。ラベルが属するグループの制限は、ラベルに継承されます。

関連トピック

ラベルグループの追加、表示、または編集

組織フィルタについて

組織フィルタは、ラベルに似ていますが、固有の用途も持っています。組織フィルタでは、デバイスがインベントリ設定されると、デバイスが自動的に組織に割り当てられます。

組織フィルタには2つのタイプがあります。

- **データフィルタ**: 検索条件に基づいて、デバイスを自動的に組織に割り当てます。デバイスがインベントリ設定されるときに、デバイスが条件を満たしている場合は、デバイスが組織に割り当てられます。このフィルタは、デバイスが指定された条件と一致する場合に自動的に組織にデバイスを割り当てるという点で、Smart Labelに似ています。
- **LDAPフィルタ**: LDAPまたはActive Directoryとの対話に基づいて、デバイスを自動的に組織に割り当てます。デバイスがインベントリ設定されると、クエリがLDAPサーバーに対して実行されます。デバイスが条件を満たすと、組織に自動的に割り当てられます。

関連トピック

組織フィルタの管理

ラベル設定の変更追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。

関連トピック

履歴設定について

手動ラベルの管理

管理者コンソールの ラベル セクションでラベルを管理できます。ラベルは、インベントリ や セキュリティ など、他のセクションのリストページからも追加および適用できます。それには、**アクションの選択 > ラベルの追加** を選択します。

手動ラベルの追加または編集

手動ラベルは、必要に応じて追加または編集できます。

1. ラベル詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**ラベル** をクリックします。
    d. ラベルの詳細 ページを表示するには、次のいずれかを実行します。

    - ラベルの名前をクリックします。
    - **アクションを選択 > 新規作成 > 手動ラベル** を選択します。

    ヒント: ラベル名にはバックスラッシュ（ \ ）を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して（ \\ ）エスケープします。

2. 次の情報を入力します。

オプション	説明
名前	ラベルの名前。この名前は、ラベル リストに表示されます。
説明	任意の追加情報を入力します。
代替の場所	（ オプション ）管理対象インストール、ファイル同期、およびこのラベルに割り当てられたアイテムに対して実行される他の展開のために用意された代替のダウンロード場所。指定した場所が文字列KACE_ALT_LOCATIONと置き換わります。 **注意: このフィールドに値を指定するラベルが2つある場合、1つのデバイスに両方のラベルを適用することはできません。**
パス	代替のダウンロード場所を指定する場合は、その場所へのパスを指定します。

オプション	説明
ログイン パスワード	代替のダウンロード場所を指定する場合は、その場所のためのユーザー名およびパスワードを指定します。
ラベル使用の制限対象	（オプション）ラベルまたはラベルグループを適用できるアイテムのカテゴリ。ラベルの使用を制限しない場合は、あらゆるアイテムにラベルまたはラベルグループを適用できます。ただし、ラベルまたはラベルグループを例えば「アプリケーション」と「パッチ」というカテゴリに制限すると、そのラベルまたはラベルグループを適用できるのが「アプリケーション」および「パッチ」のみとなります。「デバイス」などの他のアイテムには適用できません。
ソフトウェアの使用のメータリング	ラベルが割り当てられたデバイスのメータリングを有効にします。この操作でメータリングが有効になるのは、そのデバイスのみです。ソフトウェアをメータリングするには、個々のアプリケーションのメータリングも有効にする必要があります。
アプリケーション制御を許可	デバイスでアプリケーション制御を有効にします。「不許可」と指定されたソフトウェアは、ラベルが適用されたデバイス上では実行できません。
ラベルグループ	（オプション）ラベルが割り当てられるラベルグループ。ラベルをラベルグループに割り当てるには、ラベルグループ フィールドの隣にある **編集** をクリックし、ラベルグループを選択します。これは、多数のラベルをサブラベルに整理する場合に便利です。例えば、ライセンスされたアプリケーションの複数のラベルを「ライセンス」という名前のラベルグループに含めることができます。また、ラベルが属するグループの制限は、ラベルに継承されます。
ユーザーの役割に限定された範囲	このラベルに関連付けられているユーザーの役割。ラベルがユーザーの役割に関連付けられているとき、ユーザーアクションは、そのラベルに関連付けられているデバイス、スクリプト、およびスケジュールに限定されます。ユーザーの役割の詳細については、ユーザーの役割の追加または編集を参照してください。

3. **保存** をクリックします。

関連トピック

アプリケーション制御ラベルのデバイスへの適用

手動ラベル詳細の表示

ラベルのメンバー、ラベルの使用の制限、代替の場所の情報などの手動ラベル詳細を表示できます。

1. ラベル詳細 ページに移動します。

a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
c. ラベル管理 パネルで、**ラベル** をクリックします。

2. ラベルグループを表示または非表示にするには、アクションの選択 メニューから **ラベルグループの表示** または **ラベルグループの非表示** を選択します。
3. ラベルのメンバーを表示するには、デバイス、ユーザー、ソフトウェア などの列にある数字をクリックします。
4. ラベル詳細を表示するには、ラベルのリンク名をクリックします。

   ラベル詳細 ページが表示されます。
5. ラベルに割り当てられたアイテム セクションで、ビューを展開したり折りたたんだりするには、セクションヘッダーの隣にある **追加** ボタンをクリックします＋。

手動ラベルの削除

手動ラベルを削除するには、そのラベルが適用されているすべてのアイテムからラベルを削除しておく必要があります。いずれかのアイテムに適用されている手動ラベルは削除できません。

また、手動ラベルにSmart LabelまたはLDAPラベルが含まれている場合、手動ラベルを削除する前にSmart LabelまたはLDAPラベルを削除する必要があります。Smart LabelまたはLDAPラベルが含まれている手動ラベルを削除することはできません。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. ラベルが適用されているすべてのアイテムからラベルを除去します。例えば、デバイスからラベルを除去する場合は、次の手順を実行します。
   a. **インベントリ** をクリックします。

      デバイス ページが表示されます。
   b. 特定基準で表示 ドロップダウンリストで、**ラベル > Label Name**を選択します。

      デバイス ページに、ラベルが適用されたアイテムが表示されます。
   c. リスト内のすべてのアイテムを選択します。
   d. **アクションの選択 > ラベルの除去 > Label Name**を選択します。
3. ラベルがすべてのアイテムから除去されたら、**ホーム > ラベル > ラベル管理** をクリックします。

   ラベル ページが表示されます。
4. 1つ以上のラベルの隣のチェックボックスをオンにします。
5. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

Smart Labelの管理

Smart Labelは、デバイス、ソフトウェア ページのアプリケーション、パッチ、検出結果、およびDellアップデートパッケージに対して追加できます。

Smart Labelは、ソフトウェアカタログ ページのアプリケーションには作成できません。

Smart Labelの追加

Smart Labelは、ラベル セクション、およびSmart Labelが使用されているリストページ（デバイス リストなど）から追加できます。

1. ラベル詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**Smart Label** をクリックします。
    d. **アクションの選択 > 新規作成 > Smart Labelタイプ** を選択します。

    アプライアンスには、選択したラベルのタイプに対する Smart Label 基準が表示されます。例えば、**新規作成 > ソフトウェアSmart Label** を選択すると、ソフトウェア基準が表示されます。**新規作成 > デバイスSmart Label** を選択すると、デバイス 基準が表示されます。
2. 使用可能なフィールドを使用して検索条件を指定します。
    - 行を追加するには、**行の追加** をクリックします。
    - ルールのサブセットを追加するには、Smart Label基準の右側にある 演算子 ドロップダウンリストで **および** または **または** を選択してから、**グループの追加** をクリックします。

3. **テスト** をクリックして、指定した条件に一致するアイテムを表示します。
4. 目的の結果が得られるまで、必要に応じて条件を調整します。
5. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。
    - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

    注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。
    - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

    注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。
6. **保存** をクリックします。

関連トピック

デバイスのラベル付けによるグループ化

検出結果とSmart Labelの使用

例：デバイスを識別するためのSmart Labelの連結

この例では、3 つの Smart Label を連結して、McAfee® VirusScan® アプリケーションがインストールされていない、Windows 7 または Windows 8 が動作しているデバイスを識別する方法を示しています。

次に、この例で作成される3つのSmart Labelを示します。

- 最初の Smart Label、Win78 は、Windows 7 または Windows 8 オペレーティングシステムがインストールされているデバイスに適用されます。このラベルの実行順序の値は1です。
- 2つ目の Smart Label「MissingVirusScan」は、VirusScan アプリケーションがインストールされていないデバイスに適用されます。このラベルの実行順序の値も1です。
- 3つ目の Smart Label「Win78MissingVirusScan」は、「Win78」と「MissingVirusScan」の両方の Smart Label が適用されているデバイスに適用されます。このラベルの実行順序の値は2で、最初の2つのラベルの後に実行されます。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. オペレーティングシステムを識別するデバイスSmart Labelを作成します。
    a. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
    b. 右側のリストの上にある **Smart Label** タブをクリックします。

        Smart Label パネルが表示されます。

    c. 以下のように、Windows 7 オペレーティングシステムに必要な条件を指定します。

    オペレーティングシステム: 名前 | 次の値を含む | Windows 7

    d. 演算子 ドロップダウンリストで **または** を選択した状態で、**行の追加** をクリックしてから、Windows 8 オペレーティングシステムで必要な条件を指定します。

    オペレーティングシステム: 名前 | 次の値を含む | Windows 8

    e. ラベルの選択 ドロップダウンリストでラベルの名前（ 「Win78」など ）を入力し、**Smart Label** をクリックします。
3. デバイス Smart Label を作成し、VirusScan アプリケーションが見つからないデバイスを検出します。
    a. デバイス ページの Smart Label パネルで、以下のように、VirusScan アプリケーションがインストールされていないデバイスを検出するために必要な条件を指定します。

    ソフトウェア：ソフトウェアタイトル | 次の値を含まない | VirusScan

    b. ラベルの選択 ドロップダウンリストでラベルの名前（ 「MissingVirusScan」など ）を入力し、**Smart Label** をクリックします。
4. 前の手順で作成した Smart Label を使用するデバイス Smart Label を作成します。
5. アプリケーションに対する Smart Label を作成します。
    a. デバイス ページの Smart Label パネルで、以下のように、「Win78」Smart Labelが適用されているデバイスを識別するための条件を指定します。

    デバイスID情報：ラベル名 | = | Win78

    b. 演算子 ドロップダウンリストで **および** を選択した状態で、**行の追加** をクリックしてから、「MissingVirusScan」Smart Labelが適用されているデバイスを識別するための条件を指定します。

    デバイスID情報：ラベル名 | = | MissingVirusScan

    c. ラベルの選択 ドロップダウンリストでラベルの名前（ 「Win78MissingVirusScan」など ）を入力し、**Smart Label** をクリックします。
6. Smart Labelを実行する順序を設定します。

a. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
b. ラベル管理 パネルで、**Smart Label** をクリックします。
c. **アクションの選択 > ラベルの優先順位 > デバイス Smart Label** を選択します。

   デバイス Smart Label の優先順位 ページが表示されます。

d. 「Win78」ラベル行の最も右側の **編集** ボタンをクリックします：。
e. 優先順位 列で、「1」を入力し、**保存** をクリックします。
f. MissingVirusScan ラベル行の最も右側の **編集** ボタンをクリックします。
g. 優先順位 列で、「1」を入力し、**保存** をクリックします。
h. 「Win78MissingVirusScan」ラベル行の最も右側の **編集** ボタンをクリックします：。
i. 優先順位 列で、「2」を入力し、**保存** をクリックします。
j. リスト下部の**保存** をクリックします。

   「Win78」ラベルと「MissingVirusScan」ラベルは、「Win78MissingVirusScan」ラベルの前に実行されるよう設定されています。これにより、Win78MissingVirusScan ラベルが実行される前に、VirusScan アプリケーションが見つからない Windows 7 デバイスと Windows 8 デバイスにラベルを割り当てることができます。

Smart Labelの編集

必要に応じて、Smart Labelで使用するSQLクエリを変更できます。

ソフトウェアSmart Labelに使用されるSQLクエリを変更すると、アイテムが新しい条件を満たすかどうかに基づいて、Smart Labelが直ちにアイテムに適用されるか、またはアイテムから除去されます。デバイスのインベントリ情報が更新されるとデバイスSmart Labelがデバイスに適用されるか、またはデバイスから除去されます。

手動でSmart LabelのSQLを編集すると、それ以降Smart Labelテンプレートを使用してラベルを編集することができなくなります。これは、テンプレートを使用してカスタムSQLを編集することができないためです。

1. ラベル詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
   c. ラベル管理 パネルで、**Smart Label** をクリックします。
   d. Smart Labelの名前をクリックするか、Smart Label名の左側にある **編集** ボタンをクリックします。

   注: Smart LabelのSQLが手動で編集されている場合、編集 ボタンは表示されません。

2. 次のいずれかを実行します。
   - メータリングを有効にする **チェックボックスをオンまたはオフにして、デバイスSmart Labelのメータリングを有効または無効にします。**
   - 割り当てられたラベル **フィールドで、Smart Labelに関連付けるラベルを選択します。**
   - **詳細 をクリックして、割り当てられたラベルの詳細ページに移動します。**
   - **Smart LabelがSmart Labelテンプレートを使用して作成され、SQLが手動で編集されていない場合は、**元のエディタを使用 **の隣のリンクをクリックします。**
   - **手動でSmart LabelのSQLを編集するには、**このエディタを使用 **の隣のリンクをクリックします。**

注意: 手動でSmart LabelのSQLを編集すると、それ以降Smart Labelテンプレートを使用してラベルを編集することができなくなります。これは、ウィザードを使用してカスタムSQLを編集することができないためです。

3. **オプション**：同じSQLクエリを使用する新しいSmart Labelを作成するには、**複製** をクリックします。
4. **保存** をクリックします。

注: 複製 をクリックしてラベルを作成する場合は、新しいラベルにのみ割り当てが可能です。

ユーザーアカウントのラベルの設定

ラベルを使用して、インベントリ セクションでデバイスやソフトウェアをグループ化する場合と同じ方法で、ユーザーアカウントをグループ化することができます。さらに、Smart Labelを使用してさまざまなレベルのアクセス権をユーザーに付与できます。例えば、ラベルを使用して、サービスデスクチケットの送信、受領、拒否、作業、および解決を実行できるユーザーを指定できます。

また、インベントリ セクション内で作成したラベルは、制限なしで作成した場合、すべてサービスデスクのユーザーラベルとして使用できます。制限のあるラベルを作成した場合は、そのラベルを修正するほか、インベントリ セクション内で制限のないラベルを作成できます。

「すべてのチケット所有者」ラベルの追加

ユーザーにサービスデスクチケットの所有権限を与えるには、「すべてのチケット所有者」ラベルを作成し、ユーザーアカウントに適用できるようにします。

1. ラベル詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
   c. ラベル管理 パネルで、**ラベル** をクリックします。
   d. **アクションの選択 > 新しい手動ラベル** を選択します。

ヒント: ラベル名にはバックスラッシュ（ \ ）を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して（ \\ ）エスケープします。

2. 次の情報を入力します。

オプション	説明
名前	ラベルの名前。この名前は、ラベル リストに表示されます。 「すべてのチケット所有者」などの名前を入力します。
説明	任意の追加情報を入力します。

3. **保存** をクリックします。

この新しいラベルは、ユーザー ページの **アクションの選択 > ラベルの適用** メニューで使用できます。ユーザーデータをインポートする際、このラベルをサービスデスクスタッフに割り当てる方法については、LDAPサーバーからのユーザーのインポートを参照してください。

パッチ適用に対する Smart Label の使用

Smart Labelを使用してパッチとデバイスを自動的にグループ化できます。パッチとデバイスに手動でラベル付けすることもできますが、Smart Label は自動的に適用および削除されるため、作業効率が向上します。

例えば、すべての Windows 7 パッチに一致する Smart Label を作成できます。これらのパッチのいずれかがアプライアンスに利用できるようになるたびに、そのパッチにラベルが適用されます。このラベルを使用してデバイスの検出と展開が自動的に実行されるようにパッチスケジュールをセットアップした場合、インベントリの Windows 7 マシンにパッチが自動的に展開されます。

P (パッチ) オペレーティングシステム　重要度 のようにラベルの体系を作成し、オペレーティングシステムおよび重要度別に整理できます。例：

- P Win7
- P Win7 Critical
- P Win7 Important
- P MS Office
- P Leopard
- P Mac10.8 Critical Test

同様に、デバイスSmart Labelを作成して、パッチをインストールする対象のデバイス (D) を指定します。

- D All Desktops
- D All Servers
- D All Laptops

アプライアンスは、デバイスへのチェックイン時にエージェントによって送信された情報を評価し、そのデータがラベル基準に一致する場合は、そのデバイスにデバイスSmart Labelを適用します。

パッチSmart Labelは、基準に一致する既存のパッチに対して直ちに適用されます。ラベルは、条件に一致する新しいパッチがダウンロードされるときに、それらのパッチに追加されます。

緊急のOSパッチに対するSmart Labelの追加

緊急のOS (オペレーティングシステム) パッチを識別するためのSmart Labelを作成することができます。

1. パッチカタログ リストに移動します。
    a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **カタログ** をクリックします。
2. 右側のリストの上にある **Smart Label** タブをクリックします。

    Smart Label パネルが表示されます。

3. Smart Labelの条件を指定します。
    a. アクティブなパッチを識別する条件を指定します。

    パッチリスト情報: ステータス | は | アクティブ

b. **行の追加** をクリックし、緊急のパッチを識別する条件を指定します。

および | パッチリスト情報: 重大度 | は | 緊急

c. **行の追加** をクリックし、Windowsパッチを識別する条件を指定します。

および | パッチリスト情報: オペレーティングシステム | は | Windows

d. **行の追加** をクリックし、オペレーティングシステムパッチを識別する条件を指定します。

および | パッチリスト情報: カテゴリ | は | OS

4. **テスト** をクリックして、検索条件に一致するアイテムを表示します。
5. 目的の結果が得られるまで、必要に応じて条件を調整します。
6. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。
   - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

     注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。
   - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。

7. **保存** をクリックします。

Smart Labelは、条件に一致する既存のパッチに対して適用されます。ラベルは、条件に一致する新しいパッチがダウンロードされるときに、それらのパッチに追加されます。

パッチをサブスクライブします。詳細については、「パッチのサブスクライブとダウンロード」を参照してください。

新しいパッチに対するSmart Labelの追加

Smart Labelを作成して、展開する必要がある新しいパッチを即座に識別することができます。

1. パッチカタログ リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
   c. パッチ管理 パネルで **カタログ** をクリックします。
2. 右側のリストの上にある **Smart Label** タブをクリックします。

   Smart Label パネルが表示されます。

3. Smart Labelの条件を指定します。
   a. 特定の日付の後に追加されたパッチを識別する条件を指定します。

   パッチリスト情報: リリース日 | > <yyyy-mm-dd形式の日付>

   b. **行の追加** をクリックし、緊急以外のパッチを識別する条件を指定します。

   および | パッチリスト情報: インパクト | 次の値ではない | 緊急

c. **行の追加** をクリックし、アクティブなパッチを識別する条件を指定します。

および | パッチリスト情報: ステータス | は | アクティブ

4. **テスト** をクリックします。

   指定した日付の後に追加された緊急以外のすべてのパッチが表示されます。

5. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。

   - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

     注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。

   - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

   注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。

6. **保存** をクリックします。

   Smart Labelは、条件に一致する既存のパッチに対して適用されます。ラベルは、条件に一致する新しいパッチがダウンロードされるときに、それらのパッチに追加されます。

パッチをサブスクライブします。詳細については、「パッチのサブスクライブとダウンロード」を参照してください。

検出結果とSmart Labelの使用

Smart Labelを使用して、特定の条件に合致する検出結果に自動的にラベルを割り当てることができます。これには、1つまたは複数のサブネットをまたぐDNS、ソケット、およびSNMPの結果が含まれます。

検出結果Smart Labelの追加

検出結果のSmart Labelを追加して、結果をグループ化し、管理できます。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **インベントリ > 検出結果** を選択して、検出結果 ページを表示します。
3. 右側のリストの上にある **Smart Label** タブをクリックして、Smart Label パネルを表示します。

4. Smart Labelの条件を選択します。
   - **一番左のドロップダウンリストから属性を選択します。例：デバイス情報：pingテスト。**
   - **中央のドロップダウンリストから条件を選択します。例：=。**
   - **次のドロップダウンリストからステータス属性を選択します。例：失敗。**
5. **テスト** をクリックして、検索条件に一致するアイテムを表示します。
6. 目的の結果が得られるまで、必要に応じて条件を調整します。
7. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。
   - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

     注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。
   - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

   注: 新しいSmart Label名を入力したら、**EnterまたはReturn**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。
8. **保存** をクリックします。

Smart Labelは、指定された条件を満たす検出結果に自動的に適用または削除されます。次回検出スケジュールが実行されたとき、検出されたデバイスにSmart Labelが適用されます。

検出結果Smart Labelの実行順序の変更

Smart Labelが実行される順序は、それらの並べ替えの値の変更により指定できます。

Smart Labelの並べ替えのデフォルト値は100です。値が小さいSmart Labelは、値が大きいSmart Labelよりも先に実行されます。詳細については、「Smart Label の実行順序の割り当て」を参照してください。

デバイスに対するSmart Labelの追加

Smart Labelを作成して、デスクトップ、サーバー、およびノートPCなどの種類別にデバイスを整理できます。デバイスに対するSmart Labelを作成すると、デバイスに展開するパッチをそれらのラベルに基づいてスケジュールできるようになります。

デスクトップに対するSmart Labelの追加

Smart Labelを作成し、デスクトップパッチが必要なデバイスを識別することができます。

1. デバイス リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. 右側のリストの上にある **Smart Label** タブをクリックします。

Smart Label パネルが表示されます。

3. Smart Labelの条件を指定します。
   a. サーバーを除外するための条件を指定します。

   オペレーティングシステム: 名前 | 次の値を含まない | サーバー

   b. **行の追加** をクリックし、ノートPCを除外するために必要な条件を指定します。

   および | 製造元とBIOS情報: シャーシタイプ | 次の値を含まない | ノートPC

   デスクトップを識別するその他の便利な検索条件には以下のものがあります。

   - システム名。すべてのデスクトップに同様の名前を付けている場合です。
   - システムモデル名。例えば、モデル名に「**XPS**」が含まれるすべてのシステムが選択されます。
   - IPアドレス、または検索条件として「**次の値を含む**」を使用したIPアドレスの一部。
   - BIOSのシリアルナンバー、または検索条件として「**部分的なシリアルナンバーを含む**」を使用することもできます。これは、連続する番号が割り当てられたデスクトップを購入した場合に便利です。詳細については、購入元のベンダーにお問い合わせください。
   - ソフトウェアタイトル。デスクトップで共通のタイトルを使用している場合です。
4. **テスト** をクリックして、検索条件に一致するアイテムを表示します。
5. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。
   - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

     注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。
   - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

   注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。
6. **保存** をクリックして、Smart Labelを作成します。
7. **オプション**：ラベル リストに新しいラベルが表示されることを確認するには、**ホーム > ラベル > Smart Label** または **ラベル管理** を選択します。

   新しいラベルは初めは空で表示されます。デバイスがインベントリ設定される際、デバイスがSmart Label条件に一致すると、そのデバイスにラベルが適用されます。
8. Smart Labelをテストします。
   a. **インベントリ > デバイス** の順にクリックして、デバイス ページを表示します。
   b. 基準に一致するが、ラベルがまだ適用されていないデバイスの名前をクリックします。
   c. デバイスの詳細 ページで **インベントリの強制** をクリックします。

      Smart Labelが正しく機能している場合、デバイスがチェックインされ、そのデバイスにラベルが適用されます。

   強制的なインベントリ更新 は、エージェント管理対象デバイスへのエージェントのメッセージプロトコル接続がアクティブな場合、またはエージェント不要デバイスではデバイスが到達可能な場合のみ使用できます。

サーバーに対するSmart Labelの追加

Smart Labelを作成し、サーバーパッチが必要なデバイスを識別することができます。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. 右側のリストの上にある **Smart Label** タブをクリックします。

    Smart Label パネルが表示されます。

3. 検索条件を指定します。
    a. サーバーを識別するための条件を指定します。

    オペレーティングシステム: 名前 | 次の値を含む | サーバー

    b. **行の追加** をクリックし、ノートPCを除外するために必要な条件を指定します。

    および | 製造元とBIOS情報: シャーシタイプ | 次の値を含まない | ノートPC

    サーバーを識別するその他の便利な検索条件には以下のものがあります。

    - システム名。すべてのサーバーに同様の名前を付けている場合です。
    - IPアドレス、または検索条件として「**次の値を含む**」を使用したIPアドレスの一部。
    - BIOSのシリアルナンバー、または検索条件として「**部分的なシリアルナンバーを含む**」を使用することもできます。これは、連続する番号が割り当てられたサーバーを購入した場合に便利です。詳細については、購入元のベンダーにお問い合わせください。
    - ソフトウェアタイトル。サーバーで共通のタイトルを使用している場合です。
4. **テスト** をクリックして、検索条件に一致するアイテムを表示します。
5. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。
    - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

        注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。
    - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

    注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。
6. **保存** をクリックします。
7. **オプション**：ラベル リストに新しいラベルが表示されることを確認するには、**ホーム > ラベル > Smart Label** または **ラベル管理** を選択します。

    新しいラベルは初めは空で表示されます。デバイスがインベントリ設定される際、デバイスがSmart Label条件に一致すると、そのデバイスにラベルが適用されます。
8. Smart Labelをテストします。

a. **インベントリ > デバイス** の順にクリックして、デバイス ページを表示します。
b. 基準に一致するが、ラベルがまだ適用されていないデバイスの名前をクリックします。
c. デバイスの詳細 ページで **インベントリの強制** をクリックします。

Smart Labelが正しく機能している場合、デバイスがチェックインされ、そのデバイスにラベルが適用されます。

強制的なインベントリ更新 は、エージェント管理対象デバイスへのエージェントのメッセージプロトコル接続がアクティブな場合、またはエージェント不要デバイスではデバイスが到達可能な場合のみ使用できます。

ノートPCに対するSmart Labelの追加

Smart Labelを作成し、ノートPCパッチが必要なデバイスを識別することができます。

1. デバイス リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. 右側のリストの上にある **Smart Label** タブをクリックします。

   Smart Label パネルが表示されます。

3. 検索条件を指定します。
   a. サーバーを除外するための条件を指定します。

   オペレーティングシステム: 名前 | 次の値を含まない | サーバー

   b. **行の追加** をクリックし、ノートPCを識別するために必要な条件を指定します。

   および | 製造元とBIOS情報: シャーシタイプ | 次の値を含む | ノートPC

   ノートPCを識別するその他の便利な検索条件には以下のものがあります。

   - システム名、すべてのノートPCに同様の名前を付けている場合です。
   - IPアドレス、または検索条件として「**次の値を含む**」を使用したIPアドレスの一部。
   - BIOSのシリアルナンバー、または検索条件として「**部分的なシリアルナンバーを含む**」を使用することもできます。これは、連続する番号が割り当てられたノートPCを購入した場合に便利です。詳細については、購入元のベンダーにお問い合わせください。
   - ソフトウェアタイトル。ノートPCで共通のタイトルを使用している場合です。
4. **テスト** をクリックして、検索条件に一致するアイテムを表示します。
5. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。

   - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

     注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。

   - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。

6. **保存** をクリックして、Smart Labelを作成します。
7. **オプション**：ラベル リストに新しいラベルが表示されることを確認するには、**ホーム > ラベル > Smart Label** または **ラベル管理** を選択します。

   新しいラベルは初めは空で表示されます。デバイスがインベントリ設定される際、デバイスがSmart Label条件に一致すると、そのデバイスにラベルが適用されます。
8. Smart Labelをテストします。
   a. **インベントリ > デバイス** の順にクリックして、デバイス ページを表示します。
   b. 基準に一致するが、ラベルがまだ適用されていないデバイスの名前をクリックします。
   c. デバイスの詳細 ページで **インベントリの強制** をクリックします。

      Smart Labelが正しく機能している場合、デバイスがチェックインされ、そのデバイスにラベルが適用されます。

   強制的なインベントリ更新 は、エージェント管理対象デバイスへのエージェントのメッセージプロトコル接続がアクティブな場合、またはエージェント不要デバイスではデバイスが到達可能な場合のみ使用できます。

Smart Label の実行順序の割り当て

Smart Labelsを順番に実行するには、Smart Labelのプロパティで実行順序を割り当てます。

Smart Labelの実行順序の割り当ては、特定のSmart Labelを他のSmart Labelより先に実行したいときに役立ちます。例えば、あるデバイスグループを識別するSmart Labelがあったとします。1番目のラベルが適用されたデバイスグループを、2番目のSmart Labelを使用して、さらに絞り込む場合には、1番目のSmart Labelが2番目より先に実行されるよう実行順序を設定することができます。Smart Labelの並べ替えのデフォルト値は100です。値が小さいSmart Labelは、値が大きいSmart Labelよりも先に実行されます。

1. Smart Label リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
   c. ラベル管理 パネルで、**Smart Label** をクリックします。
2. アクションの選択 メニューの 優先順位 セクションで、実行順序を変更するラベルの種類を選択します。

   Order（ 優先順位 ）ページが開き、選択したタイプのすべての Smart Label が表示されます。
3. Smart Labelの実行順序を変更するには：
   a. 優先順位 列の右側の **編集** ボタンをクリックします：  。
   b. 並べ替えの値を入力し、**保存** をクリックします。
4. **保存** をクリックします。

Smart Labelの削除

Smart Labelの削除は、管理対象インストールなどのタスクで使用されるラベルを保存しているときに、Smart Labelを大きく変更する必要がある場合に役立ちます。

例えば、Smart Labelからすべての条件を削除してから、そのコンテナラベルに新しい条件を再適用することができます。つまり、これにより、管理対象インストールに必要な既存のコンテナラベルを使用して新しいSmart Labelが作成されます。

Smart Labelの削除によって、そのSmart Labelに関連付けられた条件が除去されますが、そのSmart Labelに関連付けられている他のラベルは削除されません。

1. Smart Label リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**Smart Label** をクリックします。
2. 1つ以上のSmart Labelの隣のチェックボックスをオンにします。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

ラベルグループの管理

ラベル セクションでラベルグループを管理できます。

ラベルグループの追加、表示、または編集

ラベルグループは、必要に応じて追加、表示、または編集できます。

1. ラベルグループの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**ラベル** をクリックします。
    d. ラベルグループの詳細 ページを表示するには、次のいずれかを実行します。
    - ラベルグループの名前をクリックします。
    - **アクションの選択** > **新しいラベルグループ** を選択します。
2. 次の情報を入力します。

オプション	説明
名前	ラベルグループの名前。
説明	任意の追加情報を入力します。
ラベルグループ使用の制限対象	（ オプション ）ラベルまたはラベルグループを適用できるアイテムのカテゴリ。ラベルの使用を制限しない場合は、あらゆるアイテムにラベルまたはラベルグループを適用できます。ただし、ラベルまたはラベルグループを例えば「アプリケーション」と「パッチ」というカテゴリに制限すると、そのラベルまたはラベルグループを適用できるのが「アプリケーション」および「パッチ」のみとなります。「デバイス」などの他のアイテムには適用できません。

オプション	説明
ソフトウェアの使用のメータリング	このチェックボックスをオンまたはオフにして、デバイスラベルのメータリングを有効または無効にします。
アプリケーション制御を許可	デバイスでアプリケーション制御を有効にします。「不許可」と指定されたソフトウェアは、ラベルが適用されたデバイス上では実行できません。
ラベルグループ	（オプション）ラベルが割り当てられるラベルグループ。ラベルをラベルグループに割り当てるには、ラベルグループ フィールドの隣にある **編集** をクリックし、ラベルグループを選択します。これは、多数のラベルをサブラベルに整理する場合に便利です。例えば、ライセンスされたアプリケーションの複数のラベルを「ライセンス」という名前のラベルグループに含めることができます。また、ラベルが属するグループの制限は、ラベルに継承されます。

3. **保存** をクリックします。

関連トピック

アプリケーション制御ラベルのデバイスへの適用

ラベルグループへのラベルの割り当てまたはラベルグループからのラベルの削除

ラベルはグループに割り当てることができます。また、複数のラベルグループに関連付けることもできます。ラベルが属するグループの制限は、ラベルに継承されます。

1. ラベル リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**ラベル** をクリックします。
2. グループに割り当てるラベルの隣のチェックボックスをオンにします。
3. **アクションの選択 > ラベルグループを適用** を選択し、ラベルを割り当てるラベルグループを選択します。

    アプライアンス上にラベルグループがある場合にのみ、**ラベルグループの適用** が表示されます。

    ラベルグループの名前が、選択したラベルの名前の隣に表示されます。
4. グループから削除するラベルの隣のチェックボックスをオンにします。
5. **アクションの選択 > ラベルグループを除去** を選択し、ラベルを除去するラベルグループを選択します。

    アプライアンス上にラベルグループがある場合にのみ、**ラベルグループを削除** が表示されます。

    ラベルグループの名前は、選択したラベルの名前の隣に表示されなくなります。

ラベルグループの削除

ラベルグループは、ラベルまたはサブグループが含まれない場合にのみ、削除できます。

ラベルグループにラベルまたはサブグループが含まれる場合は、グループを削除する前に、ラベルまたはサブグループを除去する必要があります。

1. ラベル リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**ラベル** をクリックします。
2. ラベルグループにラベルまたはサブグループが含まれていない場合：
    a. グループ名の隣のチェックボックスをオンにします。
    b. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

    ラベルグループが除去されます。
3. グループにラベルまたはサブグループが含まれている場合：
    a. ラベルグループの名前をクリックして、ラベルグループの詳細 ページを表示します。
    b. ページの下部の ラベルに割り当てられたアイテム セクションで、ラベル セクションを展開するため、**追加** ボタンをクリックします。
    c. ラベルまたはラベルグループの名前をクリックして、ラベルまたはラベルグループの詳細ページを表示します。
    d. ラベルグループ フィールドで **編集** をクリックします。
    e. Assign to Label Group（ ラベルグループへの割り当て ）ウィンドウで、削除するラベルの隣にある **削除** ボタンをクリックします。
    f. **OK** をクリックしてから、**保存** をクリックします。
    g. ラベルグループからすべてのラベルおよびサブグループを除去したら、ラベル ページでラベルグループの名前の隣にあるチェックボックスをオンにします。
    h. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

LDAPラベルの管理

ラベル セクションで LDAP ラベルを管理します。

LDAPラベルの追加または編集

LDAPラベルは、必要に応じて追加および編集できます。LDAPラベルを有効化する前に、LDAPラベルをテストするようにしてください。

1. LDAPラベルの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**LDAPラベル** をクリックします。
    d. LDAPラベルの詳細 ページを表示するには、次のいずれかを実行します。

    - LDAPラベルの名前をクリックします。
    - **アクションの選択** > **新規作成** を選択します。
2. 次の情報を入力します。

オプション	説明
有効	アプライアンスがLDAPラベルを実行できるようにします。 **注:** 有効 チェックボックスは、LDAPラベルをテストして、LDAP条件が適切であり、ラベルが予測どおりに適用されていることを確認した後にのみオンにします。
タイプ	LDAPラベルのタイプ。次の2つのタイプのLDAPラベルがあります。 • **デバイス**: デバイスレコードに適用されるラベル。これは、名前、説明、およびその他のLDAP条件によってデバイスを自動的にグループ化する場合に役立ちます。デバイスをインベントリに設定すると、このクエリが LDAP サーバーに対して実行されます。これにより、LDAP 検索フィルタ条件に一致する値を持つ LDAP 属性がデバイスに含まれているかどうかが判別されます。結果が返された場合、デバイスに Associated Label Name（関連するラベル名）フィールドで指定されたラベルが割り当てられます。 LDAP ラベルをデバイスに適用するには、デバイスラベルに 1 つ以上のアプライアンス変数（KBOX_COMPUTER_NAME など）を含める必要があります。この変数は、LDAP ラベルを処理する際に、LDAP ディレクトリで属性の値を比較して、LDAP オブジェクトのアプライアンスオブジェクトとの間に関係が存在するかどうかを判別するために使用されます。詳細については、「LDAP 変数」を参照してください。 • **ユーザー**: ユーザーレコードに適用されるラベル。これは、ドメイン、場所、予算コード、またはその他のLDAP条件によってユーザーを自動的にグループ化する場合に役立ちます。ユーザーが手動またはスケジュールに従ってアプライアンスにインポートされると、LDAPラベルがユーザーレコードに適用されるか、ユーザーレコードから除去されます。ユーザーラベルに KBOX_USER_NAME などのユーザー変数を使用できます。この変数は、LDAP ラベルを処理する際に、LDAP ディレクトリで属性の値を比較して、LDAP オブジェクトのアプライアンスオブジェクトとの間に関係が存在するかどうかを判別するために使用されます。詳細については、「LDAP 変数」を参照してください。 **ヒント:** ラベルをテストする際には、KBOX_ 変数を環境に合わせて適切な値に置き換えてから **テスト** を選択してください。

オプション	説明
関連するラベル	このLDAPラベルに関連付ける手動ラベル、またはコンテナラベルです。各LDAPラベルには、関連付けられたラベルが必要です。
関連するラベルの説明	関連するラベル名 フィールドで選択したラベルからのノート。
サーバー	LDAPサーバーのIPアドレスまたはホスト名。IPアドレスが有効でない場合は、タイムアウトするまで待たなければならず、その結果LDAP認証中にログイン遅延が発生します。 **注:** SSL経由で接続するには、IPアドレスまたはホスト名を使用します。例：ldaps://hostname。
ポート	LDAPポート番号。通常は、389（LDAP）または636（セキュアLDAP）です。
ベースDN	アカウントの検索に使用される基準。 この基準によって、LDAPまたはActive Directory構造における場所またはコンテナを指定します。この基準には、認証するすべてのユーザーが含まれる必要があります。基準を満たすOU、DC、またはCNの最も明確な組み合わせを入力します（一番左は最も限定的、一番右は最も一般的です）。例えば、このパスが、認証対象となるユーザーが属するコンテナを指している場合は、次の通りです。 OU=end_users, DC=company,DC=com。
高度な検索	検索フィルタ。例： (&(sAMAccountName=KBOX_USER_NAME)(memberOf=CN=financial,DC=example,DC=com))
資格情報	アプライアンスがLDAPサーバにログインして、アカウントを読み取るために必要なアカウントのLDAP 資格情報です。リストから選択するか、新しい LDAP 資格情報を作成します。LDAP の詳細については、「LDAP ユーザーとパスワード資格情報の追加および編集」を参照してください。

ベースDN および 高度な検索 の情報が分からない場合は、LDAP ブラウザを使用します。詳細については、「LDAPブラウザの使用」を参照してください。

注: NOT検索フィルタは、次のように書式設定されます：(!(sAMAccountName=David))。NOTを使用する他のいかなる書式もエラーとなります。

3. **テスト** ボタンをクリックして、新しいラベルをテストします。必要に応じてラベルのパラメータを変更し、もう一度テストします。
4. LDAPラベルを使用する準備ができた場合は、有効 チェックボックスをオンにします。準備ができていない場合は、そのラベルを有効にせず、保存します。
5. **保存** をクリックします。

関連トピック

LDAPブラウザの使用

LDAPラベルの有効化

LDAP ラベルを追加してテストしたら、有効化することができます。デバイスがアプライアンスにチェックインすると、有効化されたデバイスLDAPラベルがLDAPサーバーに対して実行されます。ユーザーが手動またはスケジュールに従ってインポートされると、有効化されたユーザーLDAPラベルがLDAPサーバーに対して実行されます。

LDAP ラベルの追加およびテスト詳細については、「LDAPラベルの追加または編集」を参照してください。

1. LDAPラベルの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**LDAPラベル** をクリックします。
    d. LDAPラベルの名前をクリックします。
2. 有効 チェックボックスをオンにします。
3. **保存** をクリックします。

LDAPラベルの削除

LDAPラベルの削除によって、そのLDAPラベルに関連付けられた条件が除去されますが、そのLDAPラベルに関連付けられている他のラベルは削除されません。

1. LDAPラベルの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**LDAPラベル** をクリックします。
2. 1つ以上のLDAPラベルの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

LDAPブラウザの使用

LDAP ブラウザを使用すると、Active Directory サーバーなどの LDAP サーバー上にあるデータを参照および検索できます。

LDAPブラウザを使用するには、LDAPサーバーにログオンするためのバインドDNとLDAPパスワードが必要です。

LDAP ブラウザは、LDAP クエリの ベースDNの検索 フィールドと 検索フィルタ フィールドに情報を入力する必要がある場合に便利です。

1. LDAPブラウザ に移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。

c. ラベル管理 パネルで、**LDAPブラウザ** をクリックします。

2. 「LDAPサーバー」の詳細を指定します。

オプション	説明
IPアドレスまたはホスト名	LDAPサーバーのIPアドレスまたはホスト名。IPアドレスが有効でない場合は、タイムアウトするまで待たなければならず、その結果LDAP認証中にログイン遅延が発生します。 **注:** SSL経由で接続するには、IPアドレスまたはホスト名を使用します。例：ldaps://hostname。
ポート	LDAPポート番号。通常は、389（LDAP）または636（セキュアLDAP）です。
ログイン	アプライアンスが LDAP サーバに ログインして、アカウントを読み取るために必要なアカウントの資格情報です。例： LDAP Login:CN=service_account,CN=Users, DC=company,DC=com。 ユーザーとパスワードが指定されていない場合、ツリー検索は実行されません。LDAPラベルごとに、異なるLDAPまたはActive Directoryサーバーに接続することが可能です。
パスワード	アプライアンスが LDAP サーバに ログインするために必要となるアカウントのパスワードです。

3. **テスト** をクリックします。

   LDAP サーバーへの接続が正常に完了すると、**次へ** ボタンがアクティブになります。

   操作が失敗した場合は、次の項目を確認します。

   - IPアドレスまたはホスト名が正しい。
   - LDAPサーバーが稼働している。
   - ログイン資格情報が正しい。

4. **次へ** をクリックします。

   Narrow the Search（検索の絞り込み）ウィンドウが表示されます。

5. 画面の下部に表示される結果の数を制限するには、検索フィルタを入力します。

オプション	説明
LDAP 簡易検索	検索する文字列を入力します。
検索先	必要に応じて、適切なオプションを選択し、インデックスありのフィールドを検索するかインデックスなしのフィールドを検索するかを示します。
その他の属性	検索する Active Directory フィールドのコンマ区切りリストを入力します。

オプション	説明
	注: 検索では、指定されたフィールドが実際に Active Directory に存在するかどうかを確認しません。

6. **開始** をクリックします。

   検索結果は、画面下部、左パネルに表示されます。
7. 子ノードをクリックし、その属性を表示します。

   属性は右のパネルに表示されます。

ユーザーアカウント、LDAP認証、およびSSOの設定

ユーザーアカウントの設定と管理、LDAP情報を使用したユーザーの認証、およびユーザーに対するシングルサインオン（SSO）の有効化を行うことができます。

ユーザーアカウントおよびユーザー認証について

ユーザーアカウントは、アプライアンス上で作成および管理することができます。これらのアカウントを使用して**管理者コンソール**と**ユーザーコンソール**にアクセスできるユーザーは、**ローカルで認証されている**と言うことができます。

ローカル認証の代替方法として、外部LDAPサーバーを使用した外部認証を設定することもできます。詳細については、「LDAPサーバーを使用したユーザー認証」を参照してください。

ローカルで認証されたユーザーアカウントのタイプは次の通りです。

- **システムレベルユーザーアカウント**。ユーザーが**システム管理コンソール**にログインしてアプライアンスのホスト名やネットワーク設定などのアプライアンス設定を管理できるようにするアカウント。システムレベルのユーザーアカウントには、アプライアンスのデフォルトの**管理者**アカウントが含まれています。これらのアカウントを使用すると、組織レベルのコンポーネント（admiui）および**ユーザーコンソール**にアクセスすることもできます。詳細については、「システムレベルユーザーアカウントの管理」を参照してください。
- **組織ユーザーアカウント**。ユーザーが**管理者コンソール**組織レベル（管理者コンソール）にログインして、組織固有のコンポーネントを管理できるようにするアカウント。これらのコンポーネントには、ユーザーの役割に応じて、インベントリ、資産、配布、スクリプト、セキュリティ、サービスデスク、**ユーザーコンソール**などが含まれます。詳細については、「組織ユーザーアカウントの管理」を参照してください。

ロケール設定について

ロケール設定に基づいて、インターフェイスのテキストに使用される言語が決定されます。ロケール設定は、**コマンドラインコンソール**、**管理者コンソール**、および**ユーザーコンソール**に選択できます。

詳細については、「ロケール設定の構成」を参照してください。

システムレベルユーザーアカウントの管理

システムレベルのユーザーアカウントを使用すると、ユーザーは**システム管理コンソール**にログインして、アプライアンスのホスト名やネットワーク設定などのアプライアンス設定を管理できます。システムレベルのユーザーアカウントは、アプライアンスにおいてローカルでユーザーを認証します。

ユーザー認証のために LDAP サーバーを使用するには、LDAPサーバーを使用したユーザー認証を参照してください。

注: デフォルトの **admin** アカウントを削除することはできません。**admin** アカウントのユーザー名を変更するか、アプライアンスで無効にすることができます（LDAP または SAML 設定が必要です）。**admin** アカウントのパスワードを変更することもできます。詳細については、「システムレベルのユーザーアカウントの追加または編集」を参照してください。また、アプライアンスで組織コンポーネントが有効になっている場合、または複数の K シリーズアプライアンスをリンクする場合、**admin** アカウントのログインとパスワードを変更する際には注意する必要があります。**システム管理コンソール**の右上隅にあるドロップダウンリストを使用して、システムレベル、組織、およびリンク先アプライアンスの **admin** アカウントログイン名とパスワードを切り替える場合、リンクされたすべてのアプライアンスおよび組織でログイン名とパスワードが同じである必要があります。ドロップダウンリストには、**admin** アカウントのログイン名とパスワードが同じアプライアンスおよび組織のみが表示されます。

注: 詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。

システムレベルのユーザーアカウントの追加または編集

必要に応じてシステムレベルのユーザーアカウントを追加または編集できます。これらのアカウントを使用すると、ユーザーは**システム管理コンソール**にログインして、アプライアンス設定を管理できます。

アプライアンス上で組織コンポーネントが有効化されている場合は、組織固有のユーザーアカウントを追加または編集することもできます。詳細については、「組織ユーザーアカウントの管理」を参照してください。

注: デフォルトの **admin** アカウントを削除することはできません。**admin** アカウントのユーザー名を変更するか、アプライアンスで無効にすることができます（LDAP または SAML 設定が必要です）。**admin** アカウントのパスワードを変更することもできます。また、アプライアンスで組織コンポーネントが有効になっている場合、または複数の K シリーズアプライアンスをリンクする場合、**admin** アカウントのログインとパスワードを変更する際には注意する必要があります。**システム管理コンソール**の右上隅にあるドロップダウンリストを使用して、システムレベル、組織、およびリンク先アプライアンスの **admin** アカウントログイン名とパスワードを切り替える場合、リンクされたすべてのアプライアンスおよび組織でログイン名とパスワードが同じである必要があります。ドロップダウンリストには、**admin** アカウントのログイン名とパスワードが同じアプライアンスおよび組織のみが表示されます。

注: 詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。

1. 管理者の詳細 ページに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左のナビゲーションバーで **設定**、**管理者** の順にクリックします。
   c. 管理者の詳細 ページを表示するには、次のいずれかを実行します。
   - 管理者の名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。
2. ユーザー情報を入力または変更します。

オプション	説明
ログイン	（必須）ユーザーがログインページのログインID フィールドに入力する名前。デフォルトの admin

オプション	説明
	アカウントを編集している場合は、ログイン名を変更できますが、admin アカウントのログイン名とパスワードを変更するときは注意が必要です。**システム管理コンソール**の右上隅にあるドロップダウンリストを使用して、システムレベル、組織、およびリンク先アプライアンスの admin アカウントを切り替える場合、リンクされたすべてのアプライアンスおよび組織で管理者アカウントのパスワードが同じである必要があります。ドロップダウンリストには、admin アカウントのログイン名とパスワードが同じアプライアンスおよび組織のみが表示されます。
名前	ユーザーのフルネーム。
プライマリEメール	ユーザーのプライマリ E メールアドレス。
追加のEメール	ユーザーに関連付けられている追加の E メールアドレス。
ドメイン	ユーザーに関連付けられるActive Directoryドメイン。
予算コード	ユーザーに関連付けられる財務部コード。
場所	ユーザーが所在している職場または建物の名前。
勤務先、自宅、携帯、およびポケベルの電話番号	ユーザーの電話番号。
カスタム1〜4	ユーザーまたはユーザーのアカウントに関する追加情報。
パスワードおよびパスワードの確認入力	（必須）ユーザーがログイン時に入力するパスワード。 アプライアンスで組織コンポーネントが有効になっている場合、または複数の K シリーズアプライアンスをリンクする場合、**管理者**アカウントのパスワードを変更する際には注意する必要があります。**管理者コンソール**の右上隅にあるドロップダウンリストを使用して、システムレベル、組織、およびリンク先アプライアンスの **admin** アカウントを切り替える場合、これらのアカウントのパスワードは同じにする必要があります。ドロップダウンリストには、adminアカウントが同じ組織とアプライアンスのみ表示されます。
役割	（必須）役割は、**管理者コンソール**および**ユーザーコンソール**へのアクセスを制御するために、ユー

オプション	説明
	ザーアカウントに割り当てられます。デフォルトの管理者役割は次のとおりです。 • **管理者**: このユーザーは、**管理者コンソール**にログインして、すべての機能にアクセスできます。 • **読み取り専用の管理者**: このユーザーは、**管理者コンソール**にログインできますが、設定の変更はできません。 デフォルトadmin管理者の役割を変更することはできません。
デフォルトにする	選択した役割を新しいユーザーのデフォルトの役割にする場合に、このオプションを選択します。
ロケール	ユーザーの**ユーザーコンソール**および**管理者コンソール**に使用するロケール。デフォルトadmin管理者のロケールを変更することはできません。
KACEセキュリティ通知を有効にする	Quest 管理者のEメールアドレスにセキュリティ通知を送信できるようにします。この機能は、システムレベルの管理者アカウントでのみ使用可能です。管理者レベルの管理者アカウントまたは管理者以外のユーザーアカウントでは使用できません。
KACE販売およびマーケティング通知を有効にする	Questがこの管理者のEメールアドレスに販売およびマーケティング通知を送信できるようにします。この機能は、システムレベルの管理者アカウントでのみ使用可能です。管理者レベルの管理者アカウントまたは管理者以外のユーザーアカウントでは使用できません。

3. **保存** をクリックします。

アプライアンス管理者のEメール通知の管理

Questでは、Eメールを使用して、セキュリティに関する問題と販売およびマーケティングに関する情報をアプライアンスの管理者に通知します。システムレベル（ アプライアンス ）の管理者アカウントのEメール通知を有効または無効にすることができます。

Eメール通知は、アプライアンスの管理者アカウントでのみ使用可能です。管理者以外のユーザーは通知を使用することはできません。アプライアンス上で組織コンポーネントが有効化されている場合、通知は、組織内の管理者レベルの管理者アカウントに対しては使用不可です。

1. ユーザー詳細 ページまたは 管理者の詳細 ページに移動します。

   ユーザー詳細 ページに移動するには：

   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。

c. ユーザー詳細 ページを表示するには、次のいずれかを実行します。

- ユーザーの名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

Administrator Detail（管理者の詳細）ページに移動するには、次の手順を実行します。

a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
b. 左のナビゲーションバーで **設定**、**管理者** の順にクリックします。
c. 管理者の詳細 ページを表示するには、次のいずれかを実行します。

- 管理者の名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

2. ユーザー情報、Eメールアドレス、および役割を確認します。

注: 通知を有効にするには、ユーザーはアプライアンスの管理者役割を持っている必要があります。

3. フォームの下部で、通知フィールドの横のチェックボックスをオンまたはオフにして、管理者のEメール通知を有効または無効にします。

オプション	説明
KACEセキュリティ通知を有効にする	Quest 管理者のEメールアドレスにセキュリティ通知を送信できるようにします。この機能は、システムレベルの管理者アカウントでのみ使用可能です。管理者レベルの管理者アカウントまたは管理者以外のユーザーアカウントでは使用できません。
KACE販売およびマーケティング通知を有効にする	Questがこの管理者のEメールアドレスに販売およびマーケティング通知を送信できるようにします。この機能は、システムレベルの管理者アカウントでのみ使用可能です。管理者レベルの管理者アカウントまたは管理者以外のユーザーアカウントでは使用できません。

4. **保存** をクリックします。

システムレベルユーザーアカウントの削除

アプライアンス上で組織コンポーネントが有効化されている場合、システムレベルでユーザーアカウントを削除できます。このオプションは、アプライアンス上で組織コンポーネントが有効化されている場合にのみ使用可能です。

アプライアンスで組織コンポーネントが有効になっていない場合は、組織ユーザーアカウントの管理の指示に従ってください。

注: デフォルトの admin アカウントを削除することはできません。

1. 管理者 リストに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左のナビゲーションバーで **設定**、**管理者** の順にクリックします。
2. 1つ以上のアカウントの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

組織ユーザーアカウントの管理

組織ユーザーアカウントが提供する資格情報を使用することで、ユーザーはアカウントに割り当てられたユーザーの役割に基づいて**管理者コンソール**または**ユーザーコンソール**にログインし、コンポーネントにアクセスできます。ユーザーの役割とユーザーアカウントは、必要に応じて追加または編集できます。

組織ユーザーアカウントは、アプライアンスにおいてローカルでユーザーを認証します。ユーザー認証のために LDAP サーバーを使用するには、LDAPサーバーを使用したユーザー認証を参照してください。

ユーザーの役割の追加または編集

ユーザーの役割は、**管理者コンソール**および**ユーザーコンソール**へのアクセスを制御するために、ユーザーアカウントに割り当てられます。ユーザーの役割は、必要に応じて追加または編集できます。

ただし、事前定義した次の役割は編集できません。管理者、アクセス権限なし、読み取り専用の管理者、およびユーザー。

アプライアンス上で組織コンポーネントが有効化されている場合、ユーザーの役割に使用できる権限は、組織に割り当てられた組織の役割によって異なります。詳細については、「組織の役割とユーザーの役割の管理」を参照してください。

1. 役割詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**役割** の順にクリックします。
    c. 役割詳細 ページを表示するには、次のいずれかを実行します。
    - 役割の名前をクリックします。
    - **アクションの選択** > **新規作成** を選択します。
2. 名前 フィールドで、「サービスデスクスタッフ」などの名前を入力します。

    定義済みの役割の名前を変更することはできません。
3. この役割を新しい役割に対するデフォルトの役割にしたい場合は、**新規ユーザーのデフォルトのロール** チェックボックスをオンにします。
4. 説明 フィールドで、役割の簡単な説明を入力します（ 「サービスデスク管理者に使用」など ）。

    この説明は、役割 リストに表示されます。定義済みの役割の説明を変更することはできません。
5. 管理者コンソール権限を設定します。
    a. 管理コンソールの権限 の下で、**すべて展開** をクリックします。
    b. 必要に応じて、各コンポーネントの権限を設定します。
6. ユーザーコンソール権限を設定します。
    a. エンドユーザーコンソール権限 の下で、**ユーザーコンソール** をクリックして、権限のリストを展開します。
    b. 必要に応じて、各コンポーネントの権限を設定します。
7. デバイスの範囲 の下で、この役割でフルアクセスを与えるデバイスを指定します。

    役割ベースのユーザーアクセスでは、管理者はユーザーの役割に関連付けられているデバイスに基づいてユーザーへのアクションを制限できます。特定の役割を担うユーザー（ 範囲を限定したユーザー ）のいるすべてのデバイスへのアクセスを付与することも、ラベルに関連付けられている選択されたデバイスのみへのアクセスを付与することもできます。

    ヒント: ラベルは、デバイスなどのアイテムをグループとして管理できるよう、整理および分類できるコンテナです。ラベルの詳細については、ラベルについてを参照してください。

ヒント: Smart Label が役割と関連付けられた場合、これは Smart Label リストの 名前 列に表示されます。

- アプライアンスまたは組織（該当する場合）のすべてのデバイスにアクセスを付与するには、**全デバイス** を選択します。
- 特定のラベルに関連付けられたデバイスのみにアクセスを付与するには、**関連ラベルの管理** をクリックし、必要に応じて、ラベルを選択します。

8. **保存** をクリックします。

役割 ページが表示されます。この役割を割り当てられたユーザーがログインすると、アプライアンスのコンポーネントバーに使用可能な機能が表示されます。

ユーザーの役割の削除

ユーザーの役割は、どのユーザーにも割り当てられておらず、かつ事前定義されたユーザーの役割でない場合に限り、削除することができます。アプライアンスで組織コンポーネントが有効化されている場合は、各組織のユーザーの役割を個別に削除します。

注: 1 つまたは複数のラベルに関連付けられているユーザーの役割は削除できません。

1. 役割 リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**役割** の順にクリックします。
2. 1つ以上の役割の隣のチェックボックスをオンにします。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

組織ユーザーアカウントの追加または編集

組織レベルでユーザーアカウントを追加または編集できます。アプライアンスで組織コンポーネントが有効化されている場合は、各組織のユーザーアカウントを個別に追加または編集します。

1. ユーザー詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
   c. ユーザー詳細 ページを表示するには、次のいずれかを実行します。
   - ユーザーの名前をクリックします。
   - **アクションの選択** > **新規作成** を選択します。

   注: お使いのシステムでは最大50の組織を使用できます。これを上回る組織を作成しようとすると、エラーメッセージが表示されます。
2. 次の情報を追加または編集します。

オプション	説明
ログイン	（必須）ユーザーがログインページのログインID フィールドに入力する名前。デフォルトの admin アカウントを編集している場合は、ログイン名を変更できますが、admin アカウントのログイン名とパスワードを変更するときは注意が必要です。**管理者コ**

オプション	説明
	ンソールの右上隅にあるドロップダウンリストを使用して、システムレベル、組織、およびリンク先アプライアンスの admin アカウントを切り替える場合、リンクされたすべてのアプライアンスおよび組織で管理者アカウントのパスワードが同じである必要があります。ドロップダウンリストには、admin アカウントのログイン名とパスワードが同じアプライアンスおよび組織のみが表示されます。
名前	ユーザーのフルネーム。
Eメール	ユーザーのプライマリメールアドレス。
追加のEメール	ユーザーがアクセスする1つまたは複数の追加のEメール。エントリが複数ある場合は、コンマで区切ります。
ドメイン	ユーザーに関連付けられるActive Directoryドメイン。
予算コード	ユーザーに関連付けられる財務部コード。
場所	ユーザーが所在している職場または建物の名前。表示されるドロップダウンリストから場所をクリックして選択します。
勤務先、自宅、携帯、およびポケベルの電話番号	ユーザーの電話番号。
カスタム1〜4	ユーザーまたはユーザーのアカウントに関する追加情報。
パスワードおよびパスワードの確認入力	（必須）ユーザーがログイン時に入力するパスワード。
役割	（必須）ユーザーに関連付けられる役割。役割は、**管理者コンソール**および**ユーザーコンソール**へのアクセスを制御するために、ユーザーアカウントに割り当てられます。デフォルトのシステム役割は次のとおりです。 • **管理者**: このユーザーは、**管理者コンソール**にログインして、すべての機能にアクセスできます。 • **読み取り専用の管理者**: このユーザーは、**管理者コンソール**にログインできますが、設定の変更はできません。 • **管理者コンソールのみ**：このユーザーは、**管理者コンソール**にのみログインできます。 • **アクセス権限なし**：ユーザーは、**管理者コンソール**または**ユーザーコンソール**にはログインできません。

オプション	説明
	デフォルトadmin管理者の役割を変更することはできません。
ロケール	ユーザーが**管理者コンソール**または**ユーザーコンソール**にログインするときに表示されるロケール。
ラベルへの割り当て	ユーザーに関連付けられるラベル。
デフォルトキュー	ユーザーが送信したサービスデスクチケットにデフォルトとして使用されるキュー。
モバイルデバイスによるアクセス	ユーザーに対してモバイルデバイスによるアクセスを有効または無効にします。モバイルデバイスによるアクセスにより、iOS または Android のスマートフォンまたはタブレットで KACE GO アプリケーションを使用してアプライアンスと対話できるようになります。管理者はこのアプリケーションを使用して、サービスデスク、インベントリ、およびアプリケーション展開機能にアクセスできます。 **注:** このフィールドは、モバイルデバイスアクセスがアプライアンスで有効な場合に利用できます。詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。
サービスデスクチケット	（読み取り専用）ユーザーが作成したチケットへのリンク。
関連付けられた資産	（読み取り専用）ユーザーに割り当てられた資産。各ユーザーに対して、資産名、資産タイプ（例えば、ソフトウェアやデバイス）、および資産サブタイプ（該当する場合）がリストに表示されます。必要に応じて、任意の列見出しでこのリストをソートできます。
割り当てられているデバイス	ユーザーに割り当てられたデバイス。各ユーザーに対して、デバイス名、サブタイプ（該当する場合）、およびデバイスがプライマリユーザーデバイスかどうかの表示がリストに表示されます。必要に応じて、任意の列見出しでこのリストをソートできます。 デバイスをユーザーに割り当てるには、＋をクリックし、資産を選択します。別のユーザーにすでに割り当てられているデバイスを選択すると、そのデバイスの所有権は新しいユーザーに移行します。 ユーザーに最初に割り当てられたデバイスは、デフォルトでプライマリデバイスになります。複数のデバイスがユーザーに割り当てられている場合、すべてのデバイスをプライマリデバイスとして設定できます。

3. **保存** をクリックします。

関連トピック

ユーザーの役割の追加または編集

ロケール設定の構成

ラベルについて

モバイルデバイスによるアクセスの設定

ユーザー詳細のカスタマイズ

必要に応じて、ユーザーアカウントで使用可能なカスタムフィールドを変更できます。

各ユーザーアカウントには、一連のカスタムフィールドが付属しています。これらのフィールドを編集して、バッジ番号など、意味のあるユーザー固有の情報を含めることができます。

1. ユーザー詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
    c. **アクションを選択 > 新規作成** の順に選択して、ユーザー詳細 ページを表示します。
2. ユーザー詳細 ページで、追加フィールドのカスタマイズ をクリックします。

    ユーザーカスタムフィールド ページが表示されます。
3. 各カスタムフィールドについて、次の情報を指定できます

オプション	説明
フィールド名	カスタムフィールドの名前。
必須	フィールドが必須であるかどうかを示すインジケータ。
デフォルト値	デフォルト値。

4. 必要に応じて、使用可能なコントロールを使用して、カスタムフィールドのコレクションを管理します。
5. **保存** をクリックします。

ユーザーアカウントのアーカイブ

ユーザーがシステムから削除されたとき、そのアカウントを削除する前にアーカイブしておくことができます。

ユーザーアカウントをアーカイブするには、ユーザーのアーカイブが一般設定ページで有効になっている必要があります。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。

アーカイブされたユーザーアカウントは、アプライアンスで読み取り専用モードで保持されます。必要に応じてそのアカウントを削除できます。ユーザーアカウントをアーカイブして再びアプライアンスに追加すると、新しいユーザーアカウントが作成され、アーカイブされたアカウントは削除されるまで保持されます。例えば、ある従業員が組織を辞職してそのユーザーアカウントがアーカイブされた後、再び組織に雇用された場合、アーカイブされたアカウントとは関連がない新しいユーザーアカウントが作成されます。同様に、組織の Active Directory を更新しないでアプライアンスのユーザーアカウントをアーカイブした場合、LDAP インポート結果は新しいユーザーアカウントになり、先にアーカイブされたユーザーとは関連付けられません。

注: ユーザーのアーカイブが有効になると、削除できるユーザーアカウントはアーカイブ済みとしてマークされているものだけになります。

1. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. 左側のナビゲーションバーで、**コントロールパネル > ユーザー**をクリックします。
3. 次の手順のいずれかを実行します。
   - **ユーザーリストで、アーカイブするユーザーアカウントを1 個以上選択して、アクションの選択 > アーカイブを選択します。**
   - **ユーザーリストで、アーカイブするユーザーの名前をクリックします。表示されたユーザー詳細ページで、アーカイブをクリックします。**
4. 表示されたダイアログボックスで、**確認**をクリックします。

   ダイアログボックスが閉じ、ユーザーリストが更新され、ユーザーがアーカイブ状態 ( ) であることが示されます。
5. アーカイブしたユーザーの詳細を確認する場合、ユーザーリストの名前列で、ユーザー名をクリックします。

   読み取り専用モードでそのユーザーの詳細を表示する、ユーザー詳細ページが表示されます。

次に、必要に応じてアーカイブされたユーザーアカウントを削除できます。

ユーザープロファイルの表示または編集

必要に応じて、ユーザープロファイルについての一般情報を表示し、一部の設定を編集することができます。

ユーザープロファイル ダイアログボックスでは、すべてのユーザーがパスワードの簡単な変更、割り当てられているデバイスと資産、および作成したサービスデスクチケットを表示できます。管理レベルの権限を持つユーザーは、名前、Eメール、管理者、ロケールなどの一部の追加パラメータも編集できます。また、これらのユーザーは ユーザー詳細 ページに簡単に移動して、自分のアカウントに関する追加情報を確認し、必要に応じて変更を加えることができます。

ユーザー詳細 ページを使用してユーザーアカウントを編集する方法の詳細については、次のトピックを参照してください。

- 組織ユーザーアカウントの追加または編集
- システムレベルのユーザーアカウントの追加または編集

1. 次のいずれかを実行します。
   - **アプライアンス 管理者コンソール（https://appliance_hostname/admin。ここで、appliance_hostname はお使いのアプライアンスのホスト名）にログインします。または、管理ヘッダーに組織メニューを表示 がアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。**
   - **アプライアンス システム管理コンソール（https://appliance_hostname/system。ここで、appliance_hostname はお使いのアプライアンスのホスト名）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。**
   - **アプライアンス ユーザーコンソール（https://appliance_hostname/user。ここで、appliance_hostname はお使いのアプライアンスのホスト名）にログインします。または、ページの右上隅にあるドロップダウンリストから ユーザーコンソール を選択します。**
2. ページの右上隅にあるドロップダウンリストから、**マイプロファイル** を選択します。

   ユーザープロファイル ダイアログボックスが表示されます。
3. ユーザープロファイル ダイアログボックスの情報を確認し、必要に応じて編集します。

注: 管理者権限がないユーザーは、自身のパスワードのみを更新でき、ダイアログボックス上の限られた情報だけを表示できます。さらに変更を加えたり、ユーザー詳細 ページにアクセスしたりできません。

タブ	オプション	説明
プロファイル	ログイン	ユーザーがログインページの ログインID フィールドに入力する名前。 **注:** デフォルトadmin管理者のログインを変更することはできません。
	名前	ユーザーのフルネーム。
	プライマリEメール	ユーザーのEメールアドレス。
	管理者	ユーザーの管理者。
	ロケール	ユーザーの**ユーザーコンソール**および**管理者コンソール**に使用するロケール。
	パスワードの更新	ユーザーがログイン時に入力するパスワード。 アプライアンスで組織コンポーネントが有効になっている場合、または複数の K シリーズアプライアンスをリンクする場合、**管理者**アカウントのパスワードを変更する際には注意する必要があります。右上隅にあるドロップダウンリストを使用して、システムレベル、組織、およびリンク先アプライアンス間で **管理者**アカウントを切り替える場合、これらのアカウントのパスワードは同じにする必要があります。ドロップダウンリストには、adminアカウントが同じ組織とアプライアンスのみ表示されます。
デバイス	名前	デバイス名。
	サブタイプ	このデバイスの資産サブタイプ（ 割り当てられている場合 ）。
	プライマリデバイス	デバイスが、選択したユーザーのプライマリデバイスかどうかを示します。
資産	名前	資産名。
	タイプ	資産タイプ。

タブ	オプション	説明
	サブタイプ	このデバイスの資産サブタイプ（割り当てられている場合）。
サービスデスクチケット	**数値**	ユーザーが記録したサービスデスクチケットの番号。
	タイトル	ユーザーが記録したサービスデスクチケットのタイトル。
	ステータス	ユーザーが記録したサービスデスクチケットのステータス。

4. （**オプション**）ユーザー詳細 ページにアクセスするには、左上隅で、**完全なプロファイルを表示** をクリックします。そして、このページでユーザープロファイルの確認および編集を続けます。

   注: このリンクは、お使いのアカウントに管理者権限がある場合にのみ表示されます。

5. 変更内容を保存するには、**更新** をクリックします。

LDAPサーバーを使用したユーザー認証

ユーザー認証は、アプライアンスで作成されたアカウントを使用してローカルで行うか、LDAP サーバを使用して外部で行うことができます。

外部LDAPサーバー認証を使用する場合、アプライアンスは、ユーザーを認証するためにディレクトリサービスにアクセスします。これにより、ユーザーは各自のドメインユーザー名とパスワードを使用して、アプライアンスの**管理者コンソール**、**ユーザーコンソール**、または**システム管理コンソール**にログインできます。

ローカルユーザー認証のためにアプライアンスにユーザーアカウントを追加する方法の詳細については、以下を参照してください。

- ユーザーアカウントおよびユーザー認証について
- 組織のユーザーアカウントの管理

LDAPサーバーのログインアカウントについて

LDAP ユーザー認証を設定するには、LDAP サーバにアプライアンス用のログインアカウントを作成する必要があります。アプライアンスは、このアカウントを使用して、LDAPサーバーからユーザー情報を読み取り、インポートします。

このアカウントには、LDAPサーバーの ベースDNの検索 フィールドに対する読み取り専用のアクセス権が必要です。アプライアンスはLDAPサーバーに書き込みを行わないため、このアカウントに書き込み権限は必要ありません。

また、このアカウントには、期限切れにならないパスワードが必要です。パスワードは期限切れにならないため、非常に安全であることを確認する必要があります。ユーザーは、（適切なセキュリティ要件に準拠した）パスワードを変更できますが、パスワードはアプライアンスで更新する必要があります。アカウントに「KACE_Login」などのユーザー名を付けることも、匿名バインドを使用してLDAPサーバーへの接続を試行することもできます。

LDAPユーザー認証の設定とテスト

アプライアンスから外部 LDAP サーバへの接続を設定してテストできます。

1. 次のいずれかを実行します。
   - **アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 がアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。**
   - **アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。**

   ダッシュボード ページまたは システム概要 ページが表示されます。
2. 管理者レベルまたはシステムレベルの 認証設定 ページに移動します。
   a. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。
   b. コントロールパネル で、**ユーザー認証**（管理者コンソールのみ）、または **システムユーザー認証**（システム管理コンソールのみ）をクリックします。
3. ローカル管理者アカウントを無効にし、LDAP または SAML を使用して管理者レベルのユーザーとしてログインしている場合は、**Disable Local Built-In Administrator (LDAP or SAML configuration required)**（ローカルビルトイン管理者の無効化（LDAP または SAML 設定が必要です））を選択します。

   組み込みの管理者アカウントを無効にしても、必要に応じて KACE サポートで使用されるテザーには影響しません。この機能の詳細については、「Quest KACE サポートへの tether を有効にする」を参照してください。
4. **LDAP認証** オプションを選択します。

オプション	説明
ローカル認証	ローカル認証を有効にします（デフォルト）。ローカル認証を有効にした場合、パスワードは、**設定** > **ユーザー** にあるローカルデータベースの既存のエントリに対して認証されます。
LDAP認証	LDAPサーバーまたはActive Directoryサーバーによる外部ユーザー認証を有効にします。 **LDAP 認証** が有効になっている場合、パスワードは外部 LDAP サーバーに対して認証されます。 認証に関するサポートが必要な場合は、**Questサポート**（ https://support.quest.com/contact-support ）にお問い合わせください。

5. 以下のアクションを実行するには、サーバー名の隣にあるボタンをクリックします。

ボタン	アクション
	このサーバーについてユーザーのインポートをスケジュールします。
	サーバーの定義を修正します。このセクションのフィールドの詳細については、Table 5を参照してください。
	サーバーを削除します。

ボタン	アクション
	サーバーのリストでサーバーの順序を変更します。

6. **オプション**：**新規作成** をクリックして、LDAPサーバーを追加します。複数のLDAPサーバーを設定できます。

   注: すべてのサーバーについて、有効なIPアドレスまたはホスト名を入力する必要があります。入力しない場合、操作はタイムアウトになり、LDAP認証の使用時にログイン遅延が生じます。

7. サーバーを追加するには、次の情報を入力します。

サーバー情報

オプション	説明
名前	サーバーの識別に使用する名前。
ホスト名またはIPアドレス	LDAPサーバーのIPアドレスまたはホスト名。IPアドレスが有効でない場合は、タイムアウトするまで待たなければならず、その結果LDAP認証中にログイン遅延が発生します。 **注:** SSL経由で接続するには、IPアドレスまたはホスト名を使用します。例：ldaps://hostname。
ポート	LDAPポート番号。通常は、389（LDAP）または636（セキュアLDAP）です。
ベースDN	アカウントの検索に使用される基準。 この基準によって、LDAPまたはActive Directory構造における場所またはコンテナを指定します。この基準には、認証するすべてのユーザーが含まれる必要があります。基準を満たすOU、DC、またはCNの最も明確な組み合わせを入力します（一番左は最も限定的、一番右は最も一般的です）。例えば、このパスが、認証対象となるユーザーが属するコンテナを指している場合は、次の通りです。 「OU=end_users,DC=company,DC=com」。 **注:** ドメインユーザーは、memberof 属性値に追加されない特別なグループです。ドメインユーザーのメンバーには、次の形式を使用します。(primaryGroupId=513)。
高度な検索	検索フィルタ。例： (&(sAMAccountName=KBOX_USERNAME)(memberOf=CN=financial,DC=example,DC=com))
ログイン	アプライアンスが LDAP サーバに ログインして、アカウントを読み取るために必要なアカウントの資格情報です。例： LDAP Login:CN=service_account,CN=Users, DC=company,DC=com。 ユーザーとパスワードが指定されていない場合、ツリー検索は実行されません。

オプション	説明
	LDAPラベルごとに、異なるLDAPまたはActive Directoryサーバーに接続することが可能です。
パスワード	アプライアンスが LDAP サーバにログインするために必要となるアカウントのパスワードです。
役割	（必須）ユーザーの役割： • **グローバル管理者**：ユーザーは、完全な読み取り / 書き込み許可を持つ管理者として **システム管理コンソール**、および各組織の **管理者コンソール** にアクセスできます。最初に**システム管理コンソール**にログインして、右上隅のドロップダウンリストを使用して該当する組織アカウントにログインする必要があります。 • **管理者**: ユーザーは、**管理者コンソール**、**ユーザーコンソール**、または**システム管理コンソール**にログインして、すべての機能にアクセスできます。 • **読み取り専用の管理者**: ユーザーは、**管理者コンソール**、**ユーザーコンソール**、または**システム管理コンソール**にログインできますが、設定の変更はできません。 • **ユーザーコンソールのみ**：ユーザーは、**ユーザーコンソール**にのみログインできます。この役割は、**管理者コンソール**でのみ使用できます。 • **アクセス権限なし**：ユーザーは、**管理者コンソール**、**システム管理コンソール**、または**ユーザーコンソール**にログインできません。「**アクセス権限なし**」はデフォルトの役割です。 **注:** これらの役割は事前定義された役割であるため編集できません。ただし、必要に応じて、カスタムの役割を作成して編集することができます。

注: このフォームに記入するために使用する検索基準とフィルタ基準を記録しておいてください。ユーザーデータのインポートや、ユーザーの定期的なインポートのスケジュール設定にも、これと同じ情報を使用します。

8. **保存** をクリックします。
9. 次の手順を実行し、外部のLDAPサーバー上で認証をテストします。
    a. **LDAP認証** を選択します。
    b. テスト対象のユーザーアカウントが登録されたサーバーの隣にある、**編集** ボタン（ ）をクリックします。
    c. 高度な検索：ボックスで、**KBOX_USER** をテスト対象のユーザー名に置き換えます。構文は、「sAMAccountName=username」です。
    d. テスト用パスワード フィールドに、ユーザーのパスワードを入力します。
    e. **テスト** をクリックします。

このテストに成功すれば、テスト対象のユーザーおよび同じLDAPコンテナに属する他のユーザーに対する認証の設定が完了します。

LDAPサーバーからのユーザーのインポート

LDAP サーバからユーザー情報をインポートして、アプライアンスにユーザーアカウントを作成できます。これにより、サービスデスクスタッフなどの管理者がユーザーに対応する際、より多くのデータを使用できるようになります。

ユーザー情報をインポートするには、2つの方法があります。

- **手動**：詳細については、次を参照してください。 手動でのユーザー情報のインポート
- **スケジュールに従う**：詳細については、次を参照してください。 スケジュールに従ったユーザー情報のインポート

注: ユーザー情報は、アプライアンスにユーザーをインポートするたびに上書きされます。ただし、パスワード情報はインポートされません。ユーザーは、**管理者コンソール**または**ユーザーコンソール**にログインするたびにパスワードを入力する必要があります。

手動でのユーザー情報のインポート

インポートするユーザーを識別する基準を指定することで、ユーザー情報を手動でインポートできます。

1. ユーザー ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
   c. **アクションの選択 > ユーザーのインポート** を選択します。
2. 次の情報を入力します。

注: LDAPブラウザを使用して、「ベースDNの検索」と「検索フィルタ」を指定します。詳細については、「LDAPブラウザの使用」を参照してください。

オプション	説明
サーバー	LDAPサーバーのIPアドレスまたはホスト名。IPアドレスが有効でない場合は、タイムアウトするまで待たなければならず、その結果LDAP認証中にログイン遅延が発生します。 **注:** SSL経由で接続するには、IPアドレスまたはホスト名を使用します。例：ldaps://hostname。
ポート	LDAPポート番号。通常は、389（LDAP）または636（セキュアLDAP）です。
ベースDN	アカウントの検索に使用される基準。 この基準によって、LDAPまたはActive Directory構造における場所またはコンテナを指定します。この基準には、認証するすべてのユーザーが含まれる必要があります。基準を満たすOU、DC、またはCNの最も明確な組み合わせを入力します（一番左は最も限定的、一番右は最も一般的です）。例えば、この

オプション	説明
	パスが、認証対象となるユーザーが属するコンテナを指している場合は、次の通りです。 「OU=end_users,DC=company,DC=com」。 **注:** LDAPブラウザを使用して、「ベースDNの検索」と「検索フィルタ」を指定します。LDAPブラウザの使用.
高度な検索	検索フィルタ。例： (&(sAMAccountName=KBOX_USERNAME)(memberOf=CN=financial,DC=example,DC=com))
ログイン	アプライアンスが LDAP サーバにログインして、アカウントを読み取るために必要なアカウントの資格情報です。例： LDAP Login:CN=service_account,CN=Users, DC=company,DC=com。 ユーザーとパスワードが指定されていない場合、ツリー検索は実行されません。LDAPラベルごとに、異なるLDAPまたはActive Directoryサーバーに接続することが可能です。
パスワード	アプライアンスが LDAP サーバにログインするために必要となるアカウントのパスワードです。

3. インポートする LDAP 属性を指定します。

オプション	説明
取得する属性	取得する LDAP 属性を指定します。例： sAMAccountName, objectguid, mail, memberof, displayname, sn, cn, userPrincipalName, name, description, manager このフィールドに指定されている LDAP 属性は、次のページでアプライアンスユーザー属性にマップできます。このフィールドを空白のままにした場合、アプライアンスによりすべての LDAP 属性が取得されます。このフィールドを空白のままにすると、属性のインポートに必要な時間が増加するため、お勧めしません。 **重要: ユーザーに関連付けられている管理者オブジェクトを取得するには、manager属性をリストに追加し、後の手順でこのマッピングを指定する必要があります。**
ラベル属性	ラベル属性を入力します。例：memberof この設定は、このユーザーがメンバーになっているグループのリストを返します。これらのラベル属性をすべて結合すると、インポートできるラベルのリストになります。検索フィルタにラベル名とユーザー名の両方が含まれている場合、ラベル属性は必要ありません。

オプション	説明
ラベルプレフィックス	ラベルプレフィックスを入力します。例：ldap_ ラベルプレフィックスは、すべてのラベルの先頭に追加される文字列です。
バイナリ属性	バイナリ属性を入力します。例：objectsid バイナリ属性では、どの属性をバイナリとして保存する必要があるかを指定します。
最大行数	取得する最大行数を入力します。これにより、次の手順で返される結果セットが制限されます。
デバッグ出力	このチェックボックスを選択し、デバッグ出力を表示します。

4. **次へ** をクリックします。

   Define mapping between User attributes and LDAP attributes（ユーザー属性と LDAP 属性との間のマップを定義します）ページが表示されます。
5. 各属性の隣のドロップダウンリストで、インポート時にアプライアンスユーザー属性に使用する値を選択します。ドロップダウンリストの値は、前のページで Attributes to retrieve（取得する属性）フィールドに指定された値です。

   次の属性マッピングが必要です。

オプション	説明
LDAP UID	ユーザーの識別子。推奨値：objectguid。
ユーザー名	ユーザーの名前。推奨値：name。
Eメール	ユーザーの E メールアドレス。推奨値：mail。
管理者	ユーザーの管理者。このマッピングは、管理者の情報を取得する場合にのみ必須です。推奨値：manager。 **重要: ユーザーに関連付けられている管理者オブジェクトを取得するには、manager属性を** 取得する属性 **ボックスに追加する必要もあります。**

次の属性マッピングは必須ではありませんが、設定することをお勧めします。

オプション	説明
APIを有効にする	ユーザーが KACE GO アプリケーションを使用してアプライアンスにアクセスできるようにするかどうか。このフィールドに数値が含まれている場合、アクセスは有効になります。このフィールドに数値が含まれていない場合、アクセスは無効になります。このため、アクセスを有効にするには、数値を返す属性を選択します。アクセスを無効にするには、**値はありません** を選択します。

オプション	説明
Ams Id	未使用。推奨値：**値はありません。**

6. **オプション**：役割 ドロップダウンリストで、インポートされたユーザーの役割を選択します。詳細については、「ユーザーの役割の追加または編集」を参照してください。
7. **オプション**：ラベル ドロップダウンリストで、インポートしたユーザーに適用するラベルを選択します。詳細については、「ラベルについて」を参照してください。
8. 属性マッピングドロップダウンリストの下にある Search Results（検索結果）セクションで、インポートするユーザーのリストが正しく、ユーザーごとに示された情報が想定どおりのものであることを確認します。検索結果を絞り込むには、**戻る** ボタンをクリックして検索パラメータおよび属性を修正します。

   例えば、「検索結果」の数を変更するには、インポートする属性の選択 ページの 最大行数 を変更します。
9. **次へ** をクリックして、Import Data into the appliance（アプライアンスへのデータのインポート）ページを表示します。
10. データが有効であり、想定されるデータが含まれていることを、ユーザーの表で確認します。

    必要な属性、Ldap Uid、ユーザー名、Eメール、および 管理者 に値が登録されているユーザーのみがインポートされます。これらの値が登録されていないレコードは、Users with invalid data（データが無効なユーザー）セクションに表示されます。
11. **今すぐインポート** をクリックして、インポートを開始します。

ユーザー ページが開き、インポートしたユーザーがリスト上に表示されます。インポートされたユーザーは、割り当てられている役割に応じて、**管理者コンソール**と**ユーザーコンソール**の機能にアクセスできます。

スケジュールに従ったユーザー情報のインポート

ユーザーデータを常に最新に保つため、LDAPサーバーから定期的にユーザーデータをインポートするようスケジュール設定します。

1. 管理者レベルの 認証設定 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。
   c. コントロールパネル で、**ユーザー認証**（管理者コンソールのみ）、または **システムユーザー認証**（システム管理コンソールのみ）をクリックします。
2. **LDAP 認証** を選択し、サーバリストのサーバー名の隣にある **スケジュール** ボタン をクリックして、ユーザーのインポートをスケジュールします。

   User Import:（ユーザーのインポート：）スケジュール – インポートする属性の選択 ページが表示されます。

   以下の 読み取り専用の管理者サーバーの詳細 が表示されます。

オプション	説明
サーバー	LDAPサーバーのIPアドレスまたはホスト名。IPアドレスが有効でない場合は、タイムアウトするまで待たなければならず、その結果LDAP認証中にログイン遅延が発生します。 **注:** SSL経由で接続するには、IPアドレスまたはホスト名を使用します。例：ldaps://hostname。

オプション	説明
ポート	LDAPポート番号。通常は、389（LDAP）または636（セキュアLDAP）です。
ベースDN	アカウントの検索に使用される基準。 この基準によって、LDAPまたはActive Directory構造における場所またはコンテナを指定します。この基準には、認証するすべてのユーザーが含まれる必要があります。基準を満たすOU、DC、またはCNの最も明確な組み合わせを入力します（一番左は最も限定的、一番右は最も一般的です）。例えば、このパスが、認証対象となるユーザーが属するコンテナを指している場合は、次の通りです。 「OU=end_users,DC=company,DC=com」。 **注:** LDAPブラウザを使用して、「ベースDNの検索」と「検索フィルタ」を指定します。LDAPブラウザの使用.
高度な検索	検索フィルタ。例： (&(sAMAccountName=KBOX_USERNAME)(memberOf=CN=financial,DC=example,DC=com))
ログイン	アプライアンスが LDAP サーバに ログインして、アカウントを読み取るために必要なアカウントの資格情報です。例： LDAP Login:CN=service_account,CN=Users, DC=company,DC=com。 ユーザーとパスワードが指定されていない場合、ツリー検索は実行されません。LDAPラベルごとに、異なるLDAPまたはActive Directoryサーバーに接続することが可能です。
パスワード	アプライアンスが LDAP サーバに ログインするために必要となるアカウントのパスワードです。

3. インポートする LDAP 属性を指定します。

オプション	説明
取得する属性	取得する LDAP 属性を指定します。例： sAMAccountName, objectguid, mail, memberof, displayname, sn, cn, userPrincipalName, name, description, manager このフィールドに指定されている LDAP 属性は、次のページでアプライアンスユーザー属性にマップできます。このフィールドを空白のままにした場合、アプライアンスによりすべての LDAP 属性が取得されます。このフィールドを空白のままにすると、属性のインポートに必要な時間が増加するため、お勧めしません。

オプション	説明
	重要: ユーザーに関連付けられている管理者オブジェクトを取得するには、manager属性をリストに追加し、後の手順でこのマッピングを指定する必要があります。
ラベル属性	ラベル属性を入力します。例：memberof この設定は、このユーザーがメンバーになっているグループのリストを返します。これらのラベル属性をすべて結合すると、インポートできるラベルのリストになります。検索フィルタにラベル名とユーザー名の両方が含まれている場合、ラベル属性は必要ありません。
ラベルプレフィックス	ラベルプレフィックスを入力します。例：ldap_ ラベルプレフィックスは、すべてのラベルの先頭に追加される文字列です。
バイナリ属性	バイナリ属性を入力します。例：objectsid バイナリ属性では、どの属性をバイナリとして保存する必要があるかを指定します。
最大行数	取得する最大行数を入力します。これにより、次の手順で返される結果セットが制限されます。
デバッグ出力	このチェックボックスを選択し、デバッグ出力を表示します。

4. E メール受信者 セクションで、**編集** ボタンをクリックして受信者の E メールアドレス を入力します。
5. 受信者 ドロップダウンリストでユーザーを選択します。
6. スケジュール セクションで、次のスケジュールオプションを指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。このオプションは、サーバーに手動でパッチを適用するか、または定期的に実行しないパッチアクションを実行する場合に便利です。
毎 _ 時間	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
毎月 / 特定月の n 日、HH:MM に実行	毎月n日（例えば、毎月1日または2日）、または特定の月、特定の時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。

オプション	説明
	* * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース ( )**：各フィールドはスペースで区切ります。 • **アスタリスク (*)**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

7. **次へ** をクリックして、User Import:（ユーザーのインポート： ）Schedule - Define mapping between User attributes and LDAP Attributes（スケジュール - ユーザー属性とLDAP属性との間のマップを定義します ）ページを表示します。
8. 各属性の隣のドロップダウンリストで、インポート時にアプライアンスユーザー属性に使用する値を選択します。ドロップダウンリストの値は、前のページで Attributes to retrieve（取得する属性 ）フィールドに指定された値です。

   次の属性マッピングが必要です。

オプション	説明
LDAP UID	ユーザーの識別子。推奨値：objectguid。
ユーザー名	ユーザーの名前。推奨値：name。
Eメール	ユーザーの E メールアドレス。推奨値：mail。
管理者	ユーザーの管理者。このマッピングは、管理者の情報を取得する場合にのみ必須です。推奨値：manager。 **重要: ユーザーに関連付けられている管理者オブジェクトを取得するには、manager属性を** 取得する属性 **ボックスに追加する必要もあります。**

次の属性マッピングは必須ではありませんが、設定することをお勧めします。

オプション	説明
APIを有効にする	ユーザーが KACE GO アプリケーションを使用してアプライアンスにアクセスできるようにするかどうか。このフィールドに数値が含まれている場合、アクセスは有効になります。このフィールドに数値が含まれていない場合、アクセスは無効になります。このため、アクセスを有効にするには、数値を返す属性を選択します。アクセスを無効にするには、**値はありません** を選択します。
Ams Id	未使用。推奨値：**値はありません**。

9. **オプション**：役割 ドロップダウンリストで、インポートされたユーザーの役割を選択します。詳細については、「ユーザーの役割の追加または編集」を参照してください。
10. 選択した役割を新しい役割のデフォルトの役割にする場合は、**デフォルトにする** チェックボックスを選択します。
11. **オプション**：ラベル ドロップダウンリストで、インポートしたユーザーに適用するラベルを選択します。詳細については、「ラベルについて」を参照してください。
12. 属性マッピングドロップダウンリストの下にある Search Results（検索結果）セクションで、インポートするユーザーのリストが正しく、ユーザーごとに示された情報が想定どおりのものであることを確認します。検索結果を絞り込むには、**戻る** ボタンをクリックして検索パラメータおよび属性を修正します。

    例えば、「検索結果」の数を変更するには、インポートする属性の選択 ページの 最大行数 を変更します。
13. **次へ** をクリックして、Import Data into the appliance（アプライアンスへのデータのインポート）ページを表示します。
14. データが有効であり、想定されるデータが含まれていることを、ユーザーの表で確認します。

必要な属性、Ldap Uid、ユーザー名、Eメール、および 管理者 に値が登録されているユーザーのみがインポートされます。これらの値が登録されていないレコードは、Users with invalid data（データが無効なユーザー）セクションに表示されます。

15. 次のいずれかを実行します。
    - **戻る をクリックして、設定を変更します。**
    - **インポート をクリックして、スケジュールを保存し、ユーザー情報を直ちにインポートします。インポートが始まり、**Scheduling（スケジュール）**セクションで選択されているオプションに従って実行されるようにスケジュールが設定されます。**
    - **終了 をクリックして、ユーザー情報をインポートせずにスケジュールを保存します。**Scheduling（スケジュール）**セクションで選択されているオプションに従って実行されるようにスケジュールが設定されます。**

    指定したスケジュールに従って、ユーザー情報がインポートされます。

シングルサインオン（SSO）について

シングルサインオンを使用すると、ドメインにログオンしているユーザーやサードパーティを通じて認証されるユーザーが、アプライアンスのログインページに資格情報を再入力する必要なく、アプライアンス**管理者コンソール**と**ユーザーコンソール**にアクセスできるようになります。

シングルサインオンに Active Directory を使用できます。

シングルサインオンは次のものに対して使用できます。

- **1つのドメインのみ**: ドメインが複数ある場合は、1つだけシングルサインオンを有効にできます。これは、アプライアンス上で組織コンポーネントが有効化されている場合に、異なるドメインに存在する複数の組織がある場合にも当てはまります。シングルサインオンはシステムレベルの設定であり、組織に対して単独でシングルサインオンを設定することはできません。
- **Microsoft Active Directoryサーバー**: スキーマバージョンが 2003 R2 以降の Microsoft Active Directory サーバーを使用して、シングルサインオンを有効にすることができます。それ以前のスキーマバージョンは使用できません。アプライアンス上で組織コンポーネントが有効化されている場合は、複数の組織で Active Directory シングルサインオン方法を使用できます。

外部 LDAP サーバーまたは Active Directory サーバーを使用したシングルサインオン

シングルサインオンの認証に Active Directory を使用している場合、外部 LDAP サーバーまたは Active Directory サーバーに、シングルサインオン用に指定された Active Directory サーバーと同じエントリが必要です。アプライアンスは、参加したドメインでユーザー資格情報の一致を確認し、外部 LDAP 設定を使用してユーザーの役割と権限を決定します。

アプライアンスのローカルアカウントを使用してユーザーを認証するには、LDAP または Active Directory サーバからアプライアンスにアカウントをインポートするか、アプライアンスでアカウントを手動で作成する必要があります。詳細については、以下を参照してください。

- LDAPサーバーからのユーザーのインポート
- システムレベルユーザーアカウントの管理
- 組織ユーザーアカウントの管理

シングルサインオンの有効化および無効化

アプライアンスセキュリティ設定でシングルサインオンを有効または無効にすることができます。

シングルサインオンの有効化

シングルサインオンを有効にするには、アプライアンスのセキュリティ設定を行い、Active Directory サーバーとアプライアンスの間で接続を確立する必要があります。

- Active Directory のシングルサインオンを設定するには、次を参照してください。 シングルサインオン方法としてのActive Directoryの設定

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **セキュリティ設定** をクリックして、セキュリティ設定 ページを表示します。
3. シングルサインオン セクションで、シングルサインオン方法を選択します。

- シングルサインオン方法としてのActive Directoryの設定

シングルサインオンの無効化

ドメインからアプライアンスを削除せずにシングルサインオンを無効化することができます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **セキュリティ設定** をクリックして、セキュリティ設定 ページを表示します。
3. シングルサインオン セクションで、**無効にする** を選択します。

   シングルサインオンが無効になります。現在**管理者コンソール**または**ユーザーコンソール**にログインしているユーザーは、そのセッションが終了するまでログインしたままになります。ただし、次に**管理者コンソール**または**ユーザーコンソール**にアクセスを試みたときは、資格情報を入力する必要があります。

Active Directory を使用したシングルサインオン

Active Directory を使用するようにシングルサインオンを設定した場合、認証されたユーザーはログイン資格情報を入力しなくても**管理者コンソール**または**ユーザーコンソール**にアクセスできます。

そのためには、ユーザーはブラウザのアドレスフィールドにアプライアンスのホスト名を入力する必要があります。ユーザーが IP アドレスを入力した場合、自動的にサインオンする代わりに、アプライアンスのログインページに移動するため、資格情報を入力して、ログインする必要があります。

シングルサインオンに Active Directory を使用する場合は、適切なセキュリティ設定を使用するように Microsoft Edge や Mozilla Firefox ブラウザを設定する必要があります。

シングルサインオン方法としてのActive Directoryの設定

Active Directory シングルサインオンを使用すると、ドメインにログオンしているユーザーが、ログオン資格情報を毎回再入力する必要なく、アプライアンス**管理者コンソール**と**ユーザーコンソール**にアクセスできるようになります。

アプライアンスを Active Directory サーバに接続する前に、次の点を確認します。

- アプライアンスが Active Directory サーバにアクセスできるように、ネットワークと DNS の設定が構成されている。詳細については、「アプライアンスのネットワーク設定の変更」を参照してください。
- Active Directory サーバの時刻設定がアプライアンスの時刻設定と一致している。アプライアンスの時刻設定に関する情報については、「アプライアンスの日付と時刻の設定」を参照してください。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. セキュリティ設定 ページの シングルサインオン セクションで、**Active Directory** を選択し、次の情報を入力します。

オプション	説明
ドメイン	Active Directory® サーバーのドメインのホスト名。例：example.com。
ユーザー名	Active Directory サーバーの管理者アカウントのユーザー名。例:「username@example.com」。
パスワード	Active Directoryサーバーの管理者アカウントのパスワード。
コンピュータオブジェクトコンテナ	Active Directory サーバーでの管理者アカウントのコンピュータオブジェクトコンテナの名前。
コンピュータオブジェクト名	Active Directory サーバーでの管理者アカウントのコンピュータオブジェクトコンテナの名前。
サービスアカウントコンテナ	Active Directory サーバーでの管理者アカウントのサービスアカウントコンテナの名前。

3. **参加** をクリックします。

アプライアンスは、読み取り専用の権限が必要な次のテストを実行し、アプライアンスのドメインへの参加が許可されるよう正確にドメインが設定されているかどうかを確認します。

- サポートされているオペレーティングシステムと正しいオペレーティングシステムパッチがあることを確認する
- QASをインストールするための十分なディスク領域があることを確認する
- システムのホスト名が「localhost」でないことを確認する
- ネームサービスがDNSを使用するように設定されているかどうかを確認する
- resolv.confにネームサービスエントリの適切なフォーマットがあること、およびホストが解決できることを確認する
- Active Directory用の適切なDNS SRVレコードを持つネームサーバーがあることを確認する
- UDPポート389が開いている書き込み可能なドメインコントローラーを検出する
- Active Directoryサイトを検出する（使用可能な場合）
- TCPポート464がKerberos kpasswdに対して開いているかどうかを確認する
- UDPポート88およびTCPポート88が、Kerberosトラフィックに対して開いているかどうかを確認する
- TCPポート389がLDAPに対して開いているかどうかを確認する
- グローバルカタログサーバーがあること、およびTCPポート3268がグローバルカタログサーバーとの通信用に開かれているかどうかを確認する
- Active Directoryに対して有効な時間差があることを確認する
- Active DirectoryでQASアプリケーション設定を確認する
- TCPポート445が、Microsoft CIFSトラフィックに対して開いているかどうかを確認する

これらのテストは書き込み権限を必要としないため、ディレクトリへの書き込み権限の有無を確認しません。また、これらのテストでは、ユーザー名とパスワードの資格情報も確認しません。資格情報が不正確な場合は、テストに成功しても、アプライアンスはドメインに参加できない場合があります。

テストの結果を示すメッセージが表示されます。エラーがある場合、**ログ** をクリックし、ログ ドロップダウンリストで **サーバーエラー** を選択して、エラーを表示することができます。

4. **オプション**：**強制的に参加** を選択し、サーバーを参加させてエラーを無視し、ドメインに参加します。
5. **保存してサービスを再起動** をクリックします。

ユーザーが Active Directory ドメインに参加したデバイスにログインすると、資格情報を再入力する必要なく、アプライアンス**ユーザーコンソール**にアクセスできます。Active Directory ドメインに参加していないデバイスのユーザーにはログインウィンドウが表示され、ローカルのアプライアンスユーザーアカウントを使用してログインすることができます。詳細については、「システムレベルのユーザーアカウントの追加または編集」を参照してください。

注: Microsoft Edge および Firefox のブラウザでシングルサインオンを使用する場合は、ユーザーがブラウザの設定を行い、適切な認証が使用されるようにする必要があります。詳細については、「シングルサインオンを使用するためのブラウザの設定」を参照してください。

シングルサインオンを使用するためのブラウザの設定

Microsoft Edge??? および Firefox?? のブラウザで Active Directory シングルサインオンを使用する場合は、ユーザーがブラウザの設定を行い、適切な認証が使用されるようにする必要があります。Chrome??? のブラウザでは、特殊な設定をする必要はありません。

Microsoft Edge ブラウザ設定の構成

Microsoft Edge で Active Directory シングルサインオンを使用する場合は、Windows のセキュリティ設定を行う必要があります。

1. Windows のコントロールパネルで、**インターネットオプションツール > インターネットオプション > セキュリティ** をクリックします。
2. 表示される インターネットのプロパティ ダイアログボックスの セキュリティ タブで、適切なセキュリティポリシーを選択します。
   - **アプライアンスがインターネット上でアクセスできる場合は、信頼済みサイト を選択します。**
   - **アプライアンスがインターネット上でアクセスできない場合は、ローカルイントラネット を選択します。**
3. **レベルのカスタマイズ** をクリックして、リストの下部までスクロールします。
4. **現在のユーザー名とパスワードで自動的にログオンする** を選択します。このオプションを選択しないと、アプライアンスでシングルサインオンを有効にした場合でも、Microsoft Edge が管理者コンソールまたはユーザーコンソールに自動的にログインできなくなります。

Firefoxブラウザ設定の設定

FirefoxでActive Directoryシングルサインオンを使用する場合は、ブラウザの認証設定を行う必要があります。

1. Firefox ブラウザで、アドレスバーに「about:config」と入力します。
2. 検索 フィールドで、「network.negotiate-auth.trusted-uris」と入力します。
3. 検索結果で、基本設定の名前をダブルクリックします。
4. 文字列値ボックスにアプライアンスの URL を入力します。例：http://kace_sma.example.com。入力したら、**OK** をクリックします。

Active Directory シングルサインオンを使用した管理者コンソールまたはユーザーコンソールへのアクセス

アプライアンスで Active Directory シングルサインオンが有効になっている場合、ドメインにログインしているユーザーは、アプライアンスログインページに資格情報を入力することなく、**管理者コンソール**または**ユーザーコンソール**にアクセスできます。

Active Directory でシングルサインオンを有効にする必要があります。詳細については、「シングルサインオンの有効化」を参照してください。

1. ドメインにログインします。
2. Web ブラウザで、ブラウザのアドレスフィールドにアプライアンスのホスト名を入力します。ホスト名を特定するには、アプライアンスのネットワーク設定の変更を参照してください。

   ヒント: アプライアンス IP アドレスを入力した場合は、自動的にサインオンする代わりに、アプライアンスのログインページに移動します。

   ユーザーアカウント権限に応じて、**管理者コンソール**または**ユーザーコンソール**が表示されます。

ドメインへの参加解除およびActive Directoryシングルサインオンの無効化

Active Directory ドメインからアプライアンスを削除できます。ドメインからアプライアンスを削除すると、自動的にシングルサインオンも無効になります。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **セキュリティ設定** をクリックして、セキュリティ設定 ページを表示します。
3. シングルサインオン セクションで、**ドメインへの参加解除** をクリックします。

注: 現在**ユーザーコンソール**または**管理者コンソール**にログインしているユーザーは、そのセッションが終了するまでログインしたままになります。ただし、次に**ユーザーコンソール**または**管理者コンソール**にアクセスを試みたときは、資格情報を入力する必要があります。

シングルサインオン用に SAML を構成する

サードパーティー製の認証ツールを使用すると、ようこそ ページに資格情報を入力しなくてもユーザーを認証するようにアプライアンスを設定できます。

SAML（ Security Assertion Markup Language ）は、ID とサービスプロバイダーの間でセキュリティトークンを使用する XML ベースのプロトコルです。セキュリティトークンには、ユーザーの ID に関する情報を提供するアサーション要素が含まれています。

アプライアンスで SAML が有効化されて設定され、ユーザーがこのシングルサインオン方式でサインオンすると、アプライアンスから ID プロバイダー（ IdP ）に認証リクエストが送信されます。次に、ID プロバイダーがユーザーの ID を確認し、アプライアンスに認証応答を送信します。次に、アプライアンスがユーザーを **管理者コンソール**（ または **ユーザーコンソール** ）にログインさせて、ユーザーセッションを確立します。SAML ユーザーがアプライアンスからログアウトすると、IdP アカウントからログアウトされます。アプライアンスを使用した後も引き続き IdP アカウントにログインしたい場合は、サインアウトせずに**管理者コンソール**ブラウザウィンドウを閉じてください。SAML ユーザーのセッションがタイムアウトになっても IdP アカウントにログインしたままの場合、アプライアンスは自動的にそのユーザーの新しいセッションを開始します。

複数の組織がある場合、この認証方式を使用する各組織で SAML を構成し、他の組織のローカルのログイン方式を保持できます。

1. アプライアンスにログインするための有効な ID 情報が、IdP にあることを確認します。
2. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
3. SAML 設定 ページに移動します。
   a. 左側のナビゲーションバーで、**設定**、**SAML 構成** の順にクリックします。
   b. SAML 設定 ページの セキュリティアサーションマークアップ言語（ SAML ）で、**SAML サービスプロバイダを有効にする** チェックボックスをオンにします。
4. ユーザーが SAML を使用してこのアプライアンスにアクセスすることのみを許可する場合は、**SAML ログインが必要** を選択します。

このオプションを選択すると、ローカル管理者ユーザーと KACE サポートアカウント（アクティブなサポートテザーでのみ使用可能）を除き、アプライアンスへのすべてのローカルログインが無効になります。

5. リモート ID プロバイダー（IDP）設定 セクションで、次のいずれかの手順を実行して、ユーザーを認証するための IdP メタデータを指定します。
   - **推奨。IdP メタデータを含む XML ページへの URL が IdP で提供されている場合（推奨するオプション）、IdP からメタデータを取得 をクリックします。**IDP メタデータの URL フィールドが表示されたら、**その URL を入力して IDP メタデータのインポート をクリックします。**
   - **IdP メタデータの XML ファイルを使用するには、XML メタデータの入力 をクリックし、**IdP メタデータの XML フィールドが表示されたら、**XML ファイルの内容をコピーしてフィールドに貼り付けます。IDP メタデータのインポート をクリックします。アプライアンスが提供された XML コンテンツを解析して、IdP との接続を確立するために必要な設定を入力します。**

   リモート ID プロバイダー（IdP）設定 セクションが更新され、IdP 構成の詳細が表示されます。一覧表示されたオプションで、SAML 認証中にアプライアンスページのリダイレクトを指定します。詳細については、https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=securityを参照してください。

   注: SAML 構成中にこの情報を確認するには、このセクションの **メタデータを表示** をクリックします。
6. IdP 属性マッピング セクションで、アプライアンスへの SAML ユーザーアクセス権の付与に使用するオプションを選択します。
   - **ローカルユーザーテーブルを使用：アプライアンスにローカルで保存されているユーザーリストに依存します。**
   - **LDAP ルックアップを使用：外部 LDAP サーバからユーザー情報をインポートします。詳細については、「LDAPサーバーを使用したユーザー認証」を参照してください。**
   - **SAML を使用：このページで指定された値を使用して、IdP がアプライアンスユーザーレコード（名前やメールアドレスなど）に使用するフィールドにマッピングします。例えば、IdP が LDAP を使用してユーザーを認証する場合、ObjectGUID および cn のそれぞれに** UID と ログイン **を設定できます。詳細については、IdP のマニュアルを参照してください。**
7. **SAML を使用** を選択した場合は、アプライアンス上にアカウントを持たない認証済み SAML ユーザーに対して、アプライアンス上に新しいユーザーを作成するかどうかを指定します。これを行うには、**認証 SAML ユーザーが SMA に存在しない場合、新しい SMA ユーザーを作成します** を選択します。
8. **SAML を使用** を選択した場合は、SAML 認証ユーザーに付与する役割を指定します。役割マッピングで、役割を付与するときにチェックする条件を指定します。

   例えば、特定のテキスト文字列（admin など）を含む名前を持つ LDAP グループのメンバーに 管理者 役割を付与するには、管理者役割を次のように設定します。

   Administrator memberOf Contains admin

   役割は優先順位に従って一覧表示されます。役割の優先順位は必要に応じてドラッグ & ドロップで変更できます。一致するものが複数ある場合、アプライアンスは SAML ユーザーに最も高い優先度を持つ役割を付与します。

   役割マッピングはオプションです。一致するものが見つからない場合、アプライアンスはデフォルトの役割を割り当てます。デフォルトの役割を指定するには、**不一致ユーザーのデフォルトの役割** をクリックし、次の利用可能なオプションから役割を適宜選択します。管理者、アクセスなし、読み取り専用管理者、またはユーザーコンソールのみ。
9. （**オプション**）アプライアンス固有の SAML 設定をアプライアンスに表示するには、ローカルサービスプロバイダ（SP）設定セクションで **メタデータの表示** をクリックし、表示されるオプションを確認します。

   これらのフィールドにはデフォルト値が入っているため、ほとんどの場合は変更不要です。
10. **保存** をクリックします。
11. SAML 構成をテストします。
    a. アプライアンスからログアウトします。

b. IdP アカウントにログインしていることを確認します。
c. 管理者コンソール または ユーザーコンソール の「ようこそ」ページを開きます。
d. ユーザー資格情報を指定せずに、**ログイン** をクリックします。

ヒント: アプライアンスで SAML が有効になっている場合は、**ローカルサインオン** をクリックし、ユーザー資格情報を指定します。

管理者コンソール または **ユーザーコンソール** ページが表示されます。

例：Azure で Microsoft Active Directory を SAML アイデンティティプロバイダとして使用する

Azure で Active Directory を SAML アイデンティティプロバイダ（IdP）として使用する場合は、いくつかの追加手順が必要です。ここでは、Active Directory を IdP として SAML を設定するプロセスについて説明します。

1. アプライアンスにログインするための有効な ID 情報が、IdP にあることを確認します。
2. 次の手順を実行します。
   a. アプライアンスの SSL を有効にします。Microsoft Azure は SSL クライアントとのみ正常に通信できるため、この手順が必要です。手順については、アプライアンスのセキュリティ設定の構成を参照してください。
   b. https://portal.azure.comにログインし、**Azure Active Directory** を選択します。
   c. **アプリの登録** で、リダイレクト URI の設定をクリアしたまま、新しい登録を作成します。
   d. 新しく作成したアプリケーション登録の エンドポイント ページで、連携メタデータドキュメント フィールドの内容をコピーします。
3. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
4. SAML 設定 ページに移動します。
   a. 左側のナビゲーションバーで、**設定**、**SAML 構成** の順にクリックします。
   b. SAML 設定 ページの セキュリティアサーションマークアップ言語（SAML）で、**SAML サービスプロバイダを有効にする** チェックボックスをオンにします。
5. リモート ID プロバイダ（IdP）設定 セクションで、次のいずれかの手順を実行して、ユーザーを認証するための IdP メタデータを指定します。
   a. **IdP からメタデータを取得** をクリックします。
   b. 表示される IdP メタデータ URL フィールドに、2.dで記録した 連携メタデータドキュメント フィールドの内容を入力し、**IdP メタデータのインポート** をクリックします。

   リモート ID プロバイダー（IdP）設定 セクションが更新され、IdP 構成の詳細が表示されます。一覧表示されたオプションで、SAML 認証中にアプライアンスページのリダイレクトを指定します。詳細については、https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=securityを参照してください。

注: SAML 構成中にこの情報を確認するには、このセクションの **メタデータを表示** をクリックします。

6. Security Assertion Markup Language（SAML）セクションで、**IdP がパッシブ認証をサポートしない** チェックボックスが選択されていることを確認します。
7. IdP 属性マッピング セクションで、アプライアンスへの SAML ユーザーアクセス権の付与に使用するオプションを選択します。
   - **ローカルユーザーテーブルを使用：アプライアンスにローカルで保存されているユーザーリストに依存します。**
   - **LDAP ルックアップを使用：外部 LDAP サーバからユーザー情報をインポートします。詳細については、「LDAPサーバーを使用したユーザー認証」を参照してください。**
   - **SAML を使用 を選択し、次のオプションを設定します。**
     - **UID**：http://schemas.microsoft.com/identity/claims/objectidentifier
     - **ログイン**：http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
     - **名前**：http://schemas.microsoft.com/identity/claims/displayname
     - **プライマリ電子メール**：http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
8. **SAML を使用** オプションを選択した場合、役割マッピング で、SAML 認証ユーザーに付与する役割（例えば、管理者役割）の次の条件を指定します。

   http://schemas.microsoft.com/ws/2008/06/identity/claims/groups equals <オブジェクト ID>

   ここで、<オブジェクト ID> はグループのオブジェクト ID です。
9. （**オプション**）アプライアンス固有の SAML 設定をアプライアンスに表示するには、ローカルサービスプロバイダ（SP）設定セクションで **メタデータの表示** をクリックし、表示されるオプションを確認します。

   これらのフィールドにはデフォルト値が入っているため、ほとんどの場合は変更不要です。
10. 次の手順を実行します。
    a. ローカルサービスプロバイダ（SP）の設定 セクションで、**メタデータの表示**をクリックします。
    b. Microsoft Azure ポータルで、新しく作成したアプリ登録を探します。
    c. アプリ登録ページで、**リダイレクト URI を追加する** をクリックします。
    d. リダイレクト URI セクションで **Web** を選択し、SAML 設定 ページの ローカルサービスプロバイダ（SP）設定 の SP アサーションコンシューマサービス（url）値に設定します。
    e. 詳細設定 で、ログアウト URL フィールドに ローカルサービスプロバイダ（SP）設定 セクションの SP SLO エンドポイント（url）値を設定します。
    f. Azure で **API を公開** をクリックし、アプリケーション ID URI の横にある **設定** をクリックします。このフィールドには、ローカルサービスプロバイダ（SP）の設定 セクションの SP エンティティ識別子（uri）値を設定します。
    g. Azure で **マニフェスト** をクリックし、右側に表示される エディタ で、「groupMembershipClaims」属性を追加または更新し、その値を「SecurityGroup」または「All」に設定します。

    例：「groupMembershipClaims」：「SecurityGroup」、
11. **保存** をクリックします。
12. SAML 構成をテストします。
    a. アプライアンスからログアウトします。
    b. IdP アカウントにログインしていることを確認します。
    c. 管理者コンソール または ユーザーコンソール の「ようこそ」ページを開きます。
    d. ユーザー資格情報を指定せずに、**ログイン** をクリックします。

ヒント: アプライアンスで SAML が有効になっている場合は、**ローカルサインオン** をクリックし、ユーザー資格情報を指定します。

管理者コンソール または **ユーザーコンソール** ページが表示されます。

ユーザーセッションの確認

アプライアンスは、ユーザーセッションを追跡します。最新のセッションのリストを確認、またはアプライアンスのすべてのセッションを表示できます。

ログインしているユーザーのパブリック IP アドレスに関連付けられている場所をアプライアンスで表示できるようにするには、ロケーションデータベースをインストールする必要があります。詳細については、「ロケーションデータベースのインストールと設定」を参照してください。

最近のセッション ページには、すべてのセッションが表示されます。ユーザーアカウントに関連付けられている最新のセッションのクイックリストを表示するには、自分の最近のセッション ペインを使用します。詳細については、「ユーザーセッションのリストを表示」を参照してください。

ロケーションデータベースのインストールと設定

ユーザーセッションの詳細には、現在ログインしているユーザーの IP アドレスが含まれます。この情報は、最近のセッション ページに表示されます。パブリック IP アドレスの場合は、特定の IP アドレスに関連付けられた地理的な場所を表示することもできますが、これには、ロケーションデータベースをアプライアンスにインストールする必要があります。MaxMind Geolocation データベースは無料でインストールでき、任意のパブリック IP アドレスのユーザーの場所を表示できます。

MaxMind では、国と都市のデータベースが利用できます。都市データベースは通常、サイズが大きく、インストールに時間がかかります。国データベースでは、各パブリック IP アドレスに関連付けられた国の名前のみが提供され、都市データベースでは、アプライアンスで都市、州または都道府県（該当する場合）、および国を表示できます。

更新されたバージョンをインストールすることで、ロケーションデータベースを定期的に更新できます。複数のデータベースを時間の経過とともにインストールすることは可能ですが、最後にインストールされたデータベースは、以前のバージョンの内容を上書きします。例えば、国データベースがすでにインストールされていて、アプライアンスに都市データベースをインストールした場合、最近のセッション ページの 場所 列に新しくインストールされた都市データベースの情報が反映されます。

MaxMind Geolocation データベースの詳細については、https://www.maxmind.com/ を参照してください。

注: アプライアンスへのアクセスにプライベート IP アドレスが使用されている場合、場所は表示されません。

1. https://www.maxmind.com/ からロケーションデータベースをダウンロードしてください。

   注: MaxMind からデータベースファイルをダウンロードするには、まずユーザープロファイルを作成します。CSV ファイルではなく、MMDB 形式を使用するファイルをダウンロードする必要があります。

2. 次のいずれかを実行します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
3. 表示される 一般設定 ページの ジオロケーション検索データベース セクションで、ダウンロードした ZIP ファイルをポイントします。

これを行うには、MaxMind Geolocation データベース で、**ファイルの選択** をクリックし、新しくダウンロードしたファイルに移動します。

4. **保存** をクリックします。

   インストールするデータベースのタイプによっては、データベースのインストールが完了するまでに数分かかる場合があります。インストールが完了すると、データベースタイプ および データベースバージョン フィールドに関連する詳細情報が表示されます。

   注: 都市データベースのインストールと更新には、通常、ファイルサイズのため、国データベースよりも長い時間がかかります。

次に、最近のセッション ページに移動して、現在のユーザーの場所データを確認します。詳細については、「ユーザーセッションのリストを表示」を参照してください。

ユーザーセッションのリストを表示

アプライアンス上のユーザーセッションを確認できます。自分の最近のセッション ペインを使用して、アカウントに関連付けられている最新のセッションを表示します。アプライアンスで現在アクティブなすべてのセッションは、最近のセッション ページで確認することもできます。

アプライアンスが現在のユーザーに対して複数のセッションを検出した場合、アイコンには赤色の感嘆符が表示されます。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. 右上隅にある 最近のセッション アイコンをクリックします。

   注: ユーザーアカウントに複数のアクティブなセッションが関連付けられている場合は、最近のセッション アイコンに感嘆符が表示されます。

3. 表示された 自分の最近のセッション ペインで、最新のユーザーセッションのリストを確認します。

   各エントリは、ブラウザ、IP アドレス、セッション期間、最新のアクティビティの日時、および該当するアクションを特定します。

   注: 必要に応じて、アクション 列の削除アイコンをクリックして、重複したセッションを削除できます。

4. アプライアンスで現在アクティブなすべてのセッションを表示するには、自分の最近のセッション ペインで、最近のすべてのセッションを表示 をクリックします。

   表示される 最近のセッション ページでは、各エントリにユーザー名、使用しているブラウザ、オペレーティングシステム、IP アドレス、セッション期間、最後のアクティビティの日時、および適用可能なアクションが表示されます。パブリック IP アドレスを持つユーザーの場合、ロケーションデータベースがインストールされている場合は、場所も表示されます。詳細については、「ロケーションデータベースのインストールと設定」を参照してください。

管理対象デバイスへの KACE エージェントの展開

KACE エージェントは、デバイスにインストールすることで、インベントリのレポーティングおよびその他の管理機能を可能にするアプリケーションです。管理対象デバイスにインストールされた KACE エージェントは、エージェントメッセージプロトコルを通じてアプライアンスと通信します。エージェントは、管理対象デバイスからのインベントリ情報の収集や、管理対象デバイスへのソフトウェアの配布などのスケジュール済みタスクを実行します。

次のいずれかの方法を使用して、KACE エージェントを管理対象デバイスに展開できます。

ヒント: 認証された KACE エージェントのみがアプライアンスとの接続を正常に確立できます。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。

- **KACE エージェントのプロビジョニング**：エージェントのプロビジョニングアシスタントを使用して、Windows、Mac OS X、およびLinuxオペレーティングシステムを搭載したデバイスのプロビジョニングを実行できます。アシスタント内で、アプライアンス GPO プロビジョニングツールを使用してエージェントを Windows デバイスに展開するか、またはオンボードプロビジョニングを使用してエージェントを Windows、Mac OS X、または Linux デバイスに展開するかを選択できます。詳細については、「KACE エージェントのプロビジョニング」を参照してください。
- **KACE エージェントを手動展開する**：手動展開の使用は、エージェントの自動プロビジョニングが現実的ではないときや、E メール、ログオンスクリプト、GPO（グループポリシーオブジェクト）、または Active Directory を使用して KACE エージェントを展開するときに便利です。アプライアンスには、異なる OS プラットフォーム用の KACE エージェントインストーラが含まれています。各プラットフォームには、KACE エージェントを展開するための 1 つ以上の方法が用意されています。開始するには、以下のセクションとそのサブトピックを参照してください。
  - Windows デバイス上で KACE エージェントを手動展開する
  - Linux デバイスでの手動による KACE エージェントの展開およびアップグレード
  - Mac デバイスでの手動による KACE エージェントの展開およびアップグレード

レプリケーション共有の使用

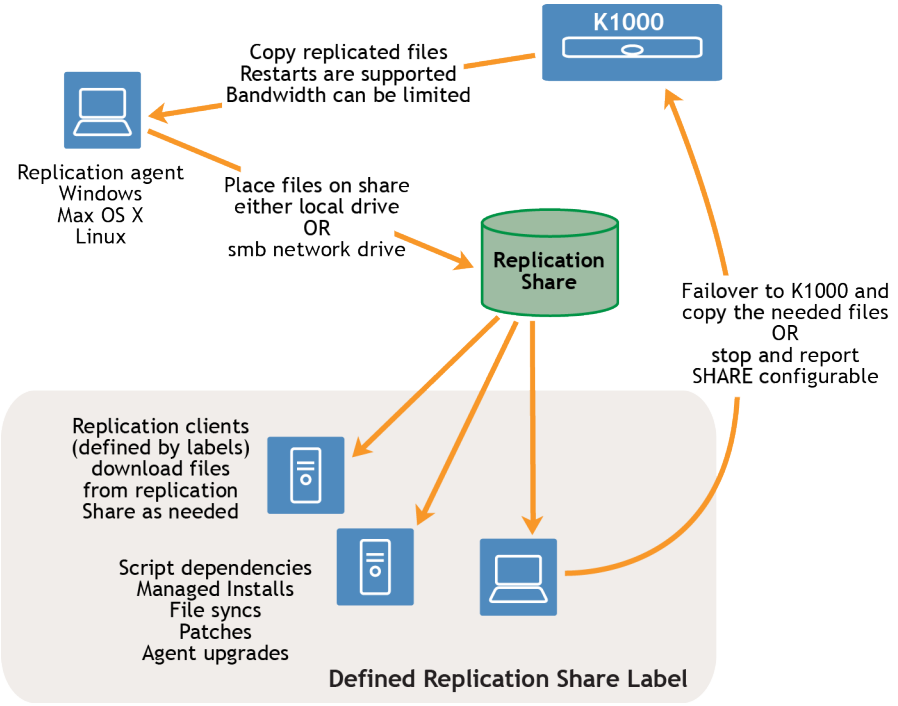
レプリケーション共有は、配布対象ファイルのコピーを保持するデバイスであり、管理対象デバイスが複数の地理的な場所に展開されている場合に特に有用です。

例えば、レプリケーション共有を使用すると、ロサンゼルスにあるアプライアンスからニューヨークにあるデバイスにファイルをダウンロードしなくても、ニューヨークの同じオフィスにある別のデバイスからファイルをダウンロードできます。レプリケーション共有は、すべてのデジタル資産の完全なレプリケーションであり、アプライアンスによって自動的に管理されます。ラベルでレプリケーション共有を指定していると、そのラベルに含まれるデバイスは、常にレプリケーション共有にアクセスしてファイルを取得します。

また、レプリケーション共有を使用すれば、ネットワーク帯域幅と速度が懸念される管理対象インストール、パッチ、またはDellアップデートも展開できます。レプリケーション共有は、アプライアンスからの直接ダウンロードに代わる便利な手段です。

レプリケーション共有により、デバイス上の共有フォルダに、アプリケーションインストーラ、パッチ、アップグレード、およびスクリプト依存関係を複製できます。レプリケーションアイテムがアプライアンスから削除されると、そのアイテムはレプリケーション共有で削除対象としてマークされ、レプリケーションタスクサイクルで削除されます。次の図に、レプリケーション共有の設定とタスクフローを示します。

レプリケーション共有の設定



レプリケーション共有を作成するには、各リモートサイトで**レプリケーションデバイス**として機能するデバイスを1つ指定します。アプライアンスは、指定したターゲットパス上のレプリケーションデバイスにすべてのレプリケーションアイテムをコピーします。レプリケーションプロセスは、ネットワークエラーやレプリケーションスケジュールのために停止されても、自動的に再開されます。停止された場合、レプリケーションプロセスは停止されたポイントで再開されます。

スニーカーネット共有：新しいフォルダを作成し、そのフォルダに既存のレプリケーションフォルダの内容をコピーできます。その後、アプライアンスで新しいレプリケーションフォルダとしてこのフォルダを指定できます。すべてのレプリケーションアイテムが新しいフォルダに含まれているかどうかが確認され、新しいアイテムのみが複製されます。これにより、帯域幅が節約されます。新しいフォルダにレプリケーションフォルダの内容を手動でコピーできます。デバイスで作成されたレプリケーションフォルダの階層は次のようになります。

\\<マシン名>\<フォルダ名>\repl2\<レプリケーションアイテム>フォルダ

デバイス名とフォルダ名はユーザーが定義します。一方、repl2 はアプライアンスによって自動的に作成されます。レプリケーションアイテムのフォルダには、パッチ、kbot、アップグレードファイル、およびアプリケーション用のフォルダが含まれます。

すべてのレプリケーションアイテムはまずレプリケーションキューに表示されます。その後、ターゲットパスに一度に1個ずつコピーされます。新しいレプリケーションアイテムは、まずレプリケーションキューに表示され、10分後にコピーされます。

レプリケーションアイテムは次の順にコピーされます。

1. スクリプト依存関係
2. アプリケーション
3. エージェントアップグレード
4. パッチ

レプリケーション共有の作成

管理対象デバイスでレプリケーション共有を作成できます。

レプリケーション共有を作成するには、以下を実行する必要があります。

- ソフトウェアファイルを書き込むターゲットパスへの**書き込み**権限を取得します。
- KACE エージェントをレプリケーション共有にインストールします。
- このプロセスを開始する前にデバイス用のラベルを作成します。

レプリケーション共有を作成できるのは、インベントリの デバイス リストに表示されているデバイスのみです。使用するデバイスが デバイス リストに表示されていない場合は、デバイスをレプリケーション共有として使用する前に、そのデバイスのインベントリレコードを作成する必要があります。

詳細については、「インベントリ情報の管理」を参照してください。

1. レプリケーションスケジュールの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**配布** をクリックして、**レプリケーション** をクリックします。
   c. **アクションの選択 > 新規作成** を選択します。
2. 設定 セクションで、**有効** チェックボックスをオンにします。
3. **オプション**：レプリケーション共有を使用できないときにアプライアンスを使用するには、**アプライアンスへのフェールオーバー** を選択します。

   注:「**アプライアンスへのフェールオーバー**」を有効化するのは、レプリケーション共有のテスト後のみとしてください。
4. デバイス ドロップダウンリストで、レプリケーション共有として使用するデバイスを選択します。

   レプリケーション共有は以下の2通りの方法で作成できます。

   - **ローカルで作成する。**
   - **共有ネットワークドライブ上に作成する。**
5. 複製するパッチの **オペレーティングシステム** と **ロケール** を選択します。パッチサブスクリプションで選択したオペレーティングシステムと ロケールにしたがって、リストが入力されます。
6. パッチと更新プログラムをレプリケーション共有にコピーするには、**アプリケーションパッチを含める**、**Windows 機能更新プログラムを含める**、および **Dell 更新プログラムを含める** チェックボックスをオンにします。
7. Destination Share（ ターゲットの共有 ） 設定を指定します。

オプション	説明
パス	レプリケーションデバイスがレプリケーション共有に使用するパス。アプリケーションはアプライアンスからこの場所にコピーされます。ローカルドライブの場合、次のようなローカルドライブ構文を使用します。C:**kace_sma_share** ネットワークドライブの場合、次のようなUNC形式を使用します。**kaceRep****kace_sma_share**\ **注:** **KaceRep**\e$のような**$**表記法はサポートされていません。
ローカル共有または UNC	ローカル共有と UNC のいずれを使用するのかを選択します。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情**

オプション	説明
	報の追加 を選択して、まだリストされていない資格情報を追加します。 詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。
ラベル	レプリケーション共有を使用しているデバイスのラベル。選択したラベルでKACE_ALT_LOCATIONが指定されていないことを確認します。KACE_ALT_LOCATIONは、デバイスへのファイルのダウンロード中、レプリケーション共有よりも優先されます。

8. Download Share（ダウンロードの共有）設定を指定します。

オプション	説明
パス	レプリケーションドライブからアイテムをコピーするためにレプリケーションラベル内のデバイスによって使用されるパス。 例えば、UNCパスは次のようになります。 \\fileservername\directory\kace_sma\ その他のデバイスには、この共有フォルダからレプリケーションアイテムをコピーするための**読み取り**権限が必要です。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。

9. スケジュール セクションで、各設定を次のように指定します。

オプション	説明
高帯域幅	レプリケーションに使用される最大帯域幅。このフィールドを空白にすると、レプリケーションに使用可能な最大帯域幅が使用されます。このフィールドは、バイト/秒単位で指定します。
低帯域幅	レプリケーションに使用される制限された帯域幅。このフィールドを空白にすると、レプリケーションに使用可能な最大帯域幅が使用されます。このフィールドは、バイト/秒単位で指定します。

オプション	説明
スケジュールテーブル	1時間（24時間形式）および曜日ごとに使用される帯域幅。 • 帯域幅の選択を変更するには、四角形内をクリックします。 • 時間（列）を選択するには、時間の数字をクリックします。 • 曜日（行）を選択するには、曜日をクリックします。 帯域幅は以下のように色分けされます。 • **白**: レプリケーションがオフになっています。 • **水色**: レプリケーションが低帯域幅で実行されます。 • **青**: レプリケーションが高帯域幅で実行されます。
スケジュールのコピー元	ドロップダウンリストから、アイテムの複製時に使用する既存のレプリケーションスケジュールを選択します。
メモ	任意の追加情報を入力します。

10. **保存** をクリックします。

    レプリケーション ページが表示されます。
11. **オプション**：レプリケーション共有をテストしたら、3に戻って **アプライアンスへのフェールオーバー** を有効にします。

関連トピック

手動ラベルの追加または編集

パッチ管理について

レプリケーション共有の詳細の表示

レプリケーション共有として使用するデバイスの詳細を表示できます。

1. レプリケーション リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**配布** をクリックして、**レプリケーション** をクリックします。

    このページには、アプライアンスで使用可能なレプリケーション共有のリストが表示されます。各レプリケーション共有のデフォルトのビューでは、ステータス、レプリケーションの タスク、関連する デバイス、ターゲットパス、KACE エージェントのバージョン、ラベル、レプリケーション共有が 有効 であるかの表示、およびコピー待ちのファイル数とそのファイル合計サイズが（ToDo 列）に表示されます。ToDo 列に表示される情報では、レプリケーションプロセスが完了しているかを調べるための個々の共有ではなく、このリスト内の各レプリケーション共有に対するレプリケーションプロセスのステータスを確認できます。
2. デバイス 列で、レプリケーション共有の名前をクリックして、レプリケーションスケジュールの詳細 ページを表示します。

このページでは、以下を実行できます。

- **レプリケーションキューの表示**: レプリケーションキューに入っているアイテムを表示するには、設定情報の下の **レプリケーションキューの表示** をクリックします。このビューは、ページにアクセスするとデフォルトで表示されます。
- **レプリケーションインベントリの表示**: 共有に複製されたアイテムを表示するには、設定情報の下の **共有インベントリの表示** をクリックします。
- **レプリケーションキューの削除**: 削除対象としてマークされているレプリケーションアイテムを表示するには、設定情報の下の **削除キューの表示** をクリックします。

資格情報の管理

アプライアンスでは、管理対象コンピュータやサーバなど他のシステムへのログインに必要なユーザー名とパスワード、および Google や SNMP 認証に必要な情報を一元的に管理できます。

インベントリ（検出、プロビジョニング、およびエージェント不要デバイス管理）、配布（管理対象インストール、ファイル同期、およびレプリケーション）、スクリプト（設定ポリシーおよびセキュリティポリシー）の各セクションのドロップダウンリストから、アプライアンスの 資格情報管理 ページに追加された資格情報を選択できます。

また、資格情報の管理 ページで更新された資格情報は、その情報がさまざまなアプライアンスコンポーネントのどこで使用されているかを問わず自動的に更新されます。資格情報を使用する各アイテムを個別に更新する必要はありません。

ただし、アプライアンスに追加する資格情報は、ターゲットシステム上の資格情報に一致する必要があります。ターゲットシステム上の資格情報を変更した場合は、アプライアンスの 資格情報管理 ページの資格情報も変更する必要があります。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織ごとに資格情報を個別に管理します。

注: LDAP 設定ページでは、資格情報の管理 ドロップダウンリストを使用できません。そのため、シングルサインオンおよび LDAP 認証を使用するアプライアンス**管理者コンソール**や**ユーザーコンソール**にアクセスするためのユーザー資格情報を管理する用途には、この機能は使用されません。詳細については、「ユーザーアカウントおよびユーザー認証について」を参照してください。

資格情報管理設定の変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。この情報には、アイテムを作成、変更、または削除した日付およびこれらの操作を実行したユーザーが含まれており、トラブルシューティングの際に役立ちます。

詳細については、「履歴設定について」を参照してください。

シークレットキー資格情報の追加および変種

インベントリ、配布、およびスクリプト作成に使用されているシークレットキー資格情報の管理を合理化するには、それらの資格情報を資格情報の管理ページに追加します。シークレットキー資格情報は、KACE Cloud Mobile Device Manager を使用して管理されているデバイスに対して作成できます。

- KACE Cloud Mobile Device Manager からシークレットキーを取得しています。
- **管理者コンソール**で管理者権限を持っています。

資格情報を追加すると、それらを毎回手動で入力するのではなく、設定ページで選択できます。また、資格情報を使用するどの設定ページからでも、それらを追加できます。設定ページで追加した資格情報は、資格情報管理ページに自動的に追加されます。

1. 資格情報管理 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。
2. **アクションの選択 > 新規作成** を選択します。
3. 資格情報の追加 フォームで、資格情報のプロパティを指定します。

    注: 検出スケジュールの詳細 ページなど資格情報を使用するページから、このフォームにアクセスすることもできます。これらのページで追加した資格情報は、資格情報管理 リストに自動的に追加されます。

オプション	説明
名前	資格情報に固有の名前。この名前は、資格情報管理 リストのほか、スクリプト などのコンポーネントセクションの資格情報選択ドロップダウンリストに表示されます。この名前は、**管理者コンソール**での識別に使用されるものであり、ターゲットデバイス上の実際の資格情報の一部ではありません。
タイプ	資格情報の分類。KACE Cloud Mobile Device Manager から取得したシークレットキーを含む資格情報を指定するには、**シークレットキー** を選択します。
シークレット	KACE Cloud Mobile Device Manager 環境のシークレットキー。
Show typing（ 入力の表示 ）	資格情報の追加 フォームの パスワード フィールドに文字を表示します。このオプションは、資格情報を追加しているときにのみ使用できます。既存の資格情報を編集している場合は、パスワードの文字を表示することはできません。
メモ	資格情報に関する任意の追加情報を入力します。

4. **保存** をクリックします。

    資格情報が 資格情報管理 リストに表示され、資格情報を使用するコンポーネントで選択可能になります。

ユーザーとパスワード資格情報の追加および編集

インベントリ、配布、および スクリプト に使用されているユーザー名とパスワードの資格情報の管理を合理化するには、それらの資格情報を 資格情報管理 ページに追加します。ユーザー名とパスワードの資格情報は、Mac、Windows、Linux の各オペレーティングシステムに対してだけでなく、VMware ESXi ホストおよび vCenter サーバーに対しても作成できます。

- 管理する資格情報のユーザー名とパスワードを持っています。
- **管理者コンソール**で管理者権限を持っています。

資格情報を追加すると、それらを毎回手動で入力するのではなく、設定ページで選択できます。また、資格情報を使用するどの設定ページからでも、それらを追加できます。設定ページで追加した資格情報は、資格情報管理ページに自動的に追加されます。

1. 資格情報管理 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。
2. **アクションの選択 > 新規作成** を選択します。
3. 資格情報の追加 フォームで、資格情報のプロパティを指定します。

    注: 検出スケジュールの詳細 ページなど資格情報を使用するページから、このフォームにアクセスすることもできます。これらのページで追加した資格情報は、資格情報管理 リストに自動的に追加されます。

オプション	説明
名前	資格情報に固有の名前。この名前は、資格情報管理 リストのほか、スクリプト などのコンポーネントセクションの資格情報選択ドロップダウンリストに表示されます。この名前は、**管理者コンソール**での識別に使用されるものであり、ターゲットデバイス上の実際の資格情報の一部ではありません。
タイプ	資格情報の分類。ユーザー名とパスワードが含まれる資格情報を指定するには、**ユーザーとパスワード**を選択します。
User or Domain\User（ユーザーまたはドメイン\ユーザー）	資格情報に必要なユーザー名。 **ヒント:** 一部の Windows 設定では、Domain\User形式が必要になることがあります。
パスワード	資格情報に必要なパスワード。
Show typing（入力の表示）	資格情報の追加 フォームの パスワード フィールドに文字を表示します。このオプションは、資格情報を追加しているときにのみ使用できます。既存の資格情報を編集している場合は、パスワードの文字を表示することはできません。
ターゲット	資格情報を使用できるデバイスタイプ。 **ヒント:** 複数のデバイスタイプを選択できるほか、指定した資格情報が複数のオペレーティングシステムでの認証に使用できる場合にはオペレーティングシステムも選択できます。
メモ	資格情報に関する任意の追加情報を入力します。

4. **保存** をクリックします。

    資格情報が 資格情報管理 リストに表示され、資格情報を使用するコンポーネントで選択可能になります。

LDAP ユーザーとパスワード資格情報の追加および編集

LDAP 資格情報を簡単に管理し、パスワード設定するには、それらの資格情報を 資格情報の管理 ページに追加します。Mac、Windows、および Linux オペレーティングシステム用の LDAP ユーザー / パスワード資格情報を作成できます。

- 管理する資格情報の LDAP ユーザー名とパスワードを持っています。
- **管理者コンソール**で管理者権限を持っています。

資格情報を追加すると、それらを毎回手動で入力するのではなく、設定ページで選択できます。また、資格情報を使用するどの設定ページからでも、それらを追加できます。設定ページで追加した資格情報は、資格情報管理ページに自動的に追加されます。

1. 資格情報管理 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。
2. **アクションの選択 > 新規作成** を選択します。
3. 資格情報の追加 フォームで、資格情報のプロパティを指定します。

注: 検出スケジュールの詳細 ページなど資格情報を使用するページから、このフォームにアクセスすることもできます。これらのページで追加した資格情報は、資格情報管理 リストに自動的に追加されます。

オプション	説明
名前	資格情報に固有の名前。この名前は、資格情報の管理 リストのほか、LDAP ラベルの詳細 ページの資格情報選択ドロップダウンリストに表示されます。この名前は、**管理者コンソール**での識別に使用されるものであり、ターゲットデバイス上の実際の資格情報の一部ではありません。
タイプ	資格情報の分類。**LDAP ユーザー / パスワード** を選択して、ユーザー名とパスワードを含む LDAP 資格情報を指定します。
User or Domain\User（ ユーザーまたはドメイン\ユーザー ）	資格情報に必要なユーザー名。 **ヒント:** 一部の Windows 設定では、Domain\User 形式が必要になることがあります。
パスワード	資格情報に必要なパスワード。
Show typing（ 入力の表示 ）	資格情報の追加 フォームの パスワード フィールドに文字を表示します。このオプションは、資格情報を追加しているときにのみ使用できます。既存の資格情報を編集している場合は、パスワードの文字を表示することはできません。

オプション	説明
メモ	資格情報に関する任意の追加情報を入力します。

4. **保存** をクリックします。

   資格情報が 資格情報管理 リストに表示され、資格情報を使用するコンポーネントで選択可能になります。

Google Workspace 資格情報の追加および編集

インベントリ、配布、スクリプト、サービスデスクに使用されている Google Workspace 資格情報の管理を合理化するには、該当する資格情報を 資格情報管理 ページに追加します。

アプライアンスは、Google API を使用して Google Workspace ドメインへのアクセス権を取得できます。次のアプライアンス管理対象コンポーネントは、Google API を使用して認証できます。

- **Google Workspace のデバイスの検出とインベントリ**：これには、Google Workspace ドメイン（以前の G Suite）で管理される Chromebook とモバイルデバイスの両方が含まれます。このタイプの認証には、以下のことが必要です。
  - Chrome デバイス管理がサポートされている Google Workspace ドメインがあること。
  - ドメインのメンバーである Google ユーザー管理者アカウントがあること。アカウントにスーパーユーザー役割が割り当てられていること。
  - この手順で開発者アカウントとして使用できるGoogleアカウントを持っています。このアカウントは、管理者アカウントと同じである必要はなく、ビジネスドメインまたはエデュケーションドメインのメンバーである必要もありません。
- **サービスデスクキュー受信 E メール**：これには、Google Workspace または Gmail のパブリックアカウントの一部である E メールアカウントが含まれます。このタイプの認証には、以下のことが必要です。
  - Gmail アカウントがあること。
  - サービスアカウントには、次の内容が適用されます。
    - Gmail アカウントは Google Workspace ドメインに属します。
    - ドメインのメンバーである Google ユーザー管理者アカウントを持っている場合、そのアカウントにスーパー管理者役割が割り当てられている必要があります。
  - この手順で開発者アカウントとして使用できるGoogleアカウントを持っています。このアカウントは、管理者アカウントと同じである必要はなく、ビジネスドメインまたはエデュケーションドメインのメンバーである必要もありません。

これらのコンポーネントタイプごとに、アプライアンスは Google API による次のメソッド認証をサポートします。選択する方法は、Google Workspace 資格情報を使用するコンポーネントと、アプライアンス管理者の設定情報または役割によって異なります。

- **サービスアカウント認証**は、一意のクライアント ID に関連付けられたサービスアカウントキーで構成されます。Google Workspace のスーパー管理者は、クライアント ID を使用して、リソースにサービスアカウントドメイン全体アクセスを許可できます。
  - **これは、Chromebook とモバイルデバイスの検出とインベントリに適した方法です。**
  - スーパー管理者が Google Workspace コンソールを使用して設定を行う必要があります。
  - 特定のリソースタイプへのドメイン全体のアクセスが許可されます。サービスデスクキューの E メールの場合は、サービスアカウントに E メール受信トレイへのアクセスが許可されます。管理者は、目的のサービスデスクの E メールでのみ使用されるようにする必要があります。
- **OAuth クライアント認証**は、OAuth クライアント ID とクライアントシークレットで構成され、ブラウザベースのワークフローを使用して特定の Google リソースへのアクセスを要求および許可します。
  - **これは、サービスデスクキュー受信 E メールの統合に適した方法です。**
  - **管理者コンソール** での資格情報の設定に使用するブラウザは、パブリックと見なされる（プライベートドメインではない）ホスト名を使用してアプライアンスに接続する必要があります。
  - これは、Gmail のパブリックアカウントで使用できます。

必要に応じて、1 つまたは複数の Google Workspace サービスアカウントまたは OAuth 資格情報を作成して開始します。資格情報を追加すると、それらを毎回手動で入力するのではなく、設定ページで選択できます。また、資格情報を使用するどの設定ページからでも、それらを追加できます。設定ページで追加した資格情報は、資格情報管理 ページに自動的に追加されます。アプライアンスは、入力時に保存された Google OAuth 資格情報を検証しませんが、無効な資格情報を使用して変更を保存しようとすると、エラーが発生します。

1. Google Cloud Platform プロジェクトを作成および設定します。
   a. https://console.cloud.google.comで、開発者アカウントにサインインします。
   b. プロジェクトに新しい名前と ID を割り当てます。
   c. 必要に応じて、目的の Admin SDK の API または Gmail API を有効にします。
2. **サービスアカウント資格情報のみ。**
   a. Google Cloud Console にログインしたまま、IAM と管理者 を選択します。
   b. 目的の名前と説明を使用してサービスアカウントを作成します。
   c. サービスアカウントキーを追加し、JSON キーファイルを保存します。
   d. 後で使用するために、サービスアカウントの OAuth 2 クライアント ID を記録します。
3. **OAuth 資格情報のみ。**
   a. Google Cloud Console にログインしたまま、API とサービス を選択し、OAuth 同意画面に進みます。
   b. 開発者アカウントがアクセスするリソースと同じ Google Workspace ドメインに属している場合は、内部 を選択し、それ以外の場合は、外部 を選択します。
   c. アプリを作成し、その名前、サポート E メールアドレス、開発者の連絡先 E メールアドレスを指定します。
   d. 次のスコープを追加します。
   - **デバイスの検出とインベントリのみ：**
     - https://www.googleapis.com/auth/admin.directory.device.chromeos
     - https://www.googleapis.com/auth/admin.directory.device.mobile
     - https://www.googleapis.com/auth/admin.directory.user
   - **サービスデスクキューの E メールのみ：**
     - https://www.googleapis.com/auth/gmail.modify

   e. 資格情報を作成し、OAuth クライアント ID を選択します。

f. アプリケーションタイプとして Web アプリケーション を選択します。
g. クライアントに名前を付けます。
h. 次の URI を指定します。https://<appliance_hostname>/common/authorize.php。ここで、appliance_hostname はアプライアンス 管理者コンソール のホスト名です。
i. 後で使用するために、クライアント ID とクライアントシークレットを記録します。

4. **サービスアカウント資格情報のみ（オプション）**。ドメイン全体の権限をサービスアカウントに委任します。この手順には、Google Workspace 管理者コンソールへのスーパー管理者アクセスが必要です。

注: サービスアカウントに対するスコープの変更を Gmail に許可すると、そのサービスアカウントにそのドメイン上のすべてのメールボックスに対するアクセスが付与されます。サービスアカウントキーの資格情報が適切に保護されていることを確認します。

a. https://admin.google.com/ で Google 管理コンソールにサインインします。
b. **セキュリティ > アクセスとデータ制御 > API 制御 > ドメイン全体の委任の管理** で、 新しい委任を作成し、2 で作成したサービスアカウントのクライアント ID を指定します。
c. 次のスコープを追加します。

- **デバイスの検出とインベントリのみ：**
  - https://www.googleapis.com/auth/admin.directory.device.chromeos
  - https://www.googleapis.com/auth/admin.directory.device.mobile
  - https://www.googleapis.com/auth/admin.directory.user
- **サービスデスクキューの E メールのみ：**
  - https://www.googleapis.com/auth/gmail.modify

5. 資格情報管理 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。
6. **アクションの選択 > 新規作成** を選択します。
7. 資格情報の追加 フォームで、資格情報のプロパティを指定します。

オプション	説明
名前	資格情報に固有の名前。この名前は、資格情報管理リストのほか、スクリプト などのコンポーネントセクションの資格情報選択ドロップダウンリストに表示されます。この名前は、**管理者コンソール**での識別に使用されるものであり、実際の資格情報の一部ではありません。
タイプ	資格情報の分類。必要に応じて、**Google Workspace** または **Gmail** を選択します。

8. **サービスアカウント資格情報のみ**。資格情報の追加 フォームで、資格情報のプロパティを指定します。

オプション	説明
サービスアカウント	このオプションを選択します。
権限借用アカウント	• **デバイスの検出とインベントリのみ**：Google 管理コンソールでデバイスにアクセスできる管理者の E メールアドレス。 • **サービスデスクキューの E メールのみ**：受信 E メールの受信元となる E メールアドレス。
サービスアカウントキー	2 で取得した JSON ファイルに移動します。
メモ	資格情報に関する任意の追加情報を入力します。

9. **OAuth 資格情報のみ**。資格情報の追加 フォームで、資格情報のプロパティを指定します。

オプション	説明
OAuth	このオプションを選択します。
クライアントID	3 で取得した Google Developer API クライアント ID。
クライアントシークレット	3 で取得した Google Developer API クライアントシークレット。
Show typing (入力の表示)	資格情報の追加 フォームの クライアントシークレット フィールドに文字を表示します。このオプションは、資格情報を追加しているときにのみ使用できます。既存の資格情報を編集している場合は、クライアントシークレット フィールドの文字を表示することはできません。
資格情報を承認	クリックしてログインし、表示されるページで目的の Google アカウントへのアクセスを許可します。 • **デバイスの検出とインベントリのみ**：Google 管理コンソールでデバイスにアクセスできる管理者のアカウント。 • **サービスデスクキューの E メールのみ**：受信 E メールの受信元となる E メールアドレス。
メモ	資格情報に関する任意の追加情報を入力します。

10. **保存** をクリックします。

資格情報を使用するコンポーネントで資格情報が選択可能になります。

SNMP 資格情報の追加および編集

インベントリ、配布、および スクリプト に使用されている SNMP 資格情報の管理を合理化するには、それらの資格情報を 資格情報管理 ページに追加します。

- SNMP 認証に必要な情報を持っています。
- **管理者コンソール**の管理者権限があります。

資格情報を追加すると、それらを毎回手動で入力するのではなく、設定ページで選択できます。また、資格情報を使用するどの設定ページからでも、それらを追加できます。設定ページで追加した資格情報は、資格情報管理ページに自動的に追加されます。

1. 資格情報管理 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。
2. **アクションの選択 > 新規作成** を選択します。
3. 資格情報の追加 フォームで、次の情報を指定します。

オプション	説明
名前	資格情報に固有の名前。この名前は、資格情報管理リストのほか、スクリプト などのコンポーネントセクションの資格情報選択ドロップダウンリストに表示されます。この名前は、**管理者コンソール**での識別に使用されるものであり、実際の資格情報の一部ではありません。
タイプ	資格情報の分類。SNMP 資格情報を指定するには、**SNMP** を選択します。

4. SNMP v1 または v2c の場合、次の情報を指定します。

オプション	説明
SNMP v1 または v2c	認証または暗号化を使用しない SNMP 資格情報。
コミュニティ文字列	SNMP v1 または v2c の場合、照会するコミュニティ文字列。デフォルトは「**Public**」です。SNMP v1 または v2c には、パブリック文字列が必要です。
メモ	資格情報に関する任意の追加情報を入力します。

5. SNMP v3 の場合、次の情報を指定します。

オプション	説明
SNMP v3SNMP v3	認証および暗号化アルゴリズムでセキュリティを高める必要がある SNMP 資格情報。
セキュリティ名	SNMP v3 の場合、USM（ユーザーベースのセキュリティモデル）ユーザーアカウントの名前。このアカウントと、認証と暗号化に必要なすべてのパス

オプション	説明
	ワードは、ターゲットデバイスで設定する必要があります。
セキュリティレベル	SNMP v3 の場合、セキュリティのレベル。セキュリティレベルは次の通りです。 • 「**authPriv**」: SNMP v3セキュリティの最も高いレベル。認証と暗号化の両方を使用します。このレベルを使用するには、SNMP V3 の認証とプライバシーの設定をすべて指定する必要があります。 • 「**authNoPriv**」: SNMP v3セキュリティの中間のレベル。認証のみを使用します。通信は暗号化されません。このレベルを使用するには、認証の設定を指定する必要があります。 • 「**noAuthNoPriv**」: SNMP v3セキュリティの最も低いレベル。通信は暗号化されません。
認証パスワード	SNMP v3 の場合、**authPriv** または **authNoPriv** のセキュリティレベルが選択されている場合に通信を認証するために使用されるパスワード。このパスワードは USM ユーザーと関連付けられます。ターゲットデバイスで設定する必要があります。
プロトコル	SNMP v3 の場合、通信に使用されるプロトコル。プロトコルは次のとおりです。 • 「**SHA**」: Secure Hash Algorithm（SHA-1）。 • 「**MD5**」: Message Digest 5。SHA よりも高速ですが、セキュリティ性はそれよりも低いと考えられています。
プライバシーパスワード	SNMP v3 の場合、**authPriv** のセキュリティレベルが選択されているときに通信を認証するために使用されるパスワード。このパスワードは USM ユーザーと関連付けられます。ターゲットデバイスで設定する必要があります。
プロトコル	SNMP v3 の場合、プライバシーパスワードに使用されるプロトコル。プロトコルは次のとおりです。 • 「**DES**」: Data Encryption Standard。このアルゴリズムの鍵長は56ビットであり、AES よりセキュリティ性が低いと考えられています。 • 「**AES**」: Advanced Encryption Standard。このアプライアンスでは128ビットの鍵長がサポートされています。
メモ	資格情報に関する任意の追加情報を入力します。

6. **保存** をクリックします。

   資格情報を使用するコンポーネントで資格情報が選択可能になります。

Microsoft Office 365 OAuth 資格情報の追加および編集

サービスデスク E メール通信で使用される Office 365 資格情報を簡単に使用するには、資格情報管理ページにそれらを追加します。

- Office 365 アカウントを持っており、クライアント ID およびクライアントシークレットを使用して Microsoft Azure に Microsoft Active Directory アプリを作成しています。詳細については、https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portalを参照してください。
- **管理者コンソール**で管理者権限を持っています。

資格情報を追加すると、それらを毎回手動で入力するのではなく、設定ページで選択できます。また、資格情報を使用するどの設定ページからでも、それらを追加できます。設定ページで追加した資格情報は、資格情報管理ページに自動的に追加されます。アプライアンスは、入力時に保存された Office 365 資格情報を検証しませんが、無効な資格情報を使用して変更を保存しようとすると、エラーが発生します。

注: この機能は、アプライアンスへの SSL（セキュア）アクセスが有効になっている場合にのみ使用できます。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。

1. 資格情報管理 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。
2. **アクションの選択 > 新規作成** を選択します。
3. 資格情報の追加 フォームで、資格情報のプロパティを指定します。

オプション	説明
名前	資格情報に固有の名前。この名前は、資格情報管理リストのほか、サービスデスクの E メール設定などのコンポーネントセクションの資格情報選択ドロップダウンリストに表示されます。この名前は、**管理者コンソール**での識別に使用されるものであり、実際の資格情報の一部ではありません。
タイプ	資格情報の分類。Office 365 の資格情報を指定するには、**Office365 OAuth** を選択します。
クライアントID	Office 365 クライアント ID。
クライアントシークレット	Office 365 クライアントシークレット。
Show typing（入力の表示）	資格情報の追加 フォームの クライアントシークレット フィールドに文字を表示します。このオプションは、資格情報を追加しているときにのみ使用できます。既存の資格情報を編集している場合は、クライアントシークレット フィールドの文字を表示することはできません。
Azure AD テナントタイプ	利用可能なオプションから Azure AD テナントタイプを選択します。テナントタイプは、Azure AD 管

オプション	説明
	理ポータルで Azure AD アプリケーションを登録するときに選択したタイプと一致する必要があります。 • **マルチテナントおよび個人用 Microsoft アカウント - デフォルト**：このオプションを使用して、幅広い Microsoft ID へのアクセスを許可し、マルチテナント構成を有効にします。仕事用または学校用、または個人用の Microsoft アカウントを持つすべてのユーザーは、この資格情報を使用してアプリケーションまたは API にアクセスできます。これは、Office 365 を使用する学校や企業、および Xbox や Skype などのサービスへのサインインに使用される個人アカウントに適用されます。これはデフォルトの設定です。 • **Azure AD ディレクトリ - マルチテナント**：このオプションを使用して、ビジネスユーザーまたは教育ユーザーにアクセス権を付与し、マルチテナント構成を有効にします。Microsoft の職場または学校のアカウントを持つすべてのユーザーは、アプリケーションまたは API を使用できます。これには、Office 365 を使用する学校や企業も含まれます。 • **個人用 Microsoft アカウントのみ**：このオプションを使用して、Xbox や Skype などのサービスへのサインインに使用する個人アカウントへのアクセスを許可します。 • **組織ディレクトリのみ（シングルテナント）**：このオプションを使用して、組織に関連付けられているユーザーにアクセスを許可します。
資格情報を承認	クリックしてログインし、表示されるページで目的の Office 365 アカウントへのアクセスを許可します。
メモ	資格情報に関する任意の追加情報を入力します。

4. **保存** をクリックします。

   資格情報を使用するコンポーネントで資格情報が選択可能になります。

資格情報使用状況の表示

資格情報管理 ページに資格情報使用状況を表示できます。

- 資格情報が 資格情報管理 ページに追加されています。詳細については、「資格情報の管理」を参照してください。
- **管理者コンソール**で管理者権限を持っています。

1. 資格情報管理 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。

資格情報を使用するコンポーネントが 使用中 列に表示されます。

2. リストを並べ替えるには、テーブルの上にある 特定基準で表示 ドロップダウンリストから **タイプ** を選択します。

資格情報管理リストに基づくレポートの作成

資格情報を保持するように履歴サブスクリプションが設定されている場合は、資格情報が作成、編集、および削除されたときに表示されるレポートを生成できます。

- アプライアンスに資格情報を追加済みで、資格情報の管理 ページに表示されます。
- 資格情報を保持するように履歴サブスクリプションが設定されています。詳細については、「オブジェクト履歴の設定」を参照してください。

資格情報管理 ページからレポートを作成するときは、名前、タイプ、作成日、使用情報など資格情報に関する情報を含めることができます。ただし、パスワードやクライアントシークレットなどの認証詳細はレポートに含まれません。

注: アプライアンス上で組織コンポーネントが有効化されている場合は、各組織の資格情報レポートを個別に作成します。

1. 資格情報管理 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。
2. **アクションの選択** > **レポートの作成** を選択します。
3. レポートの詳細 ページで、レポートの名前を指定します。
4. 追加のレポート設定を選択し、**保存** をクリックします。詳細については、「リストページからのレポートの作成」を参照してください。

   レポートが **レポート** リストに表示されます。
5. レポートを生成するには、レポートの生成 列の形式を選択します。

資格情報のエクスポート

資格情報管理 ページに表示される資格情報のリストまたは選択した資格情報をエクスポートできます。

アプライアンスに資格情報を追加済みで、資格情報の管理 ページに表示されます。

名前、タイプ、資格情報の最終変更日、使用情報などの資格情報をエクスポートできます。パスワードやクライアントシークレットなどの認証詳細はエクスポートできません。

注: アプライアンス上で組織コンポーネントが有効化されている場合は、各組織の資格情報を個別にエクスポートします。

1. 資格情報管理 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。

2. **アクションの選択** > **エクスポート** を選択し、すべての資格情報をエクスポートするのか、選択した資格情報のみをエクスポートするのかを選択し、エクスポートした情報の形式を選択します。
3. エクスポートしたファイルを開くか、または保存します。

資格情報の削除

インベントリ、配布、スクリプト などいずれのコンポーネントでも資格情報が使用されていない場合には、その資格情報を削除できます。

- 資格情報を使用しているどのコンポーネントからも資格情報が削除されています。詳細については、「資格情報使用状況の表示」を参照してください。
- **管理者コンソール**の管理者権限があります。

1. 資格情報管理 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**設定** をクリックして、**資格情報** をクリックします。
2. 削除する資格情報の隣にあるチェックボックスをオンにします。

   注: 選択した資格情報のいずれかが使用中である場合は、エラーメッセージが表示されます。選択した資格情報の中に使用中のものがある場合は、それらの資格情報をまとめて削除することはできません。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

資産の設定

必要に応じて、資産および資産タイプを設定することができます。

資産管理コンポーネントについて

資産管理コンポーネントには、資産と資産タイプ（ テンプレート ）が含まれています。資産管理コンポーネントを使用すると、インベントリによって自動的に追加された資産および手動で追加した資産を管理できます。

デフォルト資産タイプは次のとおりです。デバイス、コストセンター、部門、ライセンス、場所、ソフトウェア、およびベンダー。必要に応じて、カスタム資産タイプを作成できます。詳細については、「資産タイプのカスタマイズ」を参照してください。

資産管理コンポーネントを使用して、次を実行できます。

- **ライフサイクル全体に渡る資産の管理:** 調達から展開、使用、ライフサイクル終了まで、ソフトウェアおよびその他のアイテムを追跡します。また、プリンタ、ネットワークデバイス、電話などの周辺機器を追跡することもできます。詳細については、「追跡する資産の識別」を参照してください。
- **ソフトウェアライセンスコンプライアンスの管理。**所有するライセンスや、デバイスにインストールされているアプリケーションのコピー数を追跡します。ソフトウェアカタログ インベントリと ソフトウェア

ページインベントリとのアイテムでは、ライセンスコンプライアンスを管理するためのオプションが異なります。詳細については、「ライセンスコンプライアンスの設定」を参照してください。

- **データの追跡:** 各注文書（PO）を資産として入力し、それを購入、受領、配布したアイテムにリンクすることで、POを追跡します。詳細については、「ソフトウェア ページインベントリのライセンス資産の追加」を参照してください。
- **物理的な資産の追跡**: デバイスのハードウェアやソフトウェアといった物理的資産や、オフィスの什器のようなその他の物理的資産を追跡します。こうしたアイテムの利用状況だけでなく、保証状況も追跡できます。詳細については、「物理的資産と論理的資産の管理」を参照してください。
- **論理的な資産の追跡**: 地理的な場所、コストセンター、部門、ベンダーといった、論理的な資産を追跡します。論理的資産は通常、レポート作成の基礎情報として使用されます。例えば、「この部門にはデバイスが何台あるか」や、「ソフトウェアベンダーから購入したライセンスはいつ期限切れになるか」といった質問の答えを得るために論理的資産が使用されます。詳細については、「物理的資産と論理的資産の管理」を参照してください。
- **資産間の関連付けと追跡:** 資産間で、ピアツーピアの関係および親子関係を作成できます。これらの関係により、PO（注文書）、場所、部門、プロジェクト、またはその他の基準によって資産を追跡できるようになります。詳細については、「資産フィールド間の関連付け」を参照してください。

資産管理ダッシュボードの使用方法

資産管理ダッシュボードには、選択した組織（該当する場合）またはアプライアンスの管理対象資産の概要が表示されます。

アプライアンスで組織コンポーネントが有効化されており、管理者コンソール（http://**appliance_hostname**/admin）にログインしている場合は、資産管理ダッシュボードに選択した組織の情報が表示されます。システム管理コンソール（http://**appliance_hostname**/system）にログインしている場合は、資産管理ダッシュボードにすべての組織を含めたアプライアンス情報が表示されます。

ヒント: アプライアンスは、概要ウィジェットを定期的に更新します。任意の時間にほとんどのウィジェットを更新するには、ページの右上にある **更新** ボタンをクリックします：。ほとんどのウィジェットを個々に更新するには、ウィジェットの上にマウスを置き、ウィジェットの上の **更新** ボタンをクリックします。一部のウィジェットでは、追加の手順が必要になる場合があります。

資産管理ダッシュボードウィジェットについて

選択すると、資産管理ダッシュボード ウィジェットには、組織またはアプライアンスの管理対象資産の概要が表示されます。

このセクションでは、資産管理ダッシュボードで使用可能なウィジェットについて説明します。アプライアンス上で組織コンポーネントが有効化されている場合は、ウィジェットに選択した組織の情報が管理者レベルで表示され、アプライアンスの情報がシステムレベルで表示されます。

このダッシュボードでは、資産の使用状況の大まかな概要を示します。このウィジェットを使用すると、資産の状態をすばやく確認し、資産構成を改善するためのインジケータを見つけられます。例えば、ソフトウェアライセンスがどのように使用されるかに焦点を当て、どのソフトウェアタイトルのライセンスを更新する必要があるかを特定できます。

ウィジェット	説明
タイプ別資産	このウィジェットにはドーナツグラフが表示され、それぞれの部分はデバイス、ソフトウェア、場所、ライセンス、およびその他の資産タイプごとの資産の割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択したタイプの資産の割合が表示されます。

ウィジェット	説明
ステータス別資産	このウィジェットにはドーナツグラフが表示され、それぞれの部分は アクティブ、廃棄、欠落、およびその他のステータスごとの資産の割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択したステータスの資産の割合が表示されます。
製品別未使用ライセンスのコスト（$）	このウィジェットには棒グラフが表示され、それぞれの棒は各製品の未使用ライセンスのコストを表します。この情報を使用して、未使用ライセンスを再割り当てまたはキャンセルし、最も必要なところにリソースをリダイレクトできます。
ライセンスコンプライアンス	ソフトウェアのライセンス資産を作成済みの場合、このウィジェットにはライセンス認証された特定のソフトウェアがインストールされたエージェント管理対象デバイスの数と、使用可能なライセンスの数が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。 ライセンス資産は、ソフトウェア ページおよびソフトウェアカタログ ページにリストされたアプリケーションに対して作成できます。このウィジェットにライセンス情報が表示されるようにするには、アプリケーションのライセンスモードが Unit License（ユニットライセンス）または Enterprise（エンタープライズ）である必要があります。Shareware（シェアウェア）、Freeware（フリーウェア）、Not Specified（指定なし）など他のライセンスモードのアプリケーションは、このウィジェットに表示されません。 このウィジェットは情報提供のみを目的としており、アプライアンスは、ライセンスコンプライアンスを強制しません。例えば、ライセンスが期限切れであったり、コンプライアンスから外れていたとしても、エージェント管理対象デバイスへのソフトウェアのインストールがアプライアンスによって阻止されることはありません。 次のように、色によってしきい値レベルが示されます。 • **赤**: 使用率が緊急しきい値設定以上です。 • **オレンジ**: 使用率が警告しきい値設定以上になっていますが、緊急しきい値設定に対しては下回っています。 • **緑**: 使用率が警告しきい値設定を下回っています。 しきい値レベルを変更する方法については、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。 ライセンス資産の管理に関する情報については、インベントリの管理を参照してください。
ソフトウェアタイトル	このウィジェットには、管理対象デバイスでのインストール数が最も多い、ソフトウェアカタログで定

ウィジェット	説明
	義済みのソフトウェアタイトルが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ソフトウェア発行元	このウィジェットには、管理対象デバイスにインストールされているソフトウェアタイトルが最も多い、ソフトウェアカタログで定義済みの発行元が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
場所別資産	このウィジェットにはドーナツグラフが表示され、それぞれの部分は場所別の資産の割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択した場所の資産の割合が表示されます。
インストールされているが 60 日間使用されていないソフトウェア	このウィジェットには棒グラフが表示され、それぞれの棒は過去 60 日間使用されていないソフトウェアタイトルとその製品の対応するインスタンスの数を表します。この情報を使用して、これらのタイトルが必要かどうかをさらに調査し、未使用ライセンスを再割り当てまたはキャンセルし、最も必要なところにリソースをリダイレクトできます。
期限切れに近づいているソフトウェアライセンスのメンテナンス	このウィジェットには縦の棒グラフが表示され、それぞれの棒は一定時間経過後に期限が切れるソフトウェアライセンスの数を表します。
期限切れソフトウェアライセンスのメンテナンス	このウィジェットにはドーナツグラフが表示され、それぞれの部分は期限切れのライセンスと現在のライセンスの配分を表します。選択すると、グラフのそれぞれの部分にカーソルを置いたときに、期限切れまたは現在のソフトウェアライセンスの割合が表示されます。
期限満了に近い契約	このウィジェットには縦の棒グラフが表示され、それぞれの棒は一定時間経過後に期限が切れる契約の数を表します。
期限切れの契約	このウィジェットにはドーナツグラフが表示され、それぞれの部分は期限切れの契約と現在の契約の配分を表します。選択すると、グラフのそれぞれの部分にカーソルを置いたときに、期限切れまたは現在の契約の割合が表示されます。
ソフトウェアライセンス設定	ソフトウェアのライセンス資産を設定し、ライセンスタイプ（サイト、サブスクリプション、ユニットなど）を指定した場合、その情報がこのウィジェットに表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。

資産管理ダッシュボードのカスタマイズ

資産管理ダッシュボードをカスタマイズし、必要に応じて、ウィジェットを表示または非表示にできます。

1. 資産管理ダッシュボード に移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**ダッシュボード** をクリックします。
2. ウィジェットの上にマウスを置き、次のボタンのいずれかを使用します。
    -  : ウィジェットの情報を更新します。
    -  : ウィジェットに関する情報を表示します。
    -  : ウィジェットを非表示にします。
    -  : ウィジェットのサイズを変更します。
    -  : ウィジェットをページ上の別の場所にドラッグできます。
3. ページの右上隅にある **カスタマイズ** ボタンをクリックすると、使用可能なウィジェットが表示されます。
4. 現在非表示のウィジェットを表示するには、**インストール** をクリックします。

資産管理について

資産とは、デバイス、ソフトウェアライセンス、および管理する必要のあるその他のアイテムに関する情報を格納するエンティティです。資産は、資産の作成に使用されるテンプレートである資産タイプに基づきます。

資産情報とインベントリ情報の相違点

資産情報とインベントリ情報では、情報の収集および管理方法が異なっています。

次の表に、資産情報とインベントリ情報の比較を示します。

アイテム	資産コンポーネント	インベントリコンポーネント
情報が表示される場所	資産 セクション内。	インベントリ セクション内。
管理対象の情報のタイプ	資産情報には、デバイス、ソフトウェア、ライセンス、物理的資産、論理的資産、およびそれらの関係についての詳細が含まれます。	インベントリ情報には、デバイスとソフトウェア、プロセス、スタートアッププログラム、および管理対象デバイス上のサービスについての詳細が含まれます。ソフトウェアカタログでは、「検出」または「未検出」に分類されるアプリケーションに関する追加情報が提供されます。
情報の管理方法	資産情報は静的であり、データをインポートした場合、またはデータを手動で変更した場合にのみ変更されます。このルールはデバイス資産には当てはまりません。	インベントリ情報は、管理対象デバイスがアプライアンスにデータをレポートするたびに、自動的に生成および上書きされます。

アイテム	資産コンポーネント	インベントリコンポーネント
	デバイス資産は、管理対象デバイスがインベントリをレポートするたびに更新されるためです。ただし、ライセンス資産については、管理対象デバイスがアプライアンスにデータをレポートする際に、インストール数またはシート数が更新されます。資産履歴はアプライアンス上に保存され、**管理者コンソール**で表示できます。対象の資産が削除されるまで、履歴は資産と共に維持されます。	
ライセンスの追跡方法	資産管理コンポーネントを使用すると、ソフトウェアライセンスコンプライアンスに加えて、物理的資産と論理的資産を管理できます。	ソフトウェア ページのインベントリ情報にはソフトウェア資産の数が含まれますが、ライセンスの数は確認できません。 ソフトウェアカタログ ページでは、ライセンス資産がアプリケーションに関連付けられている場合にライセンス情報が表示されます。

追跡する資産の識別

資産管理の設定における最初のタスクの1つは、追跡する資産を識別することです。

通常、スプレッドシートには、購入データ、ベンダーの連絡先情報、プロダクトキー、ライセンスの詳細、デバイス情報など、資産の詳細が含まれています。これらの詳細は、資産追跡の対象となります。

資産管理コンポーネントに資産情報をインポートして、アプライアンスで管理および追跡できる資産を作成できます。また、インポートした資産間の関係を設定して、情報をより有益なものにすることができます。例えば、ライセンスとベンダー資産を作成して、これらをデバイスに関連付けると、ライセンスまたはベンダーに関連するデバイスを迅速に識別できます。資産情報のインポートの詳細については、CSV ファイルでのライセンスデータのインポートを参照してください。

資産の表示および資産の情報の検索

必要に応じて資産を表示したり資産の情報を検索したりすることができます。

1. 資産 リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの ー般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
2. 詳細検索を使用して、すべての資産タイプを検索するには
    a. 特定基準で表示 ドロップダウンリストで、**すべてのアイテム** を選択します。
    b. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
    c. 検索条件を指定します。

    例えば、ベンダーが **Smith** である資産をすべて検索するには、以下の条件を指定します。

    「ベンダー」「含む」「Smith」
    d. **検索** をクリックします。

デバイス、ライセンス、ソフトウェア、ベンダーなど、条件に一致するあらゆるタイプの資産が表示されます。

3. **リストの検索** フィールドで、簡易検索を使用して、すべての資産タイプにわたって資産を検索するには、検索する対象の資産に含まれる全部または一部のフィールドの内容を入力します。例えば、バーコードにzzを含む資産を検索する場合は、フィールドにzzを入力し、Enter を押します。

   条件に一致する資産が表示されます。

4. 単一の資産タイプを検索するには、次の手順を実行します。
   a. 特定基準で表示 ドロップダウンリストで、**資産タイプ** > **資産タイプ** を選択します。
   b. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
   c. 検索条件を指定します。

   例えば、2 ヶ月以内に有効期限が切れる予定のライセンス資産を検索するには、特定基準で表示 ドロップダウンリストでライセンス資産タイプを選択し、次の基準を指定します。

   「有効期限」「は次の期間内」「2ヶ月」

   d. **検索** をクリックします。

   今後2ヶ月以内に有効期限が切れるライセンス資産が表示されます。

5. 指定した検索条件を使用するカスタムビューを作成するには、右側のリストの上部にある**カスタムビュー**をクリックし、ビューを保存します。

   特定基準で表示 ドロップダウンリストにカスタムビューが表示されます。カスタムビューはユーザーに固有です。ユーザーは自分のカスタムビューにアクセスできますが、他のユーザーが作成したカスタムビューにはアクセスできません。

資産へのバーコードの追加

必要に応じて資産を表示したり資産の情報を検索したりすることができます。

バーコードを指定する資産のタイプについて、1つ、または複数のバーコードタグを指定します。詳細については、「資産タイプの追加またはカスタマイズ」を参照してください。

1. Asset Detail（資産の詳細）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
   c. 資産の名前をクリックします。
2. バーコード の下で、＋ をクリックし、以下の情報を入力します。

オプション	説明
バーコードデータ	バーコード番号。バーコード番号は常に一意で、複数の資産間で共有できません。ただし、アクティブな資産がアーカイブされた資産のバーコードを共有することはできます。
バーコードの名前	この資産タイプに関連するバーコードのタグ。同じタイプのバーコードは資産ごとに1つしかありません。
バーコードのフォーマット	バーコードのフォーマット。例えば、UPC-A、Code 11、またはUPC-Eです。

必要な数のバーコードを追加できます。

3. オプション。バーコード 領域で、最初または最後にスキャンした日付など、各バーコードタグに関する追加情報を参照するには、**すべての列を表示** をクリックします。各バーコードの列が少ない以前のビューに戻るには、**列を簡易表示** をクリックします。
4. **保存** をクリックします。

デバイス所有者の変更

必要に応じて、資産とデバイスの所有者を変更できます。

このトピックでは、資産リストを使用してデバイス所有者を変更するプロセスについて説明します。資産の詳細ページまたは デバイスの詳細 ページを使用して、デバイス所有者を変更できます。

1. 資産 リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
2. 特定基準で表示 ドロップダウンリストで、**資産タイプ**、デバイス の順に選択します。
3. 資産 リストで、特定の所有者に割り当てる1つ、または複数のデバイスを選択します。
4. **アクションの選択 > 割り当て先** の順に選択します。
5. 表示される 割り当て先 ダイアログボックスから、未割り当て をクリックし、選択した資産の所有者として割り当てるユーザーアカウントを選択します。

    リストに、各ユーザーの氏名、アカウント名、およびEメールアドレスが表示されます。
6. **保存** をクリックします。

    割り当て ダイアログボックスグが閉じ、資産 リストが更新され、代理人名 列に資産の所有者名が表示されます。
7. 資産 リストに、所有者に関連する列を追加します。
    a. 資産 リストで、⚙ をクリックします。
    b. 次のいずれかのオプションを選択し、必要に応じて、資産 リストで次の列を表示します。**代理人ログイン**、**代理人 E メール**、**代理人ドメイン**、**代理人予算コード**、**代理人の場所**、**代理人ロール**、または**代理人ロケール**。

        資産 リストに選択した列が表示されます。
8. デバイスの所有者を変更した場合は、デバイス リストで変更結果を確認できます。
    a. 左側のナビゲーションバーで、**インベントリ** をクリックして、**デバイス** をクリックします。
    b. デバイス リストで、変更する所有者のデバイスを含む行の 代理人名 列を確認します。

        代理人名 列に、デバイスの所有者の名前が表示されます。

ヒント: また、資産の詳細 または デバイスの詳細 ページで、資産またはデバイスの所有者を変更できます。

資産のライフサイクル設定の表示と設定

場所を除き、各資産タイプには、アクティブ、廃棄、期限切れなど、その用途または目的を示すステータスがあります。

該当する資産のライフサイクルを設定するには、ユーザー役割に書き込みレベルの 資産のライフサイクル 権限を付与する必要があります。資産のライフサイクル設定を表示するには、読み取りレベルの権限で十分です。ユーザーの役割の詳細については、組織の役割とユーザーの役割の管理を参照してください。

資産のライフサイクル設定 ページを使用して、既存の資産ステータスのエントリを表示し、必要に応じて新しいエントリを追加します。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. 次の手順のいずれかを実行します。
   - **左側のナビゲーションバーで、資産管理 をクリックして、資産 をクリックします。**
   - **左側のナビゲーションバーで、資産管理 をクリックして、契約 をクリックします。**
   - **左側のナビゲーションバーで、資産管理 をクリックして、ライセンス をクリックします。**
3. 表示されるリストページで、**アクションを選択 > ライフサイクルを設定** の順にクリックします。

   ヒント: 資産ステータスは、リストページで資産を選択し、**アクションを選択 > 資産ステータスを変更** の順にクリックし、資産ステータスを変更 ダイアログボックスで適切なステータスを選択して、簡単に変更できます。このコマンドへのアクセスには、書き込みレベルで、該当する、資産、契約、またはライセンス 権限が必要です。ユーザーの役割の詳細については、組織の役割とユーザーの役割の管理を参照してください。

   資産ライフサイクル設定 ページが表示されます。
4. 資産ライフサイクル設定 ページの 資産ステータス の下で、デフォルトの資産ステータスのリストを確認します。

   以下のデフォルトの資産ステータスが利用できます。
   - **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。
   - **廃棄済み**：利用できなくなった資産。
   - **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。
   - **在庫**：最近受け取った資産。
   - **不在**：場所を特定できない資産。
   - **修復**：修復されている資産。
   - **予約済み**：特定の人または用途のために確保されている資産。
   - **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。
   - **盗難**：盗難されたとして報告された資産。
5. カスタム資産ステータスを追加、削除、または編集します。

   ヒント: デフォルトの資産ステータスは変更または削除できません。

   - 新しい資産ステータスを追加するには、＋ をクリックし、資産ステータスの 名前 および 説明 を指定して、**追加** をクリックします。
   - カスタム資産ステータスを削除するには、資産ステータスを含む行で、🗑 をクリックします。
   - カスタム資産ステータスを編集するには、資産ステータスを含む行で、✎ をクリックし、該当する資産ステータスの 名前 および / または 説明 を編集します。
6. 資産ライフサイクル設定 ページに変更を加えた場合は、**保存** をクリックします。それ以外の場合は、**キャンセル** をクリックして前のページに戻ります。

資産タイプの追加とカスタマイズおよび資産情報の維持

必要に応じて、資産タイプを追加またはカスタマイズできます。また、スケジュール設定した定期的な間隔でネットワークをスキャンすることにより、資産に関するリアルタイム情報を維持することもできます。

また、資産タイプにサブタイプを追加できます。資産サブタイプを使用すると、プリンタのトナーやインクレベルなど資産のプロパティを追跡できます。

資産タイプについて

資産タイプは資産を作成するためのテンプレートです。資産タイプには、資産を定義するフィールドとその他の情報が含まれます。

デフォルト資産タイプは次のとおりです。デバイス、コストセンター、部門、ライセンス、契約、場所、購入、ソフトウェア、およびベンダー。さらに必要に応じて、カスタム資産タイプを追加できます。

また、どの資産タイプについても資産サブタイプおよびカスタムフィールドを追加できます。これは特に、プリンタなどのコンピューター以外のデバイス資産に関する追加情報を収集する場合に便利です。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。

資産タイプのカスタマイズ

資産タイプのフィールドは、必要に応じて名前変更、作成、および削除できます。アプライアンスのアップデート中は、資産タイプのカスタマイズが保持されます。

資産タイプのフィールドの名前およびタイプの変更

資産タイプのフィールド名を変更すると、その資産タイプに基づくすべての資産のフィールド名が変更されます。名前が変更されたフィールドの値は保持されます。

ただし、既にフィールドに入力されているデータをサポートしないものに**タイプ**を変更すると、そのデータは失われます。例えば、「Model Number」という「タイプ」が「テキスト」のフィールドがあり、その値が「A123」であるとします。「タイプ」を「テキスト」から「数字」に変更すると、システムは「A123」を有効な数字に変換することができません。「Model Number」フィールドの値は「0」に設定されます。

資産フィールドの追加および削除について

資産タイプにフィールドを追加した場合、追加したフィールドは、そのタイプのすべての資産で使用できます。同様に、カスタム資産フィールドを削除した場合、削除したフィールド、およびそのフィールドに入力されている値は、同じタイプのすべての資産から削除されます。

例えば、デバイス資産タイプで BIOSのシリアルナンバー という名前のカスタムフィールドを作成した場合、そのフィールドはすべてのデバイス資産タイプで使用できます。ただし、カスタム資産の BIOSのシリアルナンバー を削除した場合、削除したフィールド、およびそのフィールドに入力された値はすべてのデバイス資産タイプから削除されます。

資産フィールドを削除すると、削除されたフィールドを参照するあらゆる資産から資産関連付けが削除されます。

資産タイプの追加またはカスタマイズ

カスタム資産タイプは、必要な数だけ追加できます。また、任意の資産タイプのカスタムフィールドを作成することもできます。資産タイプのカスタムフィールドを作成すると、そのフィールドは、同じ資産タイプに基づくすべての資産で使用できるようになります。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織の資産タイプを個別に追加およびカスタマイズします。

1. 資産タイプの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
    c. 資産タイプの詳細 ページを表示するには、次のいずれかを実行します。
    - 資産タイプの名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. 名前 フィールドで、必要に応じて名前を追加または変更します。

    ヒント: デバイスおよびライセンス資産タイプで追加のオプションを使用できます。デバイス資産タイプのカスタマイズについておよびライセンス資産タイプのカスタマイズを参照してください。
3. **場所 を除くすべての資産タイプ**。デフォルトの資産ステータス フィールドに、デフォルトの資産ステータス、またはカスタムの資産ステータスを入力します（ 存在する場合 ）。

    アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。
    - **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。
    - **廃棄済み**：利用できなくなった資産。
    - **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。
    - **在庫**：最近受け取った資産。
    - **不在**：場所を特定できない資産。
    - **修復**：修復されている資産。
    - **予約済み**：特定の人または用途のために確保されている資産。
    - **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。
    - **盗難**：盗難されたとして報告された資産。
4. 管理者役割を持たないユーザーがこのタイプの資産を削除できるようにするには、**管理者以外に資産の削除を許可する** を選択します。このオプションはデフォルトでオフになっています。このオプションを設定できるのは管理者のみです。他のタイプのユーザーでは、このフィールドはページに表示されますが無効になっています。

    ユーザーの役割の詳細については、「ユーザーの役割の追加または編集」を参照してください。
5. このタイプの資産で、資産の場所を資産の詳細情報に表示するには、**場所の設定を表示** を選択します。このオプションはデフォルトでオフになっています。
6. **デバイス資産のみ**。資産のアーカイブのデフォルトステータス フィールドに、アーカイブされたときに自動的にデバイスに割り当てられる資産ステータスを入力します。
7. この資産タイプのインスタンスをバーコードに使用する場合、バーコードタグ 領域で 1 つまたは複数のタグを指定します。

    このタイプの作成したすべての資産は、バーコードタグの設定が可能になります。例えば、企業タグおよびDell資産タグを指定する場合、これらの2種類のタグで識別されるバーコードがこの資産タイプの資産を作成または編集する際に 資産の詳細 ページで選択可能になります。

    バーコードを追加するには、＋をクリックし、バーコードの名前を入力し、**保存** をクリックします。
8. 資産フィールド 領域で、＋をクリックします。

新しい行が表示されます。

9. 次の情報を入力します。

アイテム	説明
名前	カスタム資産フィールドの名前。「Asset Code」、「Purchase Date」、「Building Address Line 1」など。この名前は、選択した資産タイプの資産を作成するために使用するフォームに表示されます。
使用可能な値	値のリストを含むフィールドに表示される値。タイプ ドロップダウンリストから **単一選択** または **複数選択** を選択した場合に、このフィールドが有効になります。**単一選択** または **複数選択** を選択した場合には、このフィールドに少なくとも1つの値を入力する必要があります。複数の値を入力するには、コンマを使用して各値を区切ります。
デフォルト値	フィールドにデフォルトで表示される値。タイプ ドロップダウンリストから **単一選択** または **複数選択** を選択した場合、使用可能な値 フィールドで指定された値の1つを入力する必要があります。
必須	対象のフィールドが必須か任意かを指定します。このチェックボックスをオンにした場合、選択したタイプの資産を作成する際には、このフィールドに値を入力する必要があります。
タイプ	フィールドのタイプ。フィールドのタイプは次の通りです。 • **添付ファイル**: 資産に添付ファイルを追加できます。 • **通貨**: 金額に使用します。 • **ソフトウェアカタログ**: 資産をソフトウェアカタログのアプリケーションに関連付けできます。 • **日付**: カレンダー情報に使用します。 • **ラベル**: ラベルを資産に関連付けできます。 • **リンク**: インターネットリンクに使用します。リンクは、有効な URL（**http://quest.com**）である必要があります。 • **複数選択**: 複数の値が選択可能な場合にリストを表示します。各値の最大長は255文字です。 • **メモ**: 追加情報に使用します。 • **数字**: 整数で表される数値に使用します。 • **親**: この資産は、親子関係にある同じタイプの資産を参照できます。例えば、「場所」タイプで親接続を許可して、「New York」場所が「North America」場所を参照可能なようにできます。このタイプをレポート作成システム

アイテム	説明
	で使用して、北米にあるすべての資産を表示できます。 • **単一選択**: 1つの値しか選択できない場合に値のリストを表示します。各値の最大長は255文字です。 • **テキスト**: 追加テキストに使用します。最大長は255文字です。 • **タイムスタンプ**: レコードに日付と時間を追加するために使用します。 • **ユーザー**: ユーザーレコードを資産に関連付けるために使用します。 • **資産資産タイプ**: 資産タイプ間の関係を指定するために使用します。
複数選択	資産フィールドが他の資産を参照するかどうかを指定します。タイプ ドロップダウンリストから **資産資産タイプ** を選択した場合にチェックボックスがオンになります。チェックボックスをオンにすると、このカスタムフィールドは複数のレコードを参照できます。 例えば、特定のライセンスが付与されている複数のデバイスを参照するフィールドが必要になったとします。この場合に、チェックボックスをオンにします。単一選択の関係フィールド（1つの部署でのみ使用されるプリンタなど）を作成する場合は、チェックボックスをオフにします。 **注:** 資産を作成すると、このフィールドには、指定された資産タイプの使用可能な資産が入力されます。指定されたタイプの資産がない場合、フィールドには何も入力されません。
セクション	**ライセンス資産のみ**。ライセンス詳細 ページでこのフィールドが表示されるタブ：一般、購入、メンテナンス、関連、カスタム、または メモ。ライセンス詳細 ページに表示されるタブの詳細については、「ライセンスの追加または編集」を参照してください。
デバイス セクション	**デバイス資産のみ**。場所。デバイスの詳細 ページにフィールドがレポートされます。例えば、Toner Level というフィールドでプリンタ資産サブタイプを作成している場合、そのフィールドはプリンタ ハードウェアに関連しているため、一般には ハードウェア を選択することになります。ただし、任意のフィールドのドロップダウンリストで任意のセクションを選択できます。

10. 行の最後で **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

オプション：資産タイプの資産サブタイプを追加します。詳細については、「資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択」を参照してください。

デバイス資産タイプのカスタマイズについて

資産 セクションや インベントリ セクションに表示されるほぼすべてのデバイス資産データは、資産 セクションから生成したものです。

インベントリ セクションから取得されるデバイスインベントリ情報またはデバイス資産情報は、「マップされたインベントリフィールド」と「一致する資産フィールド」のデータのみです。これらのフィールドの値は、デバイスがインベントリ設定されるたびに収集されます。インベントリプロセス時に、アプライアンスでは、デバイスに既に資産がマップされているかどうかが確認されます。資産が見つからなかった場合は、新しい資産がアプライアンスにより作成されます。

Mapped Inventory Field（マップされたインベントリフィールド）のデフォルトデータタイプは **システム名**、Matching Asset Field（一致する資産フィールド）のデフォルトデータタイプは **名前** です。ただし、システムのイメージを再作成する場合、旧システム名の情報は資産管理コンポーネントから失われます。これを回避するには、資産の追跡にBIOSのシリアルナンバー、IPアドレス、MACアドレス、またはそれに類似するものを使用することを検討してください。

デバイス資産データは、いつでも、インポートしたり、資産 セクションで手動で変更したりできます。

注意: デフォルトの資産タイプを変更すると、変更前の資産の履歴が失われます。これは、新しい情報を使用して、アプライアンスが資産を自動的に作成するためです。そのため、こうしたデフォルト値を変更するかどうかは、セットアッププロセスのできるだけ早い段階で決定することが重要です。

例：デバイス資産タイプへのカスタムフィールドの追加

この例では、フィールドをデバイス資産タイプに追加し、Mapped Inventory Field（マップされたインベントリフィールド）および Matching Asset Field（一致する資産フィールド）で選択する方法について示します。

1. 資産タイプの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
   c. **デバイス** 資産タイプをクリックします。
2. ページの右側で、**追加** ボタンをクリックします。

   新しい行が表示されます。
3. 次の情報を入力します。
   a. 名前 フィールドに、「BIOSのシリアルナンバー」と入力します。
   b. タイプ ドロップダウンリストで、**テキスト** を選択します。
4. 行の最後で **保存** をクリックし、行を追加します。
   a. **追加** ボタンをクリックします。

      新しい行が表示されます。
   b. 新しい行について、次の情報を入力します。

   名前 フィールドに、「シリアルナンバー」と入力します。

   タイプ ドロップダウンリストで、**テキスト** を選択します。**番号** の タイプ は計算を実行するフィールドにのみ使用します。**番号** の タイプ を使用すると、シリアルナンバーの先頭にある 1 つ以上のゼロが削除される場合があります。
5. 行の最後で **保存** をクリックし、行を追加します。
   a. **追加** ボタンをクリックします。

      新しい行が表示されます。
   b. 新しい行について、次の情報を入力します。

名前 フィールドに、「購入日」と入力します。

タイプ ドロップダウンリストで、**テキスト** を選択します。

6. 行の最後で **保存** をクリックし、行を追加します。
   a. **追加** ボタンをクリックします。

      新しい行が表示されます。

   b. 新しい行について、次の情報を入力します。

      名前 フィールドに、「場所」と入力します。

      タイプ ドロップダウンリストで、**資産の場所** を選択します。
7. 行の最後で **保存** をクリックします。
8. Mapped Inventory Field（マップされたインベントリフィールド）ドロップダウンリストで、値を **BIOSのシリアルナンバー** に変更します。
9. 一致する資産フィールド フィールドで、**シリアルナンバー** を選択します。
10. ページの一番下で **保存** をクリックします。

資産フィールド間の関連付け

資産タイプを編集することで、資産間の関係を設定して、まとめて追跡できます。

次のような関係があります。

- プリンタとデバイスなどの、ピアツーピアの関係。
- コストセンターと、それに関連付けられたデバイスなどの、親子の関係。

例：場所資産タイプへのフィールドの追加 場所資産タイプにフィールドを追加し、場所との親/子関係を作成する方法を説明します。

例：場所資産タイプへのフィールドの追加

必要に応じて、フィールドを場所資産タイプに追加できます。

1. 資産タイプの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
   c. **場所** 資産タイプをクリックします。
2. ページの右側で、**追加** ボタンをクリックします。

   新しい行が表示されます。
3. 名前 フィールドに、「親の場所」と入力します。
4. タイプ ドロップダウンリストで、**親** を選択します。
5. 行の最後で **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

場所資産を開くと、親関係 フィールドが 資産詳細 ページに表示されます。

場所資産への親関係の追加

親/子関係は、場所資産などの資産を管理するときに役立つ場合があります。

例：場所資産タイプへのフィールドの追加の手順に従って、Parent Location（親の場所）カスタムフィールドを追加してください。

親関係を追加する際は、関係の最も上位のレベル（親レベル）から作業を開始します。

1. 資産 リストに移動します。

a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。

2. **オプション**：右側の表の上に表示されている 特定基準で表示 ドロップダウンリストで、**資産タイプ > 場所** を選択します。

   場所資産のみが表示されるようになります。
3. 最上位レベル（親レベル）の場所資産が表示されない場合は作成します。
   a. **アクションの選択 > 新規作成 > 場所**を選択して、場所資産詳細 ページを表示します。
   b. 新しいフィールドの名前を入力します。例えば、「Western Division」と入力します。
   c. **親の場所 を 割り当てなし** のままにし、**保存** をクリックして、資産 ページを表示します。

   注: 親の場所 フィールドは、ユーザーが作成したカスタムフィールドです。
4. 2つ目のレベルの場所が存在する場合は、その場所を選択します。2つ目のレベルの場所が存在しない場合は作成します。
   a. **アクションの選択 > 新規作成 > 場所**を選択して、場所資産詳細 ページを表示します。
   b. 新しい資産の名前を入力します。例えば、「San Jose」と入力します。
   c. この例では、親の場所 として **Western Division** を選択します。多くの場所資産がある場合は、フィルタ フィールドに最初の数文字を入力し、親の場所 フィールドの選択肢を絞ります。
5. **保存** をクリックします。
6. 必要に応じて、追加の場所資産を作成します。

   例えば、構内の建物ごと、またはデータセンターのラックごとに場所資産を作成できます。

資産タイプの削除

資産タイプに資産が割り当てられていない場合に限り、そのタイプを削除できます。

資産が割り当てられていない資産タイプがあります。

1. 資産タイプ リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
2. 資産タイプの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

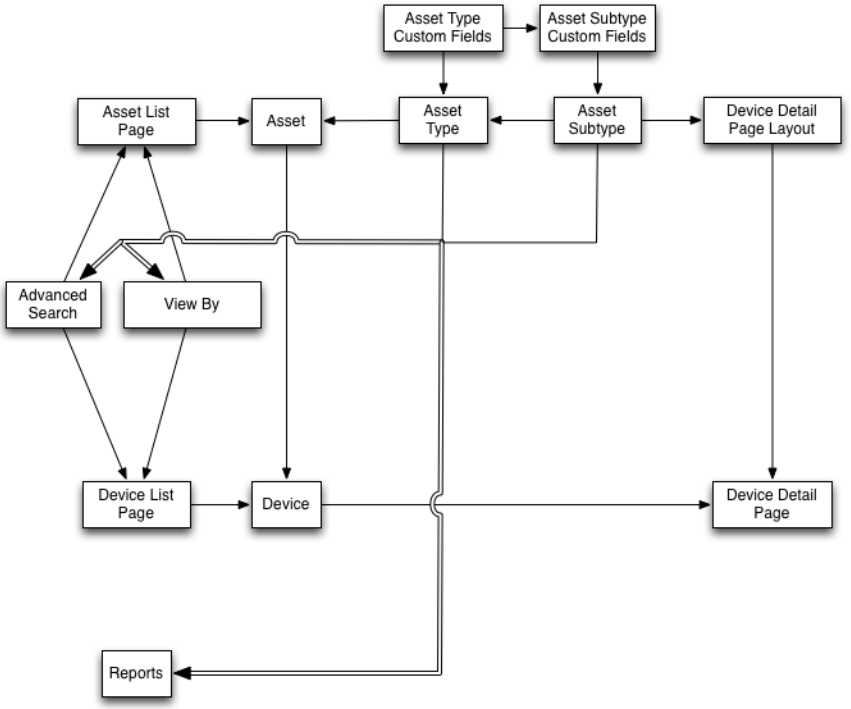
資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について

資産サブタイプは、カスタム資産タイプを含め任意の資産タイプに追加可能な資産のサブカテゴリです。これにより、資産のサブタイプを識別し、管理できます。サブタイプには、コンピュータやプリンタやルーターといったデバイス資産や、アプライアンスインベントリの Windows や Mac や Linux のシステムで動作するソフトウェア資産などがあります。

資産サブタイプは、資産タイプからフィールドを継承します。また、カスタムフィールドを追加して、アプライアンスインベントリプロセスで資産サブタイプの関連情報を収集することもできます。例えば、資産サブタイプ「**プリンタ**」を資産タイプ「**デバイス**」に追加できます。その後、サブタイプ「**プリンタ**」のカスタムフィールド（トナー など）を追加できます。これで、トナー フィールドはサブタイプが「プリンタ」のデバイス資産で利用できるようになります。

注: アプライアンスがエージェント不要デバイスから資産サブタイプフィールドにデータを入力できるようにするには、デバイスを設定するときに適切な資産サブタイプを割り当て、適切なオブジェクト識別子（OID）を取得し、SNMP インベントリ設定の詳細 ページでその識別子をサブタイプフィールドにマップする必要があります。SNMP デバイスサブタイプを設定後に追加または変更することはできません。詳細については、「管理者コンソールを使用したオブジェクト識別子（OID）のリストの取得」を参照してください。

また、デバイスの詳細 ページでデバイス資産サブタイプごとの詳細を表示するか非表示にするかを選択できます。例えば、インストール済みプログラム、検出済みソフトウェア、メータリングしたソフトウェア などプリンタに無関係な情報を、サブタイプが「**プリンタ**」の資産の デバイスの詳細 ページに表示しないようにすることができます。



SNMP デバイスで資産サブタイプを使用するためのワークフロー

資産サブタイプを使用するには、そのサブタイプおよび使用するカスタムフィールドを資産タイプに追加する必要があります。SNMP（Simple Network Management Protocol）デバイスからのデータをフィールドに入力するために、オブジェクト識別子（OID）をカスタムフィールドに追加することもできます。

SNMP デバイスで資産サブタイプを使用するためのワークフローには、次のタスクが含まれています。

1. デバイス資産サブタイプを資産タイプに追加し、カスタムフィールドをサブタイプに追加します。詳細については、「資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択」を参照してください。
2. 資産タイプおよび資産サブタイプを使用する資産を追加します。詳細については、「デバイス ページからのデバイス資産サブタイプの割り当てまたは変更」を参照してください。

   重要: デバイスを設定するときに、適切な資産サブタイプを割り当てる必要があります。SNMP デバイスサブタイプを設定後に追加または変更することはできません。

3. **オプション**：次のようにフィールドにデータを入力します。
   - SNMP デバイスからのデータがフィールドに入力されるようにするには、カスタムフィールドに使用するオブジェクト識別子（OID）を取得し、SNMP Inventory Configuration Detail（SNMP インベントリ設定の詳細）ページでエージェント不要デバイスのフィールドを追加し、資産サブタイプを選

択し、フィールドの OID 情報を追加します。詳細については、「管理者コンソールを使用したオブジェクト識別子（OID）のリストの取得」を参照してください。

- 必要に応じてフィールドを手動で更新します。詳細については、「カスタム資産フィールドの手動更新」を参照してください。

資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択

カスタム資産タイプを含め任意の資産タイプに資産サブタイプを追加し、資産サブタイプごとにカスタムフィールドを追加できます。

また、デバイスの詳細 ページに表示するフィールドとそれらのフィールドを表示するセクションを選択できます。これにより、デバイスの詳細 ページをカスタマイズし、最も重要な情報を強調できます。

注: アプライアンス上で組織コンポーネントが有効化されている場合は、各組織の資産サブタイプを個別に管理します。

1. 資産タイプの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
   c. 資産タイプの詳細 ページを表示するには、次のいずれかを実行します。
   - 資産タイプの名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。
2. サブタイプ セクションで、**サブタイプの追加** をクリックします。

   注: デフォルトのインストールでは、デバイス資産のプリンタデバイスには次の 2 つの資産サブタイプがあります。レーザープリンタ：カラー と レーザープリンタ：モノクロ：これらの各サブタイプは、ほとんどのプリンタに適用される一般的な一連のフィールドを提供します。また、これらの資産のサブタイプに基づいて、一般的な SNMP 対応プリンタモデル用の一連のプリンタテンプレートが付属しています。必要に応じて、これらのテンプレートを編集したり、新規追加したりすることができます。プリンタテンプレートをデバイスに適用するとき、次のインベントリサイクルで、トナーレベルや説明などテンプレートで定義されたデータがプリンタ用に収集されます。詳細については、「プリンタテンプレートについて」を参照してください。

   Asset Subtype Detail（資産サブタイプの詳細）ページが表示されます。資産サブタイプに使用可能なフィールドが 継承されるフィールド セクションに表示されます。既にそれらのフィールドが資産タイプに追加されているからです。
3. 一番上のセクションで、次の情報を指定し、この資産サブタイプをデフォルトにするかどうかを選択します。

オプション	説明
名前	資産サブタイプの名前。この名前は、Asset Type Detail（資産タイプの詳細）ページのリストに表示されます。
デフォルト	選択したタイプの新しい資産のデフォルトとして資産サブタイプを使用するかどうか。このチェックボックスをオンにすると、選択したタイプの新しい資産がこの資産サブタイプに自動的に割り当てられます。この設定はいつでも変更できます。

4. サブタイプフィールド セクションで、表の右側の見出し行にある **追加** ボタン ＋ をクリックします。
5. 次の情報を入力します。

アイテム	説明
名前	資産サブタイプの名前。この名前で 資産の詳細ページの資産サブタイプを識別します。
使用可能な値	値のリストを含むフィールドに表示される値。タイプ ドロップダウンリストから **単一選択** または **複数選択** を選択した場合に、このフィールドが有効になります。**単一選択** または **複数選択** を選択した場合には、このフィールドに少なくとも1つの値を入力する必要があります。複数の値を入力するには、コンマを使用して各値を区切ります。
デフォルト値	フィールドにデフォルトで表示される値。タイプ ドロップダウンリストから **単一選択** または **複数選択** を選択した場合、使用可能な値 フィールドで指定された値の1つを入力する必要があります。
必須	対象のフィールドが必須か任意かを指定します。このチェックボックスをオンにした場合、選択したタイプの資産を作成する際には、このフィールドに値を入力する必要があります。
タイプ	フィールドのタイプ。フィールドのタイプは次の通りです。 • **添付ファイル**: 資産に添付ファイルを追加できます。 • **通貨**: 金額に使用します。 • **ソフトウェアカタログ**: 資産をソフトウェアカタログのアプリケーションに関連付けできます。 • **日付**: カレンダー情報に使用します。 • **ラベル**: ラベルを資産に関連付けできます。 • **リンク**: インターネットリンクに使用します。リンクは、有効な URL（**http://quest.com**）である必要があります。 • **複数選択**: 複数の値が選択可能な場合にリストを表示します。各値の最大長は255文字です。 • **メモ**: 追加情報に使用します。 • **数字**: 整数で表される数値に使用します。 • **親**: この資産は、親子関係にある同じタイプの資産を参照できます。例えば、「場所」タイプで親接続を許可して、「New York」場所が「North America」場所を参照可能なようにできます。このタイプをレポート作成システム

アイテム	説明
	で使用して、北米にあるすべての資産を表示できます。 • **単一選択**: 1つの値しか選択できない場合に値のリストを表示します。各値の最大長は255文字です。 • **テキスト**: 追加テキストに使用します。最大長は255文字です。 • **タイムスタンプ**: レコードに日付と時間を追加するために使用します。 • **ユーザー**: ユーザーレコードを資産に関連付けるために使用します。 • **資産資産タイプ**: 資産タイプ間の関係を指定するために使用します。
複数選択	資産フィールドが他の資産を参照するかどうかを指定します。タイプ ドロップダウンリストから **資産資産タイプ** を選択した場合にチェックボックスがオンになります。チェックボックスをオンにすると、このカスタムフィールドは複数のレコードを参照できます。 例えば、特定のライセンスが付与されている複数のデバイスを参照するフィールドが必要になったとします。この場合に、チェックボックスをオンにします。単一選択の関係フィールド（1つの部署でのみ使用されるプリンタなど）を作成する場合は、チェックボックスをオフにします。 **注:** 資産を作成すると、このフィールドには、指定された資産タイプの使用可能な資産が入力されます。指定されたタイプの資産がない場合、フィールドには何も入力されません。
デバイス セクション	場所。デバイスの詳細 ページにフィールドがレポートされます。例えば、Toner Level というフィールドでプリンタ資産サブタイプを作成している場合、そのフィールドはプリンタハードウェアに関連しているため、一般には ハードウェア を選択することになります。ただし、任意のフィールドのドロップダウンリストで任意のセクションを選択できます。

6. 行の最後で **保存** をクリックします。
7. デバイス資産サブタイプの場合、デバイスの詳細 ページで表示または非表示にする情報を選択します。
    a. サブタイプ、デバイスの詳細：表示 / 非表示セクション まで下にスクロールします。
    b. 表示するアイテムの隣のチェックボックスをオンにします。

    プリンタサブタイプの場合、ハードウェア、プリンタ、ネットワークインタフェース、SNMP データなどの インベントリ情報 を表示することをお勧めします。

    c. 非表示にするアイテムの隣のチェックボックスをオフにします。

    プリンタサブタイプの場合、ソフトウェア セクションおよび Dell コマンド | モニター セクションはプリンタに関連していないため、非表示にすることをお勧めします。
8. ページの一番下で **保存** をクリックします。

デバイスの詳細 ページでカスタムフィールドに自動的にデータが入力されるようにするには、適切なオブジェクト識別子を取得してフィールド OID にマップする必要があります。詳細については、以下を参照してください。

- インベントリ表に存在するフィールドへのオブジェクト識別子のマップ
- 管理者コンソールを使用したオブジェクト識別子（OID）のリストの取得

カスタムフィールドを手動で更新するには、資産の詳細 ページに移動します。詳細については、「カスタム資産フィールドの手動更新」を参照してください。

資産サブタイプの編集

必要に応じて資産サブタイプを編集できます。アプライアンスに対して組織コンポーネントが有効化されている場合は、各組織の資産サブタイプを個別に編集します。

1. 資産タイプの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
    c. 資産サブタイプの名前をクリックして、Asset Type Detail（資産タイプの詳細）ページを表示します。
2. Subtypes（サブタイプ）セクションで、編集するサブタイプの隣にある **編集** ボタン をクリックします。

    Asset Subtype Detail（資産サブタイプの詳細）ページが表示されます。資産サブタイプに利用できるオプションについては、資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択を参照してください。
3. 行の最後で **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

資産サブタイプのデフォルト設定

サブタイプに新しい資産を自動的に割り当てるには、資産サブタイプをデフォルトとしてマーク付けします。

1. 資産タイプの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
    c. 資産タイプの詳細 ページを表示するには、次のいずれかを実行します。
    - 資産タイプの名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. Subtypes（サブタイプ）セクションで、編集するサブタイプの隣にある **編集** ボタン をクリックします。

    Asset Subtype Detail（資産サブタイプの詳細）ページが表示されます。
3. 一番上のセクションで、デフォルト の隣にあるチェックボックスをオンにします。
4. 行の最後で **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

    資産サブタイプが資産タイプのデフォルトのサブタイプとしてマーク付けされます。選択したタイプの新しい資産がこの資産サブタイプに自動的に割り当てられます。

資産タイプに利用できるサブタイプの表示

管理する資産タイプに利用できる資産サブタイプを表示できます。アプライアンスに対して組織コンポーネントが有効化されている場合は、各組織の資産サブタイプを個別に表示および管理します。

- 資産タイプの詳細 ページに移動します。
    1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    2. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
    3. 資産タイプの詳細 ページを表示するには、次のいずれかを実行します。
        - 資産タイプの名前をクリックします。
        - **アクションの選択 > 新規作成** を選択します。

    資産タイプに利用できるサブタイプが サブタイプ テーブルに表示されます。

資産 ページでの資産サブタイプの表示

特定基準で表示 メニューを使用して、資産 ページをサブタイプで並べ替えることができます。

1. 資産 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。

    資産のサブタイプ割り当てが サブタイプ 列に表示されます。**なし** は、資産がサブタイプに割り当てられていないことを示します。
2. 特定の資産タイプに割り当てられているサブタイプを表示するには、右上の 特定基準で表示 メニューに移動し、資産タイプを選択します。
3. 資産タイプの単一のサブタイプを表示するには、特定基準で表示 メニューに移動し、資産タイプを選択し、サブタイプを選択します。

    サブタイプに関連するフィールド（ プリンタ サブタイプの Ink Level など ）が、資産 ページの列として表示されます。

デバイス ページからのデバイス資産サブタイプの割り当てまたは変更

サブタイプに割り当てられていない既存のデバイス資産がある場合は、それらのデバイスが SNMP（ Simple Network Management Protocol ）デバイスでないのであれば、デバイス ページからそれらをサブタイプに割り当てたり、サブタイプ割り当てを変更したりできます。デバイスが初期設定されているときは、SNMP デバイスのサブタイプを割り当てる必要があります。

アプライアンスインベントリに既存のデバイス資産があり、デバイス資産タイプのサブタイプを作成しました。詳細については、「資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択」を参照してください。

重要: SNMP デバイスの場合、デバイスを設定するときに、適切な資産サブタイプを割り当てる必要があります。SNMP 資産サブタイプを設定後に追加または変更することはできません。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **インベントリ > デバイス** の順に選択して、デバイス ページを表示します。
3. サブタイプに割り当てられているデバイスのみを表示するようにリストをフィルタリングするには、次の手順を実行します。
    a. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
    b. 次のように、デバイスの検索に必要な条件を指定します。
    c. **検索** をクリックします。

ヒント: また、特定基準で表示 ドロップダウンリストを使用して、特定の資産サブタイプに属するデバイスを識別することもできます。

4. サブタイプに割り当てるデバイスの隣のチェックボックスをオンにします。すべてのデバイスを選択するには、表の最上部にある 名前 の隣のチェックボックスをオンにします。
5. **アクションの選択 > サブタイプを次に変更：** を選択します。

   サブタイプを選択すると、次回デバイスのインベントリがレポートされるときに変更が デバイスの詳細 ページに反映されます。

資産 ページからのタイプへの資産の割り当てまたはサブタイプ割り当ての変更

資産サブタイプに割り当てられていない既存の資産がある場合は、それらのデバイスが SNMP（Simple Network Management Protocol）デバイスでないのであれば、資産 ページからそれらをサブタイプに割り当てたり、割り当てたサブタイプを変更したりできます。デバイスが初期設定されているときは、SNMP デバイスのサブタイプを割り当てる必要があります。

アプライアンスインベントリに既存の資産があり、資産タイプのサブタイプを作成しました。詳細については、「資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択」を参照してください。

重要: SNMP デバイスの場合、デバイスを設定するときに、適切な資産サブタイプを割り当てる必要があります。SNMP 資産サブタイプを設定後に追加または変更することはできません。

1. 資産 リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
2. サブタイプに割り当てられている資産のみを表示するようにリストをフィルタリングするには、次の手順を実行します。
   a. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
   b. サブタイプを割り当てるか変更する資産を検索するために必要な条件を指定します。
   c. **検索** をクリックします。

   ヒント: また、特定基準で表示 ドロップダウンリストを使用して、特定の資産サブタイプに属する資産を識別することもできます。
3. サブタイプに割り当てる資産の隣のチェックボックスをオンにします。すべての資産を選択するには、表の最上部にある 名前 の隣のチェックボックスをオンにします。
4. **特定基準で表示 > アセットタイプ > デバイス** の順に選択し、リストから使用可能なエントリを 1 つ選択します。例えば、すべてのデバイス資産を表示するには、**すべてのデバイスサブタイプ** を選択します。
5. **アクションの選択 > サブタイプを次に変更：** を選択します。

   選択した資産が、選択したサブタイプに割り当てられます。

カスタム資産フィールドの手動更新

必要に応じてカスタム資産フィールドを手動で更新できます。これは、自動的に収集できない資産情報または資産に関して追跡する補足情報があるときに有益です。

カスタム資産サブタイプまたはカスタム資産フィールドを追加しました。

ヒント: カスタム資産フィールドを手動で更新する代わりに、スプレッドシートから情報をインポートできます。詳細については、「CSV ファイルでのライセンスデータのインポート」を参照してください。

1. Asset Detail（資産の詳細）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
c. 更新する資産の名前をクリックします。

2. 必要に応じてカスタム資産フィールドを変更します。
3. **保存** をクリックします。

資産サブタイプの削除

資産サブタイプに資産が割り当てられていない場合に限り、そのサブタイプを削除できます。

資産が割り当てられていない資産サブタイプがあります。

1. 資産タイプの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
   c. 資産サブタイプの名前をクリックして、Asset Type Detail（ 資産タイプの詳細 ）ページを表示します。
2. Subtypes（ サブタイプ ）セクションで、編集するサブタイプの隣にある **削除** ボタンをクリックします をクリックします。
3. ダイアログウィンドウで、**はい** をクリックします。

   資産サブタイプが 資産タイプ から削除され、関連するフィールドが直ちに削除されます。

ソフトウェア資産の管理

ソフトウェア ページインベントリでは、必要に応じて、ソフトウェア資産タイプをカスタマイズし、アプリケーションのソフトウェア資産を追加できます。

ソフトウェア資産は、ソフトウェア ページインベントリでのみ追加できます。ソフトウェアカタログ インベントリ内のアプリケーションには、ソフトウェア資産は必要ありません。

ソフトウェア資産タイプのカスタマイズ

ソフトウェア資産タイプの使用可能なフィールドは、必要に応じて追加、変更、または削除することができます。ソフトウェア資産タイプは、ソフトウェア資産を追加する際に使用可能なフィールドを設定するテンプレートです。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のソフトウェア資産タイプを個別にカスタマイズします。

1. 資産タイプの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
   c. **名前** 列で、**ソフトウェア**をクリックします。
2. **オプション**：資産フィールド テーブルのフィールドまたは値を変更します。
   a. 行の末尾にある **編集** ボタンをクリックします。
   b. 必要に応じて、フィールド情報を変更し、行の最後で **保存** をクリックします。
   c. フィールドを追加するには、表見出しで **追加** ボタンをクリックします。フィールド情報を追加し、行の最後で **保存** をクリックします。

d. フィールドの並び順を変更するには、行の最後にある **並べ替え** ボタンをクリックします。

e. フィールドを削除するには、**削除** ボタンをクリックします。

3. ページの一番下で **保存** をクリックします。

ソフトウェア資産の追加

ソフトウェア資産を使用すると、ソフトウェア ページインベントリのアプリケーションに関する情報を追跡できます。例えば、アプリケーションのソフトウェア資産を追加した後、その資産をライセンス資産に関連付けて、ライセンス情報を追跡できます。

アプライアンスに自動または手動で追加されたアプリケーションのソフトウェア資産を作成できます。

注: ソフトウェアカタログ インベントリ内のアプリケーションにライセンスコンプライアンスを設定する場合には、ソフトウェア資産は必要ありません。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンスについて」を参照してください。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のソフトウェア資産を個別に作成します。

ソフトウェアリストでのソフトウェア資産の追加

1 つまたは複数のアプリケーションのソフトウェア資産を一度に追加するには、ソフトウェア リストでアプリケーションを選択します。

ソフトウェア資産は、ソフトウェア リストインベントリでのみ追加できます。ソフトウェアカタログ インベントリ内のアプリケーションには、ソフトウェア資産は必要ありません。

1. ソフトウェア リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。
2. 1つまたは複数のアプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択 > 資産の作成** を選択します。

資産が作成され、それらが 資産 リストに表示されます。

資産 セクションにおけるソフトウェア資産の追加

資産 セクションでは、一度に1つずつソフトウェア資産を作成することができます。

ソフトウェア資産は、ソフトウェア リストインベントリでのみ追加できます。ソフトウェアカタログ インベントリ内のアプリケーションには、ソフトウェア資産は必要ありません。

1. ソフトウェア資産の詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
   c. **アクションの選択 > 新規作成 > ソフトウェア** を選択します。
2. 以下の要領で、資産フィールドに必要事項を入力します。

オプション	説明
サブタイプ	アセットのサブタイプ（ 該当する場合 ）。

オプション	説明
資産ステータス	資産ステータス（該当する場合）。デフォルトの資産ステータス、またはカスタムの資産ステータスを選択できます（存在する場合）。アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。 • **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。 • **廃棄済み**：利用できなくなった資産。 • **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。 • **在庫**：最近受け取った資産。 • **不在**：場所を特定できない資産。 • **修復**：修復されている資産。 • **予約済み**：特定の人または用途のために確保されている資産。 • **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。 • **盗難**：盗難されたとして報告された資産。 詳細については、「資産のライフサイクル設定の表示と設定」を参照してください。
場所	ドロップダウンメニューからこの資産の場所を選択します。このリストの値には、アプライアンスで定義されたすべての場所が含まれます。詳細については、次を参照してください。 場所の管理 **ヒント:** 場所は、コストセンター、部署、デバイス、ライセンス、ソフトウェア、ベンダーを含むすべてのデフォルトの資産タイプに定義できます。
名前	資産名。例えば、「Office Pro SW Asset」と入力します。
ソフトウェア	資産に関連付けるアプリケーションの名前を選択します。アイテムを検索するには、フィールドに入力し始めます。
ソフトウェアラベル	ドロップダウンリストでラベルを選択します。Smart Labelを作成していない場合、このリストには項目が表示されません。このボックスに入力して、特定のラベルを検索できます。
バーコードデータ **バーコードの名前** **バーコードのフォーマット**	この資産に関連付けるバーコードを確認または追加します。詳細については、「資産へのバーコードの追加」を参照してください。

a. 名前 フィールドに、資産の名前を入力します。例えば、「Office Pro SW Asset」と入力します。
b. **オプション**：ソフトウェア フィールドで、資産に関連付けるアプリケーションの名前を選択します。アイテムを検索するには、フィールドに入力し始めます。
c. **オプション**：ソフトウェアラベル フィールドで、ラベルの選択 ドロップダウンリストからラベルを選択します。Smart Labelを作成していない場合、このリストには項目が表示されません。ラベルリストを絞り込むには、ラベル名の数文字を フィルタ フィールドに入力します。

3. **保存** をクリックします。

資産 リストに新しい資産が表示されます。

物理的資産と論理的資産の管理

物理的資産には、デバイスのハードウェアやソフトウェア、オフィスの什器のようなその他の物理的資産が含まれます。論理的な資産には、場所、コストセンター、ベンダーなどが含まれます。

アプライアンスインベントリコンポーネントは、アプライアンスにソフトウェアとハードウェアのインベントリをレポートする物理的な資産（デバイスなど）に関する情報を資産管理コンポーネントに自動的に提供します。ただし、アプライアンスにインベントリをレポートしない物理的な資産および論理的な資産の場合は、情報を手動で追加および更新します。詳細については、「カスタム資産フィールドの手動更新」を参照してください。

論理的な資産の管理によって、次のことが可能になります。

- 論理的な資産を識別し、保護する。
- 論理的な資産同士を関連付け、その関係をレポートに使用する。例えば、地理的な関係や事業体間の関係などが考えられます。

また、サポート契約などのカスタム論理資産を追加し、対象のオブジェクトに関する追加メタデータを追跡できます。

物理的な資産タイプの追加

必要に応じて、物理的な資産タイプを追加できます。

1. 資産タイプの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
   c. **アクションの選択 > 新規作成** を選択します。
2. 名前 フィールドで資産の名前に、「Laptop」など分かりやすい名前を入力します。
3. デフォルトの資産ステータス フィールドに、デフォルトの資産ステータス、またはカスタムの資産ステータスを入力します（存在する場合）。

アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。

- **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。
- **廃棄済み**：利用できなくなった資産。
- **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。
- **在庫**：最近受け取った資産。
- **不在**：場所を特定できない資産。
- **修復**：修復されている資産。
- **予約済み**：特定の人または用途のために確保されている資産。
- **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。
- **盗難**：盗難されたとして報告された資産。

4. 管理者役割を持たないユーザーがこのタイプの資産を削除できるようにするには、**管理者以外に資産の削除を許可する** を選択します。このオプションはデフォルトでオフになっています。このオプションを設定できるのは管理者のみです。他のタイプのユーザーでは、このフィールドはページに表示されますが無効になっています。

   ユーザーの役割の詳細については、「ユーザーの役割の追加または編集」を参照してください。

5. このタイプの資産で、資産の場所を資産の詳細情報に表示するには、**場所の設定を表示** を選択します。このオプションはデフォルトでオフになっています。

6. バーコード の下で、＋ をクリックし、以下の情報を入力します。

オプション	説明
バーコードデータ	バーコード番号。バーコード番号は常に一意で、複数の資産間で共有できません。ただし、アクティブな資産がアーカイブされた資産のバーコードを共有することはできます。
バーコードの名前	この資産タイプに関連するバーコードのタグ。同じタイプのバーコードは資産ごとに1つしかありません。
バーコードのフォーマット	バーコードのフォーマット。例えば、UPC-A、Code 11、またはUPC-Eです。

   必要な数のバーコードを追加できます。

7. ページの右側で、**追加** ボタンをクリックします＋。

   新しい行が表示されます。

8. 新しい行に、次の情報を入力します。例：
   a. 名前 フィールドに、「ブランド」と入力します。
   b. 必須 列のチェックボックスをオンにし、このフィールドを必須にします。
   c. タイプ ドロップダウンリストで、**単一選択** を選択します。

      使用可能な値 フィールドが有効になります。

   d. 使用可能な値 フィールドに戻り、使用するブランドを入力します。入力したブランドが選択リストに表示されます。各ブランドはコンマで区切ります。

   例：Apple, Dell, IBM。こうすることで、確実に一貫したブランド名（IBMなど）を参照し、バリエーション（IBM、International Business Machinesなど）が使用されるのを防ぐことができます。

9. 行の最後で **保存** をクリックし、行を追加します。

a. **追加** ボタンをクリックします。
b. 新しい行に、その他の情報を入力します。

例：

- 名前 フィールドに、「シリアルナンバー」と入力します。
- タイプ ドロップダウンリストで、**テキスト** を選択します。

10. 行の最後で **保存** をクリックし、行を追加します。
    a. **追加** ボタンをクリックします。
    b. 新しい行に、その他の情報を入力します。

    例：

    - 名前 フィールドに、「場所」と入力します。
    - タイプ ドロップダウンリストで、**資産の場所** を選択します。
11. 行の最後で **保存** をクリックし、行を追加します。
    a. **追加** ボタンをクリックします。
    b. 新しい行に、その他の情報を入力します。

    例：

    - 名前 フィールドに 部門 と入力し、タイプ ドロップダウンリストで **資産 - 部門** を選択します。
    - 名前 フィールドに「コストセンター」と入力し、タイプ ドロップダウンリストで **資産 - コストセンター** を選択します。
12. 行の最後で **保存** をクリックし、行を追加します。
    a. **追加** ボタンをクリックします。
    b. 新しい行に、その他の情報を入力します。

    例：

    - 名前 フィールドに、「保証期間」と入力します。
    - タイプ ドロップダウンリストで、「**日付**」を選択します。入力形式は**yyyy-mm-dd**です。サポートされている範囲は、1000-01-01～9999-12-31です。
13. 行の最後で **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

デバイス資産のアーカイブ

デバイス資産は必要に応じてアーカイブできます。

アプライアンスの管理者は、使用しなくなったデバイス資産をアーカイブできます。デバイス資産をアーカイブすると、そのデバイスはアプライアンスのノードライセンス数に含まれなくなります。アーカイブ用にマークの付けられたデバイスは、一般設定 で指定した事前定義日数後にアーカイブされます。デフォルトの期間は3日です。この期間に、管理者はアーカイブ用にマークが付けられたデバイスを元に戻すことができます。

デバイス資産にアーカイブ用のマークを付けている期間の日数の変更方法の詳細については、次を参照してください。 管理者レベルまたは組織固有の一般設定項目の設定

デバイスがアーカイブされると、そのデバイスのレコードが削除され、以前のアクティブな状態に戻すことができなくなります。必要に応じて、アーカイブしたデバイス資産のデバイス詳細を確認することができます。

1. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. 左側のナビゲーションバーで、**資産** をクリックします。
3. 次の手順のいずれかを実行します。
   - 資産リストで、デバイス資産を選択します。**アクションの選択 > アーカイブ** を選択します。
   - 資産リストで、デバイス資産の名前をクリックします。表示された 資産詳細 ページで、**アーカイブ** をクリックします。
4. 表示された 資産のアーカイブ ダイアログボックスで、アーカイブ理由 フィールドにこのアクションの理由を入力し、**保存** をクリックします。

   資産のアーカイブ ダイアログボックスが閉じ、アセット リストが更新され、デバイス資産が保留中のアーカイブ状態（  ）であることが示されます。アーカイブの保留中の期間が終了すると、アプライアンスでデバイスの資産がアーカイブされ、アーカイブ済み状態（  ）になります。
5. デバイス資産を保留中のアーカイブの状態から削除したい場合は、次の手順を実行します。
   a. 資産 リストで、アーカイブの保留中の状態のデバイス資産の名前をクリックします。
   b. 表示された 資産詳細 ページで、**保留中のアーカイブの取り消し** をクリックします。

   資産詳細 ページを閉じ、資産 リストが更新され、デバイス資産が保留中のアーカイブ状態ではなくなったことが示されます。
6. アーカイブしたデバイス資産のデバイス詳細を確認する場合は、アセット リストの 名前 列で、括弧に囲まれたデバイス名をクリックします。

   デバイスの詳細ページが表示されます。このページには、アーカイブされていないデバイス資産に対して通常表示される情報のサブセットが含まれています。このページに表示されるフィールドの詳細については、デバイス詳細のアイテムのグループおよびセクションを参照してください。

手動資産情報の維持および使用

アプライアンスにインベントリを自動的にレポートしない資産の場合、資産情報を手動で追加できます。これは、場所、コストセンター、ベンダーなどの論理的な資産にも、オフィスの什器や機器などの物理的な資産にも便利です。手動でインポートまたは追加された資産情報は、情報が変更された場合に手動で更新する必要があります。

資産情報を手動で最新の状態に維持する方法が 2 つあります。

- スプレッドシートで情報を管理し、定期的にアプライアンスに再インポートする。
- 資産管理コンポーネントで情報を手動で保守する。

どちらを選択した場合も、データを最新に保つため、選択した方法を一貫して使用するようにしてください。

資産管理者役割の作成

資産管理者役割を作成すると、他のユーザーに対して、アプライアンス内での資産の更新を許可できます。

役割の作成の詳細については、ユーザーアカウントの役割の設定を参照してください。

通常のインポートのスケジュール

資産情報を効率的に維持するために、ソーススプレッドシートを継続的に更新できます。資産管理コンポーネントは、インポートのたびに、資産が作成されたときにプライマリキー（PK）として指定されたものに基づいて、レコードをインポートするか更新するかを決定します。

- プライマリキーが既存のレコードに一致する場合、資産管理コンポーネントはデータを比較し、既存のレコードを更新します。
- 行に一致するプライマリキーがない場合、新しいレコードが生成されます。

詳細については、「CSV ファイルでのライセンスデータのインポート」を参照してください。

ヒント: 新しいデータをインポートする場合は、事前にレポートを生成し、現在のデータをエクスポートしておくと効果的です。これにより、新しいデータの構造に不具合がある場合に、元のデータを復元することができます。

レポートでの資産データの使用

資産管理コンポーネントのデータは、標準のレポートにエクスポートできます。

標準のレポートには、次のようなものがあります。

- **未承認のソフトウェアインストール**: 使用許諾を受けていないデバイスで検出されたソフトウェアをレポートします。
- **簡略的なソフトウェアコンプライアンス**: 資産 リストで検出されたライセンスなど、ライセンス数をレポートします。
- **完全なソフトウェアライセンスコンプライアンス**: 各ライセンスによって影響を受けるソフトウェアとデバイスを一覧表示します。

さらに、独自のレポートを作成することもできます。詳細については、「レポートについて」を参照してください。

場所の管理

場所エンティティは、1つ、または複数の資産を含む物理サイトを表します。

必要に応じて、場所のエンティティを追加、移動、または削除できます。

場所の管理

場所は、1つ、または複数の資産を含む物理サイトを表します。これらは、場所のタイプに基づきます。

必要に応じて、場所のエンティティを追加、移動、または削除したり、場所の詳細をファイルにエクスポートしたりできます。

1. 場所 リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**場所** をクリックします。
2. 場所を追加するには、**アクションの選択 > 新規** を選択します。

    詳細については、場所の追加または編集を参照してください。
3. 場所を削除するには
    a. 削除する場所を含む行を選択します。
    b. **アクションを選択 > 削除** の順に選択します。

c. （**オプション**）表示される 場所の削除 ダイアログボックスで、削除しようとしている場所に関連するすべての資産を移動する代わりの場所を指定します。

d. **確認** をクリックします。

注: 親の場所を削除しても、システムからその子の場所は削除されません。

4. 場所を移動するには

a. 移動する場所を含む行を選択します。

b. **アクションの選択 > 移動** の順に選択します。

c. 表示される 場所の移動 ダイアログボックスで、場所を移動する親の位置を指定します。

d. **確認** をクリックします。

場所 リストが更新され、新しく移動した場所が表示されなくなります。特定の親に関連する子の場所を表示するには、親の場所を含む行で、場所の名前の右にある ▸ をクリックします。

5. 名前 フィールドで、必要に応じて名前を追加または変更します。

ヒント: デバイスおよびライセンス資産タイプで追加のオプションを使用できます。デバイス資産タイプのカスタマイズについておよびライセンス資産タイプのカスタマイズを参照してください。

6. 1 つ、または複数の場所をファイルにエクスポートするには

a. エクスポートする場所を含む行を選択します。

b. **アクションの選択 > エクスポート** を選択し、適切なオプションを選択します。

例えば、すべての場所を csv ファイルにエクスポートするには、リストで選択してから、**アクションを選択エクスポートすべてを CSV 形式でエクスポート** の順に選択します。

資産のインポート ウィザードを使用して、ファイルから場所の情報をインポートできます。詳細については、「CSVファイルを使用した資産データのインポート」を参照してください。

場所の追加または編集

場所の詳細 ページには、選択した場所の詳細が表示されます。

場所情報は静的であり、データをインポートした場合、またはデータを手動で変更した場合にのみ変更されます。

1. 場所詳細 ページに移動し、以下の手順を実行します。

a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**資産管理** をクリックして、**場所** をクリックします。

c. 以下のいずれかを実行して、場所詳細 ページを表示します。

- 場所の名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

2. 新しい行に、場所に関する次の情報を入力します。**サブタイプ**、**名前**（必須）、**説明**、**Web サイト**、**アドレス**、**ロケール**、**電話番号**。
3. 既存の口ケーションを編集する場合に、その口ケーションをデバイスに関連付けるには、割り当てられているデバイス セクションで ＋ をクリックし、デバイスを選択して、**追加** をクリックします。

選択したデバイスが下のリストに表示されます。

4. 既存の口ケーションを編集している場合に、その口ケーションを資産に関連付けるには、割り当てられている資産 セクションで ＋ をクリックし、資産を選択して、**追加** をクリックします。

選択した資産が下のリストに表示されます。

5. **保存** をクリックします。

場所に関するフィールドのカスタマイズ

必要に応じて、場所詳細 ページでフィールドの名前の変更、作成、および削除ができます。

1. 場所詳細 ページに移動し、以下の手順を実行します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**場所** をクリックします。
    c. 以下のいずれかを実行して、場所詳細 ページを表示します。
    - 場所の名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. 必要に応じて、場所のサブタイプを指定します。
    a. サブタイプ セクションで、**サブタイプの追加** をクリックします。

    場所の資産サブタイプ詳細 ページが表示されます。資産サブタイプに使用可能なフィールドが継承されるフィールド セクションに表示されます。既にそれらのフィールドが資産タイプに追加されているからです。

    b. 表示される 場所の資産サブタイプ詳細 ページで、必要に応じて、次のオプションを確認および編集します。

オプション	説明
名前	場所のサブタイプの名前。この名前は、資産タイプの詳細 ページのリストに表示されます。
デフォルト	新しい場所のデフォルトとして場所のサブタイプを使用するかどうかを示します。このチェックボックスをオンにすると、新しい場所がこの資産サブタイプに自動的に割り当てられます。この設定はいつでも変更できます。
継承されるフィールド	このセクションでは、デフォルトの場所フィールドが表示されます。このセクションは変更できません。
サブタイプのフィールド	必要に応じて、このサブタイプに固有の任意のフィールドを追加します。フィールドを追加するには、＋をクリックし、必要な情報を指定します。

    c. **保存** をクリックします。
3. この場所でバーコードを使用する場合は、バーコードタグ 領域で1つまたは複数のタグを指定します。

    それ以降に作成するすべての場所は、バーコードタグを設定可能です。例えば、企業タグおよびDell場所タグを指定する場合、これらの2種類のタグで識別されるバーコードは場所を作成または編集する際に 場所詳細 ページで選択可能になります。

    バーコードを追加するには、＋をクリックし、バーコードの名前を入力し、**保存** をクリックします。
4. 必要に応じて、追加の場所フィールドを指定します。

a. 資産フィールド 領域でフィールドを追加するには、＋ をクリックします。
b. 新しいフィールドごとに、次の情報を入力します。

オプション	説明
名前	フィールド名。
使用可能な値	値のリストを含むフィールドに表示される値。タイプ ドロップダウンリストから **単一選択** または **複数選択** を選択した場合に、このフィールドが有効になります。**単一選択** または **複数選択** を選択した場合には、このフィールドに少なくとも1つの値を入力する必要があります。複数の値を入力するには、コンマを使用して各値を区切ります。
必須	対象のフィールドが必須か任意かを指定します。このチェックボックスをオンにした場合、選択したタイプの資産を作成する際には、このフィールドに値を入力する必要があります。
タイプ	フィールドのタイプ。フィールドのタイプは次の通りです。 • **添付ファイル**: 資産に添付ファイルを追加できます。 • **通貨**: 金額に使用します。 • **ソフトウェアカタログ**: 資産をソフトウェアカタログのアプリケーションに関連付けできます。 • **日付**: カレンダー情報に使用します。 • **ラベル**: ラベルを資産に関連付けできます。 • **リンク**: インターネットリンクに使用します。リンクは、有効な URL（**http://quest.com**）である必要があります。 • **複数選択**: 複数の値が選択可能な場合にリストを表示します。各値の最大長は255文字です。 • **メモ**: 追加情報に使用します。 • **数字**: 整数で表される数値に使用します。 • **親**: この資産は、親子関係にある同じタイプの資産を参照できます。例えば、「場所」タイプで親接続を許可して、「New York」場所が「North America」場所を参照可能なようにできます。このタイプをレポート作成システム

オプション	説明
	で使用して、北米にあるすべての資産を表示できます。 • **発行者**：ソフトウェアカタログで利用できる発行元の最新のリストから選択できます。 • **単一選択**: 1つの値しか選択できない場合に値のリストを表示します。各値の最大長は255文字です。 • **テキスト**: 追加テキストに使用します。最大長は255文字です。 • **タイムスタンプ**: レコードに日付と時間を追加するために使用します。 • **ユーザー**: ユーザーレコードを資産に関連付けるために使用します。 • **資産資産タイプ**: 資産タイプ間の関係を指定するために使用します。

c. **保存** をクリックします。

5. **保存** をクリックします。

契約の管理

契約は、ベンダーとエンドユーザーの間で結ばれる購入契約の 1 つの形態であり、使用条件を説明します。契約は、ビジネスで使用するソフトウェアおよびハードウェアのアイテム、およびオフィス家具またはコーヒーマシンなどの物理的なアイテムと関連付けることができます。

組織は、必要に応じて契約を追加、編集、または削除することができます。

契約の管理

契約はビジネスで使用するハードウェアおよびソフトウェアアイテム、およびオフィスのイスまたはコーヒーサプライヤなどの任意の物理的な製品またはサービスの購入またはサービス契約を表します。

必要に応じて、契約を追加、編集、または削除することができ、また契約の詳細をファイルにエクスポートすることができます。

1. 契約 リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**契約** をクリックします。
2. 契約を追加するには、**アクションを選択 > 新規** の順に選択します。

   詳細については、契約の追加または編集を参照してください。
3. 契約を削除するには、次の手順を実行します。
   a. 削除する契約を含む行を選択します。
   b. **アクションを選択 > 削除** の順に選択します。
4. 1 つ、または複数の契約エントリをファイルにエクスポートするには、次の手順を実行します。
   a. エクスポートする契約を含む行を選択します。
   b. **アクションの選択 > エクスポート** を選択し、適切なオプションを選択します。

例えば、すべての契約を csv ファイルにエクスポートするには、リストで選択してから、**アクションを選択 > エクスポート > すべてを CSV 形式でエクスポート** の順に選択します。

資産のインポート ウィザードを使用して、ファイルから契約情報をインポートできます。詳細については、「CSVファイルを使用した資産データのインポート」を参照してください。

契約の追加または編集

契約の詳細 ページには、選択した契約の詳細が表示されます。

このページを使用して、必要に応じて、契約を追加または編集します。

1. 契約の詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**契約** をクリックします。
   c. 以下のいずれかを実行して、契約の詳細 ページを表示します。
   - 契約の名前をクリックします。
   - **アクションの選択 > 新規作成 > 契約-ハードウェア** の順に選択します。
   - **アクションの選択 > 新規作成 > 契約 - ソフトウェア** の順に選択します。
   - **アクションの選択 > 新規作成 > 契約 - その他** の順に選択します。
2. 契約に関する一般的な情報を入力します。

   契約は、資産タイプの 1 つの形態で、常に必須の 名前 フィールドを除き、各契約タイプで利用できるフィールドのコレクションは必要に応じて変更できます。資産タイプの詳細については、以下を参照してください。 資産タイプについて

   契約レコードには、通常、以下のフィールドが表示されます。

オプション	説明
サブタイプ	この契約資産のサブタイプ割り当て（ 該当する場合 ）。なし は、資産がサブタイプに割り当てられていないことを示します。 該当する契約資産サブタイプで契約サブタイプを指定できます（ **契約 - ソフトウェア**、**契約 - ハードウェア**、または**契約 - その他** ）。資産サブタイプの詳細については、資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定についてを参照してください。
資産ステータス	契約ステータス（ 該当する場合 ）。デフォルトの資産ステータス、またはカスタムの資産ステータスを選択できます（ 存在する場合 ）。アプライアンスの

オプション	説明
	デフォルトのインストールには、以下の資産ステータスが含まれます。 • **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。 • **廃棄済み**：利用できなくなった資産。 • **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。 • **在庫**：最近受け取った資産。 • **不在**：場所を特定できない資産。 • **修復**：修復されている資産。 • **予約済み**：特定の人または用途のために確保されている資産。 • **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。 • **盗難**：盗難されたとして報告された資産。 詳細については、「資産のライフサイクル設定の表示と設定」を参照してください。
場所	この資産の場所。
名前	契約の名前。
契約番号	契約番号。
契約の説明	契約に関する追加の情報。
契約開始日	契約がアクティブ化された日付。
契約終了日	契約が終了する日付。
記念日	**ソフトウェア契約およびハードウェア契約のみ。**契約がいつ更新されるかを示すインジケータ。
発行元	**ソフトウェア契約およびハードウェア契約のみ。**契約発行元。
発行元プログラム	**ソフトウェア契約のみ。**選択に使用できるエントリは、発行元 フィールドで設定した内容に応じて、ソフトウェアカタログから入力されます。発行元を選択すると、このフィールドで選択に使用できるエントリには、ソフトウェアカタログに存在する、選択した発行元に関連付けられたプログラムエントリが入力されます。
ベンダー	契約に関連付けられているベンダーの名前。使用可能なベンダーエントリから選択できます。
ベンダー契約番号	契約と関連付けられているベンダー契約の番号。

オプション	説明
製造元	**ハードウェア契約のみ。**この契約に関連付けられているデバイスの製造元。
ハードウェアタイプ	**ハードウェア契約のみ。**この契約に関連付けられているハードウェアデバイスのタイプ（ノート PC またはサーバーなど）。
ハードウェアシリーズ	**ハードウェア契約のみ。**この契約に関連付けられているハードウェアデバイスのシリーズ。
ハードウェアモデル	**ハードウェア契約のみ。**この契約に関連付けられているハードウェアデバイスのモデル番号。
注文書番号	契約と関連付けられている注文書の番号。
注文書の日付	契約と関連付けられている注文書の日付。
リンク先の契約	この契約エントリに関連付けられている別の契約。
連絡先名	契約に関連付けられている連絡先名。
連絡先 E メール	契約に関連付けられている連絡先の E メールアドレス。
連絡先電話番号	契約に関連付けられている連絡先の電話番号。
メモ	この契約に関する追加情報。
添付ファイル 1、添付ファイル 2	契約に関連付けられている任意のファイルの添付。

3. （**オプション**）必要に応じて、1 つまたは複数のバーコードを契約に追加します。
   a. バーコード の下で、＋ をクリックし、以下の情報を入力します。

オプション	説明
バーコードデータ	バーコード番号。バーコード番号は常に一意で、複数の資産間で共有できません。ただし、アクティブな資産がアーカイブされた資産のバーコードを共有することはできます。
バーコードの名前	この資産タイプに関連するバーコードのタグ。同じタイプのバーコードは資産ごとに1つしかありません。
バーコードのフォーマット	バーコードのフォーマット。例えば、UPC-A、Code 11、またはUPC-Eです。

4. サービスデスク セクションの情報を確認します。1 つまたは複数のサービスデスクチケットに関連付けられている既存の契約を編集している場合、このセクションに表示されます。
5. 関連する資産 セクションの情報を確認します。1 つまたは複数のライセンスに関連付けられている既存の契約を編集している場合、このセクションに表示されます。
6. **保存** をクリックします。

ライセンスの管理

ライセンス契約により、ソフトウェアまたはハードウェアなどの論理的または物理的資産を利用できます。

必要に応じて、ライセンスを追加、編集、または削除でき、また、物理的または論理的資産と関連付けることができます。

ライセンスの管理

ライセンスにより、ビジネスで使用するソフトウェアおよびハードウェアなどの論理的または物理的資産を利用できます。

必要に応じて、ライセンスを追加、編集、または削除することができ、またライセンスの詳細をファイルにエクスポートすることができます。

1. ライセンス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**ライセンス** をクリックします。
2. ライセンスを追加するには、**アクションを選択 > 新規** の順に選択します。

    詳細については、ライセンスの追加または編集を参照してください。
3. ライセンスを削除するには、次の手順を実行します。
    a. 削除するライセンスを含む行を選択します。
    b. **アクションを選択 > 削除** の順に選択します。
4. 1 つ、または複数のライセンスエントリをファイルにエクスポートするには、次の手順を実行します。
    a. エクスポートするライセンスを含む行を選択します。
    b. **アクションの選択 > エクスポート** を選択し、適切なオプションを選択します。

    例えば、すべてのライセンスを csv ファイルにエクスポートするには、リストで選択してから、**アクションを選択 > エクスポート > すべてを CSV 形式でエクスポート** の順に選択します。

    資産のインポート ウィザードを使用して、ファイルからライセンス情報をインポートできます。詳細については、「CSVファイルを使用した資産データのインポート」を参照してください。

ライセンスの追加または編集

ライセンスの詳細 ページには、選択したライセンスの詳細が表示されます。

このページを使用して、必要に応じて、ライセンスを追加または編集します。ライセンスは、資産タイプの 1 つの形態で、常に必須のライセンス名を除き、ライセンスレコードで利用できるフィールドのコレクションは必要に応じて変更できます。資産タイプの詳細については、「資産タイプについて」を参照してください。

1. ライセンスの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**ライセンス** をクリックします。

c. 以下のいずれかを実行して、ライセンスの詳細 ページを表示します。

- ライセンスの名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

2. ライセンス資産の詳細 ページの 全般 タブで次の情報を入力します。

オプション	説明
サブタイプ	ライセンスに関連付ける資産サブタイプ。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。
資産ステータス	ライセンスステータス（該当する場合）。デフォルトの資産ステータス、またはカスタムの資産ステータスを選択できます（存在する場合）。アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。 • **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。 • **廃棄済み**：利用できなくなった資産。 • **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。 • **在庫**：最近受け取った資産。 • **不在**：場所を特定できない資産。 • **修復**：修復されている資産。 • **予約済み**：特定の人または用途のために確保されている資産。 • **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。 • **盗難**：盗難されたとして報告された資産。 詳細については、「資産のライフサイクル設定の表示と設定」を参照してください。
場所	資産がある場所の名前。詳細については、「場所の管理」を参照してください。
名前	ライセンス名（「**Office Professional PO #1234**」など）。これは資産を検索するために使用される名前です。1 つのアプリケーションに複数のライセンスを関連付ける場合は、それらのライセンスを区別するために、以下のフィールドに注文書番号または購入日を指定します。
ライセンス数	ライセンスによって許諾されるインストール数またはシート数。例えば、「50」と表示されます。
カタログ登録済みソフトウェアへの適用	ライセンスを適用する、ソフトウェアカタログインベントリ内のアプリケーション。必要に応じて、ソフトウェアカタログの複数のアプリケーションにライセンス資産を関連付けることができます。ただし、ライセンス資産を同じアプリケーションの複数

オプション	説明
	のバージョンに関連付ける必要はありません。アップグレードおよびダウングレードをサポートするためにアプライアンスがこれを自動的に行うからです。ライセンス情報を追加するときに、現在のバージョンをライセンス資産に関連付けるだけです。 また、Microsoft Office や Adobe Acrobat などの別の発行元からアプリケーションを同じライセンス資産に割り当てた場合は、ライセンス資産に指定されているシートの総数が各アプリケーションに割り当てられます。例えば、ライセンス資産に 100 個のシートがある場合、Microsoft Office と Adobe Acrobat の両方に 100 個のシートが割り当てられます。
ソフトウェアへの適用	このフィールドは空白のままにします。ソフトウェアカタログ インベントリと ソフトウェア ページインベントリのアプリケーションに対して、同時に1つのソフトウェアライセンスを関連付けることはできません。カタログ登録済みソフトウェアに対してライセンス資産を作成する方法の詳細については、ソフトウェア ページインベントリのライセンス資産の追加を参照してください。
ライセンスモード	ライセンス資産のモード。ライセンスを必要とし、ライセンスコンプライアンス ページにライセンス使用率情報を表示するアプリケーションの場合、Enterprise（エンタープライズ）または Unit License（ユニットライセンス）のいずれかを選択します。 **注:** ライセンスコンプライアンスでは、Not Specified（指定なし）、Client License（クライアントライセンス）、サブスクリプション、Shareware（シェアウェア）、Freeware（フリーウェア）、OpenSource（オープンソース）、No Licensing（ライセンスなし）、Site License（サイトライセンス）などほとんどのモードが使用されません。 ライセンスモードは、**管理者コンソール**の次のセクションで使用されます。 • ライセンスコンプライアンス リスト。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンス情報の表示」を参照してください。 • Dashboard（ダッシュボード）に表示されるライセンスコンプライアンス グラフ。Asset Detail（資産詳細）ページで無視にマーク付けされた値は、100% の使用レベルで表示されます。詳細については、「ダッシュボードのウィジェットについて」を参照してください。

3. **次へ** をクリックします。
4. ライセンス資産の詳細 ページの 購入 タブで次の情報を入力します。

オプション	説明
契約	ライセンスに関連付けられている契約資産。
カタログ登録済みソフトウェアへの適用	ライセンスを適用する、ソフトウェアカタログインベントリ内のアプリケーション。必要に応じて、ソフトウェアカタログの複数のアプリケーションにライセンス資産を関連付けることができます。ただし、ライセンス資産を同じアプリケーションの複数のバージョンに関連付ける必要はありません。アップグレードおよびダウングレードをサポートするためにアプライアンスがこれを自動的に行うからです。ライセンス情報を追加するときに、現在のバージョンをライセンス資産に関連付けるだけです。 また、Microsoft Office や Adobe Acrobat などの別の発行元からアプリケーションを同じライセンス資産に割り当てた場合は、ライセンス資産に指定されているシートの総数が各アプリケーションに割り当てられます。例えば、ライセンス資産に 100 個のシートがある場合、Microsoft Office と Adobe Acrobat の両方に 100 個のシートが割り当てられます。
プロダクトキー	ライセンスに関連付けられているプロダクトキー。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
単価	ライセンスに関連付けられている単価。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
ベンダー	アプリケーションに関連付けるベンダー資産の名前。ベンダー資産を追加していない場合は、Vendor（ベンダー）ドロップダウンリストに何も表示されません。ベンダーを検索するには、リストに入力を開始します。 **注:** ライセンスコンプライアンス情報が不正確になることがあるため、単一のソフトウェアライセンス資産に複数のベンダーを割り当てることはお勧めしません。
注文書番号	ライセンスに関連付けられた注文書番号。
購入日	購入した日付。フィールド内をクリックし、カレンダーで日付を選択します。
購入	このライセンスに関連付けられている購入レコードを 1 つ以上選択します。詳細については、「購入レコードの管理」を参照してください。

5. **次へ** をクリックします。
6. ライセンス資産の詳細 ページの メンテナンス タブで次の情報を入力します。

オプション	説明
アップグレード権を含む	ライセンスにアップグレート権が含まれるかどうかを示します。アップグレード権とは、ライセン

オプション	説明
	ス済みソフトウェアの新しいバージョンが利用可能になったときに、その新しいバージョンにアップグレードできる資格があることを意味します。詳細については、「ライセンスのアップグレードについて」を参照してください。次のいずれかのオプションを選択します。 • **はい**: アップグレード権は、選択したソフトウェアの既存のライセンス数と、それと同一のソフトウェアで利用可能な、より新しいバージョンのライセンス数を比較することによって計算されます。 • **はい - リストから選択**: アップグレード権を付与するソフトウェアバージョンを1つまたは複数選択します。アップグレードソフトウェアリスト の下で、**追加するカタログ登録済みソフトウェアの選択** をクリックします。選択したソフトウェアにおいて、ライセンスをアップグレードすることが可能なより新しいバージョンのリストが表示されます。リスト内のエントリを選択すると、選択した内容が アップグレードソフトウェアリスト ボックスに表示されます。必要に応じて、1つまたは複数のバージョンを追加できます。リストからアイテムを削除するには、アップグレードソフトウェアリスト ボックスでそのアイテムを選択して、**削除** をクリックします。 • **いいえ**: 選択したソフトウェアにアップグレード権を付与しない場合は、このオプションを選択します。
Includes Maintenance（メンテナンスを含む）	ライセンスがユーザーにアプリケーションのインストールバージョンをアップグレードする権利を与えているかどうか。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンスについて」を参照してください。
有効期限日	ライセンスにメンテナンスが含まれている場合は、メンテナンス期間の有効期限。 アプライアンスライセンスコンプライアンス機能は、アプリケーションリリース日などソフトウェアカタログ情報を利用します。メンテナンス期間中に新規アプリケーションバージョンをリリースした場合、そのバージョンは自動的にこのライセンス資産の対象範囲になります。
ダウングレード権を含む	ライセンスにダウングレード権が含まれるかどうかを示します。ダウングレード権とは、ソフトウェアの新しいバージョンを同じソフトウェアの古いバージョンにダウングレードするライセンスを適用する資格があることを意味します。詳細については、「ライセンスのダウングレードについて」を参照し

オプション	説明
	てください。次のいずれかのオプションを選択します。 • **はい**: ダウングレード権は、選択したソフトウェアの既存のライセンス数と、それと同一のソフトウェアで利用可能な、より古いバージョンのライセンス数を比較することによって計算されます。 • **はい - リストから選択**: ダウングレード権を付与するソフトウェアバージョンを1つまたは複数選択します。ダウングレードソフトウェアリスト の下で、**追加するカタログ登録済みソフトウェアの選択** をクリックします。ライセンスをダウングレードすることが可能な、選択したソフトウェアのより古いバージョンのリストが表示されます。リスト内のエントリを選択すると、選択した内容が ダウングレードソフトウェアリスト ボックスに表示されます。必要に応じて、1つまたは複数のバージョンを追加できます。リストからアイテムを削除するには、ダウングレードソフトウェアリスト ボックスでそのアイテムを選択して、**削除** をクリックします。 • **いいえ**: 選択したソフトウェアにダウングレード権を付与しない場合は、このオプションを選択します。

7. **次へ** をクリックします。
8. ライセンス資産の詳細 ページの 関連 タブで次の情報を入力します。

オプション	説明
部門	アプリケーションを所有するビジネスグループまたは部門。
コストセンター	アプリケーションを所有する部門に関連付けられたコストセンター。
承認されたデバイス	ライセンスの使用を承認されたデバイス。この情報は、ライセンスコンプライアンスレポートの作成に使用されます。例えば、対象のアプリケーションをインストールしたデバイスが、承認されたデバイスのリストに存在しない場合、それらのデバイスは「未承認のソフトウェアインストール」というタイトルのレポートで報告されます。ただし、アプライアンスは、ライセンスコンプライアンスを強制しません。例えば、ライセンスが期限切れであったり、コンプライアンスから外れていたとしても、管理対象デバイスへのアプリケーションのインストールがアプライアンスによって阻止されることはありません。
バーコード	必要に応じて、このライセンスに関連付けられたバーコードを追加または編集します。詳細について

オプション	説明
	は、「資産へのバーコードの追加」を参照してください。

9. **次へ** をクリックします。
10. ライセンス資産の詳細 ページの カスタム タブで、追加のカスタムデータを入力します。ビジネス目標に合わせて、ライセンス資産タイプを修正し、必要な数のフィールドを追加することができます。詳細については、「資産タイプの追加またはカスタマイズ」を参照してください。
11. **次へ** をクリックします。
12. ライセンス資産の詳細 ページの メモ タブで、次の情報を入力します。

オプション	説明
メモ	任意の追加情報を入力します。
ライセンステキスト	ライセンスナンバーなどライセンスに関する補足情報。

13. **保存** をクリックします。

購入レコードの管理

購入レコードは、組織の物理的製品およびソフトウェア製品の取得を文書化します。管理者は、個々の購入レコードを追跡し、関連するライセンス契約と関連付けることができます。特定の資産のライセンス契約を 1 つまたは複数の購入レコードに関連付けることができます。例えば、組織が Adobe Acrobat について 1 つのライセンス契約があり、このソフトウェアライセンスについて複数の購入レコードがある場合、それぞれが組織内の各グループに対するものです。

購入レコードは、必要に応じて、追加、編集、または削除、および該当するライセンス契約と関連付けることができます。

購入レコードの管理

管理者は、組織のための物理的およびソフトウェア製品を取得するために使用される個々の購入レコードを追跡することができます。

必要に応じて、購入レコードを追加、編集、または削除することができ、また購入レコードの詳細をファイルにエクスポートすることができます。

1. 購入 リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**購入** をクリックします。
2. 購入レコードを追加するには、**アクションを選択 > 新規** を選択します。

    詳細については、購入レコードを追加または編集するを参照してください。
3. 購入レコードを削除するには、次の手順を実行します。
    a. 削除する購入レコードを含む行を選択します。
    b. **アクションを選択 > 削除** の順に選択します。
4. 1 つ、または複数の購入レコードをファイルにエクスポートするには、次の手順を実行します。
    a. エクスポートする購入レコードを含む行を選択します。
    b. **アクションの選択 > エクスポート** を選択し、適切なオプションを選択します。

例えば、すべての購入レコードを csv ファイルにエクスポートするには、リストで選択してから、**アクションを選択 > エクスポート > すべてを CSV 形式でエクスポート** の順に選択します。

購入レコードを追加または編集する

購入の詳細 ページには、選択した場所の詳細が表示されます。

このページを使用して、必要に応じて購入レコードを追加または編集します。ライセンスは、資産タイプの 1 つの形態で、常に必須の購入レコード名と単位数量を除き、ライセンスレコードで利用できるフィールドのコレクションは必要に応じて変更できます。資産タイプの詳細については、「資産タイプについて」を参照してください。

1. ライセンスの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの ー般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**購入** をクリックします。
   c. 以下のいずれかを実行して、購入の詳細 ページを表示します。
   - 購入レコードの名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。
2. 購入の詳細 ページで、以下の情報を入力します。

オプション	説明
サブタイプ	購入レコードに関連付ける資産サブタイプ。ハードウェア または ソフトウェア のアイテムの購入レコードを作成することができます。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。
資産ステータス	購入レコードのステータス（ 該当する場合 ）。デフォルトの資産ステータス、またはカスタムの資産ステータスを選択できます（ 存在する場合 ）。アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。 • **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。 • **廃棄済み**：利用できなくなった資産。 • **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。 • **在庫**：最近受け取った資産。 • **不在**：場所を特定できない資産。 • **修復**：修復されている資産。 • **予約済み**：特定の人または用途のために確保されている資産。 • **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。 • **盗難**：盗難されたとして報告された資産。

オプション	説明
	詳細については、「資産のライフサイクル設定の表示と設定」を参照してください。
場所	この購入で取得した資産がある場所の名前。詳細については、「場所の管理」を参照してください。
名前	購入レコードの名前（**Office Professional PO #1234** など）。これは、必要に応じて、この発注書をライセンス契約に関連付けるために使用する名前です。
説明	注文書の説明。
注文書番号	組織が発行した注文書の番号。
注文書の日付	組織が注文書を発行した日付。
数量	購入したユニットの数。
単価	購入した個々のユニットのコスト。
ベンダー	ユニットを購入したベンダーの名前。
ベンダー注文番号	ベンダーによって発行された注文書の番号。
ベンダー注文日	ベンダーが発注書を発行した日付。
購入証明	購入レコードの写真を含む画像。
メモ	任意の追加情報を入力します。
ソフトウェアタイトル	**ソフトウェアのみ。**購入したソフトウェアの名前。
発行元	**ソフトウェアのみ。**購入したソフトウェアの発行元。
契約	**ソフトウェアのみ。**ソフトウェアの購入に関連付けられた契約。
プロダクトキー	**ソフトウェアのみ。**購入したソフトウェアのプロダクトキー。
Maintenance Expiration Date（メンテナンス有効期限）	**ソフトウェアのみ。**購入したソフトウェアのメンテナンスが終了する日付。
メンテナンスの証明	**ソフトウェアのみ。**メンテナンス契約の写真を含む画像。
製造元	**ハードウェアのみ。**購入したハードウェアアイテムの製造元。

オプション	説明
モデル	**ハードウェアのみ。**購入したハードウェアアイテムのモデル名。
仕様	**ハードウェアのみ。**購入したハードウェアアイテムの仕様（該当する場合）。
シリアルナンバー	**ハードウェアのみ。**購入したハードウェアアイテムのシリアルナンバー。
契約	**ハードウェアのみ。**購入したハードウェアアイテムに関連付けられた契約。
保証開始日	**ハードウェアのみ。**購入したハードウェアアイテムに対する製造元の保証が開始する日。
保証終了日	**ハードウェアのみ。**購入したハードウェアアイテムに対する製造元の保証が終了する日付。
終了日をサポート	**ハードウェアのみ。**購入したハードウェアアイテムのサポートが終了する日付。
バーコード	この注文書で取得するアイテムに関連付けられたバーコードを追加または編集します（該当する場合）。詳細については、「資産へのバーコードの追加」を参照してください。

ライセンスコンプライアンスの設定

アプリケーションのライセンスコンプライアンス情報を追跡するには、ライセンス資産を作成する必要があります。ライセンス資産は、ソフトウェアカタログインベントリのアプリケーションと ソフトウェア ページインベントリのアプリケーションのいずれかと関連付けることができます。ライセンス資産は、同時に両方のインベントリタイプに関連付けることはできません。

ソフトウェアカタログインベントリと ソフトウェア ページインベントリとでは、ライセンスを追跡するためのオプションおよびライセンスコンプライアンスを設定するための要件が異なります。

ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンスについて

アプライアンスでは、ソフトウェアカタログインベントリのアプリケーションに関するライセンスコンプライアンス情報を表示できます。この情報は、ライセンスコンプライアンス ページおよびライセンスコンプライアンス ダッシュボードウィジェットに表示されます。

ソフトウェアカタログインベントリのアプリケーションに対してライセンス資産を設定すると、エージェント管理対象デバイスにインストールされているシートの数、使用可能なシートの数、および適用されるライセンスのタイプを表示できるほか、メータリングがアプリケーションに対して有効である場合には使用率情報も表示できます。また、アプライアンスはソフトウェアカタログの情報を利用して、アップグレード済みまたはダウングレード済みに分類されるアプリケーションバージョンに正しいライセンスを自動的に適用します。

ソフトウェアカタログインベントリのアプリケーションに対してライセンスコンプライアンスを設定するには、次の手順を実行します。

- （オプション）情報管理要件に合わせてライセンス資産タイプをカスタマイズします。詳細については、「ライセンス資産タイプのカスタマイズ」を参照してください。
- （オプション）ソフトウェアカタログのアプリケーションに対してメータリングを有効にします。メータリングが有効になっているときは、過去 30、60、90 日にアプリケーションが使用されていたかどうかがライセンスコンプライアンス ページに表示されます。詳細については、「ソフトウェアメータリングについて」を参照してください。
- ライセンス資産を作成し、ソフトウェアカタログインベントリのアプリケーションに関連付けます。詳細については、「ソフトウェアカタログ インベントリのライセンス資産の追加」を参照してください。
- （オプション）ダッシュボードウィジェットで使用されるライセンスコンプライアンスのしきい値レベルを設定します。デフォルトの Warning Threshold（警告しきい値）は 90 です。デフォルトの Critical Threshold（緊急しきい値）は 100 です。詳細については、「ライセンス使用率警告しきい値の設定」を参照してください。

ライセンスのアップグレードについて

アプリケーション保守計画では、多くの場合、新しいバージョンのアプリケーションが利用可能になったときに、ユーザーがそのバージョンにアップグレードできるようにします。アップグレード対象と見なされるインストールの数が ライセンスコンプライアンス ページに表示されます。

アップグレードを追跡するために、アプライアンスはソフトウェアカタログの情報およびライセンス詳細を利用して、新しいバージョンのアプリケーションを既存のライセンスに関連付けるかどうかを判断します。例えば、アプリケーションのバージョン 1.0 用にライセンス資産を作成し、保守計画でユーザーにアップグレードの権利を与えている場合、バージョン 2.0 のアプリケーションをリリースすると、自動的にそのバージョンがライセンス資産の対象範囲になります。この例では、ライセンス資産を次のように設定する必要があります。

- Includes Maintenance（メンテナンスを含む）フィールドを はい に設定する必要があります。
- Maintenance Expiration Date（メンテナンス有効期限）は、ソフトウェアカタログのバージョン 2.0 GA（一般向け）の日付より後である必要があります。
- ライセンスモード は、Enterprise（エンタープライズ）または Unit License（ユニットライセンス）である必要があります。
- アップグレード権を含む は、はい または はい - リストから選択 に設定されている必要があります。

これらの設定の詳細については、ソフトウェアカタログ インベントリのライセンス資産の追加を参照してください。

ライセンスのダウングレードについて

ベンダーは多くの場合、ユーザーが新しいバージョンのアプリケーションのライセンスを古いバージョンに適用できるようにしています。このようなタイプのインストールをダウングレードといいます。ライセンスコンプライアンス ページには、ダウングレードと見なされるインストールの数が表示されます。

ライセンスシートはまず、最新バージョンのアプリケーションのインストールに割り当てられます。追加のシートが利用可能である場合やベンダーがダウングレードを許可している場合は、ダウングレードと見なされるインストールにシートが自動的に割り当てられます。

アップグレードのライセンスの方が常にダウングレードのライセンスよりも先に割り当てられます。

ライセンス資産タイプのカスタマイズ

ライセンス資産タイプの使用可能なフィールドは、必要に応じて追加、変更、または削除することができます。ライセンス資産タイプは、ライセンス資産を追加する際に使用可能なフィールドを設定するテンプレートです。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のライセンス資産タイプを個別にカスタマイズします。

1. 資産タイプ リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産タイプ** をクリックします。
2. 名前 列で、**ライセンス** をクリックして、資産タイプの詳細 ページを表示します。
3. デフォルトの資産ステータス フィールドに、デフォルトの資産ステータス、またはカスタムの資産ステータスを入力します（ 存在する場合 ）。

    アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。

    - **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。
    - **廃棄済み**：利用できなくなった資産。
    - **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。
    - **在庫**：最近受け取った資産。
    - **不在**：場所を特定できない資産。
    - **修復**：修復されている資産。
    - **予約済み**：特定の人または用途のために確保されている資産。
    - **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。
    - **盗難**：盗難されたとして報告された資産。
4. 名前 フィールドに、資産タイプの名前を入力します。

    この資産タイプのデフォルトは「ライセンス」です。
5. **オプション**：ライセンスコンプライアンスのレポート作成用 セクションで、ライセンスコンプライアンスに使用するフィールドを選択します。

    選択した ライセンスモード フィールドの情報は、ダッシュボードの ライセンスコンプライアンス ウィジェットに表示されます。
6. 次のいずれかを実行します。

    - ライセンスモードフィールド **ドロップダウンリストで、デフォルトの フィールドの選択 のままにします。これにより、**ライセンスモードフィールド **のすべての値が、ライセンスコンプライアンスに使用されます。**資産フィールド **リストに複数の「単一選択」フィールドまたは「複数選択」フィールドがある場合、リストに表示される最初のフィールドと、そのすべての値が、ライセンスコンプライアンス ウィジェットで使用されます。**
    - License Mode Field **（ ライセンスモードフィールド ）ドロップダウンリストで、ライセンスコンプライアンスに使用するフィールド（ ライセンスモード など ）を選択します。デフォルトでは、このドロップダウンリストに含まれているフィールドは1つだけですが、必要に応じて追加できます。次の図に示す ライセンスモード などのフィールドを選択した場合、選択したフィールドのみがライセンスコンプライアンスに使用されます。**

また、フィールドを選択した場合は、「ライセンスコンプライアンス」グラフで無視する値（ある場合）を選択することができます。無視される値は、100%の使用率で灰色表示されます。
デフォルトでは、「ライセンスモード」は、唯一の使用可能な「単一選択」または「複数選択」フィールドです。そのため、このフィールドしか表示されません。Asset Fields（資産フィールド）テーブルに「単一選択」または「複数選択」フィールドを追加した場合、これらのフィールドは、このリストにも表示され、ライセンス資産に追加した場合は、Asset Detail（資産詳細）ページに表示されます。ただし、ライセンスコンプライアンス ウィジェットでは、選択したフィールドのみ、または Asset Fields（資産フィールド）リストの最初のフィールドのみが使用されます。

7. **オプション**：資産フィールド テーブルの ライセンスモード フィールドまたは値を変更します。
   a. 行の末尾にある **編集** ボタンをクリックします。
   b. 必要に応じて、フィールド情報を変更し、行の最後で **保存** をクリックします。
   c. フィールドを追加するには、表見出しで **追加** ボタンをクリックします。フィールド情報を追加し、行の最後で **保存** をクリックします。
   d. フィールドの順番を変更するには、**並べ替え** ボタンをドラッグします：。
   e. フィールドを削除するには、**削除** ボタンをクリックします。
8. ページの一番下で **保存** をクリックします。

関連トピック

ライセンスコンプライアンスと設定情報の表示.

ソフトウェアカタログ インベントリのライセンス資産の追加

アプリケーションのライセンス資産をソフトウェアカタログインベントリに追加できます。ライセンス資産を追加すると、ライセンスコンプライアンス リストおよびライセンスコンプライアンス ダッシュボード ウィジェットにライセンスコンプライアンス情報を表示できます。

ソフトウェアカタログのアプリケーションは、検出済み、未検出、Locally Cataloged（ローカルカタログ登録済み）のいずれかに分類する必要があります。カタログ未登録 に分類されたアプリケーションのライセンス資産を追加することはできません。

ライセンス資産をアプリケーションに関連付けると、Software Catalog Detail（ソフトウェアカタログの詳細）ページにライセンス情報を表示することもできます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のライセンス情報を個別に管理します。

ヒント: 複数のアプリケーションのライセンス資産を一度に追加するには、その情報をスプレッドシートまたは CSV ファイルからインポートできます。詳細については、「例：作成済みスプレッドシートからのライセンスデータのインポート」を参照してください。

1. ソフトウェアカタログ リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。

2. アプリケーションの名前をクリックして、ソフトウェアカタログの詳細 ページを表示します。
3. ページの一番下付近で **新しいライセンスの追加** をクリックして、ライセンス資産詳細 ページを表示します。
4. ライセンス資産の詳細 ページの 全般 タブで次の情報を入力します。

オプション	説明
サブタイプ	ライセンスに関連付ける資産サブタイプ。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。
資産ステータス	ライセンスステータス (該当する場合) 。デフォルトの資産ステータス、またはカスタムの資産ステータスを選択できます (存在する場合) 。アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。 • **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。 • **廃棄済み**：利用できなくなった資産。 • **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。 • **在庫**：最近受け取った資産。 • **不在**：場所を特定できない資産。 • **修復**：修復されている資産。 • **予約済み**：特定の人または用途のために確保されている資産。 • **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。 • **盗難**：盗難されたとして報告された資産。 詳細については、「資産のライフサイクル設定の表示と設定」を参照してください。
場所	資産がある場所の名前。詳細については、「場所の管理」を参照してください。
名前	ライセンス名 (「**Office Professional PO #1234**」など) 。これは資産を検索するために使用される名前です。1 つのアプリケーションに複数のライセンスを関連付ける場合は、それらのライセンスを区別するために、以下のフィールドに注文書番号または購入日を指定します。
ライセンス数	ライセンスによって許諾されるインストール数またはシート数。例えば、「50」と表示されます。
カタログ登録済みソフトウェアへの適用	ライセンスを適用する、ソフトウェアカタログインベントリ内のアプリケーション。必要に応じて、ソ

オプション	説明
	フトウェアカタログの複数のアプリケーションにライセンス資産を関連付けることができます。ただし、ライセンス資産を同じアプリケーションの複数のバージョンに関連付ける必要はありません。アップグレードおよびダウングレードをサポートするためにアプライアンスがこれを自動的に行うからです。ライセンス情報を追加するときに、現在のバージョンをライセンス資産に関連付けるだけです。 また、Microsoft Office や Adobe Acrobat などの別の発行元からアプリケーションを同じライセンス資産に割り当てた場合は、ライセンス資産に指定されているシートの総数が各アプリケーションに割り当てられます。例えば、ライセンス資産に 100 個のシートがある場合、Microsoft Office と Adobe Acrobat の両方に 100 個のシートが割り当てられます。
ソフトウェアへの適用	このフィールドは空白のままにします。ソフトウェアカタログ インベントリと ソフトウェア ページインベントリのアプリケーションに対して、同時に1つのソフトウェアライセンスを関連付けることはできません。カタログ登録済みソフトウェアに対してライセンス資産を作成する方法の詳細については、ソフトウェア ページインベントリのライセンス資産の追加を参照してください。
ライセンスモード	ライセンス資産のモード。ライセンスを必要とし、ライセンスコンプライアンス ページにライセンス使用率情報を表示するアプリケーションの場合、Enterprise（エンタープライズ）または Unit License（ユニットライセンス）のいずれかを選択します。 **注:** ライセンスコンプライアンスでは、Not Specified（指定なし）、Client License（クライアントライセンス）、サブスクリプション、Shareware（シェアウェア）、Freeware（フリーウェア）、OpenSource（オープンソース）、No Licensing（ライセンスなし）、Site License（サイトライセンス）などほとんどのモードが使用されません。 ライセンスモードは、**管理者コンソール**の次のセクションで使用されます。 • ライセンスコンプライアンス リスト。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンス情報の表示」を参照してください。 • Dashboard（ダッシュボード）に表示されるライセンスコンプライアンス グラフ。Asset Detail（資産詳細）ページで無視にマーク付けされた値は、100% の使用レベルで表示されます。詳細については、「ダッシュボード

オプション	説明
	のウィジェットについて」を参照してください。

5. 次へ をクリックします。
6. ライセンス資産の詳細 ページの 購入 タブで次の情報を入力します。

オプション	説明
契約	ライセンスに関連付けられている契約資産。
カタログ登録済みソフトウェアへの適用	ライセンスを適用する、ソフトウェアカタログインベントリ内のアプリケーション。必要に応じて、ソフトウェアカタログの複数のアプリケーションにライセンス資産を関連付けることができます。ただし、ライセンス資産を同じアプリケーションの複数のバージョンに関連付ける必要はありません。アップグレードおよびダウングレードをサポートするためにアプライアンスがこれを自動的に行うからです。ライセンス情報を追加するときに、現在のバージョンをライセンス資産に関連付けるだけです。 また、Microsoft Office や Adobe Acrobat などの別の発行元からアプリケーションを同じライセンス資産に割り当てた場合は、ライセンス資産に指定されているシートの総数が各アプリケーションに割り当てられます。例えば、ライセンス資産に 100 個のシートがある場合、Microsoft Office と Adobe Acrobat の両方に 100 個のシートが割り当てられます。
プロダクトキー	ライセンスに関連付けられているプロダクトキー。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
単価	ライセンスに関連付けられている単価。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
ベンダー	アプリケーションに関連付けるベンダー資産の名前。ベンダー資産を追加していない場合は、Vendor（ベンダー）ドロップダウンリストに何も表示されません。ベンダーを検索するには、リストに入力を開始します。 **注:** ライセンスコンプライアンス情報が不正確になることがあるため、単一のソフトウェアライセンス資産に複数のベンダーを割り当てることはお勧めしません。
注文書番号	ライセンスに関連付けられた注文書番号。
購入日	購入した日付。フィールド内をクリックし、カレンダーで日付を選択します。

オプション	説明
購入	このライセンスに関連付けられている購入レコードを 1 つ以上選択します。詳細については、「購入レコードの管理」を参照してください。

7. **次へ** をクリックします。
8. ライセンス資産の詳細 ページの メンテナンス タブで次の情報を入力します。

オプション	説明
アップグレード権を含む	ライセンスにアップグレート権が含まれるかどうかを示します。アップグレード権とは、ライセンス済みソフトウェアの新しいバージョンが利用可能になったときに、その新しいバージョンにアップグレートできる資格があることを意味します。詳細については、「ライセンスのアップグレードについて」を参照してください。次のいずれかのオプションを選択します。 • **はい**: アップグレード権は、選択したソフトウェアの既存のライセンス数と、それと同一のソフトウェアで利用可能な、より新しいバージョンのライセンス数を比較することによって計算されます。 • **はい - リストから選択**: アップグレード権を付与するソフトウェアバージョンを1つまたは複数選択します。アップグレードソフトウェアリスト の下で、**追加するカタログ登録済みソフトウェアの選択** をクリックします。選択したソフトウェアにおいて、ライセンスをアップグレードすることが可能なより新しいバージョンのリストが表示されます。リスト内のエントリを選択すると、選択した内容が アップグレードソフトウェアリスト ボックスに表示されます。必要に応じて、1つまたは複数のバージョンを追加できます。リストからアイテムを削除するには、アップグレードソフトウェアリスト ボックスでそのアイテムを選択して、**削除** をクリックします。 • **いいえ**: 選択したソフトウェアにアップグレード権を付与しない場合は、このオプションを選択します。
Includes Maintenance (メンテナンスを含む)	ライセンスがユーザーにアプリケーションのインストールバージョンをアップグレードする権利を与えているかどうか。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンスについて」を参照してください。
有効期限日	ライセンスにメンテナンスが含まれている場合は、メンテナンス期間の有効期限。 アプライアンスライセンスコンプライアンス機能は、アプリケーションリリース日などソフトウェアカタログ情報を利用します。メンテナンス期間中に新規アプリケーションバージョンをリリースした場

オプション	説明
	合、そのバージョンは自動的にこのライセンス資産の対象範囲になります。
ダウングレード権を含む	ライセンスにダウングレード権が含まれるかどうかを示します。ダウングレード権とは、ソフトウェアの新しいバージョンを同じソフトウェアの古いバージョンにダウングレードするライセンスを適用する資格があることを意味します。詳細については、「ライセンスのダウングレードについて」を参照してください。次のいずれかのオプションを選択します。 • **はい**: ダウングレード権は、選択したソフトウェアの既存のライセンス数と、それと同一のソフトウェアで利用可能な、より古いバージョンのライセンス数を比較することによって計算されます。 • **はい - リストから選択**: ダウングレード権を付与するソフトウェアバージョンを1つまたは複数選択します。ダウングレードソフトウェアリスト の下で、**追加するカタログ登録済みソフトウェアの選択** をクリックします。ライセンスをダウングレードすることが可能な、選択したソフトウェアのより古いバージョンのリストが表示されます。リスト内のエントリを選択すると、選択した内容が ダウングレードソフトウェアリスト ボックスに表示されます。必要に応じて、1つまたは複数のバージョンを追加できます。リストからアイテムを削除するには、ダウングレードソフトウェアリスト ボックスでそのアイテムを選択して、**削除** をクリックします。 • **いいえ**: 選択したソフトウェアにダウングレード権を付与しない場合は、このオプションを選択します。

9. **次へ** をクリックします。
10. ライセンス資産の詳細 ページの 関連 タブで次の情報を入力します。

オプション	説明
部門	アプリケーションを所有するビジネスグループまたは部門。
コストセンター	アプリケーションを所有する部門に関連付けられたコストセンター。
承認されたデバイス	ライセンスの使用を承認されたデバイス。この情報は、ライセンスコンプライアンスレポートの作成に使用されます。例えば、対象のアプリケーションをインストールしたデバイスが、承認されたデバイスのリストに存在しない場合、それらのデバイスは「未承認のソフトウェアインストール」というタイトルのレポートで報告されます。ただし、アプライアンスは、ライセンスコンプライアンスを強制しません。例えば、ライセンスが期限切れであったり、

オプション	説明
	コンプライアンスから外れていたとしても、管理対象デバイスへのアプリケーションのインストールがアプライアンスによって阻止されることはありません。
バーコード	必要に応じて、このライセンスに関連付けられたバーコードを追加または編集します。詳細については、「資産へのバーコードの追加」を参照してください。

11. **次へ** をクリックします。
12. ライセンス資産の詳細 ページの カスタム タブで、追加のカスタムデータを入力します。ビジネス目標に合わせて、ライセンス資産タイプを修正し、必要な数のフィールドを追加することができます。詳細については、「資産タイプの追加またはカスタマイズ」を参照してください。
13. **次へ** をクリックします。
14. ライセンス資産の詳細 ページの メモ タブで、次の情報を入力します。

オプション	説明
メモ	任意の追加情報を入力します。
ライセンステキスト	ライセンスナンバーなどライセンスに関する補足情報。

15. **保存** をクリックします。

    ライセンス ページに新しいライセンス資産が表示されます。ライセンス数 の数値は、資産を更新するまでは変更されません。ただし、対象のソフトウェアをインストールされた管理対象デバイスがアプライアンスにチェックインすると、インストール済み 列の数値が変更されます。これにより、購入およびインストール済みのライセンス数を追跡できます。

次のオプションのタスクを実行します。

- ソフトウェアカタログインベントリに対するメータリングを有効化します。メータリングが有効になっているときは、過去 90 日にアプリケーションが使用されていたかどうかが ライセンスコンプライアンス ページに表示されます。詳細については、「ソフトウェアメータリングについて」を参照してください。
- ライセンス使用率警告しきい値を設定します。これらのしきい値は、ライセンスコンプライアンス ダッシュボード ウィジェットでライセンスコンプライアンスの問題を識別するために使用されます。

ソフトウェア ページインベントリのライセンス資産の追加

ライセンス資産を作成して、ライセンスを必要とするアプリケーションの情報を追跡できます。

ライセンス資産を作成する前に、ライセンス資産で管理する必要のある情報 (ライセンスで許諾されたインストール数またはシート数、プロダクトキー、発注番号など) を準備します。

注: ソフトウェア ページインベントリに表示されているアプリケーションのライセンス資産を作成するには、まず、そのアプリケーションのソフトウェア資産を作成する必要があります。ソフトウェアカタログ ページインベントリのアプリケーションについてはソフトウェア資産を作成する必要がありません。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のライセンス資産を個別に作成できます。

ヒント: ライセンス資産タイプはニーズに合わせてカスタマイズできます。詳細については、「ライセンス資産タイプのカスタマイズ」を参照してください。

1. ライセンス資産詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 次のいずれかを実行します。
   - 左のナビゲーションバーで **ライセンス** をクリックします。**アクションの選択 > 新規作成** を選択します。
   - 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。アプリケーションの名前をクリックします。ソフトウェアカタログの詳細 ページで **新しいライセンスの追加** をクリックします。
2. ライセンス資産の詳細 ページの 全般 タブで次の情報を入力します。

オプション	説明
サブタイプ	ライセンスに関連付ける資産サブタイプ。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。
資産ステータス	ライセンスステータス（該当する場合）。デフォルトの資産ステータス、またはカスタムの資産ステータスを選択できます（存在する場合）。アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。 • **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。 • **廃棄済み**：利用できなくなった資産。 • **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。 • **在庫**：最近受け取った資産。 • **不在**：場所を特定できない資産。 • **修復**：修復されている資産。 • **予約済み**：特定の人または用途のために確保されている資産。 • **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。 • **盗難**：盗難されたとして報告された資産。 詳細については、「資産のライフサイクル設定の表示と設定」を参照してください。
場所	資産がある場所の名前。詳細については、「場所の管理」を参照してください。
名前	ライセンス名（「**Office Professional PO #1234**」など）。これは資産を検索するために使用される名前です。1 つのアプリケーションに複数のライセンスを関連付ける場合は、それらのライセンスを区別

オプション	説明
	するために、以下のフィールドに注文書番号または購入日を指定します。
ライセンス数	ライセンスによって許諾されるインストール数またはシート数。例えば、「50」と表示されます。
カタログ登録済みソフトウェアへの適用	ライセンスを適用する、ソフトウェアカタログインベントリ内のアプリケーション。必要に応じて、ソフトウェアカタログの複数のアプリケーションにライセンス資産を関連付けることができます。ただし、ライセンス資産を同じアプリケーションの複数のバージョンに関連付ける必要はありません。アップグレードおよびダウングレードをサポートするためにアプライアンスがこれを自動的に行うからです。ライセンス情報を追加するときに、現在のバージョンをライセンス資産に関連付けるだけです。 また、Microsoft Office や Adobe Acrobat などの別の発行元からアプリケーションを同じライセンス資産に割り当てた場合は、ライセンス資産に指定されているシートの総数が各アプリケーションに割り当てられます。例えば、ライセンス資産に 100 個のシートがある場合、Microsoft Office と Adobe Acrobat の両方に 100 個のシートが割り当てられます。
ソフトウェアへの適用	このフィールドは空白のままにします。ソフトウェアカタログ インベントリと ソフトウェア ページインベントリのアプリケーションに対して、同時に1つのソフトウェアライセンスを関連付けることはできません。カタログ登録済みソフトウェアに対してライセンス資産を作成する方法の詳細については、ソフトウェア ページインベントリのライセンス資産の追加を参照してください。
ライセンスモード	ライセンス資産のモード。ライセンスを必要とし、ライセンスコンプライアンス ページにライセンス使用率情報を表示するアプリケーションの場合、Enterprise（エンタープライズ）または Unit License（ユニットライセンス）のいずれかを選択します。 **注:** ライセンスコンプライアンスでは、Not Specified（指定なし）、Client License（クライアントライセンス）、サブスクリプション、Shareware（シェアウェア）、Freeware（フリーウェア）、OpenSource（オープンソース）、No Licensing（ライセンスなし）、Site License（サイトライセンス）などほとんどのモードが使用されません。 ライセンスモードは、**管理者コンソール**の次のセクションで使用されます。 • ライセンスコンプライアンス リスト。詳細については、「ソフトウェアカタログのアプリ

オプション	説明
	ケーションに関するライセンスコンプライアンス情報の表示」を参照してください。 • Dashboard（ダッシュボード）に表示されるライセンスコンプライアンス グラフ。Asset Detail（資産詳細）ページで無視にマーク付けされた値は、100% の使用レベルで表示されます。詳細については、「ダッシュボードのウィジェットについて」を参照してください。

3. **次へ** をクリックします。
4. ライセンス資産の詳細 ページの 購入 タブで次の情報を入力します。

オプション	説明
契約	ライセンスに関連付けられている契約資産。
カタログ登録済みソフトウェアへの適用	ライセンスを適用する、ソフトウェアカタログインベントリ内のアプリケーション。必要に応じて、ソフトウェアカタログの複数のアプリケーションにライセンス資産を関連付けることができます。ただし、ライセンス資産を同じアプリケーションの複数のバージョンに関連付ける必要はありません。アップグレードおよびダウングレードをサポートするためにアプライアンスがこれを自動的に行うからです。ライセンス情報を追加するときに、現在のバージョンをライセンス資産に関連付けるだけです。 また、Microsoft Office や Adobe Acrobat などの別の発行元からアプリケーションを同じライセンス資産に割り当てた場合は、ライセンス資産に指定されているシートの総数が各アプリケーションに割り当てられます。例えば、ライセンス資産に 100 個のシートがある場合、Microsoft Office と Adobe Acrobat の両方に 100 個のシートが割り当てられます。
プロダクトキー	ライセンスに関連付けられているプロダクトキー。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
単価	ライセンスに関連付けられている単価。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
ベンダー	アプリケーションに関連付けるベンダー資産の名前。ベンダー資産を追加していない場合は、Vendor（ベンダー）ドロップダウンリストに何も表示されません。ベンダーを検索するには、リストに入力を開始します。 **注:** ライセンスコンプライアンス情報が不正確になることがあるため、単一のソフトウェアライセンス資産に複数のベンダーを割り当てることはお勧めしません。
注文書番号	ライセンスに関連付けられた注文書番号。

オプション	説明
購入日	購入した日付。フィールド内をクリックし、カレンダーで日付を選択します。
購入	このライセンスに関連付けられている購入レコードを 1 つ以上選択します。詳細については、「購入レコードの管理」を参照してください。

5. **次へ** をクリックします。
6. ライセンス資産の詳細 ページの メンテナンス タブで次の情報を入力します。

オプション	説明
アップグレード権を含む	ライセンスにアップグレード権が含まれるかどうかを示します。アップグレード権とは、ライセンス済みソフトウェアの新しいバージョンが利用可能になったときに、その新しいバージョンにアップグレードできる資格があることを意味します。詳細については、「ライセンスのアップグレードについて」を参照してください。次のいずれかのオプションを選択します。 • **はい**: アップグレード権は、選択したソフトウェアの既存のライセンス数と、それと同一のソフトウェアで利用可能な、より新しいバージョンのライセンス数を比較することによって計算されます。 • **はい - リストから選択**: アップグレード権を付与するソフトウェアバージョンを1つまたは複数選択します。アップグレードソフトウェアリスト の下で、**追加するカタログ登録済みソフトウェアの選択** をクリックします。選択したソフトウェアにおいて、ライセンスをアップグレードすることが可能なより新しいバージョンのリストが表示されます。リスト内のエントリを選択すると、選択した内容が アップグレードソフトウェアリスト ボックスに表示されます。必要に応じて、1つまたは複数のバージョンを追加できます。リストからアイテムを削除するには、アップグレードソフトウェアリスト ボックスでそのアイテムを選択して、**削除** をクリックします。 • **いいえ**: 選択したソフトウェアにアップグレード権を付与しない場合は、このオプションを選択します。
Includes Maintenance (メンテナンスを含む)	ライセンスがユーザーにアプリケーションのインストールバージョンをアップグレードする権利を与えているかどうか。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンスについて」を参照してください。
有効期限日	ライセンスにメンテナンスが含まれている場合は、メンテナンス期間の有効期限。 アプライアンスライセンスコンプライアンス機能は、アプリケーションリリース日などソフトウェア

オプション	説明
	カタログ情報を利用します。メンテナンス期間中に新規アプリケーションバージョンをリリースした場合、そのバージョンは自動的にこのライセンス資産の対象範囲になります。
ダウングレード権を含む	ライセンスにダウングレード権が含まれるかどうかを示します。ダウングレード権とは、ソフトウェアの新しいバージョンを同じソフトウェアの古いバージョンにダウングレードするライセンスを適用する資格があることを意味します。詳細については、「ライセンスのダウングレードについて」を参照してください。次のいずれかのオプションを選択します。 • **はい**: ダウングレード権は、選択したソフトウェアの既存のライセンス数と、それと同一のソフトウェアで利用可能な、より古いバージョンのライセンス数を比較することによって計算されます。 • **はい - リストから選択**: ダウングレード権を付与するソフトウェアバージョンを1つまたは複数選択します。ダウングレードソフトウェアリスト の下で、**追加するカタログ登録済みソフトウェアの選択** をクリックします。ライセンスをダウングレードすることが可能な、選択したソフトウェアのより古いバージョンのリストが表示されます。リスト内のエントリを選択すると、選択した内容が ダウングレードソフトウェアリスト ボックスに表示されます。必要に応じて、1つまたは複数のバージョンを追加できます。リストからアイテムを削除するには、ダウングレードソフトウェアリスト ボックスでそのアイテムを選択して、**削除** をクリックします。 • **いいえ**: 選択したソフトウェアにダウングレード権を付与しない場合は、このオプションを選択します。

7. **次へ** をクリックします。
8. ライセンス資産の詳細 ページの 関連 タブで次の情報を入力します。

オプション	説明
部門	アプリケーションを所有するビジネスグループまたは部門。
コストセンター	アプリケーションを所有する部門に関連付けられたコストセンター。
承認されたデバイス	ライセンスの使用を承認されたデバイス。この情報は、ライセンスコンプライアンスレポートの作成に使用されます。例えば、対象のアプリケーションをインストールしたデバイスが、承認されたデバイスのリストに存在しない場合、それらのデバイスは「未承認のソフトウェアインストール」というタイトルのレポートで報告されます。ただし、アプライ

オプション	説明
	アンスは、ライセンスコンプライアンスを強制しません。例えば、ライセンスが期限切れであったり、コンプライアンスから外れていたとしても、管理対象デバイスへのアプリケーションのインストールがアプライアンスによって阻止されることはありません。
バーコード	必要に応じて、このライセンスに関連付けられたバーコードを追加または編集します。詳細については、「資産へのバーコードの追加」を参照してください。

9. **次へ** をクリックします。
10. ライセンス資産の詳細 ページの カスタム タブで、追加のカスタムデータを入力します。ビジネス目標に合わせて、ライセンス資産タイプを修正し、必要な数のフィールドを追加することができます。詳細については、「資産タイプの追加またはカスタマイズ」を参照してください。
11. **次へ** をクリックします。
12. ライセンス資産の詳細 ページの メモ タブで、次の情報を入力します。

オプション	説明
メモ	任意の追加情報を入力します。
ライセンステキスト	ライセンスナンバーなどライセンスに関する補足情報。

13. **保存** をクリックします。

ライセンス ページに新しいライセンス資産が表示されます。ライセンス数 の数値は、資産を更新するまでは変更されません。ただし、対象のソフトウェアをインストールされた管理対象デバイスがアプライアンスにチェックインすると、インストール済み 列の数値が変更されます。これにより、購入およびインストール済みのライセンス数を追跡できます。

関連トピック

ライセンス資産タイプのカスタマイズ

ライセンスコンプライアンスと設定情報の表示

レポートについて

CSV ファイルでのライセンスデータのインポート

ライセンスデータがスプレッドシートに入力されている場合は、それを CSV (コンマ区切り値) 形式にエクスポートすると、アプライアンスにインポートできます。または、テキストエディタを使用して、該当するデータを含む CSV ファイルを作成すれば、そのファイルをインポートできます。

定義した資産タイプについて、CSV ファイルに新しい資産が含まれる場合、新しい資産が追加されます。

インポート中の資産情報の処理方法

資産情報がインポートされると、アプライアンスでは、新しい情報と既存の情報が比較され、新しい情報の処理方法が決定されます。

情報が新規であるか、既存であるか、または複製されているかに応じて、アプライアンスでは、次のアクションが実行されます。

- **資産の作成**: プライマリキーの値と既存の値が一致しない場合は、資産が作成されます。
- **資産の更新**: プライマリキーの値と既存の値が一致する場合は、資産情報が更新されます。
- **重複資産としてのフラグ付け**: 資産タイプの複数のレコードが、プライマリキーとして選択された CSV フィールドの値と一致する場合、または複数のレコードが関連資産と一致する場合は、重複資産としてフラグ付けされます。重複レコードはインポートされません。

CSVファイルを使用した資産データのインポート

CSV (コンマ区切り形式) ファイルを使用して、ソフトウェアライセンスデータなどの資産データをインポートできます。

インポート前の資産データの準備

インポート前に資産データが適切であり、適切に書式設定されていることを確認します。

1. 資産の基本的なフィールドを定義します。製品名を使用する場合は、その名前が有用で、資産の識別に役立つことを確認してください。詳細については、「ソフトウェア資産の追加」を参照してください。
2. データにヘッダー行を追加します。資産管理コンポーネントでは、ヘッダーのない列が列番号で参照されるため、列ヘッダー行を使用することで、データをより簡単に識別できます。
3. すべての列が資産タイプの同等の Asset Fields (資産フィールド) にマップされることを検証します。

   資産タイプには 資産名、Purchase Order Number (注文書番号)、Vendor (ベンダー) などのデフォルトフィールドが含まれていますが、必要に応じてカスタム資産フィールドを追加できます。詳細については、「資産フィールドの追加および削除について」を参照してください。

   ヒント: デフォルトフィールドを表示するには、Asset Detail (資産の詳細) ページに移動します。詳細については、「資産タイプのカスタマイズ」を参照してください。
4. インポート対象の資産のプライマリキー (PK) に使用するフィールドを決定します。

   プライマリキーは、インポートする資産の一意の識別子として使用される、フィールドまたはフィールドの組み合わせです。資産がインポートされる際に、アプライアンスはプライマリキーを使用して、既存のレコードを更新するか、新しいレコードを作成するかを判断します。PKとして、1つのフィールドまたはフィールドの組み合わせを選択できます。
5. 管理者コンソールからアクセスできる場所にスプレッドシートを CSV ファイルとして保存します。

例：作成済みスプレッドシートからのライセンスデータのインポート

作成済みCSVファイルからライセンスデータをインポートできます。

この例では、ソフトウェアカタログインベントリ用のライセンス資産を 1 回しかインポートしないものとしてインポートする方法、またはネットワーク共有からファイルを使用してスケジュール済みインポートを行う方法について説明します。例では、ライセンス資産のインポートに必要なフィールドのみを示します。情報管理ニーズに合わせて単価、発行元、プロダクトキーなどのファイルを新たに追加できます。

インポートした資産を資産サブタイプに割り当てる場合は、そのサブタイプを追加してから資産をインポートします。詳細については、「資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択」を参照してください。

1. Excel などのスプレッドシートプログラムでファイルを作成します。
2. 次の列および行を追加します。先頭行はヘッダー列です。

資産名	ライセンス数	ライセンスモード	Includes Maintenance (メンテナンスを含む)	Applies to Software Catalog (ソフト

				ウェアカタログへの適用）
ソフトウェアタイトル 1	100	Enterprise	はい	ソフトウェアタイトル 1
ソフトウェアタイトル 2	150	Enterprise	はい	ソフトウェアタイトル 2
ソフトウェアタイトル 3	200	Enterprise	はい	ソフトウェアタイトル 3
ソフトウェアタイトル 4	500	Enterprise	はい	ソフトウェアタイトル 4

3. CSV 形式でファイルを保存します。

   各列の値は、コンマで区切ります。例：ソフトウェアタイトル 1,100,Enterprise,はい,ソフトウェアタイトル 1

4. 資産のインポート セクションで ファイルのアップロード ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産のインポート** をクリックします。

   - 1 つ以上の資産のインポート操作がスケジュールされている場合、インポート資産の一覧ページが表示され、インポート操作が一覧表示されます。CSV ファイルから資産をインポートするには、**アクションの選択 > 新規** をクリックして、資産のインポート ウィザードを開始します。
   - アプライアンスにスケジュール済みの資産インポートがない場合、資産のインポート ウィザードが表示されます。

5. 資産のインポート ウィザードで、次のいずれかのオプションを選択します。

オプション	説明
資産インポート CSV ファイルをアップロードする	CSV ファイルから 1 回限りの資産のインポートを完了するには、このオプションを選択します。次に、**参照** または **ファイルの選択** をクリックして、CSVファイルを選択します。
資産インポートをスケジュールする	このオプションを選択して、ネットワークドライブ上にある CSV ファイルから、選択した時間間隔で複数の資産をインポートします。次に、以下の情報を入力します。 • **資産インポートのファイル転送プロトコルを選択**： ◦ **Samba**：このオプションを選択して、Samba プロトコルを使用してファ

オプション	説明
	イルにアクセスし、次の情報を入力します。 ▪ **SAMBA 共有の UNC パスを入力**：CSV ファイルのディレクトリパスを入力します。 ◦ **FTP**：このオプションを選択して FTP サーバー上のファイルにアクセスし、次の情報を入力します。 ▪ **FTP サーバーホスト名または IP アドレスを入力**：FTP サーバーのホスト名または IP アドレスを入力します。 ▪ **FTP サブディレクトリが存在する場合は入力**：FTP サーバー上の CSV ファイルへのディレクトリパスを入力します。 ◦ **Secure FTP**：このオプションを選択して、セキュア FTP サーバー上のファイルにアクセスし、次の情報を入力します。 ▪ **セキュア FTP サーバーのホスト名または IP アドレスを入力**：セキュア FTP サーバーのホスト名または IP アドレスを入力します。 ▪ **SFTP のフルパスを入力**：セキュア FTP サーバー上の CSV ファイルへのディレクトリパスを入力します。 • **資産インポートの CSV ファイル名**：インポートする CSV ファイルの名前を入力します。 • **認証情報**：指定されたネットワークリソースにアクセスする際に使用する資格情報を選択します。アプライアンスで定義されている資格情報が一覧に表示されます。詳細については、「資格情報の管理」を参照してください。

6. CSV ファイルにヘッダー行が含まれている場合は、この例に示すように、File Header Row（ファイルヘッダー行）チェックボックスをオンにし、**次へ** をクリックします。
7. **スケジュール済み資産のインポートのみ**。資産インポートの選択スケジュール ページが表示されますので、CSV ファイルをインポートするスケジュールを作成します。
   a. 資産のインポートスケジュール名 フィールドに、このスケジュールに割り当てる名前を入力します。
   b. **資産スケジュールを有効にする** を選択します。
   c. スケジュール セクションで、必要に応じてインポートスケジュールを指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。

オプション	説明
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。

オプション	説明
	例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。

8. 資産タイプの選択 ページが表示されるので、次の手順を実行します。
   a. 資産タイプ ドロップダウンリストで、**ライセンス** を選択します。
   b. Asset Subtype（資産サブタイプ）ドロップダウンリストで、**生産性** を選択します。

   注: この例では、資産サブタイプ（生産性）がライセンス資産タイプに追加されています。ライセンス資産タイプのサブタイプをまだ追加していない場合、Subtype（サブタイプ）ドロップダウンリストは空になっています。インポート時に、選択したサブタイプにすべての資産が割り当てられます。

   c. **次へ** をクリックします。

   マッピング ページが表示されます。
9. CSV Fields（CSV フィールド）ドロップダウンリストで、アプライアンスの Required Standard Fields（必須の標準フィールド）および Required Asset Fields（必須の資産フィールド）に対応するフィールドを選択します。これらのフィールドのマッピングは、CSV ファイルおよび資産タイプの内容によって異なります。このセクションでは例えば、次の値を使用します。
   - 資産名 =**名前**
   - 場所=**場所**
   - 資産ステータス =**資産ステータス**

     注: このマッピングを指定しない場合、選択した資産タイプに関連付けられているデフォルトのステータスが、インポートされたそれぞれの資産エントリに割り当てられます。
   - License Count（ライセンス数）= **License Count**（ライセンス数）
   - Applies to Cataloged Software（カタログ登録済みソフトウェアへの適用）= **ソフトウェアカタログ**
   - ライセンスモード = **モード**

   注: インポートされた資産がデバイスでない場合、資産譲受人の値をインポートできません。
10. 資産名 フィールドの隣にある **PK** チェックボックスを選択します。

    注: プライマリキーは、インポートする資産の一意の識別子として使用される、フィールドまたはフィールドの組み合わせです。資産がインポートされる際に、アプライアンスはプライマリキーを使用して、既存のレコードを更新するか、新しいレコードを作成するかを判断します。PKとして、1つのフィールドまたはフィールドの組み合わせを選択できます。
11. インポートする資産でバーコードを使用する場合は、バーコードフィールド 領域内で、バーコードをインポートする方法を指定します。

オプション	説明
資産バーコードを選択でアップデート	この領域にすでにバーコードがあるかどうかを確認します。あれば、そのバーコードを更新します。

オプション	説明
	ない場合は、指定した資産用にバーコードが作成されます。
すべての資産バーコードを選択と置き換え	既存のバーコードを指定されたバーコードと置き換えます。
バーコードデータ	CSVファイル内のバーコードを含むフィールド。同じタイプのバーコードは資産ごとに1つしかありません。
バーコードの名前	CSVファイル内のバーコードタグを含むフィールド。バーコード番号は常に一意で、複数の資産間で共有できません。ただし、アクティブな資産がアーカイブされた資産のバーコードを共有することはできます。
バーコードのフォーマット	CSVファイル内のバーコードフォーマットを含むフィールド。例えば、UPC-A、Code 11、またはUPC-Eです。

12. **プレビュー** をクリックして、確認 ページでデータを確認します。
13. **1 回限りのインポート**のみ。次の手順を実行します。
    a. **インポート** をクリックして、インポートプロセスを完了します。

       資産のインポートの結果 ページが表示されます。

    b. **完了** をクリックして、資産 ページに戻ります。
14. **スケジュール済みインポートのみ**。次の手順のいずれかを実行します。
    - **保存** をクリックして、新しく作成したスケジュール済みインポートを保存します。資産のインポート 一覧ページが表示され、スケジュール済みインポートのエントリが一覧表示されます。
    - **今すぐ実行** をクリックして CSV ファイルから資産をインポートし、スケジュール済みインポート設定を保存します。

    資産のインポート の一覧ページが表示されます。

インポートが完了すると、資産 リストに資産が表示されます。ソフトウェアのタイトルがソフトウェアカタログインベントリのタイトルに一致した場合は、資産がインベントリアイテムに関連付けられるため、そのアイテムの Software Catalog Detail（ソフトウェアカタログの詳細 ）ページに資産を表示できます。

ライセンスコンプライアンスの管理

購入したソフトウェアライセンスの数、管理対象デバイスで使用している数、および使用可能な数を追跡できます。このタイプの追跡は、会社がソフトウェアライセンス要件に確実に準拠できるようにする場合に役立ちます。

例えば、Adobe?? Creative Suite の 100 ライセンスを保有している場合、そのうち実際に管理対象デバイスで使用されているライセンスの数を知っておく必要があります。また、保有ライセンスの80 %または90 %が使用されている場合に、それを知ることができれば、必要に応じてライセンスの上限を引き上げることができます。ライセンス使用率の警告しきい値をカスタマイズすると、ライセンスコンプライアンスを追跡できます。

ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンス情報の表示

組織がインストールされたソフトウェアの正しいライセンスを保有できるように、ライセンスコンプライアンスリストおよびライセンスコンプライアンスダッシュボードウィジェットにライセンスコンプライアンス情報を表示できます。ライセンスコンプライアンス リストには、ライセンス資産を通じて追加したすべてのソフトウェアライセンス情報と、ライセンスが必要なアプリケーションに関するソフトウェアカタログからの情報が表示されます。

- インベントリのエージェント管理対象デバイスには、ソフトウェアカタログで使用可能なソフトウェアアプリケーションが搭載されています。
- インストールされたソフトウェアカタログアプリケーションに対してライセンス資産として利用できるシートの数と、ライセンスモードは既に指定しています。詳細については、「ソフトウェア ページインベントリのライセンス資産の追加」を参照してください。
- アプライアンスまたは組織の一般設定でライセンス使用率の警告しきい値を既に確立しています。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。

1. 完全なライセンスコンプライアンス情報を表示するには、ライセンスコンプライアンス ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**ライセンスコンプライアンス** をクリックします。

    注: アプライアンスの日ベースのバックアップの完了後、ライセンスコンプライアンス リストの情報が毎日更新されます。リストが空の場合は、ソフトウェアカタログインベントリにアプリケーションがないか、またはページの情報が更新されていないことになります。また、すべての過不足数に負数が表示されている場合は、ライセンスシートよりも多くのインストールがあることを示しています。そのため、アプリケーションのライセンス資産を既に追加していることを確認してください。詳細については、「ソフトウェアカタログ インベントリのライセンス資産の追加」を参照してください。
2. アプライアンスがライセンスコンプライアンス情報を強制的に更新するようにするには、左側のリストの上にある 今すぐ更新 をクリックします。インベントリ内のアプリケーションの数によっては、このプロセスに数分かかることがあります。

    ヒント: **今すぐ更新** をクリックすると、アプライアンスがリスト上の各アイテムのデータを更新します。ただし、右側のリストの上にある **更新** ボタンをクリックした場合は、既に収集された情報が再表示されます。新しいライセンス使用率情報が取得されることはありません。

ライセンスコンプライアンス ページには、次のような情報が表示されます。

列の名前	説明
名前	アプリケーションの名前。
発行元	アプリケーション発行元の名前。
インストール済み	エージェント管理対象デバイス上のアプリケーションインストールの数。
ライセンス済み	ライセンスに基づく残りのシートの数。

列の名前	説明
過不足数	使用可能なライセンスシートの数とアプリケーションインストールの数との差異（ある場合）。負数は、ライセンスで許可されている数よりも多くのデバイスにアプリケーションがインストールされており、そのためコンプライアンスに準拠していないことを示しています。
過去 90 日間で使用済み **過去 60 日間で使用済み** **過去 30 日間で使用済み**	過去 90、60、または 30 日間に起動されたアプリケーションインストールの数。この列のダッシュは、アプリケーションのメータリングが有効になっていないことを示しています。 **注:** 正確な使用率情報を取得するには、アプリケーションおよびそのアプリケーションがインストールされているデバイスのメータリングを有効にする必要があります。詳細については、「デバイスとアプリケーションに対するメータリングの有効化および設定」を参照してください。
過去 90 日間で未使用 **過去 60 日間で未使用** **過去 30 日間で未使用**	過去 90、60、または 30 日間に起動されていないアプリケーションインストールの数。この列のダッシュは、アプリケーションのメータリングが有効になっていないことを示しています。 **注:** 正確な使用率情報を取得するには、アプリケーションおよびそのアプリケーションがインストールされているデバイスのメータリングを有効にする必要があります。詳細については、「デバイスとアプリケーションに対するメータリングの有効化および設定」を参照してください。
適用範囲	ライセンスタイプ。ライセンスタイプは次のとおりです。 • **アップグレード**：インストール済みのアプリケーションが旧バージョンからアップグレードされました（メンテナンス契約が必要です）。 • **ダウングレード**：インストール済みのアプリケーションが後続のバージョンのライセンスを使用しています（ダウングレード権が必要です）。 • **オリジナル**：インストール済みのアプリケーションがバージョン番号に一致するライセンスを使用しています。 • **「なし」**：アプリケーションがライセンスなしでインストールされています。
プラットフォーム	アプリケーションが実行されるオペレーティングシステム。

列の名前	説明
エディション	アプリケーションに関連するエディションの名前（Professional Edition や Standard Edition など）。

3. リストを並べ替えるには、**特定基準で表示** をクリックし、表示を選択します。

   アプリケーションを製品別（Microsoft Office など）または製品かつエディション別（Microsoft Office Professional や Office Standard など）で表示できます。例えば、Microsoft Office アプリケーションのすべてのエディションを 1 つの見出しで表示するようにした場合、特定基準で表示 ドロップダウンリストから **製品** を選択できます。Licensed（ライセンス済み）列には、Microsoft Office グループのすべてのアプリケーションに利用できるシートの数が表示されます。Microsoft Office アプリケーションをエディション別に表示するには、特定基準で表示 ドロップダウンリストから **製品とエディション** を選択します。Licensed（ライセンス済み）列には、Microsoft Office の各エディションに利用できるシートの数が表示されます。

   ヒント: Officeなどのグループが折りたたまれて最上位のアイテムのみが表示されている場合、そのグループ内のいずれかのアイテムで過不足数が負数になっているか、ライセンスで許可されている数よりも多くのシートを使用しているときには、名前 列の左側に警告アイコン（ ）をクリックします。

4. ライセンスコンプライアンスウィジェットを表示するには、左側のナビゲーションバーの **ホーム** をクリックして、管理者レベルの Dashboard（ダッシュボード）ページに移動します。

   ヒント: ライセンスコンプライアンスウィジェットが表示されない場合は、右上の **カスタマイズ** をクリックしてウィジェットをインストールします。詳細については、「ダッシュボード ページのカスタマイズ」を参照してください。

5. ライセンスに基づいて使用可能なシートの数に関する情報を表示または変更するには、ライセンス 資産の詳細ページに移動します。詳細については、「資産の表示および資産の情報の検索」を参照してください。

未使用のソフトウェアライセンスの再利用

アプライアンス管理者は、使用頻度の低いソフトウェアを取得し、必要な場所で再使用するために、ユーザーデバイスで特定のソフトウェアアプリケーションが使用される頻度に基づいて、カタログ化されたソフトウェアをアンインストールできるポリシーを設定できます。

過去 30、60、90 日間使用されていない特定のソフトウェアアプリケーションのライセンス、または関連付けられたすべてのライセンスをを再利用するオプションがあります。

1. ライセンスコンプライアンス ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**ライセンスコンプライアンス** をクリックします。
2. **名前** 列で、アプリケーションの名前を展開し、必要に応じて、再利用するソフトウェアライセンスのバージョンを選択します。

注: 一度に 1 つのソフトウェアのバージョンのライセンスのみを再利用することができます。複数のバージョンを選択すると、エラーが発生します。

3. ソフトウェアのバージョンのライセンスを再利用するには、**アクションを選択 > ソフトウェアの再利用** を選択し、必要に応じて、次のいずれかのオプションを選択します。
   - **過去 30 日間で未使用**
   - **過去 60 日間で未使用**
   - **過去 90 日間で未使用**
   - **すべて**

   管理対象インストールの詳細 ページが表示され、選択したソフトウェアアイテムのインストールを関連付けられたエンドユーザーデバイスから削除するプロセスを作成できます。
4. 必要に応じて、新しい管理対象インストールを作成します。詳細については、適宜以下のセクションをお読みください。
   - Windowsデバイス用の管理対象インストールの作成
   - Mac OS Xデバイス用の管理対象インストールの作成
   - RPMファイル用の管理対象インストールの作成

ソフトウェアライセンスコンプライアンス情報の手動更新

いつでもソフトウェアライセンスコンプライアンス情報を手動で更新できます。ただし、多数のアプリケーションがある場合、情報を更新するプロセスに数分かかることがあります。

インベントリのエージェント管理対象デバイスには、ソフトウェアカタログで使用可能なソフトウェアアプリケーションが搭載されています。

アプライアンスの日ベースのバックアッププロセスの実行後、ソフトウェアライセンスコンプライアンス情報が毎日自動的に更新されます。ライセンスコンプライアンス情報を手動で更新すると、使用可能な最新情報を取得できます。

注: インベントリにアプリケーションのライセンス資産をまだ追加していない場合、ライセンスコンプライアンス ページにはアプリケーションに使用可能なシートの数が 0 と表示され、ソフトウェアインストールの数が過不足数となります。

1. ライセンスコンプライアンス ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**ライセンスコンプライアンス** をクリックします。
2. リストの上にある **今すぐ更新** をクリックします。

   アプライアンスが最新のライセンス使用率情報がないか確認し、リストが更新されます。

ヒント: 右側のリストの上にある **更新** ボタンをクリックした場合は、既に収集された情報が再表示されます。新しいライセンス使用率情報が取得されることはありません。

ライセンス使用率警告しきい値の設定

ライセンス使用率警告しきい値をカスタマイズして、警告レベルまたは緊急レベルとみなされるライセンスの使用率を指定できます。

アプライアンスのダッシュボードに、ライセンスコンプライアンス情報が表示されます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のライセンス使用率警告しきい値を個別にカスタマイズします。

1. 管理者レベルの 一般設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。
    c. コントロールパネル で **一般設定** をクリックします。
2. ライセンス使用率の注意喚起設定 セクションまで下にスクロールします。
3. 注意喚起しきい値 と 緊急しきい値 の各フィールドに、新しい値を入力します。

    デフォルトの Warning Threshold（ 警告しきい値 ） は 90 です。デフォルトの Critical Threshold（ 緊急しきい値 ） は 100 です。
4. 保存するには、**保存してサービスを再起動** をクリックします。

    しきい値が設定されました。ライセンス資産を作成済みの場合、ライセンスコンプライアンス情報は、**管理者コンソール**の ダッシュボード ページに表示されます。

関連トピック

ソフトウェア ページインベントリのライセンス資産の追加

ライセンスコンプライアンスと設定情報の表示

ライセンスコンプライアンスと設定情報の表示

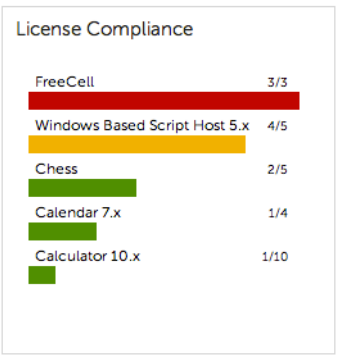
アプリケーションにライセンス資産を設定済みの場合には、そのアプリケーションのライセンスコンプライアンスと設定に関する情報を表示することができます。

ソフトウェア タブに表示されているアプリケーションおよび ソフトウェアカタログ タブに表示されているアプリケーションに関連付けられたライセンス資産で情報を使用できます。詳細については、「ライセンスコンプライアンスの設定」を参照してください。

組織が複数ある場合は、それぞれの組織にライセンス情報を個別に表示します。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **ホーム** をクリックします。

    ライセンスコンプライアンス ウィジェットにソフトウェアコンプライアンス情報が表示されます。

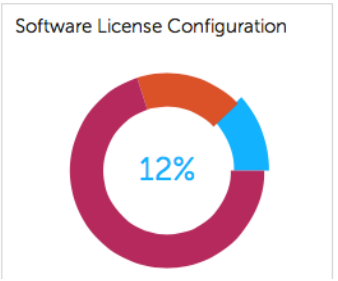


注: アプライアンスは、8 時間ごとに ライセンスコンプライアンス ウィジェットのデータを更新します。一方、**更新** ボタンをクリックしても、データは更新されません。既に収集されたデータを単に再表示するだけです。

次の色により、使用率レベルが示されます。

色	説明
赤	使用率が緊急しきい値設定以上です。
オレンジ	使用率が警告しきい値設定以上になっていますが、緊急しきい値設定に対しては下回っています。
緑	使用率が警告しきい値設定を下回っています。

Software License Configuration（ソフトウェアライセンス設定）ウィジェットには、ユニットライセンス、サイトライセンス、およびその他のライセンスモードに分類されるソフトウェア資産の割合が表示されます。



オプション：ライセンスコンプライアンス ページに追加情報を表示します。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンス情報の表示」を参照してください。

サービスデスクの設定

サービスデスクの設定には、サービスデスクスタッフの役割の設定、チケットの設定および E メールの設定が含まれます。

ユーザーアカウントの役割の設定

サービスデスクは、権限ベースの役割を使用することで、サービスデスクの機能および情報に対するアクセスを制御します。こうした役割は、ユーザーのログイン時に自動的に割り当てることができます。デフォルトの役割を使用するほか、必要に応じて役割を作成することも可能です。

デフォルトの役割について

デフォルトの役割は、管理者、エンドユーザー、制限付きアクセスなど、標準ユーザーアカウントタイプに使用できます。

デフォルトで利用可能な役割は次の通りです。組織の役割の管理の詳細については、組織の役割とユーザーの役割の管理を参照してください。

役割	説明
組織の役割	組織の役割は、組織に割り当てられる権限のスーパーセットで、組織ユーザーが使用できる権限を定義します。例えば、配布 タブが非表示になっている組織の役割が組織に割り当てられている場合、その組織のユーザー（管理者ユーザーを含む）は、配布 タブにアクセスできません。 **注:** 組織の役割は、組織コンポーネントが有効になっているアプライアンスでのみ使用可能です。
デフォルト役割	組織の役割 セクションのデフォルト役割には、すべてのタブに対する読み取り/書き込み権限があります。追加の組織の役割を作成できますが、デフォルト役割を編集または削除することはできません。
ユーザーの役割	**管理者コンソール**および**ユーザーコンソール**へのアクセスを制御するためにユーザーに割り当てられた役割。アプライアンスで組織コンポーネントが有効になっている場合、これらの役割で利用できる権限は、組織に割り当てられている組織の役割によって決まります。
管理者	アプライアンスにおいて最も強力なユーザーの役割。デフォルトでは、**管理者**役割を割り当てられたユーザーには、情報および設定を表示または変更する権限が与えられます。例えば、役割を変更することで他のユーザーの昇格または降格が行えます。**管理者**役割は変更したり、削除したりすることはできません。この役割は、信頼された管理者のみに割り当ててください。 **管理者**役割を割り当てられたスタッフメンバーは、**管理者コンソール**の チケット タブでサービスデスクチケットを管理し、修正する権限を持ちますが、自分自身はチケットを所有できない場合があります。 **管理者**役割を持つユーザーも、セキュリティ、スクリプト作成、および配布機能を使用してサービスデスクチケットを解決し、サポート技術情報に問題の詳細を記録できます。 **管理者**役割は、主に**管理者コンソール**を通じてアプライアンスを操作します。
アクセス権限なし	この役割を割り当てられたユーザーは、**管理者コンソール**または**ユーザーコンソール**にログオンできません。
読み取り専用の管理者	この役割はアプライアンスの情報や設定を表示できますが、変更することはできません。この役割は、スーパーバイザなどの監督担当者向けとして便利です。 この役割は、主に**管理者コンソール**からアプライアンスを操作します。

役割	説明
ユーザーコンソールのみ	アプライアンスのユーザー用の役割です。デフォルトでは、この役割はサービスデスクチケットの作成、表示、および修正を行う権限を持ちます。 この役割は、**ユーザーコンソール**からのみアプライアンスを操作します。

サービスデスクスタッフ役割の作成

サービスデスクスタッフ役割を作成して、サービスデスクの設定およびコンポーネントに対して作業を行うユーザーの権限を指定できます。

デフォルトでは、**管理者**役割を割り当てられたユーザーには、ユーザーの作成および削除を含め、すべてのサービスデスクコンポーネントを変更する権限があります。さらに、より限定的な権限を持つサービスデスク役割を組織に作成できます。この役割を持つユーザーには、チケットに対応し、**ユーザーコンソール**からダウンロードできるアイテムを追加し、記事をサポート技術情報に追加し、**ユーザーコンソール**ホームページに表示される告知を管理する権限が与えられます。ただし、ユーザーの管理、レポートの作成、アプライアンス設定の変更などはできません。このガイドでは、このユーザーのグループを「**サービスデスク管理者**」と呼びます。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のサービスデスク管理者のユーザー役割を個別に作成できます。

1. 役割詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**役割** の順にクリックします。
    c. **アクションの選択** > **新規作成** を選択します。
2. 名前 フィールドで、「サービスデスク管理者」などの名前を入力します。
3. 説明 フィールドで、役割の簡単な説明を入力します（ 「サービスデスク管理者に使用」など ）。

    これは、役割 リストに表示されます。
4. 管理者コンソールの 権限 の隣にある **すべて展開** リンクをクリックして、すべてのカテゴリの権限設定を表示します。
5. 新しい役割の権限を、以下からカスタムで選択します。

カテゴリ	アイテム	権限レベル
ホーム	**すべて**	すべて読み取り
インベントリ	**デバイス**	書き込み
	ソフトウェア	書き込み
	ソフトウェアカタログ	書き込み
	ライセンスコンプライアンス	非表示
	プロセス (複数)	非表示
	スタートアッププログラム	非表示

カテゴリ	アイテム	権限レベル
	サービス	非表示
	検出スケジュール	非表示
	検出結果	非表示
	SNMPインベントリ設定	非表示
監視	デバイス	読み取り
	警告	書き込み
	プロファイル	非表示
	メンテナンスウィンドウ	非表示
	Log Enablement Packages	非表示
資産	すべて	非表示
配布	すべて	非表示
スクリプト	すべて	非表示
セキュリティ	すべて	非表示
サービスデスク	チケット (複数)	書き込み
	ユーザーダウンロード	書き込み
	サポート技術情報	書き込み
	告知	書き込み
	アーカイブ	読み取り
	設定	読み取り
レポート作成	すべて	すべて非表示
設定	すべて	すべて非表示
ユーザーコンソール	すべて	すべて読み取り

6. **保存** をクリックします。

役割 ページに新しい役割が表示されます。この役割を割り当てられたユーザーがログインすると、アプライアンスのコンポーネントバーに使用可能な機能が表示されます。

ユーザーの役割の割り当て

ユーザーアカウントをインポートまたは作成したら、そのアカウントにユーザーの役割を割り当てることができます。

注: ユーザーアカウントは、LDAPサーバーからインポートできます。詳細については、「LDAPサーバーからのユーザーのインポート」を参照してください。

1. ユーザー リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
2. サービスデスク管理者に**管理者**役割を割り当てます。
    a. 1つまたは複数のユーザーの隣のチェックボックスをオンにします。
    b. **アクションの選択 > 役割の適用 > 管理者**を選択します。

    デフォルトでは、**管理者**ユーザーは所有者/送信者権限を有します。
3. チームユーザーに、**サービスデスクスタッフ**役割を割り当てます。
    a. 1つまたは複数のユーザーの隣のチェックボックスをオンにします。
    b. **アクションの選択 > 役割の適用 > サービスデスクスタッフ**を選択します。
4. サービスデスクチームに、**すべてのチケット所有者**ラベルを割り当てます。
    a. 1つまたは複数のユーザーの隣のチェックボックスをオンにします。
    b. **アクションの選択 > ラベルの適用 > すべてのチケット所有者**を選択します。

    ラベルが適用され、ユーザー名の隣に表示されます。
5. 「**ユーザー**」という名前のラベルを作成し、その**ユーザー**ラベルと役割を各ユーザーに適用します。

関連トピック

カスタムチケットフィールドの定義

サービスデスクスタッフ役割の作成

「すべてのチケット所有者」ラベルの追加

サービスデスクスタッフへのラベルおよび役割の適用

ラベルと役割をサービスデスクスタッフメンバーに適用して、サービスデスクスタッフの権限を管理できます。

ラベルと役割の作成手順については、ユーザーアカウントの役割の設定およびユーザーアカウントのラベルの設定を参照してください。

1. **DefaultTicketOwners@mydomain.com** エイリアスにユーザーを追加します。
2. ユーザー詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。

c. ユーザー詳細 ページを表示するには、次のいずれかを実行します。

- ユーザーの名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

3. ラベルへの割り当て フィールドで **編集** をクリックします。
4. ラベル ウィンドウで、**すべてのチケット所有者** ラベルを 割り当て先 フィールドにドラッグし、**保存** をクリックします。

注: このラベルが存在しない場合は、作成する必要があります。

5. 役割 フィールドで、**サービスデスクスタッフ** 役割を選択します。
6. **保存** をクリックします。

指定したユーザーに、チケットの所有、変更、修正、終了を行う権限が与えられます。チケットが作成されると、このユーザーに自動的にEメールが送られます。

関連トピック

「すべてのチケット所有者」ラベルの追加

サービスデスクスタッフ役割の作成

DefaultTicketOwnersアカウントの作成

新しいチケットが作成された際に、サービスデスクスタッフがEメール通知を受け取れるように、DefaultTicketOwnersユーザーアカウントを作成します。

次に、チケット設定の構成の手順に従って Ticket Detail（ チケットの詳細 ）ページを設定すると、そのアカウントを使用することができます。

E メール通知の詳細については、Eメール通知についてを参照してください。

1. ユーザー詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
   c. **アクションの選択 > 新規作成** を選択します。
2. 最低でも、次の情報を提供します。

フィールド	説明
ログイン	DefaultTicketOwners
名前	DefaultTicketOwners
Eメール	DefaultTicketOwners@**mydomain.com**
パスワード	パスワードを入力します
パスワードの確認入力	もう一度パスワードを入力します
役割	アクセス権限なし

フィールド	説明
ラベルへの割り当て	すべてのチケット所有者

3. **保存** をクリックします。
4. この新規ユーザーをデフォルトのチケット所有者として割り当てるには、チケット設定の構成の手順に従って、**DefaultTicketOwners** を選択します。

> **注:** 最初のデフォルト所有者は、常にチケットのデフォルト所有者となります。例えば、既存のチケットを異なるデフォルト所有者を持つ別のカテゴリに移しても、チケットのデフォルト所有者は変更されません。

Eメール設定の設定

キューのEメール通知方法を設定できます。キューが複数ある場合は、それぞれのキューのEメール設定を個別に定義できます。

E メール通知方法については、システム要件で説明されています。

デフォルトでは、チケットが特定の状態のまま一定期間を超えると、サービスデスクがスタッフに対し、自動的に警告のEメールを送信します。さらに、優先度が「高」のチケットが30分以内に修正またはクローズされないと、そのチケットがエスカレーションされます。エスカレーション時間と、それが適用されるチケットのリストを変更するには、チケット詳細 ページのカスタマイズを参照してください。

一般には、アプライアンス自体に E メールを送信するように設定すべきではありません。例えば、キューの E メールアドレスが helpdesk@example.com の場合、カテゴリ CC リストや E メールアドレスを指定できるその他の設定で、この helpdesk@example.com という E メールアドレスを有効な選択肢にすべきではありません。

Quest KACEのお客様のほとんどは、不要な通知をできるだけ受信しないようにするために、次のEメール通知方法を使用しています。

- 新しいチケットが作成されると、サービスデスクの全スタッフにEメール通知が送信されます。E メール通知の注意事項については、Eメール通知についてを参照してください。
- あるサービスデスクスタッフメンバーがチケットの所有権を取得すると、チケットがエスカレーションされない限り、残りのスタッフはそのチケットに関するEメールは受け取りません（チケットを検索することはできます）。
- チケットの送信者と所有者は、チケットの状態またはステータスが変更されるたびに、Eメールによる通知を受け取ります。
- チケット所有者は、チケットに対する変更の通知を受けます。
- チケットがエスカレーションされると、チケット所有者と、カテゴリCC リストに含まれるユーザーが通知を受けます。

Eメール通知について

サービスデスクチケットが作成または変更されると、アプライアンスによって、チケット送信方法、「イベント発生時にEメールを送信」の設定、および実行されたアクションに基づいてEメール通知が送信されます。

Eメール通知には、次のルールが適用されます。

- サービスデスクキュー E メール設定 ページの イベント発生時に E メールを送信 セクションで、送信者 のポータル経由の新規チケット を選択している場合を覗いて、**管理者コンソール**または**ユーザーコンソール**を使用してチケットを送信または修正した場合、チケットの送信者に確認の E メールは送られません（キュー固有の E メール設定の詳細については、「Eメールトリガの設定」を参照してください）。そのチケットに関連付けられているその他のユーザー（**所有者**、**承認者**、**CC リスト**、および**カテゴリ CC**）は、キューの詳細 ページの イベント発生時に E メールを送信 セクションでの指定に基づいて E メール通

知を受信します。詳細については、「Eメールトリガとメールテンプレートの設定」を参照してください。

- Eメールを通じてチケットが作成された場合、そのチケットの送信者は確認のEメールを受け取ります。ただし、Eメールでチケットを修正した場合、送信者に確認メッセージは送られません。
- チケットが変更された場合、変更通知のEメールメッセージは、意図的に遅延されます。この遅延は、変更が行われた際に送信されるEメール通知の数を削減することを目的としています。例えば、チケット所有者がコメントを追加し、チケットを保存した直後に、チケットに2回目の変更を行う場合があります。この場合、変更通知は1回しか送信されません。

  注: Eメールメッセージには、次の文章が追加されます。+++++ Please reply above this line to add a comment +++++.

- 管理対象デバイスまたはユーザーアカウントがインベントリから削除された場合、不要な通知を避けるため、このデバイスに関連するサービスデスクチケットのEメール通知は送信されません。

チケットルールについて

標準のEメール動作がニーズに合わない場合、チケットルールを使用して、その動作を変更できます。

チケットルールの詳細については、チケットルールの使用を参照してください。

E メール通知の動作の修正など、より複雑なチケットルールの多くは、**Questサポート**サイト（ https://support.quest.com/contact-support ）で公開されています。

POP3 Eメールアカウントについて

POP3 サーバから E メールを受信するようにアプライアンスを設定できます。

そのためには、次の手順を実行する必要があります。

- アプライアンスのネットワーク設定で外部 SMTP サーバーを有効化し、設定します。詳細については、「外部SMTPサーバーまたはセキュアなSMTPサーバーの使用」を参照してください。
- （**オプション**）サービスデスクの E メールプリファレンスを設定します。詳細については、「E メールプリファランスの設定」を参照してください。
- サービスデスクチケットキューで SMTP サーバーおよび POP3 設定を設定します。詳細については、「キュー固有の E メールの設定」を参照してください。

POP3 E メールサーバーを使用しない場合は、KACE SMA の組み込みの SMTP サーバーを使用して、内部の E メールサーバーからの E メールメッセージを受信することができます。

重要: アプライアンスの POP3 E メールサーバは、認証情報と E メールテキスト自体を、クリアテキストとして渡す必要があります。

POP3 Eメールアカウントの作成と設定

サービスデスクのユーザーとスタッフが使用する、POP3 Eメールアカウントを作成および設定できます。

以下の2つのアカウントを使用します。

- **Support@mydomain.com**。このEメールアドレスは、次の用途で使用されます。
  - 作成されたすべての新規チケットを受信する。
  - ユーザーとサービスデスクスタッフがチケットの作成や修正を自動的に行えるようにする。
  - ユーザーの返信先のEメールアドレスとして使用する。

このアドレスに送信されたEメールは読まれませんが、サービスデスクスタッフは、Eメールの結果として生じたチケット変更について通知を受け取ります。

- **DefaultTicketOwners@mydomain.com**。このEメールエイリアスは、次の用途で使用されます。
  - サービスデスクスタッフが互いに通信できるようにする。
  - アプライアンスで、新規および未解決のチケットに関する自動Eメール通知を送信できるようにする。

1. POP3 Eメールサーバー上で有効なEメールアドレスとして、Support@**mydomain**.comを作成します。
2. DefaultTicketOwners@**mydomain**.comをサービスデスクスタッフのEメールエイリアスとして設定し、そこにサービスデスクスタッフのEメールアドレスをすべて追加します。これが、サービスデスクスタッフ同士での連絡に使用する汎用的なEメールエイリアスになります。
3. アプライアンスが使用する外部 SMTP サーバーを使用する場合、システム管理コンソール の ネットワーク設定 ページで設定します。詳細については、「アプライアンスのネットワーク設定の変更」を参照してください。

   ヒント: サービスデスクチケット E メールに POP3 を使用する場合、キューレベルで POP3 を設定できます。

4. （**オプション**）サービスデスクの E メールプリファレンスを設定します。詳細については、「E メールプリファランスの設定」を参照してください。
5. 各キューに異なる SMTP または POP3 設定を使用する場合、キューレベルで指定できます。詳細については、「キュー固有の E メールの設定」を参照してください。

E メールプリファランスの設定

サービスデスクのユーザーとスタッフとの間で送受信される E メールのプリファレンスを作成し設定できます。

デフォルトでは、サービスデスクはチケット関連 E メールの送信に内部 SMTP サーバーを使用するように設定されています。外部 SMTP サーバーを使用するオプションはありますが、アプライアンスネットワーク設定で設定する必要があります。詳細については、「アプライアンスのネットワーク設定の変更」を参照してください。

1. サービスデスクの E メールプリファレンス ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルの E メール設定 セクションで、**サービスデスク E メール環境設定の構成** をクリックします。
2. 表示される サービスデスクの E メールプリファレンス ページの 送信メール セクションで、送信メールに、「この行の上にご返信ください」という文言を含める チェックボックスを選択します。

   この機能を使用して、メールチェーン全体が各コメントに追加されないようにすることをお勧めします。

3. Eメールの件名で検出するテキストを指定します。指定した件名のチケット関連のEメールを受信した場合に、サービスデスクはそのEメールの処理を中止します。
   a. 受信Eメール セクションの 件名に次のテキストが含まれるEメールは無視する フィールドで検出対象の言葉を入力します。セミコロンを区切り文字として使用し、複数のエントリを指定することができます。例：不在;メール送信失敗。
4. 特定の期間内でのすべての受信Eメール通知に対してしきい値を設定します。しきい値に達すると、サービスデスクはEメール通知の送信を中止します。

   注: 全体がしきい値に達した場合、すべてのチケットの通知が停止します。チケットごとにしきい値に達した場合、該当するチケットの通知のみが停止します。所定期間内のEメールの更新件数が設定したしきい値よりも下回ると、通知が再開されます。

オプション	説明
合計Eメール数	サービスデスクが受信して返信するEメール通知に関するすべてのEメールの最大数。デフォルトでは100通です。
x分の期間内に受信	指定した数のEメールが受信される分単位の期間。デフォルトは1分です。 この制限を無効にするには、この値を99999などのより大きな値に設定します。

5. 特定の期間に受信するチケット毎のEメール通知のしきい値を設定します。しきい値に達すると、サービスデスクはEメール通知の送信を中止します。

オプション	説明
チケット毎の合計Eメール数	チケット毎にサービスデスクが受信して返信するEメール通知に関するすべてのEメールの最大数。デフォルトではチケット毎に5通です。
x分の期間内に受信	チケット毎に受信する、指定した数のEメールが受信される分単位の時間間隔を指定します。デフォルトは1分です。この制限を無効にするには、このオプションを99999などのより大きな値に設定します。

6. **保存** をクリックします。

次に、特定のサービスデスクキューのPOP3 Eメールアカウントを設定できます。詳細については、「キュー固有の E メールの設定」を参照してください。

Eメールトリガと Eメールテンプレートの設定

アプライアンスから E メールを自動的に送信するトリガを設定し、テンプレートを使用して E メールメッセージの内容を設定できます。

イベント発生時に E メールを送信 セクションは、アプライアンスのさまざまなユーザー宛ての E メールをトリガするアクションを決定します。Eメールテンプレートを使用すると、メッセージの内容を決定できます。

E メールメッセージのタイミング

次の E メールイベントは、E メールを直ちに送信するようにアプライアンスをトリガします。

- **コメント**：ユーザーがチケットフォームでコメントを追加し、**送信** をクリックすると、コメントの E メール通知が送信されます。一方、ユーザーがチケットフォームでコメントを追加し、**保存** をクリックすると、任意の変更 通知のみが送信されます。
- **チケット終了**：満足度調査が有効になっている場合は、チケットが終了すると、満足度調査について説明した E メールが直ちに送信されます。

次の E メールイベントは、E メールのオーバーロードを回避するため、数分ごとに E メールを送信するようにアプライアンスをトリガします。

- 任意の変更
- 所有者の変更
- ステータスの変更
- 承認の変更
- 解決の変更
- エスカレーション
- SLA違反
- E メールを使用した新しいチケット

Eメールトリガの設定

キューのEメールトリガを設定できます。キューが複数ある場合は、それぞれのキューのEメールトリガを個別に定義できます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの詳細 ページを表示するには、次のいずれかを実行します。
    - キューの名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. キューの詳細 ページの E メールアドレス の下で、**キューの E メールを設定する** リンクをクリックして、サービスデスクキュー E メール設定 ページを表示します。
3. サービスデスクキュー E メール設定 ページの イベント発生時に E メールを送信 セクションで、指定されたイベントが発生したときに E メールを送信するオプションを選択します。各列はサービスデスクユーザー（ 役割 ）のタイプを表し、各行はチケットイベントを表します。

サービスデスクユーザー（ 役割 ）	説明
所有者	チケットを解決すべきユーザー。
送信者	チケットの元となる問題を提起したユーザー。
承認者	処理するチケットを承認または拒否できるユーザー。
チケットCC	チケットの CC フィールドに保存されている 1 つ以上の E メールアドレス。
カテゴリCC	チケットの Category Value（ カテゴリ値 ） の CC リスト に保存されている 1 つ以上の E メールアドレス。詳細については、「チケットカテゴリのための CC リストの設定」を参照してください。
キューの所有者	所有者 ラベルで指定されたチケットキューの 1 人または複数の所有者。これは、E メールを使用した

サービスデスクユーザー（役割）	説明
	新しいチケット イベントと ポータル経由の新規チケット イベントにのみ適用されます。

チケットイベントが発生すると、選択した役割またはユーザーに E メールが送信されます。例えば、所有者 列で **任意の変更** ボックスを選択した場合、チケットが変更されるたびにチケット所有者に E メールが送信されます。コメント および Ticket Closed（チケット終了）トリガの場合、E メールが直ちに送信されます。一方、その他のチケットの変更の場合、E メールのオーバーロードを回避するため、数分ごとに E メールが送信されます。

注: スマートフォンまたはタブレットにKACE GOモバイルアプリケーションがインストールされている場合、システムは、選択したサービスデスクチケットイベントのプッシュ通知を送信します。

オプション	説明
任意の変更	チケットに関する任意の情報が変更されます。
所有者の変更	チケットの 所有者 フィールドが変更されます。
ステータスの変更	チケットの ステータス フィールドが変更されます。
コメント	情報、添付ファイル、またはスクリーンショットがチケットの コメント セクションに追加されます。ユーザーがチケットフォームでコメントを追加し、**送信** をクリックすると、コメントの E メール通知が送信されます。一方、ユーザーがチケットフォームでコメントを追加し、**保存** をクリックすると、任意の変更 通知のみが送信されます。
承認の変更	チケットの承認ステータスが変更されました。
解決の変更	チケットの解決が変更されました。
エスカレーション	チケットは、チケット優先度で定義されるエスカレーション時間内に停止または閉じられたステータスに更新されていません。
SLA違反	チケットは、その期日までに解決されていません。
Ticket Closed（チケット終了）	チケットの ステータス フィールドが **閉じられた** に変更されます。このイベントは、送信者に満足度調査を提示するために使用します。詳細については、「満足度調査の利用」を参照してください。
E メールを使用した新しいチケット	ユーザーがサービスデスクに E メールメッセージを送信し、チケットが作成されます。
ポータル経由の新規チケット	チケットは**ユーザーコンソール**を通じて作成されます。

4. **保存** をクリックします。

関連トピック

モバイルデバイスによるアクセスの設定

Eメールテンプレートの設定

サービスデスクがキューのEメールメッセージを生成する際に使用する、Eメールテンプレートを設定できます。キューが複数ある場合は、キューごとに個別に E メールテンプレートをカスタマイズします。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの詳細 ページを表示するには、次のいずれかを実行します。
    - キューの名前をクリックします。
    - **アクションの選択** > **新規作成** を選択します。
2. キューの詳細 ページの E メールアドレス の下で、**キューの E メールを設定する** リンクをクリックして、サービスデスクキュー E メール設定 ページを表示します。
3. サービスデスクキュー E メール設定 ページで、次のいずれかの手順を実行します。
    - **すべての E メールテンプレートを編集するには、すべての E メールのカスタマイズ をクリックします。**
    - **特定の E メールテンプレートを編集するには、**イベント **領域で、編集する E メールテンプレートを含む行の** E メールのカスタマイズ **列で** **をクリックします。**
4. 表示されたページで、必要に応じて、1 つまたは複数の選択した E メールテンプレートを変更します。

    注: いずれかのテンプレートのデフォルトのテキストが変更されても、Eメールメッセージが各種言語に翻訳されることはありません。

    次の E メールテンプレートが使用可能です。

チケット関連のテンプレート	説明	デフォルトの受信者
Ticket Escalated（チケットのエスカレーション）	キュー内のチケット優先度用に設定された エスカレーション時間に従って、定期的な通知を送信するために使用します。例えば、優先度が 高 のチケットの エスカレーション時間が 30 分の場合、チケット優先度が変更されるか、またはチケットが終了するまで、高 優先度のチケットに対してこの E メールが 30 分ごとに送信されます。	所有者、チケットの CC リスト、およびチケットカテゴリの CC リスト
Ticket Created from Email（E メールからのチケット作成）	E メールを通じてチケットが作成されたことを確認するために使用します。	所有者、送信者
ポータルからのチケット作成	**ユーザーポータル** を通じてチケットが作成されたことを確認するために使用します。	所有者、送信者

チケット関連のテンプレート	説明	デフォルトの受信者
Ticket Modified（チケット変更）	チケット情報が変更または追加されたら受信者に通知するために使用します。	所有者およびチケットの CC リスト
コメントが送信されました	チケットにコメントが追加されたことを受信者に通知するために使用します。	所有者、送信者、承認者、チケットの CC リスト、およびチケットカテゴリの CC リスト
Ticket Closed（チケット終了）	チケットが終了したときに、送信者に満足度調査を提示するために使用します。詳細については、「満足度調査の利用」を参照してください。	送信者
Email Ticket Manually（E メールでチケットを手動送信）	Ticket Detail（チケットの詳細）ページで Eメールチケット アクションを使用して転送されるメッセージのために使用します。 **ヒント:** HTML/Markdown を使用した場合は、改行などの書式が破棄されないように $ticket_fields_visible トークンを <pre> タグで囲む必要があります。例： <pre>$ticket_fields_visible</pre>	送信者による手動入力
SLAに違反しています	SLA（サービスレベル契約）設定およびチケット優先度を使用して計算された期日を過ぎてもチケットが開かれたままであることを受信者に通知するために使用します。	なし：Queue Detail（キューの詳細）ページで設定可能

エラー関連のテンプレート	説明	受信者
Error Creating Ticket from Email（E メールからチケット作成時のエラー）	**不明な E メールアドレス**以外の理由でチケットを作成できなかったことを送信者に通知するために使用します。	送信者
不明なEメールアドレス応答	送信者の E メールアドレスが不明であるためにチケットを作成できなかったことを送信者に通知するために使用します。	送信者

すべての E メールテンプレートに使用されるトークン

トークン	説明
$helpdesk_email	サービスデスクキューに関連付けられた E メールアドレス。このアドレスは、キューの詳細ページで設定します。

トークン	説明
$helpdesk_name	サービスデスクキューの名前。この名前は、Queue Detail（キューの詳細）ページで設定します。
$userui_url	**ユーザーコンソール**へのリンク。**ユーザーコンソール**へのアクセスには、ログイン資格情報が必要です。

チケット関連の E メールテンプレートに使用されるトークン

トークン	説明
$change_desc	フィールドの変更とコメントの両方を含め、前回チケットを保存したときに加えられた変更の書式設定済み表現。
$last_attachment	チケットに追加された最新の添付ファイル。
$last_comment	チケットに追加された最新のコメント。
$mobile_ticket_url	チケット KACE GO モバイルアプリへのリンク。Android または iOS モバイルデバイスで E メールに表示されたとき、このリンクは KACE GO モバイルアプリで関連付けられたチケットを開きます。
$process_description	プロセスの説明。ユーザーがプロセステンプレートに基づいてチケットの作成を始める前に、完了する必要がある重要な前提条件を含めることができます。
$process_name	プロセステンプレートの名前。
$process_status	「承認が必要」、「承認は期限切れです」、「承認は受信済みです」、「承認が拒否されました」、「処理のキャンセル」、「プロセス完了」などのプロセステンプレートのステータス。
$process_type	プロセスのタイプ。既定のインストールでは、サービスデスク プロセスタイプが含まれます。必要に応じて、新しいプロセスタイプを作成できます。例えば、特定のアプリケーション、またはアプリケーションのグループにアクセスするためのプロセスタイプを作成できます。詳細については、「プロセスタイプの定義」を参照してください。
$summary	チケットの現在の概要。
$ticket_approver_email	チケット承認者の E メールアドレス。コメント の E メール通知では、このアドレスを保有すると特に有益です。
$ticket_approver_name	チケット承認者の名前。

トークン	説明
	注: 承認者名および連絡先情報は、チケット上のフィールドに関連付けられたユーザーレコードから取得されます。
$ticket_approver_phone_home	チケット承認者の連絡先情報。
$ticket_approver_phone_mobile	チケット承認者の連絡先情報。
$ticket_approver_phone_pager	チケット承認者の連絡先情報。
$ticket_approver_phone_work	チケット承認者の連絡先情報。
$ticket_custom_X_label $ticket_custom_X_value	カスタムフィールドに使用されるラベルおよび値。**X** は、カスタムフィールドのインデックス番号を表します。 例えば、キューにラベルの付いた CUSTOM_5 というチケットフィールドがあり、そのフィールドに Location Name（場所名）というラベルが設定されている場合、$ticket_custom_5_label が Location Name（場所名）というテキストに置き換えられます。$ticket_custom_5_value というトークンが、Location Name（場所名）フィールドに対して保存されたチケット値（Topeka（トピーカ）や Albuquerque（アルバカーキ）など）と置き換えられます。 デフォルトでは、すべてのチケットキューが 15 個のカスタムフィールドで設定されていますが、この数は必要に応じて増やすことができます。 **注:** キューごとに、カスタムフィールドと E メールテンプレートの設定を異なるものにすることができます。
$ticket_due_date	チケットで保存される期日。管理者は、自動的に設定された期日を必要に応じて手動で設定した期日で上書きできます。
$ticket_escalation_minutes	定期的な通知の送信間隔（分単位）。この時間は、キュー内のチケット優先度用に設定されたエスカレーション時間によって決まります。例えば、優先度が 高 のチケットのエスカレーション時間が 30 分の場合、チケット優先度が変更されるか、またはチケットが終了するまで、高 優先度のチケットに対してこの E メールが 30 分ごとに送信されます。このトークンは一般に、受信者に E メール通知の頻度を通知するために、チケットのエスカレーション E メールテンプレートで使用されます。
$ticket_fields_visible	E メールでチケットを転送しているユーザーに対して表示されるすべてのチケットフィールドが含まれています。

トークン	説明
	ヒント: HTML/Markdown を使用した場合は、改行などの書式が破棄されないように $ticket_fields_visible トークンを <pre> タグで囲む必要があります。例： <pre>$ticket_fields_visible</pre>
$ticket_history	チケットの完全な履歴。 **注:** チケットによっては、履歴情報が非常に詳細になり、サイズが大きくなりすぎて、E メールでは送信できなくなることがあります。完全な履歴が必要ない場合は、$ticket_history_X を使用して、含まれるレコードの数を制限します。
$ticket_history_X	チケット履歴に指定するレコードの数。X は含まれるレコードの数を示し、最新のものが先頭に配置されます。
$ticket_id	チケットに割り当てられた一意の識別子で、チケット番号とも呼ばれます。ユーザーがチケットを識別するための第一の手段として、この識別子が使用されます。
$ticket_number	チケット ID の書式設定バージョン。このバージョンは TICK で始まり、その後に最低 5 つの数字が続きます。例えば、ID が 4321 のチケットは TICK:04321 と表示されます。特に、E メールの件名行でこの形式を使用すると、E メールが正しいチケットへのリンクで返信できるようになるので便利です。
$ticket_owner_email	チケットに割り当てられたサービスデスク管理者の E メールアドレス。
$ticket_owner_name	チケットに割り当てられたサービスデスク管理者の名前。 **注:** 所有者名および連絡先情報は、チケット上のフィールドに関連付けられたユーザーレコードから取得されます。
$ticket_owner_phone_home	チケットに割り当てられたサービスデスク管理者の連絡先情報。
$ticket_owner_phone_mobile	チケットに割り当てられたサービスデスク管理者の連絡先情報。
$ticket_owner_phone_pager	チケットに割り当てられたサービスデスク管理者の連絡先情報。
$ticket_owner_phone_work	チケットに割り当てられたサービスデスク管理者の連絡先情報。

トークン	説明
$ticket_priority	チケットに割り当てられた優先度。デフォルト値には高、中、低があります。
$ticket_resolution	チケットの Resolution（解決）フィールドで説明しているように、チケットを解決するために何を行ったかに関する情報。
$ticket_status	チケットのステータス。デフォルトには、新規作成、開かれた、閉じられた、Need More Info（追加の情報が必要）、Reopened（再度開かれた）、Waiting Overdue（待機の期限超過）、Waiting on Customer（お客様待ち）、Waiting on Third Party（サードパーティ待ち）があります。
$ticket_submitter_email	送信者の E メールアドレス。
$ticket_submitter_name	送信者の名前。 **注:** 送信者名および連絡先情報は、チケット上のフィールドに関連付けられたユーザーレコードから取得されます。
$ticket_submitter_phone_home	送信者の連絡先情報。
$ticket_submitter_phone_mobile	送信者の連絡先情報。
$ticket_submitter_phone_pager	送信者の連絡先情報。
$ticket_submitter_phone_work	送信者の連絡先情報。
$ticket_title	Ticket Detail（チケットの詳細）ページに表示されるとおりのチケットのタイトル。
$ticket_url	**ユーザーコンソール**でのチケットへのリンク。**ユーザーコンソール**へのアクセスには、ログイン資格情報が必要です。
$ticket_http_url	**ユーザーコンソール**でのチケットへのリンク。この形式は、旧式のシステムでの下位互換性のために使用されます。**ユーザーコンソール**へのアクセスには、ログイン資格情報が必要です。
$ticket_https_url	**ユーザーコンソール**でのチケットへのセキュアなリンク。アプライアンスで SSL が有効になっている場合に、このトークンを使用します。これにより、E メールで送信されるリンクが正しく機能するようになります。
$userui_url	**ユーザーコンソール**のホームページへのリンク。**ユーザーコンソール**へのアクセスには、ログイン資格情報が必要です。

マージされたチケット E メールテンプレートに使用されるトークン

トークン	説明
$ticket_merged_number	マージされたチケットの番号。
$ticket_merged_title	Ticket Detail（チケットの詳細）ページに表示されるとおりのマージされたチケットのタイトル。
$ticket_merged_changer_name	チケットをマージしたユーザーの名前。
$ticket_merged_url	**ユーザーコンソール**でのマージされたチケットへのリンク。**ユーザーコンソール**へのアクセスには、ログイン資格情報が必要です。

エラー関連の E メールテンプレートに使用されるトークン

トークン	説明
$error_text	送信したトークンの処理中に発生した問題を識別するために使用します。このエラーは、次の場合に表示されます。 • 変数が認識されない • 変数は認識されるものの、ユーザーにはフィールドを変更する権限がない • 変数がチケットの承認ステータスを変更しようとするものの、ユーザーが承認者ではない
$quoted_mail	元の E メールメッセージの内容。
$subject	元の E メールメッセージの件名。

注: 無効なトークンは無視され、E メールメッセージに再配置されません。例えば、$today など不明なトークンを追加した場合、それは無視され、そのまま $today として E メールメッセージに表示されます。

5. **オプション**：各 E メールテンプレートで、プレーンテキストを使用する代わりに HTML ベースのコンテンツを作成します。
   a. **HTML として送信** を選択して、書式なしのテキストではなく、HTML ベースの E メールを使用します。

      太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションをすべて備えた HTML エディタが表示されます。

   b. エディタのコントロールを使用して、テンプレートの内容を書式設定します。例：

   - 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。
   - イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファイルパスを指定するか、指定された領域にイメージをドロップします。
     - スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。
     - この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。
     - テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイルは、チケットページの 添付ファイル セクションで管理できます。詳細

については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。

- 外部リンクを追加するには、 をクリックします。
- 外部でホストされるビデオを埋め込むには、 をクリックします。

c. トークンをすばやく追加するには、 をクリックし、表示されたリストから該当するトークンを選択します。

各トークンの詳細については、手順 4 を参照してください。

6. テンプレートごとに、E メールの添付ファイルの処理方法を指定します。
   - サービスデスクが添付ファイルを送信できるようにするには、**添付ファイルを含める** を選択します。次に、送信する添付ファイルを指定します。
     - **最近の変更（該当する場合）**：最新のチケット更新で追加された添付ファイルのみを含めます。
     - **前回アップロード日**：最後にアップロードされた添付ファイルを含めます。
     - 「**すべて**」：すべての添付ファイルを含めます。
   - **サービスデスクがチケット関連の E メールで添付ファイルを送信できないようにするには、添付ファイルを含める チェックボックスをオフにします。**
7. **保存** をクリックします。

アプライアンスで SMTP E メールを使用するように設定する手順については、SMTP Eメールサーバーの設定を参照してください。

チケットカテゴリのための CC リストの設定

ハードウェアやソフトウェアやネットワークなど指定のカテゴリにチケットが提出されたら、そのことをユーザーまたはユーザーグループに自動的に通知できます。このためには、各チケットカテゴリの CCリスト 値に E メールアドレスを追加します。

カテゴリにチケットが提出されたら、そのカテゴリに関心を持つユーザーまたはユーザーグループに通知するようにする場合は、チケットカテゴリの CCリスト 値を設定すると便利です。例えば、ネットワークカテゴリの CCリスト にシステム管理者全員を追加して、ネットワークに問題が発生したら通知されるようにすることができます。

キューが複数ある場合は、キューごとに個別にチケットカテゴリ CCリスト 値を設定します。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。
      - キューの名前をクリックします。
      - **アクションの選択 > 新規作成** を選択します。
2. イベント発生時にEメールを送信 セクションで、カテゴリCC 列の全チェックボックスをオンにします。詳細については、「Eメールトリガの設定」を参照してください。
3. **保存** をクリックします。
4. チケットのデフォルト セクションで、**これらの値のカスタマイズ** をクリックします。
5. Category Values（ カテゴリ値 ） セクションで、CCリスト エントリに E メールアドレスを追加します。
   a. カテゴリ行の **編集** ボタンをクリックします 。

b. CCリスト フィールドに、対象のカテゴリのデフォルトEメールアドレスを入力します。コンマを使用して、Eメールアドレスを区切ります。複数のEメールアドレスを入力する場合は、配布リストの使用を検討します。
c. 行の最後で **保存** をクリックします。
d. その他のカテゴリについても、この手順を繰り返して CCリスト エントリを追加します。

6. ページの一番下で **保存** をクリックします。

チケット所有者のデフォルトの E メールアドレスを作成します。詳細については、「DefaultTicketOwnersアカウントの作成」を参照してください。

チケットの CC リストフィールドへの E メールアドレスの自動追加

サービスデスクを利用すると、E メールで送信または更新されたチケットの To フィールドおよび Cc フィールドに E メールアドレスが表示されるたびに、チケットの CCリスト フィールドにその E メールアドレスを自動的に追加するようにすることができます。

この設定が有効になっているときは、To フィールドおよび Cc フィールドの E メールアドレスがチケットの CC リスト フィールドに自動的に追加されます。ただし、そのアドレスが System Email Exclusion List（システム E メールの除外リスト）に指定されている場合を除きます。詳細については、「チケットの CC リストフィールドからのアドレスの除外」を参照してください。

注: バージョン 6.3 以前が動作するアプライアンスにサービスデスクを作成した場合、この設定はデフォルトで無効になります。一方、システムで組織コンポーネントが有効になっている場合に、新しい組織を作成すると、この設定はデフォルトで有効になります。この設定は、バージョン 6.4 以降が動作する新しい KACE SMA でも有効になります。

1. サービスデスクの 設定 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. 設定 パネルで **設定** をクリックします。
2. Inbound Email（インバウンド E メール）セクションで、Add email addresses from the CC List to ticket（CC リストからチケットに E メールアドレスを追加する）の隣にあるチェックボックスをオンにします。
3. **保存** をクリックします。

サービスデスクが不要な E メールアドレスをチケットの CCリスト フィールドに自動的に追加しないように E メール除外リストを設定します。詳細については、「チケットの CC リストフィールドからのアドレスの除外」を参照してください。

チケットの CC リストフィールドからのアドレスの除外

サービスデスクでは、チケットが E メールを通じて送信または更新されたときに、チケットの CCリスト フィールドに E メールアドレスを自動的に追加できます。ただし、配布リストや一般的な企業 E メールアドレスなど一部のアドレスは、不要な E メールトラフィックを増やすことになるため、自動的に追加する必要はありません。サービスデスクが不要な E メールアドレスを追加しないようにするには、除外する E メールアドレスを指定します。

E メール除外リストは、アプライアンスレベルの設定です。アプライアンス上で組織コンポーネントが有効化されている場合は、あらゆる組織およびサービスデスクキューに E メール除外リストが適用されます。

注: サービスデスクキューに関連付けられた E メールアドレスがチケットの CCリスト フィールドに自動的に追加されることはありません。これらのアドレスにメッセージを送信すると、新しいチケットが誤って開かれる可能性があるからです。これらのアドレスを除外リストに追加する必要はありません。

1. サービスデスクの 設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. 設定 パネルで **設定** をクリックします。
2. 受信Eメール セクションで、**システムのEメール除外リストを定義** をクリックして、システムEメールの除外リストの定義 ページを表示します。
3. リストに E メールアドレスを追加するには、追加 をクリックします。
4. Add Email（ E メールの追加 ）ダイアログで、E メールアドレスを入力し、**保存** をクリックします。

    E メールアドレスが除外リストに追加されます。

Eメールループの回避

Eメールによってチケットが提出またはアップデートされた場合、サービスデスクからは各参加者にチケットの通知が送られます。ただし、この通知メールを受け取った1人以上のユーザーから自動返信による不在の返信がきた場合は、サービスデスクは新たなアップデートチケットを付けて返信しますが、そのEメール通知が延々と続くEメールループの原因になる可能性があります。

不在の返信を受信した場合に、サービスデスクでEメールが処理されるのを回避することができます。チケットに関連するEメールを大量に受信していることが検出された場合に、Eメール通知の送信を中止するオプションもあります。サービスデスクからのEメール通知の送信を中止する要因となるEメールは、すべてログ記録されます。

1. サービスデスクの E メールプリファレンス ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルの E メール設定 セクションで、**サービスデスク E メール環境設定の構成** をクリックします。
2. Eメールの件名で検出するテキストを指定します。指定した件名のチケット関連のEメールを受信した場合に、サービスデスクはそのEメールの処理を中止します。
    a. 受信Eメール セクションの 件名に次のテキストが含まれるEメールは無視する フィールドで検出対象の言葉を入力します。セミコロンを区切り文字として使用し、複数のエントリを指定することができます。例：不在;メール送信失敗。
3. 特定の期間内でのすべての受信Eメール通知に対してしきい値を設定します。しきい値に達すると、サービスデスクはEメール通知の送信を中止します。

注: 全体がしきい値に達した場合、すべてのチケットの通知が停止します。チケットごとにしきい値に達した場合、該当するチケットの通知のみが停止します。所定期間内のEメールの更新件数が設定したしきい値よりも下回ると、通知が再開されます。

オプション	説明
合計Eメール数	サービスデスクが受信して返信するEメール通知に関するすべてのEメールの最大数。デフォルトでは100通です。

オプション	説明
x分の期間内に受信	指定した数のEメールが受信される分単位の期間。デフォルトは1分です。 この制限を無効にするには、この値を99999などのより大きな値に設定します。

4. 特定の期間に受信するチケット毎のEメール通知のしきい値を設定します。しきい値に達すると、サービスデスクはEメール通知の送信を中止します。

オプション	説明
チケット毎の合計Eメール数	チケット毎にサービスデスクが受信して返信するEメール通知に関するすべてのEメールの最大数。デフォルトではチケット毎に5通です。
x分の期間内に受信	チケット毎に受信する、指定した数のEメールが受信される分単位の時間間隔を指定します。デフォルトは1分です。この制限を無効にするには、このオプションを99999などのより大きな値に設定します。

5. **保存** をクリックします。

サービスデスクウィジェットのキャッシュライフタイムの設定

ダッシュボードページで利用可能なサービスデスクウィジェットにより、サービスデスクチケットの全体的なアクティビティに対する理解を深められます。例えば、アクティブなチケットの数が、カテゴリまたはキューごとに並び替えられ表示されます。パフォーマンス上の理由により、サービスデスクウィジェットの元になるデータは、一定期間ローカルにキャッシュされます。デフォルトの最小時間は 30 分です。これは、必要に応じて長くできます。ウィジェットの更新アイコンをクリックすると、特定のウィジェットのデータを強制的に更新できます。

ダッシュボードウィジェットの詳細については、ダッシュボードのウィジェットについてを参照してください。

1. サービスデスクの 設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. 設定 パネルで **設定** をクリックします。
2. サービスデスクダッシュボードウィジェットの下のキャッシュライフタイムフィールドで、サービスデスクダッシュボードウィジェットに生成されたデータがデータベースに保持される時間の長さを分単位で指定します。最小時間は 30 分です。
3. **保存** をクリックします。

組織の作成と管理

アプライアンス上で**組織**コンポーネントが有効化されている場合は、ビジネスニーズに合うように個別のインベントリと設定を持つ、個別の組織を作成および管理できます。

ヒント: 組織コンポーネントがアプライアンスで有効になっているが、ドロップダウンリストが**管理者コンソール**の右上隅（ログイン情報の隣）に表示されていない場合は、高速切り替えが有効化されていないか、または、組織を管理するための権限がユーザーの役割に付与されていない可能性があります。

ヒント: 詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。

組織について

組織は、単一のアプライアンスで動作するのアプライアンスの論理インスタンスです。各組織には専用のデータベースが用意されます。また、各組織のインベントリとその他のコンポーネントは別々に管理します。

例えば、学校という環境であれば、教員に対して1つの組織を、学生に対して別の組織を作成できます。管理対象デバイスを各組織に自動的に割り当て、個別に管理できます。さらに、組織固有の役割を管理者とユーザーに割り当て、アプライアンス**管理者コンソール**および**ユーザーコンソール**に対する管理者とユーザーのアクセスを制御できます。1つの組織の管理者は、その他の組織のデバイスおよびインベントリアイテムを表示する必要はありません。単一のアプライアンスに最大 50 個の組織を追加できます。

アプライアンスの一般的な組織設定については、組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定を参照してください。

「Default」組織について

「**Default**」という名前の組織は、アプライアンスを最初にセットアップしたときに使用できる唯一の組織です。フィルタによって組織に割り当てられていない新しいデバイスは、「Default」組織に割り当てられます。

「Default」組織の名前を変更し、必要に応じて設定を編集することができます。詳細については、「組織の追加または編集」を参照してください。

組織設定の変更追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

組織の役割とユーザーの役割の管理

アプライアンスで組織コンポーネントが有効化されている場合、2つのタイプの役割を使用できます。組織に割り当てられる組織の役割と、個々のユーザーアカウントに割り当てられるユーザーの役割です。

アプライアンスで組織コンポーネントが有効化されている場合、2つのタイプの役割を使用できます。組織に割り当てられる組織の役割と、個々のユーザーアカウントに割り当てられるユーザーの役割です。

このセクションでは、デフォルトの組織の役割とユーザーの役割、および組織の役割の管理方法について説明します。ユーザーの役割の管理の詳細については、ユーザーアカウントおよびユーザー認証についてを参照してください。

使用可能なデフォルトの役割

デフォルトの役割によって、組織およびユーザーのさまざまな権限設定が提供されます。

デフォルトで利用可能な役割は次の通りです。

役割	説明
組織の役割	組織の役割は、組織に割り当てられる権限のスーパーセットで、組織ユーザーが使用できる権限を定義します。例えば、配布 タブが非表示になっている組織の役割が組織に割り当てられている場合、その組織のユーザー（管理者ユーザーを含む）は、配布 タブにアクセスできません。 **注:** 組織の役割は、組織コンポーネントが有効になっているアプライアンスでのみ使用可能です。
デフォルト役割	組織の役割 セクションのデフォルト役割には、すべてのタブに対する読み取り/書き込み権限があります。追加の組織の役割を作成できますが、デフォルト役割を編集または削除することはできません。
ユーザーの役割	**管理者コンソール**および**ユーザーコンソール**へのアクセスを制御するためにユーザーに割り当てられた役割。アプライアンスで組織コンポーネントが有効になっている場合、これらの役割で利用できる権限は、組織に割り当てられている組織の役割によって決まります。
管理者	アプライアンスにおいて最も強力なユーザーの役割。デフォルトでは、**管理者**役割を割り当てられたユーザーには、情報および設定を表示または変更する権限が与えられます。例えば、役割を変更することで他のユーザーの昇格または降格が行えます。**管理者**役割は変更したり、削除したりすることはできません。この役割は、信頼された管理者のみに割り当ててください。 **管理者**役割を割り当てられたスタッフメンバーは、**管理者コンソール**の チケット タブでサービスデスクチケットを管理し、修正する権限を持ちますが、自分自身はチケットを所有できない場合があります。 **管理者**役割を持つユーザーも、セキュリティ、スクリプト作成、および配布機能を使用してサービスデスクチケットを解決し、サポート技術情報に問題の詳細を記録できます。 **管理者**役割は、主に**管理者コンソール**を通じてアプライアンスを操作します。
アクセス権限なし	この役割を割り当てられたユーザーは、**管理者コンソール**または**ユーザーコンソール**にログオンできません。

役割	説明
読み取り専用の管理者	この役割はアプライアンスの情報や設定を表示できますが、変更することはできません。この役割は、スーパーバイザなどの監督担当者向けとして便利です。 この役割は、主に**管理者コンソール**からアプライアンスを操作します。
ユーザーコンソールのみ	アプライアンスのユーザー用の役割です。デフォルトでは、この役割はサービスデスクチケットの作成、表示、および修正を行う権限を持ちます。 この役割は、**ユーザーコンソール**からのみアプライアンスを操作します。

組織の役割の追加または編集

組織の役割は、必要に応じて追加または編集できます。

組織を作成する前に、このセクションで説明する方法で、作成する組織に割り当てる組織の役割を作成する必要があります。組織の役割は、組織ユーザーが使用できる権限を定義します。

1. Organization Role Detail（組織の役割の詳細）ページに移動します。
    a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
    b. 左側のナビゲーションバーで、**組織** をクリックして、**役割** をクリックします。
    c. Organization Role Detail（組織の役割の詳細）ページを表示するには、次のいずれかを実行します。
    - 役割の名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。

    注: デフォルト役割は編集できません。
2. 次の情報を入力します。

オプション	説明
名前	（必須）役割の名前を入力します。

オプション	説明
説明	（オプション）役割の説明を入力します。

3. 管理者コンソールの権限を割り当てるには、次の手順を実行します。
   - **管理者コンソールの 権限 セクションで、コンポーネント名をクリックしてそのコンポーネントを展開するか、すべて展開 をクリックしてすべてのコンポーネントを展開します。**
   - **すべてのセクションに同じアクセスレベルを割り当てるには、すべて書き込み、すべて読み取り、または すべて非表示 を選択します。**
   - **セクションごとに異なるアクセスレベルを割り当てるには、カスタム オプションを選択してから、それぞれのセクションの名前の隣にあるドロップダウンリストで、アクセスレベルを選択します。**
4. ユーザーコンソールの権限を割り当てるには、次の手順を実行します。
   - **ユーザーコンソールの 権限 セクションで、ユーザーコンソール リンクをクリックして、権限セクションを展開します。**
   - **ユーザーコンソールのすべてのセクションに同じアクセスレベルを割り当てるには、すべて書き込み、すべて読み取り、または すべてを非表示 を選択します。**
   - **セクションごとに異なるアクセスレベルを割り当てるには、カスタム オプションを選択してから、それぞれのセクションの名前の隣にあるドロップダウンリストで、アクセスレベルを選択します。**
5. **保存** をクリックします。

注: 設定 の **一般** と **ユーザー認証** に対して**非表示**権限を割り当てた場合、コントロールパネル は非表示になります。

役割が 役割 ページに表示されます。組織を追加するときに、役割が 役割 ドロップダウンリストに表示されます。詳細については、「組織の追加、編集、および削除」を参照してください。

組織の役割の複製

組織の役割を複製するときに、そのプロパティが新しい役割にコピーされます。既存の役割とほぼ同じ役割を作成する場合、役割を複製することで、役割をゼロから作成するよりも素早く作成できます。

1. Organization Role Detail（組織の役割の詳細）ページに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左側のナビゲーションバーで、**組織** をクリックして、**役割** をクリックします。
   c. 役割の名前をクリックします。
2. ページの一番下で **複製** をクリックして、組織の詳細を複製します。

   ページが更新されます。
3. 次の情報を入力します。

オプション	説明
名前	（必須）役割の名前を入力します。

オプション	説明
説明	（オプション）役割の説明を入力します。

4. 管理者コンソールの権限を割り当てるには、次の手順を実行します。
   - **管理者コンソールの 権限 セクションで、コンポーネント名をクリックしてそのコンポーネントを展開するか、すべて展開 をクリックしてすべてのコンポーネントを展開します。**
   - **すべてのセクションに同じアクセスレベルを割り当てるには、すべて書き込み、すべて読み取り、または すべて非表示 を選択します。**
   - **セクションごとに異なるアクセスレベルを割り当てるには、カスタム オプションを選択してから、それぞれのセクションの名前の隣にあるドロップダウンリストで、アクセスレベルを選択します。**
5. ユーザーコンソールの権限を割り当てるには、次の手順を実行します。
   - **ユーザーコンソールの 権限 セクションで、ユーザーコンソール リンクをクリックして、権限セクションを展開します。**
   - **ユーザーコンソールのすべてのセクションに同じアクセスレベルを割り当てるには、すべて書き込み、すべて読み取り、または すべてを非表示 を選択します。**
   - **セクションごとに異なるアクセスレベルを割り当てるには、カスタム オプションを選択してから、それぞれのセクションの名前の隣にあるドロップダウンリストで、アクセスレベルを選択します。**
6. **保存** をクリックします。

役割の削除

デフォルト役割を除く組織の役割は、必要に応じて削除できます。デフォルト役割は削除できません。また、役割が組織に割り当てられている場合、その組織は削除できません。

以下の役割は削除できません。

- デフォルトの役割
- 組織に割り当てられた任意の役割
- ラベルに関連付けられている任意の役割

1. 役割 リストに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左側のナビゲーションバーで、**組織** をクリックして、**役割** をクリックします。
2. 1つ以上の役割の隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

組織の追加、編集、および削除

組織は、必要に応じて追加、編集、および削除することができます。また、「Default」組織の名前を変更し、設定を編集することができます。

組織の追加または編集

単一のアプライアンスに最大 50 個の組織を追加または編集できます。

組織を追加するとき、組織に対して組織の役割を割り当てる必要があります。デフォルト役割を使用できますが、カスタムの組織の役割を使用する場合は、組織を追加する前に、その役割を追加します。詳細については、「組織の役割の追加または編集」を参照してください。

1. 組織の詳細 ページに移動します。
    a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
    b. 左側のナビゲーションバーで、**組織** をクリックして、**組織** をクリックします。
    c. 組織の詳細 ページを表示するには、次のいずれかを実行します。

    - 組織の名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。

2. 組織を追加する場合、次の情報を入力し、**保存** をクリックします。

オプション	説明
名前	組織の名前を入力します。名前は必要に応じて後から修正できます。高速切り替え オプションが有効になっている場合は、ページの右上隅にあるドロップダウンリストにこの名前が表示されます。詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。
説明	組織の説明。説明は必要に応じて後から修正できます。
役割	組織に割り当てるユーザーの役割。このセクションは必要に応じて後から修正できます。 **注:** 役割を作成するには、**組織 > 役割** の順に選択します。
クライアントドロップサイズ	組織のクライアントドロップの場所のファイルサイズフィルタ。 クライアントドロップの場所は、アプライアンス上にある組織のストレージエリア（ SAMBA 共有 ）です。このストレージエリアは、アプリケーションインストーラーやアプライアンスバックアップファイルなどの大規模ファイルをアプライアンスにアップロードするために使用されます。クライアントドロップの場所へのファイルのアップロードは、大規模ファイルではブラウザがタイムアウトする可能性がある、**管理者コンソール**でデフォルトの HTTP メカニズムを使用してファイルをアップロードする方法の代わりになります。 Client Drop Size（ クライアントドロップサイズ ）フィルタにより、組織のクライアントドロップの場所にアップロードされるファイルを Software Detail（ ソフトウェア詳細 ） ページの Upload and Associate Client Drop File（ クライアントドロップファイルのアップロードと関連付け ） リストに表示するかどうかを決定します。例えば、Client Drop Size（ クライアントドロップサイズ ） フィルタを 1 GB に設定すると、Upload and Associate Client Drop File（ クライアントドロップファイルのアップロードと関連付け ） リストにはサイズが 1 GB 以上

オプション	説明
	のファイルが表示されます。サイズが 1 GB 未満のファイルは、リストに表示されません。 Software Detail（ソフトウェア詳細）ページでアプリケーションファイルを選択して保存すると、そのファイルは組織のクライアントドロップの場所から適切なエリアに移動します。 クライアントドロップの場所に配置されるアプライアンスバックアップファイルは、アプライアンスバックアップファイルとして自動的に識別され、5 分以内に バックアップ設定 ページで選択できるようになります。 組織が複数ある場合は、組織ごとに独自のクライアントドロップの場所および Client Drop Size（クライアントドロップサイズ）フィルタ設定があります。詳細については、「アプライアンスクライアントドロップの場所へのファイルのコピー」を参照してください。

3. 次の情報を追加、編集、または表示します。

オプション	説明
名前	必要に応じて組織の名前を変更します。高速切り替え オプションが有効になっている場合は、ページの右上隅にあるドロップダウンリストにこの名前が表示されます。詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。
ロケール	組織の**ユーザーコンソール**と**管理者コンソール**に使用する言語。
仮想ホスト名	この組織の固有ドメイン名。このフィールドが設定されていて、指定された場所からアプライアンスにログインする場合、この組織はアプライアンスによって自動的に選択されるため、ユーザー資格情報を提供するだけで済みます。セキュリティアサーションマークアップ言語（SAML）ログインを使用する場合、構成された仮想ホスト名は、その組織のアイデンティティプロバイダ（IdP）に直接ログインします。SAML ログインの詳細については、「シングルサインオン用に SAML を構成する」を参照してください。
仮想ホスト IP	この組織の一意の IP アドレス。このフィールドが設定されていて、指定された場所からアプライアンスにログインする場合、この組織はアプライアンスによって自動的に選択されるため、ユーザー資格情報を提供するだけで済みます。SAML ログインを使用する場合、構成済みの仮想ホスト IP アドレスを使用すると、その組織の IdP に直接ログインします。SAML ログインの詳細については、「シングルサインオン用に SAML を構成する」を参照してください。

オプション	説明
説明	組織の説明。説明は必要に応じて後から修正できます。
データベース名	（読み取り専用）組織が使用しているデータベースの名前を表示します。
レポートユーザー	（読み取り専用）レポートの生成に使用されるユーザー名。ユーザー名のレポートを使用すると、書き込み権限を与えることなく、データベースへのアクセスを可能にできます（追加のレポート作成ツールを提供）。
レポートユーザーのパスワード	レポートユーザーのパスワード。このパスワードは、レポート作成システムおよびMySQLのみによって使用されます。
役割	組織に割り当てるユーザーの役割。このセクションは必要に応じて後から修正できます。 **注:** 役割を作成するには、**組織 > 役割** の順に選択します。
クライアントドロップサイズ	組織のクライアントドロップの場所のファイルサイズフィルタ。 クライアントドロップの場所は、アプライアンス上にある組織のストレージエリア（SAMBA 共有）です。このストレージエリアは、アプリケーションインストーラーやアプライアンスバックアップファイルなどの大規模ファイルをアプライアンスにアップロードするために使用されます。クライアントドロップの場所へのファイルのアップロードは、大規模ファイルではブラウザがタイムアウトする可能性がある、**管理者コンソール**でデフォルトの HTTP メカニズムを使用してファイルをアップロードする方法の代わりになります。 Client Drop Size（クライアントドロップサイズ）フィルタにより、組織のクライアントドロップの場所にアップロードされるファイルを Software Detail（ソフトウェア詳細）ページの Upload and Associate Client Drop File（クライアントドロップファイルのアップロードと関連付け）リストに表示するかどうかを決定します。例えば、Client Drop Size（クライアントドロップサイズ）フィルタを 1 GB に設定すると、Upload and Associate Client Drop File（クライアントドロップファイルのアップロードと関連付け）リストにはサイズが 1 GB 以上のファイルが表示されます。サイズが 1 GB 未満のファイルは、リストに表示されません。 Software Detail（ソフトウェア詳細）ページでアプリケーションファイルを選択して保存すると、そのファイルは組織のクライアントドロップの場所から適切なエリアに移動します。 クライアントドロップの場所に配置されるアプライアンスバックアップファイルは、アプライアンスバックアップファイルとして自動的に識別され、5

オプション	説明
	分以内に バックアップ設定 ページで選択できるようになります。 組織が複数ある場合は、組織ごとに独自のクライアントドロップの場所および Client Drop Size（クライアントドロップサイズ）フィルタ設定があります。詳細については、「アプライアンスクライアントドロップの場所へのファイルのコピー」を参照してください。
フィルタ	アプライアンスへのデバイスのチェックイン時に新しいデバイスを組織に割り当てるために使用するフィルタ。複数のフィルタを選択するには、**Ctrl** キーを押しながらクリックするか、**Command** キーを押しながらクリックします。
デバイス	（読み取り専用）組織に割り当てるデバイスの数を表示します。

4. 次の設定を指定します。

注: アプライアンスへの負荷を軽減する場合は、エージェントの接続数を 1 時間あたり 500 までに制限します。インベントリ、スクリプト作成、およびメータリング間隔の隣に表示される接続数は、現在の組織のみに適用されます。アプライアンスで組織コンポーネントが有効化されている場合は、すべての組織のエージェント接続の合計数を1時間あたり500より多くしないでください。

オプション	設定案	メモ
エージェントのログ記録	有効	管理対象デバイスにインストールされたエージェントから提供されるスクリプト結果を、アプライアンスが保存するかどうか。エージェントログは、データベース内のディスク領域を最大約1 GB消費します。ディスク領域に問題がない場合は、エージェントのログ記録 を有効にして、エージェント管理対象デバイスのログ情報をすべて保持します。これらのログは、トラブルシューティング時に役立ちます。ディスク領域を節約し、エージェント通信を高速化するには、エージェントのログ記録 を無効にします。
エージェントのデバッグトレース	有効	選択した場合、このオプションを使用してエージェントのデバッグトレースを記録できます。この情報を使用すると、管理者はエージェントのパフォーマンスを監視して一般的な問題を診断できます。
エージェントインベントリ	12時間	管理対象デバイスのエージェントがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。

オプション	設定案	メモ
エージェント不要インベントリ	1日	エージェント不要デバイスがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
カタログインベントリ	24時間	管理対象デバイスが ソフトウェア カタログ ページにインベントリをレポートする頻度。
メータリング	4時間	管理対象デバイスがアプライアンスにメータリング情報をレポートする頻度。デバイスとアプリケーションに対してメータリングを有効にする必要があります。
スクリプト更新	4時間	管理対象デバイスのエージェントが、管理対象デバイスで有効にされているスクリプトの更新されたコピーを要求する頻度。この間隔はスクリプトの実行頻度に影響を与えません。
最大ダウンロード速度	必要に応じて	必要に応じた最大ダウンロード速度。使用可能なオプションから選択します。
プロセスのタイムアウト	1 時間	エージェントプロセスが終了するまでの最大実行時間。詳細については、https://support.quest.com/kb/177093/how-to-allow-more-time-for-a-kace-script-to-run-before-it-times-out-を参照してください。
起動を待機 タスクを無効にする	無効	選択した場合、このオプションによってエージェントで起動タスクが実行されなくなります。
ログインを待機 タスクを無効にする	無効	選択した場合、このオプションによってエージェントでログインタスクを実行しないようになります。

5. エージェントステータスアイコンの設定 セクションで、各設定を次のように指定します。

オプション	設定案	メモ
デバイスでのエージェントのステータス アイコン	有効	このオプションを選択すると、管理対象デバイス上でエージェントのステータスを表示できます。
デバイスでのエージェントの再通知	有効	このオプションを選択すると、管理対象デバイス上のエージェントのシステムトレイ（Windows）またはメニューバー（Mac OS）を

オプション	設定案	メモ
		使用したアクティビティを一時停止できます。 **注:** インベントリ、レプリケーションタスク、緊急アラートなど、一部の重要なバックグラウンドタスクは引き続き実行できます。
エージェントの再通知の最大数（1 日あたり）	1 回の再通知	管理対象デバイスで 1 日にエージェントを再通知できる最大回数。
エージェントステータスアイコンのショートカット	必要に応じて	このセクションを使用して、エージェント管理対象デバイスの KACE エージェントメニューにリンクを表示します。最大 10 個のリンクを指定できます。https、ssh、ftp URL など、標準の統一資源位置指定子（URI）リンクがサポートされています。リンクを追加するには、次の手順を実行します。 a. ＋ をクリックします。 b. 表示名 列に、メニューに表示するテキストを入力します。たとえば、マイ FTP リンクなどです。 c. URL 列に、完全修飾 URL アドレスを入力します。例：https://www.quest.com/。URL では、次の置換変数がサポートされています。 ◦ $(KACE_SYS_DIR) ◦ $(KACE_MAC_ADDRESS) ◦ $(KACE_IP_ADDRESS) ◦ $(KACE_SERVER_URL) ◦ $(KACE_SERVER) ◦ $(KACE_COMPANY_NAME) ◦ $(KACE_KUID) ◦ $(KACE_APP_DIR) ◦ $(KACE_DATA_DIR) ◦ $(KACE_AGENT_VERSION) これらの変数およびその他の置換変数の詳細については、「トークン置換変数」を参照してください。 列見出しを使用してリストを並べ替えできます。KACE エージェン

オプション	設定案	メモ
		トメニューには、このページに表示される順序でリンクが表示されます。

注: このセクションで行った変更は、個々のエージェントまたはアプライアンスを再起動した後に、管理対象デバイス上の KACE エージェントがアプライアンスに再接続した後でのみ有効になります。

6. 通知 セクションで、エージェント通信に使用するメッセージを指定します。

オプション	設定案	メモ
エージェントのスプラッシュページのメッセージ	デフォルトのテキストは次の通りです。 **KACE システム管理アプライアンス** は、PC 設定の検証およびソフトウェア更新プログラムの管理を行います。お待ちください…	エージェントがデバイス上でスクリプト実行などのタスクを実行しているときに、ユーザーに表示されるメッセージ。
エージェントのスプラッシュビットマップ	必要に応じて	スプラッシュロゴとして使用する既存の.bmpファイルへのパス。
起動スプラッシュを無効にする	無効	選択した場合、このオプションによってエージェントは起動スプラッシュロゴを表示しなくなります。
ログインスプラッシュを無効にする	無効	選択した場合、このオプションによってエージェントはログインスプラッシュロゴを表示しなくなります。

7. エージェント不要の設定 セクションで、エージェント不要デバイスの通信設定を次のように指定します。

オプション	説明
SSHタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
SNMPタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
再試行回数	接続が試行される回数。
WinRMタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
VMwareのタイムアウト	VMwareホスト上で実行しているVMware vSphere APIに接続する際の待機時間（秒単位）。

8. エージェント不要の設定 セクションで、エージェント不要デバイスの通信設定を次のように指定します。

オプション	説明
SSHタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。

オプション	説明
SNMPタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
再試行回数	接続が試行される回数。
WinRMタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
VMwareのタイムアウト	VMwareホスト上で実行しているVMware vSphere APIに接続する際の待機時間（秒単位）。

9. **保存** をクリックします。

   組織が追加されます。「組織の高速切り替え」が有効で、デフォルトの **admin** アカウントのパスワードがシステムと組織の両方で同じ場合は、ページの右上隅にあるドロップダウンリストを使用して組織とシステムを切り替えることができます。リストに新しい組織を表示するには、**管理者コンソール**からログアウトした後、再度ログインする必要があります。また、ログイン時に組織の選択を要求するオプションは、システムレベルで有効化されます。組織は、管理者コンソールのログインページ（http://appliance_hostname/admin）のドロップダウンリストで選択できます。ここで、**appliance_hostname** は、アプライアンスのホスト名です。

   注: 新しい組織の場合、デフォルト **admin** アカウントのパスワードは、システムレベルのデフォルト **admin** アカウントのパスワードと同じです。これは自動的に割り当てられます。**管理者**アカウントのパスワードを変更するには、管理者ユーザーアカウントを編集します。

   注: ただし、**admin** アカウントのパスワードが異なる組織間では、ページの右上隅にあるドロップダウンリストから**高速切り替え**を実行することができません。

システムレベルの設定の詳細については、組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定を参照してください。

関連トピック

組織フィルタの管理

アプライアンスログの表示

組織のユーザーアカウントの管理

組織のための 2 要素認証の設定

2 要素認証（2FA）は、ログインプロセスにさらにステップを追加することで、ユーザーがアプライアンスにログインするためのセキュリティを強化します。これは、Google Authenticator アプリケーションに依存して検証コードを生成します。このアプリは、定期的に新しい 6 桁のコードを生成します。有効にすると、エンドユーザーはログインするたびに現在の検証コードを要求されます。

Google Authenticator アプリケーションをダウンロードするには、必要に応じて、次のいずれかのサイトをご覧ください。

- **Android デバイス**： https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- **iOS デバイス**： https://itunes.apple.com/ca/app/google-authenticator/id388497605?mt=8

以下で説明しているように、**システム管理コンソール**を使用して、1 つまたは複数の組織の**管理者コンソール**および**ユーザーコンソール**への 2FA アクセスを有効または無効にすることができます。また、**管理者コンソール**の 2 要素認証 ページを使用して、組織内のすべてのユーザーについて**管理者コンソール**および**ユーザーコンソール**への 2FA アクセスを有効にできます。詳細については、「すべてのユーザーに対して 2 要素認証を有効にする」を参照してください。

1. 組織 リストページに移動します。

a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
b. 左側のナビゲーションバーで、**組織** をクリックして、**組織** をクリックします。

2. 表示される 組織 リストページで、2FA を設定する組織を 1 つ以上選択します。
3. 管理者コンソールで選択した組織のすべてのユーザーに対して 2FA を有効にするには、**アクションを選択 > 2 要素認証 > 管理ポータル > すべてのユーザーに必須** をクリックします。
4. 管理者コンソールで選択した組織のすべてのユーザーに対して 2FA を無効にするには、**アクションを選択 > 2 要素認証 > 管理ポータル > 必須でありません** をクリックします。
5. ユーザーコンソールで選択した組織のすべてのユーザーに対して 2FA を有効にするには、**アクションを選択 > 2 要素認証 > ユーザーポータル > すべてのユーザーに必須** をクリックします。
6. ユーザーコンソールで選択した組織のすべてのユーザーに対して 2FA を無効にするには、**アクションを選択 > 2 要素認証 > ユーザーポータル > 必須でありません** をクリックします。

組織の削除

必要に応じて組織を削除できます。ただし、アプライアンスの組織が1つの場合は、別の組織を追加するまでその組織を削除することはできません。アプライアンスには、常に、少なくとも1つの組織が必要です。

1. 組織の詳細 ページに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左側のナビゲーションバーで、**組織** をクリックして、**組織** をクリックします。
   c. 組織の名前をクリックします。
2. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

組織と、その組織データベースに存在する情報がアプライアンスから削除されます。

ユーザーコンソールと組織レポートに使用するロゴのカスタマイズ

ユーザーコンソールと組織レポートに表示されるロゴを会社のブランド設定に合わせて変更できます。

ユーザーコンソール、および**管理者コンソール**を通じて組織にログインしているときに実行するレポートは、デフォルトでは、Quest のロゴを使用します。独自のロゴをアップロードするには、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定の ロゴのオーバーライド セクションを参照してください。

組織のユーザーアカウントの管理

組織ユーザーアカウントを使用することで、ユーザーは、アカウントに割り当てられた役割に基づいて、**管理者コンソール**、**ユーザーコンソール**、およびサービスデスクの機能にアクセスできます。

ユーザー認証にLDAPサーバーを使用することも、手動でユーザーアカウントを追加して編集することもできます。詳細については、以下を参照してください。

- 組織ユーザーアカウントの管理
- システムレベルユーザーアカウントの管理
- LDAPサーバーを使用したユーザー認証

注意: **組織のデフォルト admin アカウントのパスワードを変更する際は注意してください。admin アカウントのパスワードが異なる組織間では、ページの右上隅にあるドロップダウンリストから高速切り替えを実行することができません。**

注意: **詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。**

組織フィルタの管理

組織フィルタでは、デバイスがインベントリ設定されると、デバイスが組織に割り当てられます。

組織フィルタは、ラベルに似ていますが、固有の用途も持っています。組織フィルタでは、デバイスがインベントリ設定されると、デバイスが自動的に組織に割り当てられます。

組織フィルタには2つのタイプがあります。

- **データフィルタ**: 検索条件に基づいて、デバイスを自動的に組織に割り当てます。デバイスがインベントリ設定されるときに、デバイスが条件を満たしている場合は、デバイスが組織に割り当てられます。このフィルタは、デバイスが指定された条件と一致する場合に自動的に組織にデバイスを割り当てるという点で、Smart Labelに似ています。
- **LDAPフィルタ**: LDAPまたはActive Directoryとの対話に基づいて、デバイスを自動的に組織に割り当てます。デバイスがインベントリ設定されると、クエリがLDAPサーバーに対して実行されます。デバイスが条件を満たすと、組織に自動的に割り当てられます。

組織フィルタを追加または編集する方法については、次を参照してください。

- 組織データフィルタの追加または編集
- 組織LDAPフィルタの追加または編集

フィルタの追加後、組織の詳細 ページの組織にフィルタを関連付けることができます。詳細については、「組織の追加、編集、および削除」を参照してください。

組織フィルタの仕組み

組織では複数のフィルタを使用できますが、同じフィルタを複数の組織に割り当てることはできません。

組織フィルタは次のルールに従って実行されます。

- デバイスがインベントリ設定されると、それに対して1つ以上のフィルタが実行されます。複数のフィルタがある場合は、フィルタの詳細の「**優先順位**」または「**評価優先順位**」の番号に従って実行されます。
- デバイスが条件を満たすと、組織に割り当てられます。
- デバイスが条件を満たさない場合は、「Default」組織に割り当てられます。その後、管理者は、デバイスを「Default」組織から適切な組織に手動で移動できます。詳細については、「デバイスのリダイレクト」を参照してください。

組織データフィルタの追加または編集

組織データフィルタを追加または編集して、デバイスを組織に自動的に割り当てることができます。

1. 組織フィルタの詳細 ページに移動します。
    a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
    b. 左側のナビゲーションバーで、**組織** をクリックして、**フィルタ** をクリックします。

c. 組織フィルタの詳細 ページを表示するには、次のいずれかを実行します。

- フィルタの名前をクリックします。
- **アクションの選択 > 新しいデータフィルタ** を選択します。

2. 次の情報を入力します。

オプション	説明
有効	フィルタが有効になっているかどうか。フィルタを適用するには、フィルタを有効にする必要があります。
名前	フィルタの名前。この名前は、組織フィルタ リストに表示されます。
説明	フィルタの説明。
優先順位	フィルタの実行順序。フィルタは指定した番号に従って実行されます。小さい番号は、大きい番号より先に実行されます。

3. **デバイスフィルタ基準** セクションで、フィルタ基準を選択します。
   a. 最上行の一番左のドロップダウンリストからデバイスの属性を選択します。

   例：**IPアドレス** を選択します。

   ヒント: アプライアンスは IPv6（インターネットプロトコルバージョン 6）と IPv4 アドレスの両方をサポートします。

   b. 2番目のドロップダウンリストから条件を選択します。

   例えば、**次の値を含む** を選択します。

   c. テキストボックスに属性の値を入力します。

   例えば、サブネット全体（67.18.250.255）など、指定されたIPアドレス範囲からデバイスを検索するには、ワイルドカードとしてパーセント記号（%）を使用します。例：67.18.250.%。

   d. **オプション**：属性を追加するには、2番名の行の一番左のドロップダウンリストから演算子（**[and]** など）を選択します。

   その行のフィールドがアクティブになります。

   e. **オプション**：基準セクションに行を追加するには、**基準の追加** をクリックします。

   追加行が表示されます。

4. **保存** をクリックします。

組織LDAPフィルタの追加または編集

LDAPフィルタを追加して、LDAP基準により、デバイスを組織に自動的に割り当てることができます。

注: LDAPサーバーが、管理ログイン（つまり非匿名のログイン）の資格情報を必要とする場合は、資格情報を提供します。ユーザーとパスワードが指定されていない場合、ツリー検索は実行されません。LDAPフィルタごとに、異なるLDAPサーバーに接続される可能性があります。

1. 組織フィルタの詳細 ページに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左側のナビゲーションバーで、**組織** をクリックして、**フィルタ** をクリックします。

c. 組織フィルタの詳細 ページを表示するには、次のいずれかを実行します。

- LDAPフィルタの名前をクリックします。
- **アクションの選択 > 新しいLDAPフィルタ** を選択します。

2. 次の情報を入力します。

オプション	説明
有効	フィルタが有効になっているかどうか。フィルタを適用するには、フィルタを有効にする必要があります。
名前	フィルタの名前。この名前は、組織フィルタ リストに表示されます。
説明	フィルタの説明。
評価優先順位	フィルタの実行順序。フィルタは指定した番号に従って実行されます。小さい番号は、大きい番号より先に実行されます。

3. LDAP基準を指定します。

オプション	説明
LDAPサーバ	LDAPサーバーのIPアドレスまたはホスト名。IPアドレスが有効でない場合は、タイムアウトするまで待たなければならず、その結果LDAP認証中にログイン遅延が発生します。 **注:** SSL経由で接続するには、IPアドレスまたはホスト名を使用します。例：ldaps://hostname。
ポート	LDAPポート番号。通常は、389（LDAP）または636（セキュアLDAP）です。
ベースDN	デバイスのメインの場所をフィルタするためのLDAP基準。 この基準によって、LDAPまたはActive Directory構造における場所またはコンテナを指定します。識別するすべてのデバイスをこの基準に含める必要があります。基準を満たすOU、DC、またはCNの最も明確な組み合わせを入力します（一番左は最も限定的、一番右は最も一般的です）。例えば、このパスが、識別対象となるデバイスが属するコンテナを指している場合は、次の通りです。 OU=computers,DC=company,DC=com
高度な検索	検索フィルタ。例： (&(objectCategory=Computer)(sAMAccountName=KBOX_COMPUTER_NAME))
LDAPログイン	アプライアンスが LDAP サーバにログインして、アカウントを読み取るために必要なアカウントの資格情報です。例：

オプション	説明
	LDAP Login:CN=service_account,CN=Users,DC=company,DC=com ユーザー名を指定していない場合は、匿名のバインドが試みられます。LDAPラベルごとに、異なるLDAPまたはActive Directoryサーバーに接続することが可能です。
LDAP パスワード	アプライアンスが LDAP サーバにログインするために必要となるアカウントのパスワードです。

フィルタ処理中に、アプライアンスはすべての KBOX_ 定義変数をそれぞれの実行時値に置き換えます。

組織デバイスフィルタで現在サポートされている変数は、次の通りです。

KBOX_COMPUTER_NAME
KBOX_COMPUTER_DESCRIPTION
KBOX_COMPUTER_MAC
KBOX_COMPUTER_IP
KBOX_USER
KBOX_USER_DOMAIN
KBOX_DOMAINUSER

外部サーバの管理ログイン（または非匿名ログイン）について資格情報が必要な場合は、それらの資格情報を指定してください。LDAP ユーザー名を指定していない場合は、匿名のバインドが試みられます。LDAP フィルタごとに、異なる LDAP/AD サーバに接続される可能性があります。

注: フィルタをテストするには、KBOX_変数を実際の値に置き換えてください。**テスト** をクリックし、結果を確認します。

4. **保存** をクリックします。

組織フィルタのテスト

組織フィルタをテストして、期待通りの結果が得られるかどうかを確認できます。

1. 組織の デバイス リストに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左側のナビゲーションバーで、**組織** をクリックして、**デバイス** をクリックします。
2. ページの右側にあるリストの上の **組織フィルタのテスト** タブをクリックします。
3. **フィルタの選択** ドロップダウンリストでフィルタを選択します。
4. **テスト** をクリックします。

テスト結果が表示されます。必要に応じて、リストに表示されたデバイスを再フィルタリングできます。詳細については、「デバイスのフィルタリング」を参照してください。

注: テスト結果にデバイスが表示されない場合は、既存のデバイスの中に基準に一致するものがないか、基準が無効になっているかのいずれかです。基準を編集するには、組織データフィルタの追加または編集を参照してください。

組織フィルタの削除

組織フィルタは、組織と関連付けられていない場合に限り、削除できます。

1. 組織 リストに移動します。
   a. アプライアンスシステム管理コンソール（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。

b. 左側のナビゲーションバーで、**組織** をクリックして、**組織** をクリックします。

2. フィルタが組織に関連付けられている場合:
   a. 組織の名前をクリックして、組織の詳細 ページを表示します。
   b. フィルタ フィールドで、削除するフィルタの隣にある **x** をクリックします。
   c. ページの一番下で **保存** をクリックします。

   保存 をクリックした後でないと、フィルタは更新されません。

   フィルタが組織に関連付けられていない場合 :
3. **組織 > フィルタ** をクリックして、組織フィルタ ページを表示します。
4. フィルタを削除するには、次のいずれかを行います。
   - **1つまたは複数のフィルタの横にあるチェックボックスをオンにして、アクションの選択 > 削除 を選択します。**
   - **フィルタのリンク名をクリックし、組織フィルタの詳細 ページで 削除 をクリックします。**
5. **はい** をクリックして確定します。

組織内のデバイスの管理

組織に割り当てられているデバイスの検索、フィルタリング、およびリダイレクトを行うことができます。

高度な検索の使用

キーワード検索よりも細かい条件で検索したい場合は、高度な検索を使用できます。高度な検索を使用すると、インベントリレコードに表示されている各フィールドの値を指定し、その値のインベントリリスト全体で検索できます。

例えば、特定バージョンのBIOSがインストールされたデバイスを特定し、それらの影響のあるデバイスのみをアップグレードする必要がある場合、BIOS情報を検索できます。詳細については、「高度なオプションによるページレベルの検索」を参照してください。

ヒント: 検索結果に表示されたデバイスにフィルタを適用できます。

デバイスのフィルタリング

組織フィルタがある場合は、デバイスをフィルタリングして、フィルタが正しく適用されているかどうかを確認できます。

1. 組織のデバイス リストに移動します。
   a. アプライアンスシステム管理コンソール (http://**appliance_hostname**/system) にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左側のナビゲーションバーで、**組織** をクリックして、**デバイス** をクリックします。
2. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
3. **アクションの選択 > フィルタの適用** を選択します。

   選択したデバイスが、既存フィルタに照らして確認されます。デバイスが組織に再割り当てされると、組織 列にある古い組織名の隣に新しい組織名が表示されます。

デバイスのリダイレクト

必要に応じてデバイスを組織にリダイレクトしたり、手動で再割り当てしたりすることができます。

例えば、組織**A**に割り当てられているデバイスを、組織**B**のインベントリに表示されるように、組織**B**に手動でリダイレクトできます。

1. 組織のデバイス リストに移動します。
    a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
    b. 左側のナビゲーションバーで、**組織** をクリックして、**デバイス** をクリックします。
2. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
3. **アクションの選択 > 割り当て** を選択し、組織名を選択します。これにより、選択したデバイスがその組織にリダイレクトされるようになります。

デバイスの詳細について

システムレベルの 組織 セクションの デバイスの詳細 ページには、組織に割り当てられているデバイスに関する詳細情報が表示されます。

組織 セクションの デバイスの詳細 ページにアクセスするには、アプライアンスのシステムレベルに移動して、**組織 > デバイス** を選択し、リストでデバイス名を選択します。デバイスの詳細については、インベントリ情報の管理を参照してください。

各組織レポートと総合レポートの実行

アプライアンス上で組織コンポーネントが有効化されている場合に、アプライアンス上に複数の組織が存在する時には、各組織の組織レポートを個別に実行できます。また、すべての組織の情報を単一レポートに表示する総合レポートも実行できます。

レポートを作成する方法の詳細については、レポートの作成を参照してください。

アプライアンスリソースのインポートとエクスポート

アプライアンス上の組織間でリソースを転送できます。複数のアプライアンスを使用している場合は、アプライアンス間でもリソースを転送できます。

リソースのインポートとエクスポートについて

管理対象インストール、Smart Labelなどのリソースは、組織およびアプライアンス間でインポートやエクスポートを行うことができます。

複数の KACE SMA を使用している場合は、アプライアンスに組み込まれている SAMBA 共有ディレクトリを使用することにより、アプライアンス間でリソースを転送できます。同様に、アプライアンスで組織コンポーネントが有効化されている場合は、組織間でリソースを転送できます。これは、ある組織のために作成されたものであるが、他の組織でも利用可能なリソース（ スクリプトなど ）を転送する場合に便利です。

インポートおよびエクスポートできるリソースは、以下の通りです。

- 通知
- 管理対象インストール
- レポート
- スクリプト
- Smart Label
- ソフトウェア
- サービスデスクプロセス、チケットキュー、およびチケットルール

SAMBA共有ディレクトリを使用したアプライアンス間でのリソースの転送

SAMBA共有ディレクトリをステージング領域として使用することにより、アプライアンス間でリソースを転送できます。

これを行うには、転送元のアプライアンスからリソースをエクスポートし、それを転送先のアプライアンスにインポートします。

アプライアンスからのリソースのエクスポート

アプライアンスからリソースをエクスポートして、他のアプライアンスにインポートできるようにします。

1. リソースが置かれているアプライアンスの管理者コンソールにログインします。
2. SAMBA共有によるファイル共有を有効にします。

   詳細については、「システムレベルでのファイル共有の有効化」を参照してください。
3. 共有リソース リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**リソース** の順にクリックします。
   c. リソースパネル で **エクスポート** をクリックします。
4. **オプション**：リストをフィルタリングするには、右側のテーブルの上に表示される 特定基準で表示 ドロップダウンリストと 検索 フィールドを使用します。

   例えば、特定基準で表示 ドロップダウンリストからリソースを選択して、対象のリソースカテゴリのみを表示させたり、検索 フィールドにキーワードを入力して、そのキーワードに一致するアイテムのみを表示させたりできます。
5. 1つ以上のリソースの隣のチェックボックスをオンにします。
6. 次のいずれかを実行します。
   - **アクションの選択 > ローカル共有へのエクスポート**
   - **アクションの選択 > ネットワーク共有へのエクスポート**

注: データをネットワーク上の共有場所に保存し、他のデバイスからアクセスできるようにするには、**ネットワーク共有へのエクスポート** を選択します。データをデバイス上の場所に保存し、そのデバイスからのみアクセスできるようにするには、**ローカル共有へのエクスポート** を選択します。

7. **オプション**：エクスポートされたリソースに注釈を付ける ページで、追加したい情報を **メモ** フィールドに入力します。
8. **保存** をクリックします。

   エクスポート対象のリソースは、まず、リソース共有ステータス ページに表示されます。この時点では、ステータス が 要求の新規作成 となっています。

エクスポートが完了すると、ステータス が 完了 に変更されます。エクスポートしたリソースがSAMBA共有でインポート可能な状態になります。詳細については、「組織へのリソースのインポート」を参照してください。

ほとんどのインポート/エクスポートタスクはすぐに完了しますが、非常に大きいリソースの場合には時間がかかります。

アプライアンスへのリソースのインポート

必要に応じて、リソースをアプライアンスにインポートできます。

アプライアンスからリソースをエクスポートしていること。詳細については、「SAMBA共有ディレクトリを使用したアプライアンス間でのリソースの転送」を参照してください。

1. SAMBA共有ディレクトリの場所を確認するには、以下のいずれかを実行します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、設定 > セキュリティ設定 を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、ページの右上隅にあるドロップダウンリストから組織を選択して、設定 > 一般設定 を選択します。**
2. サードパーティ製ファイルコピーユーティリティを使用して、**エクスポート側**のアプライアンスのSAMBA共有ディレクトリから、**インポート側**のアプライアンスのSAMBA共有ディレクトリにリソースをコピーします。
3. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
4. **インポート側**のアプライアンスで、**設定 > リソース** を選択して、リソースパネルを表示します。
5. **インポート** をクリックすると、Import Appliance Resources（アプライアンスリソースのインポート）ページに、インポート可能なアプライアンスリソースがすべて表示されます。
6. **アクションの選択 > ネットワーク共有からのインポート** を選択して SAMBAディレクトリからのリソースのインポート ページを表示します。
7. インポートするリソースを選択して、**リソースのインポート** をクリックします。

   インポート対象のリソースは、まず、リソースマネージャキュー ページに表示されます。この時点では、ステータス が 要求の新規作成 となっています。

インポートが完了すると、ステータス が 完了 に変更されます。インポートされたリソースが使用可能となり、レポート作成 などの各タブに表示されます。

ほとんどのインポート/エクスポートタスクはすぐに完了しますが、非常に大きいリソースの場合には時間がかかります。

組織間でのリソースの転送

アプライアンスで組織コンポーネントが有効化されている場合は、組織からリソースをエクスポートし、それを別の組織にインポートすることにより、組織間でリソースを転送できます。

組織からのリソースのエクスポート

組織からリソースをエクスポートして、他の組織にインポートできるようにします。

1. ページの右上で、リソースをエクスポートする組織を選択します。
2. リソースのエクスポート リストに移動します。
    a. 左のナビゲーションバーで **設定**、**リソース** の順にクリックします。
    b. リソースパネル で **エクスポート** をクリックします。

    エクスポート可能な組織リソースの一覧が記載された リソースのエクスポート ページが表示されます。
3. 1つ以上のリソースの隣のチェックボックスをオンにします。
4. **アクションの選択 > ローカル共有へのエクスポート** または **ネットワーク共有へのエクスポート** を選択して、エクスポートされたリソースに注釈を付ける ダイアログを表示します。
5. **オプション**：追加したい情報がある場合は、メモ フィールドに入力してください。
6. **保存** をクリックします。

    エクスポート対象のリソースは、まず、リソースマネージャキュー ページに表示されます。この時点では、ステータス が 「要求の新規作成」となっています。

エクスポートが完了すると、ステータス が 完了 に変更されます。エクスポートしたリソースがアプライアンス上の他の組織にインポート可能な状態になります。手順については、組織へのリソースのインポートを参照してください。

ほとんどのインポート/エクスポートタスクはすぐに完了しますが、非常に大きいリソースの場合には時間がかかります。

組織へのリソースのインポート

必要に応じて、リソースを組織にインポートできます。

組織からリソースをエクスポートしていること。詳細については、「組織間でのリソースの転送」を参照してください。

別のアプライアンスからアプライアンスリソースをインポートする場合は、SAMBA共有ディレクトリを使用したアプライアンス間でのリソースの転送の手順に従ってください。

1. ページの右上隅にあるドロップダウンリストから、リソースをインポートする組織を選択します。
2. リソースのインポート リストに移動します。
    a. 左のナビゲーションバーで **設定**、**リソース** の順にクリックします。
    b. リソースパネル で **インポート** をクリックします。
3. 1つ以上のリソースの隣のチェックボックスをオンにします。
4. **アクションの選択 > ローカル共有からのインポート** を選択します。

    インポート対象のリソースは、まず、リソース共有ステータス ページに表示されます。この時点では、ステータス が 要求の新規作成 となっています。

インポートが完了すると、ステータス が 完了 に変更されます。インポートされたリソースが使用可能となり、レポート作成 などの各タブに表示されます。

ほとんどのインポート/エクスポートタスクはすぐに完了しますが、非常に大きいリソースの場合には時間がかかります。

エクスポートするリソースのシステムレベルでの管理

アプライアンス上で組織コンポーネントが有効化されている場合、エクスポートするリソースまたは共有リソースをシステムレベルで管理できます。

このため、エクスポートされたリソースまたはアプライアンス上の組織から共有できるようになったリソースにアクセスできます。

共有リソースの表示または削除

アプライアンス上で組織コンポーネントが有効化されている場合、アプライアンス上の組織からエクスポートされたリソースを参照できます。

1. 共有リソース リストに移動します。
    a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
    b. 左のナビゲーションバーで **設定**、**リソース** の順にクリックします。
    c. **共有** をクリックします。
2. リソースを削除するには
    a. 1つ以上のリソースの隣のチェックボックスをオンにします。
    b. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

ローカルアプライアンスからネットワーク上の場所への共有リソースの移動

アプライアンス上で組織コンポーネントが有効化されている場合、ローカルアプライアンスからネットワーク共有に共有リソースを移動できます。

1. 共有リソース リストに移動します。
    a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
    b. 左のナビゲーションバーで **設定**、**リソース** の順にクリックします。
    c. **共有** をクリックします。
2. **アクションの選択** > **ネットワーク共有へのエクスポート** を選択し、**はい** をクリックして確定します。

リソースエクスポートのステータスの表示または削除

アプライアンス上で組織コンポーネントが有効化されている場合、システムレベルで組織からエクスポートされたリソースのステータスを参照できます。

ステータス情報は24時間後に削除されますが、必要に応じてステータスを手動で削除できます。

1. リソース共有ステータス リストに移動します。
    a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
    b. 左のナビゲーションバーで **設定**、**リソース** の順にクリックします。
    c. リソースパネル で **ステータス** をクリックします。
2. ステータスを削除するには
    a. ステータスの隣のチェックボックスをオンにします。

b. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

インベントリの管理

アプライアンスを使用して、インベントリ内のデバイス、ソフトウェア、プロセス、およびサービスを管理できます。

インベントリダッシュボードの使用

インベントリダッシュボードには、選択した組織（該当する場合）またはアプライアンスの管理対象デバイスの概要が表示されます。

アプライアンスで組織コンポーネントが有効化されており、管理者コンソール（http://**appliance_hostname**/admin）にログインしている場合は、インベントリダッシュボードに選択した組織の情報が表示されます。

ユーザーアカウントに関連付けられた 1 つまたは複数の役割によってこのダッシュボードへのアクセス権が与えられている場合は、インベントリダッシュボードにアクセスできます。非表示にする場合は、必要に応じて、ユーザーの役割を編集します。詳細については、「ユーザーの役割の追加または編集」を参照してください。

ヒント: アプライアンスは、概要ウィジェットを定期的に更新します。任意の時間にほとんどのウィジェットを更新するには、ページの右上にある **更新** ボタンをクリックします：。ほとんどのウィジェットを個々に更新するには、ウィジェットの上にマウスを置き、ウィジェットの上の **更新** ボタンをクリックします。一部のウィジェットでは、追加の手順が必要になる場合があります。

インベントリダッシュボードウィジェットについて

インベントリダッシュボードウィジェットでは、選択に応じて、組織またはアプライアンスの管理対象デバイスの概要が示されます。

このセクションでは、インベントリダッシュボード で使用可能なウィジェットについて説明します。アプライアンス上で組織コンポーネントが有効化されている場合は、ウィジェットに選択した組織の情報が管理者レベルで表示され、アプライアンスの情報がシステムレベルで表示されます。

このダッシュボードでは、デバイスの使用率の高レベルな概要を示します。このダッシュボードを使用すると、デバイスの状態をすばやく確認し、デバイスのインベントリを改善するためのインジケータを見つけられます。例えば、デバイスのディスク容量に重点を置き、最も必要とされているところにリソースを割り当て直すことができます。

ウィジェット	説明
デバイスレポート	このウィジェットには、一般的なインベントリレポートへのリンクがあります。これらのリンクを使用して、メモリごとのデバイス、OS ごとのデバイス など、特定のレポートを迅速に生成します。
接続	このウィジェットには、アプライアンス Web サーバへの接続の数が表示されます。高い数値はサーバーに高い負荷がかかっていることを示し、これによってアプライアンスの応答速度が低下する場合があります。アプライアンスで組織コンポーネントが

ウィジェット	説明
	有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
デバイスチェックイン率	このウィジェットには、過去 60 分間にアプライアンスに接続したデバイスの数が表示されます。アプライアンス上で組織コンポーネントが有効化されている場合、このウィジェットはシステムレベルで利用可能になります。
プロビジョニング	このウィジェットには、KACE エージェントのプロビジョニングまたはインストールタスクのステータスが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ショートカット	このウィジェットには、一般的なインベントリページとウィザードへのリンク含まれています。これらを使用して、エージェントのプロビジョニングアシスタント、検出スケジュール ページなど、特定のページにすばやく移動します。
エージェントバージョン数	このウィジェットには、各バージョンのエージェント数が表示されます。この情報は、アップグレード時に役立つ場合があります。
インベントリ数	このウィジェットでは、エージェント管理、エージェントレスなどの、各デバイス管理方法に関連付けられているデバイスの数が表示されます。また、過去 8 時間に更新されたエージェントの数も表示されます。
ディスク容量ごとのデバイス	このウィジェットにはドーナツグラフが表示され、それぞれの部分は管理対象デバイスの空きディスク領域の割合を表します。ウィジェットのタイトルをクリックすると、関連付けられてたデバイスへのリンクを含むレポートが表示されます。円グラフのそれぞれの部分の上にマウスを置くと、選択した空きディスク領域の割合に対応する管理対象デバイスの割合が表示されます。例えば、円グラフの赤い部分の上にマウスを置くと、空きディスク領域が 25% 未満のデバイスの割合が表示されます。
管理対象オペレーティングシステム	このウィジェットには、各オペレーティングシステムを実行中の管理対象デバイスの割合が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、このウィジェットには、選択した組織のデバイスの割合が表示されます。
プロビジョニングプラットフォーム	このウィジェットには、エージェント管理対象デバイスにインストールされているオペレーティングシステムの割合が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。

ウィジェット	説明
デバイス (製造元別)	このウィジェットには、デバイスインベントリに表示されている主なデバイスの製造元が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、このウィジェットには、選択した組織のデバイスの割合が表示されます。
デバイス (モデル別)	このウィジェットには、デバイスインベントリに表示されている主なデバイスのモデルが表示されます。アプライアンスで組織コンポーネントが有効になっている場合、このウィジェットには、選択した組織のデバイスの割合が表示されます。
メモリごとのデバイス	このウィジェットには棒グラフが表示され、それぞれの棒はインストールされている RAM ごとのデバイスの数を表します。
プロセッサごとのデバイス	このウィジェットには棒グラフが表示され、それぞれの棒は固有のプロセッサ設定ごとのデバイスの数を表します。
サブタイプごとのデバイス	このウィジェットにはドーナツグラフが表示され、それぞれの部分は管理対象デバイスのサブタイプ別デバイスの割合を表します。
VMware デバイス数	このウィジェットには、vCenter、ESXi ホスト、仮想マシン、プロビジョニングされた仮想マシンなど、各 VMware デバイスタイプの数が表示されます。ウィジェットのタイトルをクリックすると、デバイス リストページが表示されます。
VMware デバイスレポート	このウィジェットには、5 つの一般的な VMware インベントリレポートへのリンクが含まれます。ウィジェットのタイトルをクリックすると、仮想インフラストラクチャ フィルタが適用された レポート リストページが表示されます。
ステータス別の VMware ESXi デバイス	このウィジェットには、ESXi デバイスの現在のステータスを示すドーナツグラフが表示されます。可能な値には、次の 4 つがあります。OK、警告、エラー、および 不明。ウィジェットのタイトルをクリックすると、現在のステータス別にすべての ESXi デバイスを一覧表示する新しい VMware インベントリレポートが表示されます。
VMware ESXi バージョン数	このウィジェットには、上位 5 つの ESXi バージョンの数が表示されます。ウィジェットのタイトルをクリックすると、バージョン別にすべての ESXi デバイスを表示する新しい VMware インベントリレポートが表示されます。

インベントリダッシュボードのカスタマイズ

インベントリダッシュボードをカスタマイズして、必要に応じて、ウィジェットを表示または非表示にできます。

1. インベントリダッシュボードに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. ウィジェットの上にマウスを置き、次のボタンのいずれかを使用します。
    -  : ウィジェットの情報を更新します。
    -  : ウィジェットに関する情報を表示します。
    -  : ウィジェットを非表示にします。
    -  : ウィジェットのサイズを変更します。
    -  : ウィジェットをページ上の別の場所にドラッグできます。
3. ページの右上隅にある **カスタマイズ** ボタンをクリックすると、使用可能なウィジェットが表示されます。
4. 現在非表示のウィジェットを表示するには、**インストール** をクリックします。

デバイス検出の使用

デバイス検出を使用して、ネットワークに接続されているデバイスを識別し、それらのデバイスに関する情報を取得します。

検出結果を使用して、デバイスにラベルを付けたり、デバイスをインベントリに追加したりできます。

デバイス検出とデバイス管理について

検出可能なデバイスには、ノートPC、デスクトップ、サーバー、モバイルデバイス、仮想デバイス、プリンタ、ネットワークデバイス、ワイヤレスアクセスポイント、ルーター、スイッチなどがあります。

これらのデバイスは、デバイス上に KACE エージェントがインストールされていなくても識別できます。検出スキャンはオンデマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。

検出結果には、デバイスの利用可否と詳細情報が表示されます。デバイスを検出した後、次の手順でデバイスをインベントリに追加できます。

- **デバイスでの KACE エージェントのインストール**。KACE エージェントは、Windows、Mac®、Red Hat®、SUSE®、Ubuntu® デバイスにインストールできます。詳細については、「KACE エージェントのプロビジョニング」を参照してください。
- **デバイスのエージェント不要管理の有効化**。エージェント不要管理は、サポート対象外のオペレーティングシステムを持つデバイスなど、デバイスに KACE エージェントをインストールできない場合に特に役立ちます。詳細については、「エージェント不要デバイスの管理」を参照してください。

検出設定の変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

ネットワーク上のデバイスの検出

デバイスを検出するには、検出スケジュールを作成して、ネットワークをスキャンできます。検出スケジュールは、スキャン中に使用するプロトコル、スキャンするIPアドレス範囲、およびスキャンの頻度を指定します。

検出スキャンから何を求めているか、およびどのデバイスで作業しているかに応じて、さまざまな検出タイプから選択できます。

- **「何をどこで」高速検出**：詳細については、「ネットワークの「何をどこで」高速スキャンを実行する検出スケジュールの追加」を参照してください。
- **詳細検出**：このタイプの検出を使用すると、「何をどこで」タイプよりも多くのデバイス情報を取得できます。詳細については、「Windows、Mac、Linux、および UNIX 管理対象コンピューターの詳細スキャンの検出スケジュールの追加」を参照してください。
- **外部統合の検出**：Windows ベースでも Mac OS X ベースでも Linux ベースでもない特定のコンピューターデバイス向けの異なるタイプの詳細検出。詳細については、次を参照してください。
  - KACE Cloud Mobile Device Manager デバイスの検出スケジュールの追加
  - G Suiteデバイスへの検出スケジュールの追加
  - Workspace ONE デバイスの検出スケジュールの追加
- **コンピューター以外の検出**：詳細については、「コンピューター以外の SNMP 対応デバイスの検出スケジュールの追加」を参照してください。

1つのサブネット内または複数のサブネットにまたがって、デバイスをスキャンすることができます。特定のポートをリッスンするデバイスを検索するよう、スキャンを定義することもできます。

検出スケジュールを追加するときは、ネットワークやアプライアンスに過度の負荷がかからないように、調査の深度（スキャンする属性の数）とスキャンのスコープ（スキャンする IP アドレスの数）のバランスを調整する必要があります。例えば、多くのIPアドレスを頻繁にスキャンする必要がある場合は、ポート数、TCP/IP接続数などを比較的少なく設定します。一般に、特定のサブネットをスキャンする頻度は、数時間に1回以下です。

ネットワークの「何をどこで」高速スキャンを実行する検出スケジュールの追加

使用可能なスケジュールの1つを使用して、どのデバイスが利用可能かを表示する検出結果をすばやく取得します。

このタイプの検出は、管理対象コンピューターやコンピューター以外のデバイスも含め、ネットワーク内のすべてのデバイスタイプをスキャンします。

Nmap 検出スケジュールを追加する場合に考慮が必要な複数の問題があります。詳細については、「Nmap検出についての考慮事項」を参照してください。

1. 検出スケジュールの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。

c. **アクションの選択 > 新規作成** を選択します。

2. 検出タイプ を選択して、選択したタイプのオプションを含むフォームを表示します。

   選択したタイプに応じて、次のオプションが 通知 セクションの前に表示されます。

   - **Ping**。「DNS参照」と「Ping」の検出オプションが表示されます。
   - **ソケット**。「DNS参照」と「ソケット」の検出オプションが表示されます。
   - **Active Directory**。「DNS参照」と「Active Directory」の検出オプションが表示されます。
   - **外部統合 [KACE Cloud Mobile Device Manager、G Suite、Workspace ONE]**。KACE Cloud Mobile Device Manager、G Suite、および Workspace ONE の検出オプションが表示されます。

     注: 外部統合から検出されたすべてのデバイス（KACE Mobile Device Manager、G Suite、Workspace ONE デバイス）は、アプライアンスのライセンス数の上限の計算には含まれません。

   - **認証済み [WinRM、SNMP、SSH、VMware、Hyper-V]**。DNS参照、リレー、WinRM、Hyper-V、VMM、SNMP、SSH および VMware 検出オプションが表示されます。
   - **Nmap**。「DNS参照」と「Nmap」の検出オプションが表示されます。
   - **カスタム**。DNS 参照、Ping、**Nmap**、WinRM、SNMP、SSH、および VMware 検出オプションが表示されます。

3. 名前 フィールドに、スキャンの名前を入力します。

   この名前は、検出スケジュール ページに表示されます。

4. IP Address Range（IP アドレス範囲）フィールドに、スキャンする IP アドレス範囲を入力します。ハイフンを使用して個々のIPアドレスクラス範囲を指定します。例えば、192.168.2-5.1 から 192.168.2-5.200 までのそれぞれの値を含むすべての IP アドレスをスキャンするには、192.168.2-5.1-200 と入力します。

   ヒント: アプライアンスは IPv6（インターネットプロトコルバージョン 6）と IPv4 アドレスの両方をサポートします。

   注意: 最大 25,000 件の IP アドレスがサポートされます。25,000 アドレスより多くなる IP 範囲を指定した場合、プロビジョニングスケジュールを保存しようとすると、警告が表示されます。

5. 検出オプションを選択します。選択した検出タイプに応じて表示されるオプション:

オプション	アイテム	説明
DNS参照		デバイス名を識別するために検出を有効化します。DNS参照は、検出結果とインベントリリストにデバイス名を表示する場合は重要です。各検出タイプに対して、DNS参照 オプションを選択します。
	参照対象の名前サーバー	ネームサーバーのホスト名またはIPアドレス。 **ヒント:** アプライアンスは IPv6（インターネットプロトコルバージョン 6）と IPv4 アドレスの両方をサポートします。

オプション	アイテム	説明
	タイムアウト	DNS参照がタイムアウトになるまでの時間（秒単位）。この時間内にアドレスが見つからない場合、プロセスは「タイムアウト」となります。
リレー		KACE エージェントが、WinRM、SSH、およびSNMP 検出スケジュールのエージェント接続プロトコル、エージェント不要インベントリ、およびエージェントのプロビジョニングに対して、トンネルWinRM、SSH および SNMP トラフィックとして動作させることができます。
	リレーデバイス	エージェント不要デバイスインベントリのリレーとして使用するデバイスを指定します。 検出中にリレーとして使用されるリレーデバイスは、検出結果から新しいデバイスが自動的にプロビジョニングされるとき、エージェント不要インベントリに使用されます。 選択したリレーデバイスは、次のページにリストされます。 • エージェント不要デバイス接続の詳細 ページ（検出結果から新しいデバイスが自動的にプロビジョニングされるとき）。このページの詳細については、「デバイス情報の手動入力によるエージェント不要管理の有効化」を参照してください。 • プロビジョニングスケジュールの詳細 ページ（エージェントのプロビジョニングが検出結果から開始されるとき）詳細については、「単一または複数のデバイスへの KACE エージェントのインストール」を参照してください。 • エージェント不要デバイス接続の詳細 ページ（検出結果から新しいデバイスが自動的にプロビジョニングされるとき）。このページの詳細については、「デバイス情報の手動入力によ

オプション	アイテム	説明
		るエージェント不要管理の有効化」を参照してください。
ping		ネットワークスキャン中にpingテストが実行されます。このテスト中、アプライアンスはpingテストを送信して、システムが応答するかどうかを確認します。
ソケット		ネットワークスキャン中に接続テストが実行されます。このテスト中にパケットがポートに送信され、ポートが開いているかどうかを判定します。
	TCPポートリスト	TCP（伝送制御プロトコル）を使用したポートのスキャンを可能にします。コンマを使用して、各ポート番号を区切ります。
	UDPポートリスト	UDP（ユーザーデータグラムプロトコル）を使用したポートのスキャンを可能にします。コンマを使用して、各ポート番号を区切ります。
Active Directory		アプライアンスでActive Directoryサーバー上のデバイス情報を確認できるようにします。Active Directoryスキャン中のステータスは、スキャンしたデバイス数ではなく、おおよそのパーセントで示されます。
	セキュア LDAP（LDAPS）を使用	アプライアンスが LDAP 通信にセキュアポートを使用できるようにします。
	特権のあるユーザー	Active Directoryサーバーの管理者アカウントのユーザー名。例:「username@example.com」。
	特権のあるユーザーのパスワード	Active Directoryサーバーの管理者アカウントのパスワード。
	コンテキストの検索	デバイスの検索に使用される条件。この条件は、検索するActive Directory構造内の場所またはコンテナを指定します。基準を満たすOU、DC、またはCNの最も明確な組み合わせを入力します（一番左は最も限定的、

オプション	アイテム	説明
		一番右は最も一般的です）。 例：DC=company,DC=com。
KACE Cloud Mobile Device Manager		このオプションを使用すると、KACE Cloud Mobile Device Manager（MDM）に接続されたスマートフォンやタブレットなどのモバイルデバイスにアクセスできます。KACE Cloud MDM に関連付けられたデバイスにアクセスするには、KACE Cloud MDM からテナント名とシークレットキーを取得する必要があります。
	テナント名	KACE Cloud MDM で管理しようとしているデバイスに関連付けられたテナントの名前です。
	資格情報	KACE Cloud MDM デバイスに接続するために使用されるアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。 詳細については、「シークレットキー資格情報の追加および変種」を参照してください。
	デバイスの自動プロビジョニング	選択した場合、次のスキャンで検出されたすべてのモバイルデバイスがインベントリに追加されます。 **注:** 予期しない範囲までインベントリが展開するのを避けるため、このオプションは注意して使用してください。
G Suite		G Suite デバイスを使用するには、Admin SDK の API を使用して Google Apps ドメインへのアクセス権をアプライアンスに付与する資格情報が必要です。Google からクライアント ID とクライアントシークレットを取得して、使用するアプライアンスの承認コードを取得できるようにする必要があります。
	Chromeデバイスの検出	選択した場合、Chromeデバイスは次のスキャン時に検出されます。

オプション	アイテム	説明
	モバイルデバイスの検出	選択した場合、G Suiteモバイルデバイスは次のスキャン時に検出されます。
	資格情報	Chromeデバイスに接続するために使用されるアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。選択した資格情報は適切なデバイスタイプに関連付けられる承認コードが必要です。例えば、G Suiteモバイルデバイスを検出する場合、Chromeデバイス用の承認コードが生成された資格情報は使用できません。 詳細については、「Google Workspace 資格情報の追加および編集」を参照してください。
	デバイスの自動プロビジョニング	選択した場合、次のスキャンで検出されたすべてのChromeおよびモバイルデバイスがインベントリに追加されます。 **注:** 予期しない範囲までインベントリが展開するのを避けるため、このオプションは注意して使用してください。
Workspace ONE		VMware ® Workspace ONE® では、企業レベルのモビリティ管理プラットフォームで、さまざまなデバイスタイプを管理できます。
	ホスト	Workspace ONE 管理コンソールのホスト名。
	REST APIキー	Workspace ONE 管理コンソールで使用できる REST API キー。このキーは、API 呼び出しを介して Workspace ONE と統合可能にするために必要です。
	資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。

オプション	アイテム	説明
		「ユーザーとパスワード資格情報の追加および編集」を参照してください。
	デバイスの自動プロビジョニング	選択した場合、次のスキャンで検出されたすべての Workspace ONE デバイスがインベントリに追加されます。 **注:** 予期しない範囲までインベントリが展開するのを避けるため、このオプションは注意して使用してください。
WinRM、Hyper-V、VMM		WinRMは、Windowsデバイスに対して使用する接続タイプです。
	タイムアウト	時間（秒単位、最大1分）。この時間内にアクティビティがないと接続が切断されます。
	Kerberosが必要	選択した場合、認証にはKerberosが必要です。Kerberos を使用できない場合に、代替認証として NTLM は使用されません。 Kerberosを使用するには、同じ検出設定でDNS参照を有効にする必要があります。DNS サーバは、ローカルアプライアンスネットワーク設定でも必要になります。
	Hyper-V および Virtual Machine Manager のスキャン	このオプションを選択すると、アプライアンスがエージェント不要管理を使用して、Microsoft Hyper-V または System Center Virtual Machine Manager インフラストラクチャをインポートします。この機能の詳細については、「Microsoft Hyper-V または System Center Virtual Machine Manager の検出スケジュールの追加」を参照してください。
	ポート	このフィールドを空白のままにした場合、デフォルトポートの5985が使用されます。
	資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。

オプション	アイテム	説明
		「ユーザーとパスワード資格情報の追加および編集」を参照してください。
SNMP		SNMP（簡易ネットワーク管理プロトコル）は、ネットワーク上の管理対象デバイスを監視するためのプロトコルです。
	SNMPの完全なウォーク	デバイスのMIB（管理情報ベース）データの完全なウォークを有効化します。このオプションをオフにすると、3つのコアOID（オブジェクト識別子）を検索するBULK GETが実行されます。このオプションを選択すると、完全なウォークは各デバイスにつき最大20分かかる場合があります。デフォルトのBULK GETは約1秒で検出に必要な情報をすべて取得します。 **重要: SNMPのインベントリウォークは、Windowsデバイスで英語以外の文字をサポートしていません。英語以外の文字が出現すると、SNMPのインベントリプロセスでエラーが報告され、インベントリ情報のロードが中止されます。**
	タイムアウト	時間（秒単位）。この時間内に応答がないとスキャンが終了します。
	最大試行回数	接続が試行される回数。
	資格情報（SNMPv1/v2）	デバイスに接続してコマンドを実行するために必要な SNMP v1/v2 資格情報の詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。 「SNMP資格情報の追加および編集」を参照してください。
	資格情報（SNMPv3）	デバイスに接続してコマンドを実行するために必要な SNMP v3 資格情報の詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。

オプション	アイテム	説明
		「SNMP資格情報の追加および編集」を参照してください。
SSH		認証には SSH プロトコルを使用します。 **重要: SSH 経由の検出は Windows デバイスではサポートされていません。** **重要: 検出スケジュールを保存した後に、SSH 認証を SNMP 認証に変更することはできません。**
	タイムアウト	時間（最大5分）。この時間内にアクティビティがないと接続が切断されます。
	SSH2接続の試行	デバイスへの接続と通信にSSH2プロトコルを有効化します。 デバイスとの通信をよりセキュアにするにはSSH2を使用します（推奨）。
	資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。 「ユーザーとパスワード資格情報の追加および編集」を参照してください。
VMware	タイムアウト	時間。この時間内に応答がないとスキャンが終了します。
	資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。 「ユーザーとパスワード資格情報の追加および編集」を参照してください。

オプション	アイテム	説明
Nmap		**注:** 4 つの Nmap 検出タイプのうちの複数を同時に実行することはできますが、お勧めしません。実行時間が長くなる可能性があり、誤ったOS検出の結果につながる可能性があります。
	タイムアウト	時間。この時間内に応答がないとスキャンが終了します。
	高速スキャン	アプライアンスが一般的に使用される100のポートを短時間でスキャンできるようにします。このオプションをオフにすると、すべての利用可能なTCPポートがスキャンされ、高速スキャンよりもはるかに長い時間がかかります。
	NMapオペレーティングシステムの検出（最適な推測）	フィンガープリントとポート情報に基づいて、デバイスのオペレーティングシステムを検出できるようにします。このオプションにより、スキャンに時間が長くかかる可能性があります。
	TCPポートスキャン	TCP（伝送制御プロトコル）を使用した、一般的に使用される1000のTCPポートのポートスキャンを可能にします。このオプションをオフにしてUDPを選択すると、UDPスキャンが実行されます。TCPとUDPどちらもクリアにすると、TCPスキャンが使用されます。 このオプションを選択する場合、エラー発生の可能性を低くするために、「タイムアウト」値を10分に設定することをお勧めします。 このスキャンと「高速スキャン」オプションを併用しないでください。そうすることにより、一般的に使用される100のポートのみがスキャンされることになります。
	UDPポートスキャン	UDP（ユーザーデータグラムプロトコル）を使用した、最大1000のUDPポートのポートスキャンを可能にします。一般にUDPスキャンは、TCPスキャンより信頼性が低く、プロセッサオーバーヘッドも低いです。これはTCPではデバイスとの通信にハンドシェイクが必要なのに対して、UDPは必要ではないためです。しかし、UDPス

オプション	アイテム	説明
		キャンはTCPスキャンより長い時間がかかる可能性があります。これはUDPがポートを検出するために複数のパケットを送信するのに対して、TCPは1つのパケットを送信するためです。 このオプションを選択する場合、エラー発生の可能性を低くするために、「タイムアウト」値を30分に設定することをお勧めします。 このスキャンと「高速スキャン」オプションを併用しないでください。そうすることにより、一般的に使用される100のポートのみがスキャンされることになります。 このオプションをオフにすると、ポートのスキャンにUDPは使用されません。

6. **オプション**：検出スキャン完了の通知先となるEメールアドレスを入力します。このEメールには、検出スケジュールの名前が記載されます。
7. スキャンスケジュールを指定します。

ヒント: スキャンを行わずにスキャンインベントリを維持するには、スキャンスケジュールの設定で「**なし**」を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59)

オプション	説明
	値の指定は次の要領で行います。 • **スペース ( )**：各フィールドはスペースで区切ります。 • **アスタリスク (*)**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

8. **保存** をクリックします。

関連トピック

検出結果について

検出結果の表示および検索

実行中の検出スキャンの停止

検出スケジュールの削除

Nmap検出についての考慮事項

Nmap検出で正しい結果を得るには、速度と正確性を向上させ、問題を避けるために、考慮する必要のある項目と、適用する必要のあるベストプラクティスがいくつかあります。

検出の速度と正確性を向上させるためのベストプラクティス

Nmap検出の速度と正確性を向上させるためのベストプラクティス：

- **DNS参照の使用を避けます。**DNS参照を使用した場合、DNSに無効または到達不可なIPアドレスを指定すると、スキャン時間が最大500%遅くなる可能性があります。
- **一度に1つの検出タイプを実行します。**複数の検出タイプを同時に実行できますが、そのような場合、実行時間が長くなり、誤ったOS検出が発生する可能性があります。
- **実行する検出タイプが不明な場合は、Nmapオペレーティングシステム検出（最適な推測）を選択します。**これを選択すると、1 つ以上のサブネットを簡易的に確認できます。少なくとも、最適な推測により、どのデバイス上にどのOSが搭載されているかを識別できます。期待した結果が得られない場合、例えば、一部のデバイスの「オペレーティングシステム」が「不明」と表示される場合は、タイムアウト値を増やして、検出を再実行してみてください。
- **検出は、VPNを介した場合、正常に機能しません。**デバイスへのアクセスに別のソースを使用します。

検出を妨げる可能性のある問題

スキャン時にオフラインであるなどの理由でアクセスできないデバイスは、存在しないと認識されるため、無視されることに注意してください。

レポートされると想定されるにもかかわらず、レポートされないデバイスがある場合は、次のいずれかのことが考えられます。

- ファイアウォールによってブロックされている
- ping をアクティブにブロックしている
- 実際にオフラインである（電源が入っていない）
- さまざまな方法を通してフィンガープリントが解除されている

デバイスによっては（通常はセキュリティデバイス）、検出を避けるために、デバイス自体を非表示にしたり、表示を偽ったりする場合があります。

オペレーティングシステムが「不明」と表示される問題のトラブルシューティング

「オペレーティングシステム」が、検出結果 リストページで「不明」と表示された場合は、次のようにします。

- Nmapのチェックマークが Nmap 列にあるかどうかを確認します。ない場合、そのデバイスはスキャン中オフラインであったため、オペレーティングシステムが特定されませんでした。
- Nmapのチェックマークが存在するが、「オペレーティングシステム」が不明な場合、最も可能性のある原因は、Nmapがデバイス上で実行されているOSの特定に使用するポートをブロッキングしているファイアウォールです。

  例えば、UDPポート7と161のみを使用してスキャンすると、デバイスはオンラインと表示され、そこにはNmapのチェックマークが表示されます。ただし、UDPポートだけではデバイス上で実行されているOSの特定には十分でないため、「オペレーティングシステム」が「不明」と表示されます。

Windows、Mac、Linux、および UNIX 管理対象コンピューターの詳細スキャンの検出スケジュールの追加

ネットワークでデバイスをスキャンし、デバイスに関する情報を取得するには、検出スケジュールを使用します。Active Directory または認証済みの検出タイプを使用してデバイスを検出した後、検出したそれらのデバイスをインベントリに追加できます。

1. 検出スケジュールの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。
c. **アクションの選択 > 新規作成** を選択します。

2. 検出タイプ を選択して、選択したタイプのオプションを含むフォームを表示します。

   選択したタイプに応じて、次のオプションが 通知 セクションの前に表示されます。

   - **Active Directory**。「DNS参照」と「Active Directory」の検出オプションが表示されます。
   - **認証済み [WinRM、SNMP、SSH、VMware、Hyper-V]**。DNS参照、リレー、WinRM、Hyper-V、VMM、SNMP、SSH および VMware 検出オプションが表示されます。

3. 名前 フィールドに、スキャンの名前を入力します。

   この名前は、検出スケジュール ページに表示されます。

4. IPアドレス範囲 フィールドで、次のいずれかを行います。

   - Active Directory **検出タイプを選択した場合は、スキャンする Active Directory サーバーの IP アドレスを入力します。**
   - **スキャンするIPアドレス範囲を入力します。個々のIPアドレスクラス範囲を指定するにはハイフンを使用します。例えば、192.168.2-5.1 から 192.168.2-5.200 までのそれぞれの値を含むすべての IP アドレスをスキャンするには、192.168.2-5.1-200 と入力します。**

   ヒント: アプライアンスは IPv6（インターネットプロトコルバージョン 6）と IPv4 アドレスの両方をサポートします。

   注意: **最大 25,000 件の IP アドレスがサポートされます。25,000 アドレスより多くなる IP 範囲を指定した場合、プロビジョニングスケジュールを保存しようとすると、警告が表示されます。**

5. 検出オプションを選択します。選択した検出タイプに応じて表示されるオプション:

オプション	アイテム	説明
DNS参照		デバイス名を識別するために検出を有効化します。DNS参照は、検出結果とインベントリリストにデバイス名を表示する場合は重要です。各検出タイプに対して、DNS参照 オプションを選択します。
	参照対象の名前サーバー	ネームサーバーのホスト名または IPアドレス。 ヒント: アプライアンスは IPv6（インターネットプロトコルバージョン 6）と IPv4 アドレスの両方をサポートします。
	タイムアウト	DNS参照がタイムアウトになるまでの時間（秒単位）。この時間内にアドレスが見つからない場合、プロセスは「タイムアウト」となります。
リレー		KACE エージェントが、WinRM、SSH、および SNMP 検出スケジュールのエージェント接続プロトコル、エージェント不要インベントリ、およびエージェントのプロビ

オプション	アイテム	説明
		ジョニングに対して、トンネル WinRM、SSH および SNMP トラフィックとして動作させることができます。
	リレーデバイス	エージェント不要デバイスインベントリのリレーとして使用するデバイスを指定します。 検出中にリレーとして使用されるリレーデバイスは、検出結果から新しいデバイスが自動的にプロビジョニングされるとき、エージェント不要インベントリに使用されます。 選択したリレーデバイスは、次のページにリストされます。 • エージェント不要デバイス接続の詳細 ページ（検出結果から新しいデバイスが自動的にプロビジョニングされるとき）。このページの詳細については、「デバイス情報の手動入力によるエージェント不要管理の有効化」を参照してください。 • プロビジョニングスケジュールの詳細 ページ（エージェントのプロビジョニングが検出結果から開始されるとき）詳細については、「単一または複数のデバイスへの KACE エージェントのインストール」を参照してください。 • エージェント不要デバイス接続の詳細 ページ（検出結果から新しいデバイスが自動的にプロビジョニングされるとき）。このページの詳細については、「デバイス情報の手動入力によるエージェント不要管理の有効化」を参照してください。
Active Directory		アプライアンスでActive Directoryサーバー上のデバイス情報を確認できるようにします。Active Directoryスキャン中のステータスは、スキャンしたデバイス数ではなく、おおよそのパーセントで示されます。

オプション	アイテム	説明
	セキュア LDAP（LDAPS）を使用	アプライアンスが LDAP 通信にセキュアポートを使用できるようにします。
	特権のあるユーザー	Active Directoryサーバーの管理者アカウントのユーザー名。例:「username@example.com」。
	特権のあるユーザーのパスワード	Active Directoryサーバーの管理者アカウントのパスワード。
	コンテキストの検索	デバイスの検索に使用される条件。この条件は、検索するActive Directory構造内の場所またはコンテナを指定します。基準を満たすOU、DC、またはCNの最も明確な組み合わせを入力します（一番左は最も限定的、一番右は最も一般的です）。例： DC=company,DC=com。
WinRM、Hyper-V、VMM		WinRMは、Windowsデバイスに対して使用する接続タイプです。
	タイムアウト	時間（秒単位、最大1分）。この時間内にアクティビティがないと接続が切断されます。
	Kerberosが必要	選択した場合、認証にはKerberosが必要です。Kerberos を使用できない場合に、代替認証として NTLM は使用されません。 Kerberosを使用するには、同じ検出設定でDNS参照を有効にする必要があります。DNS サーバは、ローカルアプライアンスネットワーク設定でも必要になります。
	Hyper-V および Virtual Machine Manager のスキャン	このフィールドは、Microsoft Hyper-V または System Center Virtual Machine Manager インフラストラクチャを監視する場合のみ使用されます。このオプションがオフになっていることを確認します。この機能の詳細については、「Microsoft Hyper-V または System Center Virtual Machine Manager の検出スケジュールの追加」を参照してください。
	ポート	このフィールドを空白のままにした場合、デフォルトポートの5985が使用されます。

オプション	アイテム	説明
	資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。
SSH		認証には SSH プロトコルを使用します。 **重要: SSH 経由の検出は Windows デバイスではサポートされていません。** 注: 検出スケジュールを保存した後に、SSH 認証を SNMP 認証に変更することはできません。
	タイムアウト	時間（最大5分）。この時間内にアクティビティがないと接続が切断されます。
	SSH2接続の試行	デバイスへの接続と通信にSSH2プロトコルを有効化します。 デバイスとの通信をよりセキュアにするにはSSH2を使用します（推奨）。
	資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。

6. **オプション**：検出スキャン完了の通知先となるEメールアドレスを入力します。このEメールには、検出スケジュールの名前が記載されます。
7. スキャンスケジュールを指定します。

ヒント: スキャンを行わずにスキャンインベントリを維持するには、スキャンスケジュールの設定で「**なし**」を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。

オプション	説明
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。

オプション	説明
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

8. **保存** をクリックします。

関連トピック

検出結果について

検出結果の表示および検索

実行中の検出スキャンの停止

検出スケジュールの削除

Chromeデバイスの検出に使用するクライアントIDとクライアントシークレットの取得

Chrome デバイスを使用するには、Admin SDK の API を使用して Google Apps ドメインへのアクセス権をアプライアンスに付与する資格情報が必要です。Google からクライアント ID とクライアントシークレットを取得して、使用するアプライアンスの承認コードを取得できるようにする必要があります。

- Chromeデバイス管理サポートが提供されるGoogle Apps for BusinessドメインまたはGoogle Apps for Educationドメインを使用できます。
- ビジネスドメインまたはエデュケーションドメインのメンバーであるGoogleユーザー管理者アカウントを使用できます。アカウントをスーパーユーザー役割に割り当てる必要があります。
- この手順で開発者アカウントとして使用できるGoogleアカウントを持っています。このアカウントは、管理者アカウントと同じである必要はなく、ビジネスドメインまたはエデュケーションドメインのメンバーである必要もありません。

アプライアンスに Admin SDK の API へのアクセス権がある場合は、アプライアンスを有効にして、デバイスおよびユーザーに関するデバイス情報を Google Apps ドメインからインポートします。資格認定プロセスの一部として、Googleプロジェクトの設定、プロジェクト内からのAdmin SDKのAPIの有効化、およびクライアントIDとクライアントシークレットの作成を実行する必要があります。

1. https://console.developers.google.com/で、開発者アカウントにサインインします。
2. プロジェクトを作成します。
    a. 左側のナビゲーションバーで、**Projects** をクリックします。
    b. **プロジェクトの作成** をクリックして、New Project（新規プロジェクト）ダイアログを表示します。
    c. プロジェクト名を入力します。
    d. 自動生成された「Project ID」を使用するか、自分で選択した固有IDを入力します。
    e. **Create** をクリックします。

    新しいプロジェクトの「Project Dashboard」が表示されます。
3. Admin SDKのAPIを有効化します。
    a. 左側のナビゲーションバーで、**APIs & auth** をクリックして、セクションを展開し、**API** をクリックします。
    b. API を参照 で Admin SDK を検索し、行の右端にある **オフ**ステータス ボタンをクリックして、ステータスを **オン** に切り替え、API を有効にします。
    c. サービス利用規約を読んで同意して、**Accept** をクリックします。
4. OAuthクライアントIDおよびクライアントシークレットを作成します。

注: Quest では、Chrome デバイスを検出するように設定されている各アプライアンスに対し、クライアント ID をそれぞれ作成することをお勧めします。

a. 左側のナビゲーションバーの**APIs & auth** セクションで、**Credentials** をクリックします。
b. OAuth セクションで、**クライアント ID の新規作成** をクリックして、クライアント ID の作成 ダイアログを表示します。
c. **同意画面の設定** をクリックして、Consent screen（同意画面）ダイアログを表示します。
d. EMAIL ADDRESS（E メールアドレス）ドロップダウンリストから自分の E メールを選択し、PRODUCT NAME（製品名）に製品の名前を入力し、**保存** をクリックして クライアント ID の作成 ダイアログに戻ります。
e. **Installed application** を選択します。
f. Installed Application Type（インストールされているアプリケーションタイプ）として **その他** を選択し、**クライアント ID の作成** をクリックします。

Credentials ページに、作成された「Client ID」と「Client Secret」が表示されます。

g. クライアントIDとクライアントシークレットの値をメモしておきます。

これらの値は、アプライアンスで Chrome デバイス検出用の承認資格情報を設定する場合に必要となります。

サードパーティ検出スケジュールを追加して、ネットワークで G Suite デバイスをスキャンし、これらのデバイスに関する情報を取得します。詳細については、「G Suiteデバイスへの検出スケジュールの追加」を参照してください。

KACE Cloud Mobile Device Manager デバイスの検出スケジュールの追加

KACE Cloud Mobile Device Manager（MDM）を使用してスマートフォンおよびタブレットへのアクセスを管理する場合、検出スケジュールを使用して管理対象モバイルデバイスを検出できます。ネットワークで KACE Cloud MDM デバイスをスキャンし、デバイスに関する情報を取得するには、外部統合検出スケジュールを追加します。

注: この方法で検出されたすべての KACE Cloud MDM デバイスは、アプライアンスのライセンスの上限の計算には含まれません。

1. 検出スケジュールの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。
   c. **アクションの選択 > 新規作成** を選択します。
2. 検出タイプ を選択して、選択したタイプのオプションを含むフォームを表示します。この場合は、外部統合 [KACE Cloud Mobile Device Manager、G Suite、Workspace ONE] です。
3. 名前 フィールドに、スキャンの名前を入力します。

   この名前は、検出スケジュール ページに表示されます。
4. KACE Cloud Mobile Device Manager を展開して、検出オプションを選択します。

オプション	説明
テナント名	KACE Cloud MDM で管理しようとしているデバイスに関連付けられたテナントの名前です。
資格情報	KACE Cloud MDM デバイスに接続するために使用されるアカウントの詳細。ドロップダウンリストか

オプション	説明
	ら既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。 詳細については、「シークレットキー資格情報の追加および変種」を参照してください。
デバイスの自動プロビジョニング	選択した場合、次のスキャンで検出されたすべてのモバイルデバイスがインベントリに追加されます。 **注:** 予期しない範囲までインベントリが展開するのを避けるため、このオプションは注意して使用してください。

5. **オプション**：Notify（通知）セクションで、検出スキャンの完了時に通知するための E メールアドレスを入力します。このEメールには、検出スケジュールの名前が記載されます。
6. スキャンスケジュールを指定します。

ヒント: スキャンを行わずにスキャンインベントリを維持するには、スキャンスケジュールの設定で「**なし**」を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。

オプション	説明
	例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

7. **保存** をクリックします。

関連トピック

検出結果について

検出結果の表示および検索

実行中の検出スキャンの停止

検出スケジュールの削除

G Suiteデバイスへの検出スケジュールの追加

ネットワークで G Suite デバイスをスキャンし、デバイスに関する情報を取得するには、外部統合スケジュールを追加します。

- Chromeデバイス管理サポートが提供されるGoogle Apps for BusinessドメインまたはGoogle Apps for Educationドメインを使用できます。
- ビジネスドメインまたはエデュケーションドメインのメンバーであるGoogleユーザー管理者アカウントを使用できます。アカウントをスーパーユーザー役割に割り当てる必要があります。
- 開発者アカウントとして使用するGoogleアカウントを持っており、クライアントIDおよびクライアントシークレットを使用してプロジェクトを作成しています。詳細については、「Chromeデバイスの検出に使用するクライアントIDとクライアントシークレットの取得」を参照してください。

注: この方法で検出されたすべての G Suite デバイスは、アプライアンスのライセンスの上限の計算には含まれません。

1. 検出スケジュールの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。
   c. **アクションの選択 > 新規作成** を選択します。
2. 検出タイプ を選択して、選択したタイプのオプションを含むフォームを表示します。この場合は、外部統合 [KACE Cloud Mobile Device Manager、G Suite、Workspace ONE] です。
3. 名前 フィールドに、スキャンの名前を入力します。

   この名前は、検出スケジュール ページに表示されます。
4. G Suite を展開し、検出オプションを選択します。

オプション	説明
Chromeデバイスの検出	選択した場合、Chromeデバイスは次のスキャン時に検出されます。
モバイルデバイスの検出	選択した場合、G Suiteモバイルデバイスは次のスキャン時に検出されます。
資格情報	Chromeデバイスに接続するために使用されるアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 **重要: 選択した資格情報は適切なデバイスタイプに関連付けられる承認コードが必要です。例えば、G Suiteモバイルデバイスを検出する場合、Chromeデバイス用の承認コードが生成された資格情報は使用できません。** 詳細については、「Google Workspace 資格情報の追加および編集」を参照してください。
デバイスの自動プロビジョニング	選択した場合、次のスキャンで検出されたすべてのChromeデバイスがインベントリに追加されます。

オプション	説明
	注: 予期しない範囲までインベントリが展開するのを避けるため、このオプションは注意して使用してください。

5. **オプション**：Notify（通知）セクションで、検出スキャンの完了時に通知するための E メールアドレスを入力します。このEメールには、検出スケジュールの名前が記載されます。
6. スキャンスケジュールを指定します。

ヒント: スキャンを行わずにスキャンインベントリを維持するには、スキャンスケジュールの設定で「**なし**」を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（,）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（-）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（/）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3

オプション	説明
	は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

7. **保存** をクリックします。

関連トピック

検出結果について

検出結果の表示および検索

実行中の検出スキャンの停止

検出スケジュールの削除

Workspace ONE デバイスの検出スケジュールの追加

VMware ® Workspace ONE® では、企業レベルのモビリティ管理プラットフォームで、さまざまなデバイスタイプを管理できます。REST API 呼び出しを使用して、Workspace ONE で管理されているデバイスを検出、収集するために、Workspace ONE と統合することができます。

注: この方法で検出されたすべての Workspace ONE デバイスは、アプライアンスのライセンスの上限の計算には含まれません。

1. 検出スケジュールの詳細 ページに移動します。
    a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) に口グインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、口グイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. 検出タイプ を選択して、選択したタイプのオプションを含むフォームを表示します。この場合は、外部統合 [KACE Cloud Mobile Device Manager、G Suite、Workspace ONE] です。
3. 名前 フィールドに、スキャンの名前を入力します。

   この名前は、検出スケジュール ページに表示されます。
4. Workspace ONE を展開し、検出オプションを選択します。

オプション	説明
ホスト	Workspace ONE 管理コンソールのホスト名。
REST APIキー	Workspace ONE 管理コンソールで使用できる REST API キー。このキーは、API 呼び出しを介して Workspace ONE と統合可能にするために必要です。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 「ユーザーとパスワード資格情報の追加および編集」を参照してください。
デバイスの自動プロビジョニング	選択した場合、次のスキャンで検出されたすべての Workspace ONE デバイスがインベントリに追加されます。 **注:** 予期しない範囲までインベントリが展開するのを避けるため、このオプションは注意して使用してください。

5. **オプション**：Notify（通知）セクションで、検出スキャンの完了時に通知するための E メールアドレスを入力します。このEメールには、検出スケジュールの名前が記載されます。
6. スキャンスケジュールを指定します。

ヒント: スキャンを行わずにスキャンインベントリを維持するには、スキャンスケジュールの設定で「**なし**」を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59)

オプション	説明
	値の指定は次の要領で行います。 • **スペース ( )**：各フィールドはスペースで区切ります。 • **アスタリスク (*)**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

7. **保存** をクリックします。

関連トピック

検出結果について

検出結果の表示および検索

実行中の検出スキャンの停止

検出スケジュールの削除

VMware ESXi ホストまたは vCenter サーバーへの検出スケジュールの追加

ビジネスで仮想 VMware ベースの環境を使用する場合、検出スケジュールを使用して VMware ESXi ホストまたは vCenter サーバーを検出できます。ネットワークで VMware ESXi ホストまたは vCenter サーバーをスキャンし、それらのデバイスに関する情報をキャプチャするには、認証済み検出スケジュールを追加します。

プロビジョニングされた VMware ESXi ホストは、エージェントベースのライセンスを消費します。そのホストに関連付けられた仮想マシンは、ライセンスを消費しません。ESXi ホストが実行されている vCenter は、ライセンスを消費しません。プロビジョニングされた ESXi ホストに接続するためのブリッジとして機能します。

1. 検出スケジュールの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. 検出タイプ を選択して、選択したタイプ（ この場合は 認証済み [WinRM、SNMP、SSH、VMware、Hyper-V] ）のオプションを含むフォームを表示します。
3. 名前 フィールドに、スキャンの名前を入力します。

    この名前は、検出スケジュール ページに表示されます。
4. VMware セクションを展開し、検出 オプションを設定します。

オプション	説明
タイムアウト	時間。この時間内に応答がないとスキャンが終了します。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 「ユーザーとパスワード資格情報の追加および編集」を参照してください。

5. **オプション**：Notify（ 通知 ）セクションで、検出スキャンの完了時に通知するための E メールアドレスを入力します。このEメールには、検出スケジュールの名前が記載されます。
6. スキャンスケジュールを指定します。

    ヒント: スキャンを行わずにスキャンインベントリを維持するには、スキャンスケジュールの設定で「**なし**」を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。

オプション	説明
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。

オプション	説明
	詳細については、「タスクスケジュールの表示」を参照してください。

7. **保存** をクリックします。

関連トピック

検出結果について

検出結果の表示および検索

実行中の検出スキャンの停止

検出スケジュールの削除

Microsoft Hyper-V または System Center Virtual Machine Manager の検出スケジュールの追加

仮想 Hyper-V ベースの環境をビジネスで使用している場合、検出スケジュールを使用して Microsoft Hyper-V または System Center Virtual Machine Manager（ SCVMM ）デバイスを検出できます。ネットワークで Hyper-V または SCVMM デバイスをスキャンしてこれらのデバイスに関する情報を取得するには、認証済み検出スケジュールを追加します。

この方法でアプライアンスにインポートされたデバイスは、ライセンス不要です。それぞれの SCVMM および Hyper-V デバイスが消費するライセンスは、基盤となる Windows システムのインベントリに使用されるエージェント不要ライセンスのみです。KACE エージェントを使用してプロビジョニングされた SCVMM および Hyper-V デバイスは、それぞれ 2 つのライセンスを消費します。

1. 検出スケジュールの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. 検出タイプ を選択して、選択したタイプ（ この場合は 認証済み [WinRM、SNMP、SSH、VMware、Hyper-V] ）のオプションを含むフォームを表示します。
3. 名前 フィールドに、スキャンの名前を入力します。

    この名前は、検出スケジュール ページに表示されます。
4. WinRM、Hyper-V、VMM セクションを展開し、検出オプションを設定します。

オプション	説明
タイムアウト	時間（ 秒単位、最大1分 ）。この時間内にアクティビティがないと接続が切断されます。
Kerberosが必要	選択した場合、認証にはKerberosが必要です。Kerberos を使用できない場合に、代替認証として NTLM は使用されません。 Kerberosを使用するには、同じ検出設定でDNS参照を有効にする必要があります。DNS サーバは、ローカルアプライアンスネットワーク設定でも必要になります。

オプション	説明
Hyper-V および Virtual Machine Manager のスキャン	アプライアンスがエージェント不要管理を使用して Microsoft Hyper-V または System Center Virtual Machine Manager インフラストラクチャをインポートできるようにするには、このオプションを選択します。この機能の詳細については、「Microsoft Hyper-V または System Center Virtual Machine Manager の検出スケジュールの追加」を参照してください。
ポート	このフィールドを空白のままにした場合、デフォルトポートの5985が使用されます。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、必要に応じて**新しい資格情報の追加**を選択して新しい資格情報を追加します。 「ユーザーとパスワード資格情報の追加および編集」を参照してください。 **注:** SCVMM デバイスに指定されたものと同じ資格情報が、管理対象の各 Hyper-V デバイスへの接続に使用されます。詳細については、「System Center Virtual Machine Manager 資格情報の要件」を参照してください。

5. **オプション**：Notify（通知）セクションで、検出スキャンの完了時に通知するための E メールアドレスを入力します。このEメールには、検出スケジュールの名前が記載されます。
6. スキャンスケジュールを指定します。

ヒント: スキャンを行わずにスキャンインベントリを維持するには、スキャンスケジュールの設定で「**なし**」を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12)

オプション	説明
	| | +??????????????????????day of month (1-31) | +??????????????????????hour (0-23) +??????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース ( )**：各フィールドはスペースで区切ります。 • **アスタリスク (*)**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

7. **保存** をクリックします。

関連トピック

検出結果について

検出結果の表示および検索

実行中の検出スキャンの停止

検出スケジュールの削除

System Center Virtual Machine Manager 資格情報の要件

System Center Virtual Machine Manager（SCVMM）デバイスおよびそのすべての管理対象 Hyper-V デバイスのインベントリに使用される資格情報には、特定の要件があります。

- ドメインアカウントは、SCVMM **読み取り専用管理者**プロファイルのメンバーであるか、同じ権限またはそれ以上の権限を持つプロファイルである必要があります。
- ドメインアカウントは、各 Hyper-V デバイスのローカル **Hyper-V 管理者**グループのメンバーである必要があります。
- ドメインアカウントには、SCVMM および Hyper-V デバイスで WinRM を使用して Windows エージェント不要インベントリを実行する権限が必要です。

コンピューター以外の SNMP 対応デバイスの検出スケジュールの追加

ネットワークでコンピューター以外のデバイスをスキャンし、デバイスに関する情報を取得するには、認証済み - SNMP 検出スケジュールを追加します。

SNMPを有効化するには、ポート161がアプライアンスとデバイスで開いている必要があります。

SNMP（簡易ネットワーク管理プロトコル）は、ネットワーク上の管理対象デバイスを監視するためのプロトコルです。SNMP v3では認証アルゴリズムと暗号化アルゴリズムが使用され、SNMP通信のセキュリティ性が向上します。SNMP v3のオプションを設定すると、選択したデバイスでSNMP v3スキャンが実行されます。このスキャンが失敗すると、指定したパブリック文字列を使用して、SNMP v2またはv1スキャンが試行されます。

SNMP スキャン結果には、すべての SNMP 対応デバイスが含まれます。リモートシェル拡張によって、アプライアンスがデバイスに接続し、コマンドを実行し、検出情報をキャプチャすることが可能になります。

注: 検出スケジュールを保存した後に、SNMP 認証を SSH 認証に変更することはできません。

1. 検出スケジュールの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. 検出タイプ を選択して、選択したタイプ（この場合は 認証済み [WinRM、SNMP、SSH、VMware、Hyper-V]）のオプションを含むフォームを表示します。

    Notify（通知）セクションの前に、次のオプションが表示されます。

    - DNS参照
    - リレー
    - WinRM、Hyper-V、VMM
    - SSH
    - SNMP

    この手順では、DNS Lookup（DNS 参照）および SNMP のみが適切です。
3. 名前 フィールドに、スキャンの名前を入力します。

この名前は、検出スケジュール ページに表示されます。

4. IP Address Range（IP アドレス範囲）フィールドに、スキャンする IP アドレス範囲を入力します。ハイフンを使用して個々のIPアドレスクラス範囲を指定します。例えば、192.168.2-5.1 から 192.168.2-5.200 までのそれぞれの値を含むすべての IP アドレスをスキャンするには、192.168.2-5.1-200 と入力します。

   ヒント: アプライアンスは IPv6（インターネットプロトコルバージョン 6）と IPv4 アドレスの両方をサポートします。

   注意: 最大 25,000 件の IP アドレスがサポートされます。25,000 アドレスより多くなる IP 範囲を指定した場合、プロビジョニングスケジュールを保存しようとすると、警告が表示されます。

5. DNS Lookup（DNS 参照）を展開し、検出オプションを選択します。

   DNS Lookup（DNS 参照）を含めると、検出時にデバイスの名前を識別できるようになります。DNS参照は、検出結果とインベントリリストにデバイス名を表示する場合は重要です。

オプション	説明
参照対象の名前サーバー	ネームサーバーのホスト名またはIPアドレス。 ヒント: アプライアンスは IPv6（インターネットプロトコルバージョン 6）と IPv4 アドレスの両方をサポートします。
タイムアウト	DNS参照がタイムアウトになるまでの時間（秒単位）。この時間内にアドレスが見つからない場合、プロセスは「タイムアウト」となります。

6. リレー を展開し、検出オプションを選択します。

   リレー オプションを設定すると、KACE エージェントが、WinRM、SSH、および SNMP 検出スケジュールのエージェント接続プロトコル、エージェント不要インベントリ、およびエージェントのプロビジョニングに対して、トンネル WinRM、SSH および SNMP トラフィックとして動作させることができます。

オプション	説明
リレーデバイス	エージェント不要デバイスインベントリのリレーとして使用するデバイスを指定します。 検出中にリレーとして使用されるリレーデバイスは、検出結果から新しいデバイスが自動的にプロビジョニングされるとき、エージェント不要インベントリに使用されます。 選択したリレーデバイスは、次のページにリストされます。 • エージェント不要デバイス接続の詳細 ページ（検出結果から新しいデバイスが自動的にプロビジョニングされるとき）。このページの詳細については、「デバイス情報の手動入力によるエージェント不要管理の有効化」を参照してください。 • プロビジョニングスケジュールの詳細 ページ（エージェントのプロビジョニングが検出結果から開始されるとき）詳細については、「単一または複数のデバイスへの KACE エージェントのインストール」を参照してください。 • エージェント不要デバイス接続の詳細 ページ（検出結果から新しいデバイスが自動的にプロビジョニングされるとき）。このページの

オプション	説明
	詳細については、「デバイス情報の手動入力によるエージェント不要管理の有効化」を参照してください。

7. SNMP を展開し、検出オプションを選択します。

オプション	説明
SNMPの完全なウォーク	デバイスのMIB（管理情報ベース）データの完全なウォークを有効化します。このオプションをオフにすると、3つのコアOID（オブジェクト識別子）を検索するBULK GETが実行されます。このオプションを選択すると、完全なウォークは各デバイスにつき最大20分かかる場合があります。デフォルトのBULK GETは約1秒で検出に必要な情報をすべて取得します。 **注:** SNMPのインベントリウォークは、Windowsデバイスで英語以外の文字をサポートしていません。英語以外の文字が出現すると、SNMPのインベントリプロセスでエラーが報告され、インベントリ情報のロードが中止されます。
タイムアウト	時間（秒単位）。この時間内に応答がないとスキャンが終了します。
最大試行回数	接続が試行される回数。
資格情報（SNMPv1/v2）	デバイスに接続してコマンドを実行するために必要な SNMP v1/v2 資格情報の詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 詳細については、「SNMP 資格情報の追加および編集」を参照してください。
資格情報（SNMPv3）	デバイスに接続してコマンドを実行するために必要な SNMP v3 資格情報の詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 詳細については、「SNMP 資格情報の追加および編集」を参照してください。

8. **オプション**：Notify（通知）セクションで、検出スキャンの完了時に通知するための E メールアドレスを入力します。このEメールには、検出スケジュールの名前が記載されます。
9. スキャンスケジュールを指定します。

ヒント: スキャンを行わずにスキャンインベントリを維持するには、スキャンスケジュールの設定で「**なし**」を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。

オプション	説明
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。

オプション	説明
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

10. **保存** をクリックします。

関連トピック

検出結果について

検出結果の表示および検索

実行中の検出スキャンの停止

検出スケジュールの削除

検出結果について

検出結果には、検出スケジュールスキャン中に識別された情報が表示されます。

インベントリ内のデバイスが、検出結果の記録に該当する場合は、そのデバイスの現在の接続ステータスが表示されます。デバイス名はそのデバイスの インベントリの詳細 ページにリンクし、DNS参照 列の デバイスのアクション ドロップダウンリストに、選択可能なデバイスのアクションが表示されます。

注: デバイスのアクションのブラウザ要件については、https://support.quest.com/kb/148787を参照してください。

検出結果は「特定の時点」での状態を表し、新たに監視対象として定義されたデバイスは、次に検出が実行されたときに状態が反映されます。

詳細については、「インベントリ情報の管理」を参照してください。

DHCPによって割り当てられたIPアドレスが変更されていると、スキャン時点のIPアドレスを表示する結果には、特定のデバイスの最新のIPアドレスが反映されないことがあります。

検出結果の表示および検索

検出結果を表示および検索して、デバイス情報、およびデバイスの検出に使用したスキャンのプロパティを取得できます。

1. 検出結果 リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出結果** をクリックします。
2. リストを並べ替えるには、次のいずれかを実行します。
    - **アクションの選択 > 到達できないアイテムを含める を選択します。アプライアンスに接続したデバイス、および現在到達できないデバイスがリストに表示されます。**
    - 特定基準で表示 **ドロップダウンリストで、検出名 を選択します。それらが検出された検出スケジュール名ごとにグループ化されて、リストが並べ替えられます。**
3. デバイスの詳細を表示するには、ホスト名 列または IPアドレス[ラベル] 列のリンクをクリックします。
4. デバイスを検索するには、次の操作を実行します。
    a. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。

b. 検索条件を選択します。

- 一番左のドロップダウンリストから属性を選択します。例：**デバイス情報：pingテスト。**
- 次のドロップダウンリストから条件を選択します。例：**=。**
- 次のドロップダウンリストからステータス属性を選択します。例：**失敗。**

c. **検索** をクリックします。

検出されたIPアドレスまたはホスト名を使用したエージェントのプロビジョニング

検出結果 ページからIPアドレスまたはホスト名を使用して、デバイスにエージェントのプロビジョニングを行うことができます。

検出結果でデバイスが識別された後、検出結果 ページのリンクを使用して、これらのデバイスにエージェントをプロビジョニングまたはインストールできます。この検出により、プロビジョニングするデバイスを開始時から特定でき、プロビジョニングフェーズでデバイスを特定するためにスキャンを行う必要がなくなります。

エージェントのプロビジョニングは特にWindowsデバイスで役に立ちます。Windowsデバイスは検出可能ですが、エージェントがこれらのデバイスにインストールされていない限り、管理オプションが限定されています。

1. 検出結果 リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出結果** をクリックします。
2. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
3. **アクションの選択** を選択し、次の操作のいずれかを行います。
   - **プロビジョニング > エージェント：IPアドレス を選択します。**
   - **プロビジョニング > エージェント：ホスト名 を選択します。**

   プロビジョニングスケジュールの詳細 ページが表示されます。選択したデバイスに関する情報が、このページに表示されます。
4. 必要に応じてプロビジョニングオプションを編集します。

   詳細については、「単一または複数のデバイスへの KACE エージェントのインストール」を参照してください。

実行中の検出スキャンの停止

実行中のスキャンを進行状況のある時点で停止できます。

検出スケジュール リストまたは Discovery Schedule Detail（ 検出スケジュールの詳細 ）ページから、実行中の検出スキャンを停止できます。検出スケジュール リストから複数のスキャンを停止できます。

停止 でスキャンを中断すると、IP 範囲内のデバイスのうち、その時点までスキャンされていたすべてのデバイスが 検出結果 に表示されます。

1. 検出スケジュール リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。

2. 次の 2 つの方法のいずれかを使用して、実行中のスキャンを停止します。

- **アクションの選択 メニューを使用して、1 つ以上の実行中のスキャンを停止します。**
  1. 1つまたは複数のスケジュールの隣のチェックボックスをオンにします。
  2. **アクションの選択停止** を選択し、**はい** をクリックして確定します。

     注: 選択したスケジュールのいずれも実行中でない場合は、**停止** を選択しても、その次にスケジュールされた時間にスキャンの実行が阻止されることはありません。

- **対応する** Discovery Schedule Detail **（検出スケジュールの詳細）ページから、実行中のスキャンを停止します。**
  1. 名前 列の検出スケジュールをクリックして、Discovery Schedule Detail（検出スケジュールの詳細）ページを表示します。
  2. ページの一番下までスクロールし、**停止** をクリックし、**はい** をクリックして確定します。

     注: スキャンが実行中のときは、**停止** ボタンが **今すぐ実行** ボタンに代わって表示されます。

指定の検出スケジュールのスキャン動作が停止します。スキャンが完全に停止して、進行状況ステータスが Stopped（停止済み）に変わるまで、検出スケジュール リストの Progress（進行状況）列に Stopping（停止中）と表示されます。

検出スケジュールの削除

必要に応じて検出スケジュールを削除できます。検出スケジュールを削除すると、そのスケジュールに関連したスキャン結果も削除されます。スケジュールを使用して検出され、インベントリに追加されたデバイスは、インベントリに保持されます。

1. 検出スケジュール リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出スケジュール** をクリックします。
2. 1つまたは複数のスケジュールの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

デバイスインベントリの管理

アプライアンスを使用してデバイスを管理できます。アプライアンスによって管理されるデバイスは、デバイスインベントリと呼ばれます。

デバイスの管理について

デバイスの管理とは、ネットワーク上のデバイスに関する情報をアプライアンスを使用して収集し保持するプロセス、およびデバイスのステータス監視とレポート作成などのタスクを実行するプロセスのことです。

アプライアンスインベントリにデバイスを追加するには、次の手順を実行します。

- **デバイスに KACE エージェントをインストールします。**デバイスにエージェントがインストールされて、エージェントによってインベントリがアプライアンスにレポートされると、それらのデバイスが自動的に

インベントリに追加されます。詳細については、「KACE エージェントのプロビジョニング」を参照してください。

- **デバイスでエージェント不要管理を有効にします。**エージェント不要管理は、サポート対象外のオペレーティングシステムを持つデバイスなど、デバイスに KACE エージェントをインストールできない場合に特に役立ちます。詳細については、「エージェント不要デバイスの管理」を参照してください。
- **デバイスのインベントリ情報を手動でアップロードします。**詳細については、「管理者コンソールでの、または API を使用したデバイスの手動追加」を参照してください。

注: 製品ライセンス契約に従い、管理対象コンピュータ、資産、監視対象サーバに分類された、指定された数のデバイスを管理できます。デバイスがMIA (未同期) となっている場合や既に使用されなくなった場合であっても、ライセンス数にカウントされます。手動で、またはAPIを通じてインベントリに追加されたデバイスは、ライセンス数にカウントされません。詳細については、「製品ライセンス情報の表示」を参照してください。

デバイスで使用可能な機能に関する情報は、「各デバイス管理方法で使用可能な機能」を参照してください。

各デバイス管理方法で使用可能な機能

デバイス管理機能は、デバイスの管理に使用する方法とデバイスのオペレーティングシステムによって異なります。

Windowsデバイスの場合は、エージェントをインストールすることですべての機能が提供されます。Linux?? デバイスと、プリンタやネットワークデバイスなどのエージェントをインストールできないデバイスの場合は、エージェント不要管理オプションを推奨します。

次の表に、管理対象デバイスで使用可能なコンポーネントと機能の概要を示します。

注: エージェント不要 で、Win 以外の OS は Mac OS X、CentOS???、Debian??、FreeBSD??、Oracle?? Enterprise Linux、Red Hat Enterprise Linux、SUSE、Solaris??、および Ubuntu です。

管理対象デバイスで使用可能な機能

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動
?? ??	Win、Mac?? Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
ホーム									
ダッシュボード: 必要に応じてデバイス情報を表示します。詳細については、「ダッシュボードについて」を参	X	X	X	X	X	X	X	X	

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
照してください。									
ラベル管理: ラベルはデバイスに割り当てることができます。詳細については、「ラベルについて」を参照してください。	X	X	X	X	X	X	X	X	X
検索: 検索結果にはデバイスが含まれます。詳細については、「情報の検索およびリストのフィルタリング」を参照してください。	X	X	X	X	X	X	X	X	X
インベントリ									
デバイス: デバイスを含んだリスト。詳細については、「インベントリ情報の管理」を参照して	X	X	X	X	X	X	X	X	X

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
ください。									
デバイス > 強制的なインベントリ更新: 詳細については、「インベントリ更新の強制実行」を参照してください。	X	X	X	X	X	X	X	X	
デバイス > MIA設定。詳細については、「MIAデバイスの管理」を参照してください。	X	X	X	X	X	X	X	X	
デバイス > SNMP設定の適用。詳細については、「インベントリに追加する特定のSNMPオブジェクトおよびコンピューター以外のデバイスを特定するためのSNMP								X	

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
インベントリ設定の使用」を参照してください。									
ソフトウェアページ: デバイスのソフトウェアを含んだリスト。詳細については、「ソフトウェアページについて」を参照してください。	X	X	X	X	X	X	X		
ソフトウェアカタログページ: デバイスのソフトウェアを含んだリスト。詳細については、「ソフトウェアカタログ情報の表示」を参照してください。	X Windows および Macのみ								
メータリング: デバイスでメータリングを有効化で	X Windows および Macのみ								

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
きます。詳細については、「ソフトウェアメータリングの使用」を参照してください。									
ソフトウェアのブロック（不許可に指定する）：ソフトウェアをデバイスで実行できないようにすることができます。詳細については、「アプリケーション制御の使用」を参照してください。	X Windows および Macのみ								
プロセス：デバイスで使用可能なインベントリ。詳細については、「プロセスインベントリの管理」を参照し	X	X	X						

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
てください。									
スタートアッププログラム: デバイスで使用可能なインベントリ。詳細については、「スタートアッププログラムインベントリの管理」を参照してください。	X	X	X						
サービス: デバイスで使用可能なインベントリ。詳細については、「サービスインベントリの管理」を参照してください。	X	X							
検出スケジュール: デバイスを検出できます。詳細については、「デバイス検出とデバイス管理	X	X	X	X	X	X	X	X	X

??	??	??							WSAPI
機能またはコンポーネント	エージェント	エージェント不要							手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
について」を参照してください。									
検出結果: デバイスは、結果リストからプロビジョニングできます。詳細については、「デバイス検出とデバイス管理について」を参照してください。	X	X	X	X	X	X	X	X	
SNMPインベントリ設定: デバイスのリストを拡張できます。詳細については、「インベントリに追加する特定のSNMPオブジェクトおよびコンピューター以外のデバイスを特定するためのSNMPインベントリ設定								X	

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
の使用」を参照してください。									
インベントリ: カスタムインベントリルール。詳細については、「カスタムインベントリルールの記述」を参照してください。	X								
監視									
警告: 受信された警告。詳細については、「警告の操作」を参照してください。	X	X	X						
デバイス: リストには、監視が有効化されたデバイスが含まれます。詳細については、「デバイスの監視の管理」を参照し	X	X	X						

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
てください。									
プロファイル: 警告は、プロファイルにより定義されます。詳細については、「監視プロファイルの操作」を参照してください。	X	X	X						
メンテナンスウィンドウ: 監視を一時停止する定期的なスケジュールを設定できます。詳細については、「その期間中デバイスから警告が収集されないメンテナンスウィンドウのスケジュール設定」を参照してください。	X	X	X						
Log Enablement Packages：これらの	X	X	X						

??	??	??							WSAPI
機能またはコンポーネント	エージェント	エージェント不要							手動
??	Win、Mac??		??	G Suite	KACE MDM	DMM	Workspac?? ONE		??
??	Linux	Win	Win以外	デバイス				SNMP	??
パッケージを導入すると、パフォーマンスしきい値およびExchangeやInternet Information Services（IIS）などのアプリケーションを監視できます。詳細については、「Log Enablement Packageを使用したアプリケーションおよびしきい値監視の設定」を参照してください。									
資産									
資産: デバイスに作成できます。詳細については、「資産管理について」を参照してください。	X	X	X	X	X	X	X	X	X
資産タイプ: デバイスに作成できま	X	X	X	X	X	X	X	X	X

??	??	??							WSAPI
機能またはコンポーネント	エージェント	エージェント不要							手動
??	Win、Mac、Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	??
??									
す。詳細については、「資産タイプの追加とカスタマイズおよび資産情報の維持」を参照してください。									
場所：デバイス、ユーザー、資産に対して定義できます。詳細については、「場所の管理」を参照してください。	X	X	X	X	X	X	X	X	X
資産のインポート：デバイスにインポートできます。詳細については、「CSV ファイルでのライセンスデータのインポート」を参照してください。	X								
配布									

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動

??	Win、Mac??		??	G Suite	KACE MDM	DMM	Workspac?? ONE		??
??	Linux	Win	Win以外	デバイス				SNMP	??
管理対象インストール: デバイスにソフトウェアをインストールするのに使用します。詳細については、「管理対象インストールの使用」を参照してください。	X								
ファイル同期: デバイス上のファイル管理に使用します。詳細については、「ファイル同期の作成および使用」を参照してください。	X								
Wake-on-LAN: 有効なIPアドレスとMACアドレスを持つデバイスで使用できます。詳細については、「Wake	X	X	X					X	

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
On LAN の使用」を参照してください。									
レプリケーション: レプリケーション共有として使用できます。詳細については、「レプリケーション共有の使用」を参照してください。	X								
警告: デバイスに表示するためにブロードキャストできます（サーバーの警告の監視とは異なります）。詳細については、「管理対象デバイスへの警告のブロードキャスト」を参照してください。	X Windows および Macのみ								

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
スクリプト									
今すぐ実行: デバイスでスクリプトを実行するのに使用します。詳細については、「実行 および 今すぐ実行 コマンドの使用」を参照してください。	X								
今すぐ実行のステータス: デバイスに表示することができます。詳細については、「「今すぐ実行のステータス」の監視とスクリプト詳細の表示」を参照してください。	X								
スクリプトログの検索: 検索結果でデバイスのリスト	X								

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
が表示されます。詳細については、「スクリプトログの検索」を参照してください。									
設定ポリシー: デバイスの設定に使用します。詳細については、「設定ポリシーテンプレートについて」を参照してください。	X Windows および Macのみ								
Mac Profiles：Mac OS X デバイスでユーザーレベルおよびシステムレベルのポリシーおよび設定を設定できます。詳細については、「Mac プロファイルの管理」を参照してください。	X Mac のみ								

??	??	??						WSAPI
機能またはコンポーネント	エージェント	エージェント不要						手動

??	Win、Mac??		??	G Suite	KACE MDM	DMM	Workspac?? ONE		??
??	Linux	Win	Win以外	デバイス				SNMP	??
セキュリティ									
パッチ管理: デバイスへのパッチ適用に使用します。詳細については、「パッチ管理について」を参照してください。	X Windows および Macのみ								
OVALスキャン: テスト対象にはデバイスが含まれます。詳細については、「OVALセキュリティチェックについて」を参照してください。	X Windows のみ								
SCAPスキャン: スキャン対象にはデバイスが含まれます。詳細については、「SCAPについて」を参	X Windows のみ								

??	??	??							WSAPI
機能またはコンポーネント	エージェント	エージェント不要							手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP	?? ??
照してください。									
Dellアップデート: デバイスのアップデートに使用します。詳細については、「Dellデバイスおよびアップデートの管理」を参照してください。	X Windowsのみ								
サービスデスク									
チケット：チケットを作成してデバイスに割り当てることができます。詳細については、「管理者コンソールおよびユーザーコンソールからのチケットの作成」を参照してください。	X	X	X	X	X	X	X	X	

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要							WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
ユーザーダウンロード：ユーザーコンソールからデバイスにソフトウェアをダウンロードできます。詳細については、「ユーザーダウンロードの管理」を参照してください。	X								
サポート技術情報：詳細については、「サポート技術情報記事の管理」を参照してください。	X	X	X	X	X	X	X	X	
通知：ユーザーコンソールホームページに表示される告知を作成できます。詳細については、「ユーザーコンソールの告知の	X	X	X	X	X	X	X	X	

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
追加、編集、非表示、または削除」を参照してください。									
設定：詳細については、「サービスデスクの設定」を参照してください。	X	X	X	X	X	X	X	X	
レポート作成									
レポート作成: レポートにはデバイス情報を使用できます。詳細については、「レポートの作成」を参照してください。	X	X	X	X	X	X	X	X	
レポートスケジュール: 作成されたレポートスケジュールを表示します。詳細については、「レポートのスケ	X	X	X	X	X	X	X	X	

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
ジュール」を参照してください。									
通知: 通知にはデバイスを含めることができます。詳細については、「通知のスケジュール」を参照してください。	X	X	X	X	X	X	X	X	
設定：コントロールパネル									
デバイスのアクション: デバイスで実行可能なアクション。詳細については、「デバイスでのアクションの実行」を参照してください。	X	X	X					X	
ライセンス使用率の注意喚起レベル: デバイス上のアプリケーショ	X	X	X	X	X	X	X	X	

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
ンに使用できます。詳細については、「アプリケーションへの脅威レベルの割り当て」を参照してください。									
履歴: デバイス情報を追跡できます。詳細については、「資産履歴の管理」を参照してください。	X	X	X	X	X	X	X	X	
ログ: 使用可能なデバイス情報。詳細については、「アプライアンスログの表示」を参照してください。	X	X	X	X	X	X	X	X	
バックアップと復元: デバイス情報が含まれます。詳細については、「アプライアン	X	X	X	X	X	X	X	X	

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspac ONE	?? SNMP	?? ??
スバックアップについて」を参照してください。									
組織									
フィルタ: デバイスに組織フィルタを割り当てることができます。詳細については、「組織フィルタの管理」を参照してください。	X	X	X	X	X	X	X	X	
デバイスのリダイレクト: デバイスを組織に再割り当てすることができます。詳細については、「デバイスのリダイレクト」を参照してください。	X	X	X	X	X	X	X	X	X
デバイスのフィルタ: デバイスをフィルタ	X	X	X	X	X	X	X	X	

?? 機能またはコンポーネント	?? エージェント	?? エージェント不要						WSAPI 手動
?? ??	Win、Mac、Linux	?? Win	?? Win以外	G Suite デバイス	KACE MDM	DMM	Workspace ONE	?? SNMP ??
リングして、組織に再割り当てすることができます。詳細については、「デバイスのフィルタリング」を参照してください。								
組織の設定: インベントリの間隔を設定します。詳細については、「管理対象デバイスでのインベントリデータ収集のスケジュール」を参照してください。	X	X	X	X	X	X	X	X

インベントリ情報について

インベントリには、ネットワーク上の管理対象デバイスのデバイス、アプリケーション、プロセス、スタートアッププログラム、およびサービスに関する情報が含まれます。

インベントリ：

- 管理対象デバイスにインストールされている KACE エージェントによって収集される
- インベントリAPIを使用してアップロードされる
- エージェント不要デバイスへの接続を通じて取得される

個々の管理対象デバイスの詳細データを参照することも、すべての管理対象デバイスから収集された集計データを参照することもできます。また、インベントリ情報はレポートに使用することもできれば、アップグレード、トラブルシューティング、購入、ポリシーなどについて決定を下す際に使用することもできます。

このセクションでは、デバイスインベントリを中心に説明します。その他のインベントリアイテムに関する情報については、以下を参照してください。

- ソフトウェア ページでのアプリケーション管理
- ソフトウェアカタログインベントリの管理
- プロセス、スタートアッププログラム、およびサービスインベントリの管理

インベントリ設定に対する変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

インベントリの変更履歴について

デバイスの変更履歴は、最初のレポート作成時に収集された情報に変更が加えられたときに初めて記録されます。

管理対象デバイスによってアプライアンスにインベントリが初めてレポートされたときに、その情報がベースラインレポートとして考慮されます。そのため、その情報は変更履歴に記録されません。

インベントリ情報の管理

インベントリ情報を管理するには、カスタムデータフィールドを追加し、インベントリ内のデバイスを表示し、デバイスの詳細を表示します。

カスタムデータフィールドの追加

ソフトウェア リストから手動で追加されたアプリケーションのカスタムデータフィールドを追加できます。

カスタムデータフィールドを追加すると、デバイス上のレジストリおよびその他の場所にある情報を取得できます。この情報を デバイスの詳細 ページで表示したり、レポートで使用したりできます。

例えば、カスタムフィールドを追加して、レジストリからの「DATファイルのバージョン番号」、「ファイルの作成日」、「ファイルの発行元」などのデバイスのデータを取得することができます。この情報に基づいてラベルを作成して同様のデバイスをグループ化したり、この情報を使用してレポートを作成したりできます。

1. ソフトウェア リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。
2. **アクションの選択 > 新規作成** を選択します。
3. 名前、バージョン、および 発行元 の各フィールドに値を入力します。

   この情報は、詳細ページでカスタムデータフィールドを識別するために使用されます。
4. カスタムインベントリルール フィールドで、返す必要のある情報に該当する構文を入力します。
   - **レジストリ値を返すには、以下のように入力します。valueTypeは、TEXT、NUMBER、またはDATEに置き換えてください。NUMBERは整数値です。RegistryValueReturn(string absPathToKey, string valueName, string valueType)**

例：RegistryValueReturn(HKEY_LOCAL_MACHINE\Software\McAfee.com\Virusscan Online,SourceDisk, TEXT)

- **Windows、Mac、およびLinuxデバイスでは、stat()関数から以下の属性を取得できます。**

  access_time、creation_time、modification_time、block_size、blocks、size、device_id、group、inode、mode、number

- **Windowsデバイスでは、VerQueryValue()関数から以下の属性を取得できます。**

  FileName、Comments、CompanyName、FileDescription、FileVersion、InternalName、LegalCopyright、LegalTradem

5. **保存** をクリックします。

詳細については、「カスタムインベントリルールの記述」を参照してください。

管理対象デバイスでのインベントリデータ収集のスケジュール

アプライアンスは、設定したアプライアンスデータ収集スケジュールに従って、エージェント管理対象デバイスおよびエージェント不要デバイスからハードウェアおよびソフトウェアのインベントリデータを収集します。

エージェント管理対象デバイスの場合、ソフトウェアのインベントリ情報は、ソフトウェア ページと ソフトウェアカタログ ページの両方で入手可能です。これらのページの詳細については、ソフトウェア ページと ソフトウェアカタログ ページの相違点を参照してください。

エージェント不要デバイスの場合、ソフトウェア情報はソフトウェア ページにのみリストされています。詳細については、「ソフトウェア ページでのアプリケーション管理」を参照してください。

アプライアンスで組織コンポーネントが有効化されている場合は、各組織のインベントリデータ収集を個別にスケジュールします。

1. 次のいずれかを実行します。

   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから システム を選択します。続いて、組織 をクリックします。組織の情報を表示するには、組織の名前をクリックします。**

     表示される 組織の詳細 ページで、通信とエージェントの設定 セクションを探します。

   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。次に、設定 > プロビジョニング を選択し、プロビジョニング パネルで 通信設定 をクリックします。**

     通信設定 ページが表示されます。

2. エージェントおよび通信設定 セクションで、各設定を次のように指定します。

注: アプライアンスへの負荷を軽減する場合は、エージェントの接続数を 1 時間あたり 500 までに制限します。インベントリ、スクリプト作成、およびメータリング間隔の隣に表示される接続数は、現在の組織のみに適用されます。アプライアンスで組織コンポーネントが有効化されている場合は、すべての組織のエージェント接続の合計数を1時間あたり500より多くしないでください。

オプション	設定案	メモ
エージェントのログ記録	有効	管理対象デバイスにインストールされたエージェントから提供されるスクリプト結果を、アプライアンスが保存するかどうか。エージェントログは、データベース内のディスク領域を最大約1 GB消費します。ディスク領域に問題がない場合は、エージェントのログ記録 を有効にして、エージェント管理対象デバイスの ログ情報をすべて保持します。これらのログは、トラブルシューティング時に役立ちます。ディスク領域を節約し、

オプション	設定案	メモ
		エージェント通信を高速化するには、エージェントの ログ記録 を無効にします。
エージェントインベントリ	12時間	管理対象デバイスのエージェントがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
エージェント不要インベントリ	1日	エージェント不要デバイスがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
カタログインベントリ	24時間	管理対象デバイスが ソフトウェア カタログ ページにインベントリをレポートする頻度。
メータリング	4時間	管理対象デバイスがアプライアンスにメータリング情報をレポートする頻度。デバイスとアプリケーションに対してメータリングを有効にする必要があります。
スクリプト更新	4時間	管理対象デバイスのエージェントが、管理対象デバイスで有効にされているスクリプトの更新されたコピーを要求する頻度。この間隔はスクリプトの実行頻度に影響を与えません。

3. 通知 セクションで、エージェント通信に使用するメッセージを指定します。

オプション	設定案	メモ
エージェントのスプラッシュページのメッセージ	デフォルトのテキストは次の通りです。 **KACE システム管理アプライアンス** は、PC 設定の検証およびソフトウェア更新プログラムの管理を行います。お待ちください...	エージェントがデバイス上でスクリプト実行などのタスクを実行しているときに、ユーザーに表示されるメッセージ。

4. エージェント不要 セクションで、エージェント不要デバイスの通信設定を次のように指定します。

オプション	説明
SSHタイムアウト	時間（秒または分単位）。この時間内にアクティビティがないと接続が切断されます。
SNMPタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
最大試行回数	接続が試行される回数。

オプション	説明
WinRMタイムアウト	時間（秒または分単位）。この時間内にアクティビティがないと接続が切断されます。

5. アプライアンスで組織コンポーネントが有効になっていない場合は、エージェント 設定を選択します。

   注: アプライアンスで組織コンポーネントが有効化されていない場合、エージェント 設定はアプライアンスの 一般設定 ページにあります。

オプション	説明
前回のタスクスループットの更新	この値は、アプライアンスのタスクスループットが最後に更新された日付と時刻を示します。
現在の読み込み平均	このフィールドの値は、任意の時点のアプライアンスに対する負荷を示します。アプライアンスが正常に動作するには、このフィールドの値が0.0と10.0の間になければなりません。
タスクスループット	スケジュール済みタスク（インベントリの収集、スクリプト作成、パッチの更新など）のアプライアンスでの調整方法を制御する値。 **注:** この値は、「現在の読み込み平均」の値が10.0以下で、かつ「前回のタスクスループットの更新」の時間が15分を超える場合にのみ増やすことができます。

6. **保存** をクリックします。

   変更は、エージェントがアプライアンスにチェックインするときに有効になります。

7. 複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

関連トピック

アプライアンスログの表示

組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定

デバイスインベントリおよび詳細の表示

デバイス ページではインベントリ内のデバイスのリストを表示でき、デバイスの詳細 ページでは選択したデバイスに関する情報を表示できます。

1. デバイスの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**デバイス** をクリックします。
   c. デバイスの名前をクリックします。
2. デバイスの詳細 ページでセクションを展開するには、概要 セクションの上にある **すべて展開** をクリックします。

   表示されるフィールドは、デバイスとそのオペレーティングシステムのタイプによって異なります。例えば、デバイスが仮想マシンの場合、モニタ フィールドは表示されず、「ビデオコントローラー」が表示されます。また、一部のフィールドはオペレーティングシステムによっては使用できない場合があります。例えば、「システムの説明」はWindowsまたはSNMPデバイスでのみ使用できます。

このページに表示されるグループおよびセクションの内容について説明した表を表示するには、デバイス詳細のアイテムのグループおよびセクションを参照してください。

3. **オプション**：インベントリ情報に対する変更追跡が有効になっている場合は、概要 セクションの上の **すべての履歴の表示** をクリックすると、インベントリ変更の履歴が表示されます。

関連トピック

履歴設定の定義

エージェント通信の管理

管理対象デバイスでのインベントリデータ収集のスケジュール

OVALセキュリティチェックについて

SCAPについて

資産管理コンポーネントについて

KACE Cloud MDM に登録されているデバイスに関する情報の表示

このアプライアンスには、統合 KACE Cloud Device Manager（MDM）インスタンスに登録されている Mac OS X デバイスに関する情報が表示されます。

このようなデバイスで使用できる情報のタイプは、KACE エージェントがインストールされているかどうかによって異なります。KACE Cloud MDM に登録されている Mac OS X デバイスから収集される情報のタイプを決定するシナリオとして次の 3 つが考えられます。

- ハイブリッドアプライアンス-第一デバイス管理
- KACE Cloud MDM デバイス管理
- ハイブリッド KACE Cloud MDM-第一デバイス管理

ハイブリッドアプライアンス-第一デバイス管理

1. Mac OS X デバイスに、KACE エージェントがインストールされ、アプライアンスに接続するように設定されます。
2. デバイスは、アプライアンスと統合された KACE Cloud MDM に登録されます。
3. アプライアンスは、デバイスを標準のエージェントベースデバイスとして認識します。

KACE Cloud MDM デバイス管理

1. Mac OS X デバイスが、アプライアンスと統合された KACE Cloud MDM に登録されます。
2. KACE Cloud MDM は、デバイスからインベントリ情報を収集します。
3. アプライアンスは、デバイスを標準のエージェント不要 KACE Cloud MDM デバイスとして認識します。

ハイブリッド KACE Cloud MDM-第一デバイス管理

1. Mac OS X デバイスが、アプライアンスと統合された KACE Cloud MDM に登録されます。
2. KACE Cloud MDM は、デバイスからインベントリ情報を収集します。
3. アプライアンスは、デバイスを標準のエージェント不要 KACE Cloud MDM デバイスとして認識します。
4. KACE エージェントがデバイスにインストールされ、アプライアンスに接続するように設定されます。
5. アプライアンスは、デバイスを標準のエージェントベースデバイスとして認識します。

デバイス詳細 ページに表示されるデバイスフィールドの詳細については、「デバイス詳細のアイテムのグループおよびセクション」を参照してください。

デバイス詳細のアイテムのグループおよびセクション

デバイスの デバイスの詳細 ページでは、グループ単位で収集されるセクションにインベントリ情報が表示されます。ページに含まれる情報の範囲および焦点は、表示されるデバイスおよびサブタイプによって異なります。

注: 資産サブタイプを割り当てた場合は、デバイスの詳細 ページでデバイスごとの詳細を表示するか非表示にするかを選択できます。例えば、サブタイプ プリンタ の場合、Installed Programs（インストールされているプログラム）、Discovered Software（検出されたソフトウェア）、メータリングしたソフトウェア の各アイテムなど、プリンタに無関係な情報は非表示にすることができます。グループ全体を非表示にすることもできます。詳細については、「資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択」を参照してください。

範囲を限定したユーザーはすべてのデバイスの詳細を表示できますが、編集できるのは自分の役割に関連付けられているデバイスの詳細のみです。ユーザーの役割の詳細については、ユーザーの役割の追加または編集を参照してください。

次のグループが デバイスの詳細 ページに表示されることがあります。

- Summary（摘要）グループ
- Inventory Information（インベントリ情報）グループ
- ソフトウェア グループ
- Activities（アクティビティ）グループ
- セキュリティ グループ
- Dell Command | Monitor - Monitor グループ
- Dellアップデート グループ
- ログと診断 グループ
- 資産 グループ

Summary（摘要）グループ

基本的なデバイス識別情報。アイテムは、ページの他のグループと同じく、セクションに分離されていません。デバイスの詳細 ページに表示されるエントリは、デバイス、オペレーティングシステム（関連する場合）、接続タイプなどによって異なります。

アイテム	説明	データベースフィールド
システム名	デバイスのホスト名またはIPアドレス。	名前
資産サブタイプ	このデバイスの資産サブタイプ（割り当てられている場合）。資産サブタイプは、カスタム資産タイプを含め任意の資産タイプに追加可能な資産のサブカテゴリです。これにより、コンピューターやプリンタやルーターなど資産のサブタイプを識別し、管理できます。	
資産の場所	この資産の場所。	なし
割り当て先	デバイスの所有者。このフィールドは、デバイスユーザーレコードがアプライアンスに存在する	なし

アイテム	説明	データベースフィールド
	場合にのみ生成されます。KACE Cloud MDM と統合するときに、アプライアンスが KACE MDM テナントの Active Directory と同期している場合、KACE MDM デバイスの所有者の名前が表示されます。他の種類の外部デバイスの場合、デバイスユーザーレコードがアプライアンスに見つからないと、フィールドは 未割り当て に設定されます。	
手動エントリ	インベントリ情報がWSAPIまたはXMLアップロードを通じて手動で追加されたことを示すフィールド。**編集** をクリックして情報を変更します。	MANUAL_ENTRY
デバイスエントリタイプ	デバイスの管理方法を示すフィールド: エージェントデバイス、エージェント不要デバイス、手動で入力されたレコード、またはエージェント/エージェント不要（ハイブリッド KACE Cloud MDM インベントリ）。接続プロトコルを変更するには、**編集** をクリックします。	なし
システムの説明	デバイスの説明。WindowsおよびSNMPデバイスのエージェント不要インベントリによって入力されます。	SYSTEM_DESCRIPTION
システムモデル	デバイスモデル。	CS_MODEL
シャーシタイプ	デバイスのタイプ（デスクトップ、ノートPCなど）。	CHASSIS_TYPE
所有権	**KACE MDM デバイスのみ。**デバイスの所有権を示します。会社、個人、または 不明。	所有権
IPアドレス	デバイスのIPアドレス。	IP
MACアドレス	デバイスのメディアアクセス制御（MAC）アドレス番号。	MAC
RAMの合計	デバイス上のランダムアクセスメモリ（RAM）の合計容量。	RAM_TOTAL
オペレーティングシステム名	デバイスのオペレーティングシステム（Windows、Mac OS X??、またはLinuxなど）。	OS_NAME

アイテム	説明	データベースフィールド
サービスパック	サービスパックのバージョン番号（Windows または SUSE Linux Enterprise サーバーのみ）。	SERVICE_PACK
前回の再起動からの稼働時間	再起動以降のデバイスの稼働時間。	UPTIME
エージェントのバージョン	デバイスにインストールされている KACE エージェントのバージョン番号。	CLIENT_VERSION
デバイスのタイムゾーン	デバイスにインストールされている KACE エージェントで使用されるタイムゾーン。	TZ_AGENT
ソース	収集されたデバイス詳細のソース。 • **エージェント管理対象デバイス**：このフィールドはエージェント に設定されます。 • **エージェント不要デバイス**：このフィールドには、接続タイプが反映されます。例えば、VMware です。 • **KACE Cloud MDM にも登録されているエージェント管理対象デバイス**：このフィールドは、Agent/KACE Cloud Mobile Device Manager に設定されます。**KACE Cloud Mobile Device Manager** リンクをクリックすると、このデバイスが KACE MDM Cloud インベントリに表示されます。	なし
ユーザー名	前回デバイスにログインしたユーザーの名前。一部のデバイスは複数のユーザーが利用している場合があります。	ユーザー
エージェント接続	デバイスのエージェントのメッセージプロトコルサービスがアプライアンスに接続した時間および現在の接続ステータス（エージェント管理対象デバイスのみで使用	KBSYS.SMMP_CONNECTION

アイテム	説明	データベースフィールド
	可）。接続ステータスには次のものが含まれます。 •  : エージェント管理対象デバイスがアプライアンスに接続されています。 •  : サーバー監視が有効になっているエージェント管理対象デバイスはアプライアンスに接続されています。 •  : エージェント管理対象デバイスがアプライアンスに接続されていません。 •  : エージェントのアクティビティは、システムトレイ（Windows）またはメニューバー（Mac OS）を使用して、指定された日時までデバイス上で中断されます。 •  : 手動で追加されたデバイスがアプライアンスに接続されています。 •  : エージェント管理対象デバイスで問題が検出されました。デバイスの問題の詳細を確認するには、デバイスの問題 ページに移動します。詳細については、「デバイスの問題の識別」を参照してください。	
エージェント不要接続	エージェント不要デバイスがアプライアンスに接続した時間および現在の接続ステータス（エージェント不要デバイスのみで使用可）。接続ステータスには次のものが含まれます。 •  : デバイスでエージェント不要管理が有効になっています。 •  : デバイスでエージェント不要管理およびサー	なし

アイテム	説明	データベースフィールド
	バー監視が有効になっています。 •  : デバイスに対してエージェント不要管理が有効化されていますが、現在デバイスは到達できません。	
エージェント不要接続方法	デバイスからのインベントリ情報の収集に使用されるプロトコル（SNMPなど）。	なし
前回のインベントリ	前回のインベントリレポート作成日時。	LAST_SYNC
デバイス作成日時	デバイスの最初のインベントリレコードが作成された日時。	CREATED
デバイス変更日時	デバイスのインベントリレコードが修正された日時。	MODIFIED
連絡先	**プリンタのみ**。選択したプリンタの連絡先情報（E メールアドレスなど）。この情報は、管理対象プリンタの SNMP sysContact フィールドに保存されます。	
場所	**プリンタのみ**。組織の名前など、選択したプリンタの場所。この情報は、管理対象プリンタの SNMP sysLocation フィールドに保存されます。	
ボリューム **n**	ディスクドライブのファイルシステムのタイプとサイズ、およびディスクドライブで使用済みの容量。ドライブ使用状況の変化を確認するには、このフィールド内の **使用状況の履歴を表示** リンクをクリックします。この情報は、使用率が5 %以上増減すると更新されます。 ボリュームごとに1つのエントリがあります。 VMware?? ESXi?? ホストのデバイスについては、ESXi ホストに関連付けられた各データストアがボリュームとしてリストに表示されます。	MACHINE_DISKS
強制的なインベントリ更新	**強制的なインベントリ更新** をクリックすると、デバイスのインベントリ情報が即座に更新され、デ	なし

アイテム	説明	データベースフィールド
	バイスとアプライアンスが同期されます。 **強制的なインベントリ更新** は、エージェント管理対象デバイスへのエージェントのメッセージプロトコル接続がアクティブな場合、またはエージェント不要デバイスではデバイスが到達可能な場合のみ使用できます。	
VMware UUID	このフィールドは、VMwareデバイスを選択したときにのみ表示されます。UUIDは、vCenterサーバーまたはESXiホストのグローバルに一意な識別子です。	INSTANCE_UUID
Hyper-V UUID	このフィールドは、Hyper-V デバイスを選択したときにのみ表示されます。UUID は、SCVMM または Hyper-V サーバのグローバルに一意な識別子です。	INSTANCE_UUID
仮想マシンマネージャの管理	管理 vCenter（VMware デバイス）または SCVMM（Hyper-V デバイス）の名前。 管理対象の vCenter または SCVMM がすでに KACE エージェントによってプロビジョニングされている場合、この列に表示される名前はハイパーリンクとして表示されます。リンクをクリックすると、ページが更新されてプロビジョニングされた仮想マシンマネージャのデバイスの詳細が表示されます。	なし
アクションの選択	• エージェントファイルをアップロードするには、**アクションの選択 > エージェントファイル（診断）をアップロードする** をクリックします。完了すると、アップロードされたファイルへのリンクがこのページの ログと診断 グループに表示されます。 • KACE システム展開アプライアンス（SDA）起動アクションにデバイスを追加するには、**アクションの選択 > SDA 起動アクションに追加する** をクリックします。KACE SDA 起動アクションは、ターゲットデバイスへのイメージ展開を	なし

アイテム	説明	データベースフィールド
	自動化するために使用されます。リンクされた KACE SDA が存在し、デバイスに有線ネットワーク接続がある場合にのみ、選択したデバイスから起動アクションを作成できます。このコマンドは、デバイス リスト ページの **アクションの選択** メニューからも使用できます。このコマンドをクリックすると、KACE SDA 自動展開の詳細 ページが表示されます。このページの詳細については、KACE SDA の『管理者ガイド』を参照してください。 • 選択したデバイスを削除するには、**アクションの選択 > 削除** をクリックします。	
KACE Cloud Mobile Device Manager（MDM）のコマンド	KACE Cloud MDM と統合し、KACE Cloud MDM デバイスを選択すると、このセクションで追加のコマンドセットが利用できます。 • **強制的なインベントリ更新**：KACE Cloud MDM からのデバイスの新しいインベントリを開始するリクエスト。完了すると、アプライアンスはインベントリ情報を同期します。 • **ロック**：選択したデバイスへのアクセスをブロックします。次にユーザーがデバイスとやり取りすると、デバイスのパスコードを入力するように求めるプロンプトが表示されます。 • **パスコードを設定**：選択したデバイスの新しいパスコードを指定できます。 **注:** このコマンドは Android デバイスでのみ利用できます。 • **パスコードをクリア**：選択したデバイスをロック解除します。新しいパスコードが指定されるまで、デバイ	なし

アイテム	説明	データベースフィールド
	スはロック解除されたままになります。 • **制限をクリアする**：**Android および iOS デバイスのみ**。選択したデバイスの機能を制限する設定をすべて削除します。 • **デバイスを登録解除**：選択したデバイスを KACE Cloud MDM から登録解除します。 • **工場出荷状態にリセット**：選択したデバイスで工場出荷時設定を復元します。 • **デバイスを再起動する**：**Android（管理対象）、iOS（監視対象）、および Mac OS デバイスのみ**。選択したデバイスを再起動します。 • **デバイスをシャットダウンする**：**iOS（監視対象）および Mac OS デバイスのみ**。選択したデバイスをオフにします。 • **リモートデスクトップを有効化する**：**Mac OS デバイスのみ**。選択したデバイスへのリモートデスクトップ接続を有効にします。 • **リモートデスクトップを無効化する**：**Mac OS デバイスのみ**。選択したデバイスへのリモートデスクトップ接続を無効にします。 • **ファームウェアパスワードを設定する**：**Mac OS デバイスのみ**。選択したデバイスのファームウェアパスワードを指定できます。 • **ファームウェアパスワードをクリアする**：**Mac OS デバイスのみ**。選択したデバイスのファームウェアパスワードを削除します。	

アイテム	説明	データベースフィールド
	ヒント: KACE Cloud MDM 一括アクションが有効になっている場合、これらのコマンドは、**アクションの選択** メニューの デバイス リストページからもアクセスできます。この機能は、デフォルトでは無効になっています。有効にするには、一般設定 ページの 許可される一括アクション の下で、**KACE Cloud MDM の一括アクションを有効にする** チェックボックスをオンにします。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。**強制的なインベントリ更新** コマンドはメインメニューに表示されますが、その他のコマンドは **KACE Cloud MDM** メニューで利用できます。	
VMware 仮想マシンのコマンド	管理環境に 1 つまたは複数のプロビジョニングされた VMware 仮想マシンが含まれている場合、仮想マシンの電源オンまたはオフなど、デバイスのアクションをこのページから実行できます。これらのコマンドは、以下の前提条件が満たされている場合に使用できます。 • プロビジョニングされた仮想マシンが、プロビジョニングされた VMware ESXi サーバーのバージョン 5.5.x 以上で実行されている必要があります。	なし

アイテム	説明	データベースフィールド
	注: 製品のライセンス契約により、管理者は特定の数のコンピュータ、サーバ、および資産を管理できます。プロビジョニングされた各 VMware ESXi サーバは、エージェント不要ライセンスを消費します。この機能を使用する場合、プロビジョニングされたすべての ESXi ホストが製品ライセンス契約の対象であることを確認する必要があります。詳細については、「http://quest.com/docs/Product_Guide.pdf」を参照してください。ライセンスの容量を増やすには、「https://quest.com/buy」を参照してください。 • **ゲスト OS をシャットダウンする** コマンドおよび **ゲスト OS を再起動する** コマンドを発行するには、ターゲット仮想マシンに VMware Tools をインストールする必要があります。その他のコマンドに VMware Tools は必要ありません。 • これらのアクションを実行するには、インベントリで設定されているユーザーアカウントに十分な管理レベルの権限が必要です。 次のコマンドは、プロビジョニングされた VMware 仮想マシンを選択した場合に使用できます。 • **電源オン**：選択した仮想マシンの電源をオンにします。仮想マシンがサスペンド状態の場合は、このアクションによってサスペンド状態の仮想マシンの電源がオンになります。 • **電源オフ**：選択した仮想マシンの電源をオフにします。仮想マシンがフォールトトレラントなプライマリ仮想マシンである場合、こ	

アイテム	説明	データベースフィールド
	れにより、1 台または複数のセカンダリ仮想マシンの電源もオフになります。 • **サスペンド**：選択した仮想マシンの実行を中断します。 • **リセット**：選択した仮想マシンの電源をリセットします。仮想マシンの電源がオンになっている場合、このアクションでは最初に電源をオフにしてから電源を投入します。 • **ゲスト OS をシャットダウンする**：選択した仮想マシン上のゲストオペレーティングシステムに、すべてのサービスのクリーンシャットダウンを実行するコマンドを発行します。 • **ゲスト OS を再起動する**：選択した仮想マシン上のゲストオペレーティングシステムに、再起動を実行するコマンドを発行します。 **ヒント:** これらのコマンドは、デバイスの詳細 ページで常に使用できます。また、仮想マシンに対する一括アクションが有効になっている場合、**アクションの選択** メニューの デバイス リストページにも表示されます。この機能は、デフォルトでは無効になっています。有効にするには、一般設定 ページの 許可された一括アクションの下で、**仮想マシンの一括アクションを有効にする** チェックボックスをオンにします。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。 これらの仮想マシンのアクションの詳細については、VMware ESXi のドキュメントを参照してください。	
Hyper-V 仮想マシンコマンド	管理環境に 1 つまたは複数のプロビジョニングされた Hyper-V 仮想マシンが含まれている場合、仮想マシンの電源オンまたはオフな	なし

アイテム	説明	データベースフィールド
	ど、デバイスのアクションをこのページから実行できます。 次のコマンドは、プロビジョニングされた Hyper-V 仮想マシンを選択した場合に使用できます。 • **電源オン**：選択した仮想マシンの電源をオンにします。仮想マシンがサスペンド状態の場合は、このアクションによってサスペンド状態の仮想マシンの電源がオンになります。 • **電源オフ**：選択した仮想マシンの電源をオフにします。仮想マシンがフォールトトレラントなプライマリ仮想マシンである場合、これにより、1 台または複数のセカンダリ仮想マシンの電源もオフになります。 • **サスペンド**：選択した仮想マシンを中断（一時停止）します。 • **再開**：一時停止中の仮想マシンを再開します。 • **リセット**：選択した仮想マシンの電源をリセットします。仮想マシンの電源がオンになっている場合、このアクションでは最初に電源をオフにしてから電源を投入します。 • **ゲスト OS をシャットダウンする**：選択した仮想マシン上のゲストオペレーティングシステムに、すべてのサービスのクリーンシャットダウンを実行するコマンドを発行します。 • **ゲスト OS を再起動する**：選択した仮想マシン上のゲストオペレーティングシステムに、再起動を実行するコマンドを発行します。	

アイテム	説明	データベースフィールド
	ヒント: これらのコマンドは、デバイスの詳細 ページで常に使用できます。また、仮想マシンに対する一括アクションが有効になっている場合、**アクションの選択** メニューの デバイス リストページにも表示されます。この機能は、デフォルトでは無効になっています。有効にするには、一般設定 ページの 許可された一括アクションの下で、**仮想マシンの一括アクションを有効にする** チェックボックスをオンにします。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。 これらの仮想マシンのアクションの詳細については、Hyper-V のドキュメントを参照してください。	
Chrome デバイスコマンド	管理対象の環境に 1 つ以上のプロビジョニングされた Chrome デバイスが含まれている場合は、Chrome デバイスを選択すると次のコマンドを使用できます。 • **移動**：プロビジョニングされたデバイスを別の組織ユニットに移動します。 • **無効にする**：プロビジョニングされたデバイスを無効にします。このコマンドは、デバイスが紛失または盗難にあった場合に使用できます。 • **再有効化**：以前に無効にしたデバイスを有効にします。 • **プロビジョニング解除**：デバイスからすべてのプロビジョニングポリシーを削除します。通常は、管理する必要がなくなるように、組織で使用されなくなったデバイスに対して実行する必要があります。	

アイテム	説明	データベースフィールド
	ヒント: これらのコマンドは、デバイスの詳細 ページで常に使用できます。また、仮想マシンに対する一括アクションが有効になっている場合、**アクションの選択** メニューの デバイス リストページにも表示されます。この機能は、デフォルトでは無効になっています。有効にするには、一般設定 ページの 許可される一括アクションの下で、**Chrome OS の一括アクションを有効にする** チェックボックスをオンにします。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。 これらの Chrome デバイスのアクションの詳細については、Google のドキュメントを参照してください。	
Microsoft Defender コマンド	管理対象デバイスがこれらのコマンドにアクセスできるようにするには、次の要件を満たす必要があります。 • エージェント管理対象デバイスまたはエージェント不要デバイス • Windows 10 以降、または Windows Server 2016 以降 • PowerShell が必要です 使用可能なコマンドは以下の通りです。 • **Microsoft Defender クイックスキャンを実行**：レジストリキーや Windows スタートアップディレクトリなど、マルウェアの登録が可能な場所をスキャンします。 • **Microsoft Defender フルスキャンを実行**：まず、クイックスキャンを実行し、次に、必要に応じてすべての固定ドライブ、リムーバブルドライブ、およびネッ	

アイテム	説明	データベースフィールド
	トワークドライブのスキャンを実行します。 • **Microsoft Defender の署名を更新**：マルウェア対策の定義を更新します。 • **Microsoft Defender を有効にする**：選択したデバイスで Microsoft Defender をオンにします。 • **ネットワークトラフィックを無効にする**：選択したデバイスとの間のネットワークトラフィックを無効にします。 **ヒント:** Microsoft Defender 一括アクションが有効になっている場合、これらのコマンドは、**アクションの選択** メニューの デバイス リストページからもアクセスできます。この機能は、デフォルトでは無効になっています。有効にするには、一般設定 ページの 許可される一括アクション の下で、**Microsoft Defender の一括アクションを有効にする** チェックボックスをオンにします。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。	

Inventory Information（インベントリ情報）グループ

概要 セクションのアイテムに関する追加の詳細。

セクションまたはアイテム	説明	データベースフィールド
ハードウェア	デバイスのハードウェアに関する情報。 このセクションの変更履歴が有効で、セクションの情報が変更されている場合、見出しの隣に **変更の表示** リンクが表示されます。**変更の表示** をクリックすると、変更されたアイテムのみが表示されます。**変更を非表示** をクリックすると、すべてのアイテムが表示されます。	

セクションまたはアイテム	説明	データベースフィールド
RAMの合計	デバイスにインストールされているランダムアクセスメモリ（RAM）の合計容量。	RAM_TOTAL
使用中のRAM	デバイスで使用中のランダムアクセスメモリ（RAM）の容量。	RAM_USED
RAMの最大容量	デバイスがサポートできるランダムアクセスメモリ（RAM）の合計容量。	RAM_MAX
システム製造元	デバイスの製造元。	CS_MANUFACTURER
システムモデル	デバイスモデル。	CS_MODEL
CSP ID番号	システムのシリアルナンバー。	CSP_ID_NUMBER
資産タグ	**Windows、Chrome および KACE MDM デバイスのみ。**システムのBIOS資産タグ。管理者は、BIOSユーティリティを使用して、この値をシステムで設定できます。	ASSET_TAG
ドメイン	デバイスが参加するWindowsドメイン。	CS_DOMAIN
マザーボードプライマリバス	メインのバス。	MOTHERBOARD_PRIMARY_BUS
マザーボードセカンダリバス	周辺のバス。	MOTHERBOARD_SECONDARY_BUS
プロセッサ	CPUの数、タイプ、および製造元。	PROCESSORS
アーキテクチャ	デバイスのオペレーティングシステムのアーキテクチャ（x86、x64など）。	SYS_ARCH
仮想デバイス	仮想デバイス（VMwareプラットフォームで実行されているデバイスなど）の識別に使用されます。物理デバイス（ノートPC、サーバーなど）には表示されません。	VIRTUAL
Trusted Platform Module (TPM)（信頼済みプラットフォームモジュール（TPM））	TPM 専用のマイクロプロセッサがインストールされているデバイスの場合、TPM が有効化されてアクティブになっているかどうかに関する指定と情報を表示します。 詳細については、「デバイス詳細の Dell Data Protection | Encryption（DDP|E）および暗号	MACHINE_TPM

セクションまたはアイテム	説明	データベースフィールド
	化情報について」を参照してください。	
インテルAMTデバイス	インテル AMT テクノロジ搭載の Intel ベースの Windows デバイスの場合、設定に関する情報を表示します。 詳細については、「デバイス詳細のインテル AMT 情報について」を参照してください。	INTEL_AMT
CD/DVDドライブ	デバイスにインストールされたCD-ROMおよびDVD-ROMドライブの設定。	CDROM_DEVICES
サウンドデバイス	デバイス上のオーディオデバイスに関する情報。	SOUND_DEVICES
ビデオコントローラー	デバイス上のビデオコントローラーに関する情報。	VIDEO_CONTROLLERS
モニタ	デバイスに接続されているモニタのタイプおよび製造元。仮想デバイスの場合、監視情報を表示します（オペレーティングシステムから監視情報がレポートされた場合）。	MONITOR
Appleサポートの情報	Appleのサポートページへのリンク。	なし
SMCバージョン	デバイスCPUのシステム管理コントローラのバージョン。	BIOS_NAME
シリアルナンバー	デバイスのシリアルナンバー。	BIOS_SERIAL_NUMBER
起動ROMのバージョン	デバイスの起動ROMまたはファームウェアのバージョン。	BIOS_VERSION
Dellサービスの情報	デル製ハードウェアに関する情報（「サービスタグ」、「システムタイプ」、「出荷日」、「国」、および保証情報など）。このセクションには、保証期間の残日数を示す 残り日数 列、および保証情報の前回更新日時を示す 前回更新日 列も含まれます。Dellサービスの情報を更新するには、更新 をクリックします。	DELL_WARRANTY
BIOS名	BIOS名。	BIOS_NAME
BIOSバージョン	BIOSのバージョン。	BIOS_VERSION

セクションまたはアイテム	説明	データベースフィールド
BIOSのリリース日	BIOSのバージョンがリリースされた日。	BIOS_DATE
BIOS製造元	BIOSの製造元。	BIOS_MANUFACTURER
BIOSの説明	BIOSの説明。	BIOS_DESCRIPTION
BIOSのシリアルナンバー	BIOSのシリアルナンバー。	BIOS_SERIAL_NUMBER
黒のトナー - 説明	**プリンタのみ**。黒のトナーの形式とモデル。	
黒のトナー - 最大レベル	**プリンタのみ**。黒のトナー粉末の最大レベル。	
黒のトナー - 現在のレベル	**プリンタのみ**。黒のトナー粉末の現在のレベル。トナーが取り付けられていない場合は、このフィールドにメッセージが表示されます。	
シアンのトナー - 説明	**カラープリンタのみ**。シアンのトナーの形式とモデル。	
シアンのトナー - 最大レベル	**カラープリンタのみ**。シアンのトナー粉末の最大レベル。	
シアンのトナー - 現在のレベル	**カラープリンタのみ**。シアンのトナー粉末の現在のレベル。トナーが取り付けられていない場合は、このフィールドにメッセージが表示されます。	
マゼンタのトナー - 説明	**カラープリンタのみ**。マゼンタのトナーの形式とモデル。	
マゼンタのトナー - 最大レベル	**カラープリンタのみ**。マゼンタのトナー粉末の最大レベル。	
マゼンタのトナー - 現在のレベル	**カラープリンタのみ**。マゼンタのトナー粉末の現在のレベル。トナーが取り付けられていない場合は、このフィールドにメッセージが表示されます。	
ｲﾛｰのトナー - 説明	**カラープリンタのみ**。イエローのトナーの形式とモデル。	
イエローのトナー - 最大レベル	**カラープリンタのみ**。イエローのトナー粉末の最大レベル。	

セクションまたはアイテム	説明	データベースフィールド
イエローのトナー - 現在のレベル	**カラープリンタのみ**。イエローのトナー粉末の現在のレベル。トナーが取り付けられていない場合は、このフィールドにメッセージが表示されます。	
ボリューム **n**	ディスクドライブのファイルシステムのタイプとサイズ、およびディスクドライブで使用済みの容量。ドライブ使用状況の変化を確認するには、このフィールド内の **使用状況の履歴を表示** リンクをクリックします。この情報は、使用率が5 %増減すると更新されます。 ボリュームごとに1つのエントリがあります。	MACHINE_DISKS
Hewlett-Packard サービスの情報	**Hewlett-Packard のデバイスのみ**。選択した Hewlett-Packard（HP）デバイスに関する情報。このセクションは、一般設定 ページに製造元の API キーを指定すると入力されます。詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。	
	シリアルナンバー選択された HP デバイスのシリアルナンバー。	シリアル
	製品番号：選択された HP デバイスの固有番号。	PN
	製品名：選択された HP デバイスの名前。	製品
	前回更新日：デバイス情報の前回更新時のタイムスタンプ。	
	サービスステータスタイプ：選択したデバイスのサービスタイプ： • W：保証 • P：固定ケアパック、延長保証に相当 • C：契約、延長保証に相当	SERVICE_TYPE
	タイプ：サービスステータスタイプの説明。例：保証、など。	タイプ
	開始日：保証の開始日。	START_DATE

セクションまたはアイテム	説明	データベースフィールド
	終了日：保証の終了日。	END_DATE
	サービスレベル：デバイスのサービスコードのコンマ区切りリスト。	SERVICE_LEVEL
Lenovo サービスの情報	**Lenovo デバイスのみ**。選択した Lenovo デバイスに関する情報。このセクションは、一般設定 ページに製造元の API キーを指定すると入力されます。詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。	
	製品：選択した Lenovo デバイスの名前。	製品
	購入日：選択した Lenovo デバイスを購入した日付。	購入日
	出荷日：選択した Lenovo デバイスが出荷された日付。	出荷済み
	保証期間：選択した Lenovo デバイスが保証の対象かどうかを示します（ はい または いいえ ）。	IN_WARRANTY
	国：選択した Lenovo プリンタを購入した国。	国
	UpgradeUrl：アップグレード情報を含む URL。	UPGRADE_URL
	前回更新日：デバイス情報の前回更新時のタイムスタンプ。	
	ID：保証の ID。	ID
	タイプ：保証タイプ：不明、ベース、アップグレード、拡張、または インスタント。	タイプ
	開始日：保証の開始日。	START_DATE
	終了日：保証の終了日。	END_DATE
	名前：保証の名前。	
	説明：保証の説明（ 該当する場合 ）。	説明

セクションまたはアイテム	説明	データベースフィールド
プリンタ	このデバイスで使用されるよう構成されたプリンタ。	PRINTERS
ネットワークインターフェイス	イーサネットカードまたは Bluetooth アダプタなどのネットワークインターフェイスのタイプ、および IP アドレス、DHCP（動的ホスト構成プロトコル）が関連付けられている IPv4（インターネットプロトコルバージョン 4）に対して有効か無効かなどの詳細。	MACHINE_NICS
SNMPデータ	デバイス上の MIB（Management Information Base）でデータの SNMP の完全なウォークを実行した結果（完全なウォークを実行するように Authenticated（認証済み）デバイス検出タイプを設定した場合）。Bulk GET で検出を実施した場合には、このセクションは表示されません。	
MACアドレス	デバイスのワイヤレスMACアドレス。	MAC_ADDRESS
DHCP	DHCP がこのネットワークインターフェイスに関連付けられている IPv4 アドレスに対して有効かどうかのインジケータ。	
IPv6 のホスト設定	ネットワークインターフェイスで利用できる 1 つまたは複数の IPv6（インターネットプロトコルバージョン 6）アドレスが記載されているリスト。リストされている各アイテムについて、このセクションでは完全な IPv6 アドレスと IPv6 アドレスプレフィックスでのビット数が表示されます。IPv6 プレフィックスは通常、64 ビットで構成されます。	
DNSホスト名	このネットワークインターフェイスに関連付けられているホスト名。	
Wi-Fi	**KACE MDM デバイスのみ**。デバイスの IP アドレスまたは MAC アドレスです。	
Chrome OS	Chrome関連の情報。	なし

セクションまたはアイテム	説明	データベースフィールド
	注: Chrome値は、MACHINE_CHROMEOS_DETAIL表にあり、MACHINE表にはありません。	
ディレクトリ API ID	Chromeデバイスの固有ID。	DEVICE_ID
ステータス	Chromeデバイスのステータス：アクティブ、プロビジョニング解除済み、非アクティブ、承認済みリターン、リターン要請、出荷済み、不明。	STATUS
終了日をサポート	デバイスがサポートされる最終日。これは、Googleから直接購入されたデバイスのみに適用されます。	SUPPORT_END_DATE
カスタムユーザー	管理者が注釈を付けた、デバイスのユーザー。	ANNOTATED_USER
カスタムの場所	管理者が注釈を付けた、デバイスのアドレスまたは場所。	ANNOTATED_LOCATION
注文番号	デバイスの注文番号。Googleから直接購入したデバイスにのみ注文番号があります。	ORDER_NUMBER
Chrome バージョン	Chromeデバイスのオペレーティングシステムバージョン。	OS_VERSION
プラットフォームバージョン	Chromeデバイスのプラットフォームバージョン。	PLATFORM_VERSION
ファームウェアバージョン	Chromeデバイスのファームウェアバージョン。	FIRMWARE_VERSION
ブートモード	デバイスのブートモード。	BOOT_MODE
組織ユニット	デバイスに関連付けられたGoogle組織単位の名前を使用した完全な親パス。	ORG_UNIT_PATH
自動更新の有効期限	デバイスが自動更新を受信する最終日時。	AUTO_UPDATE_EXPIRATION
モバイル情報	KACE Mobile Device Manager（KMDM）、およびWorkspace ONE?? によって管理されるデバイスからの情報。	なし

セクションまたはアイテム	説明	データベースフィールド
UDID	デバイスの固有デバイス識別子。iOS デバイス専用。	UDID
モデムのファームウェア	モバイルデバイスのファームウェアバージョン。	FIRMWARE_VERSION
デバイスタイプ	**DMMデバイスのみ**です。モバイルデバイスのタイプ。例として、iPhone、iPad、iPod、Android Phone、Android タブレットなどがあります。	DEVICE_TYPE
ICCID	**KACE MDM および DMM デバイスのみ**。デバイスの SIM カードの固有のシリアル番号。	ICCID
IMEI	**KACE MDM および DMM デバイスのみ**。デバイスの国際移動体装置識別番号。	IMEI
音声ローミング有効	**KACE MDM Android フォンのみ**。選択した KACE MDM Android フォンの音声ローミングが有効になっているかどうかを示すインジケータ。	VOICE_ROAMING_ENABLED
データローミング有効	**KACE MDM Android フォンのみ**。選択した KACE MDM Android フォンのデータローミングが有効になっているかどうかを示すインジケータ。	DATA_ROAMING_ENABLED
MEID	**KACE MDM デバイスのみ**。移動体装置識別子。これは、選択したモバイルデバイスの固有の識別子です。	MEID
電話番号	**DMMデバイスのみ**です。デバイスに関連付けられた電話番号。	PHONE_NUMBER
携帯電話会社	**KACE MDM および DMM デバイスのみ**。モバイルネットワークキャリア。	CARRIER
Bluetooth MAC アドレス	**DMMデバイスのみ**です。デバイスの Bluetooth 用のメディアアクセス制御アドレス。	BLUETOOTH_MAC
バッテリレベル	**KACE MDM および DMM デバイスのみ**。前回更新時のバッテリ充電量（パーセント単位）。	BATTERY_LEVEL

セクションまたはアイテム	説明	データベースフィールド
前回チェックイン	デバイス情報の前回更新時のタイムスタンプ。	LAST_CHECK_IN
前回の登録時	Google管理コンソールでデバイスが最後に登録された日付と時刻。	LAST_ENROLLMENT_TIME
登録済み	**KACE MDM および Workspace ONE デバイスのみ。** KACE MDM または Workspace ONE コンソールでデバイスが最後に登録された日付と時刻。	IS_ENROLLED
監視あり	**KACE MDM iOS デバイスのみ。**選択した KACE MDM iOS デバイスが監視されているかどうかを示すインジケータ。これは、iOS デバイスで最高レベルの制御です。	IS_SUPERVISED
アクセス不可モード	**KACE MDM iOS 監視対象デバイスのみ。**選択した KACE MDM iOS デバイスがアクセス不可モードであるかどうかを示すインジケータ。アクセス不可モードでは、サードパーティによるデバイスのロック解除はできません。	IS_LOST
Encrypted（暗号化済み）	**KACE MDM デバイスのみ。**選択した KACE MDM iOS デバイスが暗号化モードであるかどうかを示すインジケータ。	IS_ENCRYPTED
ロケータサービス有効	**KACE MDM iOS デバイスのみ。**選択した KACE MDM iOS デバイスでロケータサービスが有効になっているかどうかを示すインジケータ。このサービスは、デバイスが応答している場合、デバイスの位置情報を取得します。	LOCATOR_SERVICE_ENABLED
アクティベーションロック有効	**KACE MDM iOS デバイスのみ。**選択した KACE MDM iOS デバイスでアクティベーションロックが有効になっているかどうかを示すインジケータ。この機能は、iOS デバイスを紛失した場合、または盗難にあった場合に、他の人が iOS デバイスを使用できないようにします。	ACTIVATION_LOCK_ENABLED
ルート化	**KACE MDM Android デバイスのみ。**選択した KACE MDM Android デバイスの OS がロック解除されているかどうかを示すインジケータ。	IS_ROOTED

セクションまたはアイテム	説明	データベースフィールド
コンプライアンス	**Workspace ONE デバイスのみ**。デバイスが事前設定された Workspace ONE コンプライアンスルールに適合しているかどうかを示します。	IS_COMPLIANT
現在のモバイルネットワーク	**Workspace ONE デバイスのみ**。Workspace ONE デバイスに関連付けられているモバイルネットワークの名前。	なし
アクティベーションロックのバイパスコード	**KACE MDM iOS DEP 管理対象デバイスのみ**。アクティベーションロックが有効な場合にデバイスパスワードとして使用できるバイパスコード。	ACTIVATION_LOCK_BYPASS_CODE
監視付きアクティベーションロックを許可	**KACE MDM iOS DEP 管理対象デバイスのみ**。デバイスに対してアクティベーションロックが有効かどうかを示します。アクティベーションロックを使用すると、ユーザーはパスワードをバイパスし、アクティベーションロックのバイパスコードを使用してデバイスにログインできます。	ACTIVATION_LOCK_ALLOWED
DEP 管理対象	**KACE MDM iOS デバイスのみ**。デバイスが Apple デバイス登録プログラム（DEP）によって管理されているかどうかを示します。	IS_DEP_MANAGED
DEP プロファイル	**KACE MDM iOS DEP 管理対象デバイスのみ**。デバイスに関連付ける DEP プロファイルの名前。	DEP_PROFILE
次によって割り当てられた DEP プロファイル	**KACE MDM iOS DEP 管理対象デバイスのみ**。デバイスに DEP プロファイルを割り当てたユーザーアカウントの名前。	DEP_ASSIGNED_BY
DEP プロファイル割り当て日	**KACE MDM iOS DEP 管理対象デバイスのみ**。デバイスに DEP プロファイルが割り当てられた日付。	DEP_ASSIGNED_DATE
DEP プロファイルステータス	**KACE MDM iOS DEP 管理対象デバイスのみ**。デバイスの管理ステータス： • **割り当て済み**：Apple DEP がプロファイルを受信し、	DEP_PROFILE_STATUS

セクションまたはアイテム	説明	データベースフィールド
	デバイスに割り当てる準備ができました。 • **空**：プロファイルがデバイスに割り当てられていません。 • **プッシュ済み**：プロファイルがアクティブ化されたデバイスに配信されます。 • **削除済み**：プロファイルがデバイスに割り当てられましたが、削除されました。デバイスが再アクティブ化されると、KACE MDM はデバイスを管理しなくなります。	
設定されたデバイス	**KACE MDM iOS DEP 管理対象デバイスのみ。**	IS_DEP_CONFIGURED
応答不可	デバイスが応答不可モードかどうかを示します。	DO_NOT_DISTURB_ENABLED
Exchange デバイス ID	デバイスに割り当てられている Microsoft Exchange ID。	EAS_DEVICE_ID
最初の登録	デバイスが KACE MDM に登録された日付。	ENROLLMENT_DATE
iCloud が有効	**KACE MDM iOS デバイスのみ。** デバイスでクラウドが有効かどうかを示します。	ICLOUD_ENABLED
最後の iCloud バックアップ	**KACE MDM iOS デバイスのみ。** Apple iCloud が最後にデバイスにバックアップされた日付。	ICLOUD_LAST_BACKUP
iTunes にログイン	**KACE MDM iOS デバイスのみ。** デバイスが iCloud にログインしているかどうかを示します。	IS_ITUNES_ACCOUNT_ACTIVE
Wi-Fi 受信済み	**KACE MDM Android デバイスのみ。** Wi-Fi ネットワーク経由でデバイスが受信したバイト数。	WIFI_BYTES_RECV
Wi-Fi 送信済み	**KACE MDM Android デバイスのみ。** デバイスが Wi-Fi ネットワーク経由で送信したバイト数。	WIFI_BYTES_SENT
WWAN 受信済み	**KACE MDM Android デバイスのみ。** モバイルネットワーク経由でデバイスが受信したバイト数。	WWAN_BYTES_RECV

セクションまたはアイテム	説明	データベースフィールド
WWAN 送信済み	**KACE MDM Android デバイスのみ**。モバイルネットワーク経由でデバイスが送信したバイト数。	WWAN_BYTES_SENT
エージェント	エージェント関連の情報。	なし
エージェントのバージョン	デバイスにインストールされている KACE エージェントのバージョン番号。	CLIENT_VERSION
接続済み	デバイス上のエージェントのメッセージプロトコルサービスがアプライアンスに接続した時間。	CONNECT_TIME
切断	切断されている場合、デバイス上のエージェントのメッセージプロトコルサービスがアプライアンスから切断された時間。	DISCONNECT_TIME
KACE ID	アプライアンスデータベースでデバイスの識別に使用される文字列。	KUID
データベースID	アプライアンスデータベースでデバイスの識別に使用される一意の番号。	ID
手動エントリ	インベントリ情報が、WSAPIまたはXMLアップロードを通じて手動で追加されたことを示すフィールド。	MANUAL_ENTRY
デバイスエントリタイプ	デバイスの管理方法を示すフィールド: エージェントデバイス、エージェント不要デバイス、または 手動で入力されたレコード。接続プロトコルを変更するには、**編集** をクリックします。	なし
前回のインベントリ	前回のインベントリレポート作成日時。	LAST_INVENTORY
前回の同期	エージェント管理対象デバイスの場合は、デバイスが前回アプライアンスにログインした時間。エージェント不要デバイスの場合は、アプライアンスが前回デバイスに接続してインベントリを収集した時間。	LAST_SYNC
前回のエージェントのアップデート	KACE エージェントに対する前回の更新時間（ある場合）。	LAST_CLIENT_UPDATE

セクションまたはアイテム	説明	データベースフィールド
Konductor タスク	エージェント管理対象デバイスで、現在実行されているタスク、またはスケジュールされているタスクのステータス。このセクションには、各タスクに関する次の情報が表示されます。 • **タスクタイプ**：タスクのタイプ。アプライアンス設定に応じて、警告、インベントリ、kbot、krashアップロード、スクリプト更新などのタスクタイプが存在します。 • **開始時間**：タスクの開始時刻。 • **完了**：タスクの完了時刻。 • **次のスケジュール**：スケジュールに基づく次のタスク実行時刻。 • **タイムアウト**: タスクの完了における時間制限。 • **優先度**：タスクの重要度またはランク。 この情報は、エージェントタスクリストページにも表示されます。詳細については、「エージェントタスクのステータスの表示」を参照してください。	なし
検疫	KACE エージェントの認証に関連する情報。	なし
検疫レコード	このエージェントの検疫の詳細へのリンク。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。	KUID
承認時刻	KACE エージェントがアプライアンスによって認証される日付と時刻。	APPROVED_TIME
使用中のトークン	KACE エージェントがトークンを使用してアプライアンスに登録した場合、このフィールドにはトークン名とトークンの詳細へのリンクが含まれます。	TOKEN_ID
承認者	アプライアンス管理者によりアクセスが許可された後に KACE エージェントがアプライアンスに接続した場合、このフィールドに	APPROVED_BY

セクションまたはアイテム	説明	データベースフィールド
	はエージェントの接続を承認した管理ユーザーの名前が表示されます。	
ユーザー	デバイスユーザーに関連する情報。	なし
ログに記録されたユーザー	デバイスに現在ログインしているユーザー。このエントリには、ユーザー名と、そのユーザーが属しているドメインが含まれます。	USER_LOGGED
ユーザーフルネーム	デバイスを所有しているユーザーのフルネーム。	USER_FULLNAME
ユーザー名	現在のユーザーの名前。	USER_NAME
ユーザードメイン	ユーザーが属しているドメイン。	USER_DOMAIN
オペレーティングシステム	デバイスのオペレーティングシステムに関する情報。	なし
名前	デバイスのオペレーティングシステム（Windows、Mac OS X、またはLinuxなど）。	OS_NAME
サービスパック	サービスパックのバージョン番号（Windows または SUSE Linux Enterprise サーバーのみ）。	SERVICE_PACK
オペレーティングシステムのバージョン	オペレーティングシステムのバージョン番号。	OS_VERSION
オペレーティングシステムのビルドのバージョン	オペレーティングシステムのビルド番号。	OS_BUILD
数値	オペレーティングシステムの番号。	OS_NUMBER
オペレーティングシステムのアーキテクチャ	デバイスのオペレーティングシステムのアーキテクチャ（x86、x64など）。	OS_ARCH
ドメイン	デバイスが参加するWindowsドメイン。	CS_DOMAIN
オペレーティングシステムのインストール日	オペレーティングシステムがインストールされた日付。	OS_INSTALLED_DATE
前回のスタートアップ	オペレーティングシステムの稼働時間。	LAST_REBOOT

セクションまたはアイテム	説明	データベースフィールド
前回の再起動からの稼働時間	再起動以降のデバイスの稼働時間。	UPTIME
システムディレクトリ	システムディレクトリの場所。	SYSTEM_DIRECTORY
レジストリサイズ	レジストリのサイズ。	REGISTRY_SIZE
レジストリの最大サイズ	レジストリの最大サイズ。	REGISTRY_MAX_SIZE
ページファイルサイズ	Windowsページファイルの現在のサイズ。	PAGEFILE_SIZE
ページファイル最大サイズ	Windowsページファイルの最大サイズ。	PAGEFILE_MAX_SIZE
IEバージョン	デバイスにインストールされているInternet Explorerのバージョン。	IE_VERSION
Edge のバージョン	デバイスにインストールされている Microsoft Edge のバージョン。	EDGE_VERSION
WMIのステータス	Windows Management Instrumentation（WMI）サービスのステータス（Windowsデバイスのみ）。	WMI_STATUS
ドライブ暗号化	暗号化に関する情報（DDP|E クライアントの他に、BitLocker または FileVault2 もデバイスにインストールされている場合）。 詳細については、「デバイス詳細の Dell Data Protection | Encryption（DDP|E）および暗号化情報について」を参照してください。	
ドライブ暗号化摘要	導入されている暗号化テクノロジと、その暗号化が有効になっているかどうかを識別します。	なし
Dell Data Protection | Encryption（DDP|E）	DDP|E に関する設定およびステータス情報。	なし
BitLocker	Windows BitLocker に関する設定およびステータス情報。	なし
FileVault	Mac OS X FileVault 2 に関する設定およびステータス情報。	なし

セクションまたはアイテム	説明	データベースフィールド
場所	Workspace ONE または KACE MDM Cloud によって管理されるデバイスからの情報。	
アドレス	選択したデバイスの住所。	STREET_ADDRESS
市町村	選択したデバイスがある市町村。	LOCALITY
都道府県	選択したデバイスがある都道府県。	地域
国	デバイスがある国。	国
緯度	最後の更新中に検出されたデバイスの緯度。	LATITUDE
経度	最後の更新中に検出されたデバイスの経度。	LONGITUDE
前回の更新	デバイス情報の前回更新時のタイムスタンプ。	LAST_UPDATE
メモ	任意の追加情報を入力します。	NOTES
仮想マシン	ESXi ホストまたは Hyper-V サーバが選択されている場合、選択したデバイスに関連付けられている仮想マシンがこのグループに一覧表示されます。このリストの一部の情報は、VMware Tools/Microsoft 統合サービスが仮想マシンにインストールされている場合にのみ使用可能です。一部の列が入力されていない場合、VMware ツールまたは Microsoft 統合サービスがないことが原因である可能性があります。	
名前	仮想マシンの名前。	名前
ホスト名	仮想マシンに割り当てられたホスト名。仮想マシンがすでに KACE エージェントによってプロビジョニングされている場合、この列に表示される名前はハイパーリンクとして表示されます。リンクをクリックすると、ページが更新されてプロビジョニングされた仮想マシンのデバイスの詳細が表示されます。	HOSTNAME

セクションまたはアイテム	説明	データベースフィールド
IPアドレス	仮想マシンに割り当てられたプライマリIPアドレス。	IP
状態	仮想マシンが実行されているかどうかを示します。可能な値は次のとおりです。 • **0 - 実行中**：仮想マシンが正常に実行されています。 • **1 - シャットダウン中**：仮想マシンには、保留中のシャットダウンコマンドがあります。 • **2 ??? リセット**：仮想マシンには、保留中のリセットコマンドがあります。 • **3 ??? スタンバイの保留中**：仮想マシンには、保留中のスタンバイコマンドがあります。 • **4 ??? 実行されていません**：仮想マシンは実行されていません。 • **5 ??? 不明**：仮想マシン情報は使用できません。	MACHINE_VIRTUAL_STATE
ステータス	仮想マシンのステータス。可能な値は次のとおりです。 • **0 ??? OK**: 問題はありません。 • **1 ??? 警告**：問題がある可能性があります。 • **2 ??? エラー：明らかな問題**です。 • **3 ??? 不明**：ステータスが不明です。	MACHINE_VIRTUAL_STATUS
ハードウェアバージョン	仮想マシンのハードウェアバージョンには、仮想マシンでサポートされている仮想ハードウェア機能が反映されます。	HARDWARE_VERSION
ハイパーバイザ	vCenter または SCVMM 環境が選択されている場合、vCenter または SCVMM によって管理されるハイパーバイザがこのグループに一覧表示されます。	
ホスト名	ESXi ホストまたは Hyper-V サーバに割り当てられたホスト名。ESXi または Hyper-V デバイ	なし

セクションまたはアイテム	説明	データベースフィールド
	スがすでにインベントリに追加されている場合は、この列に表示される名前はハイパーリンクとして表示されます。リンクをクリックすると、ページが更新され、選択済みデバイスのデバイス詳細が表示されます。	
プラットフォーム	関連する ESXi または Hyper-V ハイパーバイザのプラットフォームとバージョン。	PLATFORM
IPアドレス	ESXiホストに割り当てられているIPアドレス。	なし
仮想マシン	ESXi または Hyper-V ハイパーバイザ上の仮想マシンの数。	なし
システムのシリアル番号	ESXi または Hyper-V ハイパーバイザをホストしているデバイスのシリアル番号。	なし
ステータス	ESXiホストのステータス。	なし
SDA 導入情報	KACE システム導入アプライアンス (SDA) から導入されたデバイスを選択すると、このグループに導入の詳細が表示されます。	
導入時間	導入が正常に完了した時刻。	SDA_DEPLOYMENT_TIME
導入タイプ	スクリプト形式のインストール、システムイメージ、カスタム導入など、導入のタイプ。	SDA_DEPLOYMENT_TYPE
導入名	KACE SDA で指定されている導入の名前。	SDA_DEPLOYMENT_NAME
導入 URL	関連付けられた KACE SDA での導入の URL。	SDA_DEPLOYMENT_URL
導入 ID	KACE SDA での導入の ID。	SDA_SCRIPTED_INSTALLATION_ID
SDA 名	KACE SDA のホスト名または IP アドレス。	SDA_NAME
SDA URL	KACE SDA の URL。	SDA_URL
バッテリ	このグループには、Windows、Linux、および MacOS エージェントおよびエージェント不要の管理対象デバイスのバッテリ情報が表示されます。	

セクションまたはアイテム	説明	データベースフィールド
充電	現在のバッテリ容量の割合。	CHARGE_PERCENT
Chemistry	**Windows および Linux デバイスのみ**。リチウムイオンなどのバッテリタイプ。	CHEMISTRY
現在の容量（mWh）	現在のバッテリ容量。	CURRENT_CAPACITY
Design Capacity (mWh)（設計容量（mWh））	設計上のバッテリの最大容量。	DESIGN_CAPACITY
Full Charge Capacity (mWh)（フル充電容量（mWh））	バッテリの現在の最大容量。この値は時間の経過とともに低下します。	FULL_CHARGE_CAPACITY
正常性（%）	最大設計容量に対する現在のバッテリ容量の割合。	HEALTH_PERCENT
製造元	バッテリの製造元。	MANUFACTURER
名前	バッテリの名前またはモデル。	名前
電源に接続済み	バッテリが現在電源に接続されているかどうかを示すインジケータ。	PLUGGED_IN
Recharge Count（再充電カウント）	**MacOS デバイスのみ**。バッテリが再充電された回数。	RECHARGE_COUNT
シリアルナンバー	バッテリのシリアルナンバー。	シリアル
残り時間（分）	バッテリが放電するまでの時間（分）。バッテリが接続されている場合、このフィールドは空白になります。	TIME_REMAINING

ソフトウェア グループ

デバイスにインストールされているアプリケーションの詳細（パッチ適用情報、実行中のプロセス、およびスタートアッププログラムなど）。

セクション	説明	データベースフィールド
インストールされているプログラム	デバイスにインストールされているソフトウェアのリスト。 このセクションの変更履歴が有効で、セクションの情報が変更されている場合、見出しの隣に **変更の表示** リンクが表示されます。**変更の表示** をクリックすると、変更されたアイテムのみが表示されます。**変更を非表示** をクリックする	なし

セクション	説明	データベースフィールド
	と、すべてのアイテムが表示されます。	
検出されたソフトウェア	検出されたアプリケーションはアプライアンスインベントリ内で実行可能で、ソフトウェアカタログに定義されたアプリケーションと一致します。検出されたアプリケーションおよびスイートに対して、メータリングの有効化や「不許可」としてのマーク付けを行ったり、ライセンス情報の追加を行うことができます。また、検出されたアプリケーションのリストをCSV形式でエクスポートすることもできます。検出されたアプリケーションのリスト、カタログ未登録のリスト、ローカルカタログ登録済みのリストはエクスポートできますが、ソフトウェアカタログ全体のエクスポートはできません。	なし
メータリングしたソフトウェア	メータリングが有効化されているアプリケーション。	なし
カスタムインベントリフィールド	このデバイスに対して作成されたカスタムインベントリフィールドのフィールド名と値が示されたリスト。	なし
アップロードファイル	「ファイルのアップロード」スクリプトアクションを使用してこのデバイスからアプライアンスにアップロードされたファイル。	なし
ソフトウェアインベントリにインストール済みと報告されているパッチ	このデバイスにインストールされたMicrosoftのパッチ。 このセクションの変更履歴が有効で、セクションの情報が変更されている場合、見出しの隣に **変更の表示** リンクが表示されます。**変更の表示** をクリックすると、変更されたアイテムのみが表示されます。**変更を非表示** をクリックすると、すべてのアイテムが表示されます。	なし
実行中のプロセス	デバイスで実行されているプロセスのリスト。 このセクションの変更履歴が有効で、セクションの情報が変更されている場合、見出しの隣に **変更の表示** リンクが表示されます。**変更の表示** をクリックすると、変更されたアイテムのみが表示されま	なし

セクション	説明	データベースフィールド
	す。**変更を非表示** をクリックすると、すべてのアイテムが表示されます。	
スタートアッププログラム	デバイスのスタートアッププログラムのリスト。 このセクションの変更履歴が有効で、セクションの情報が変更されている場合、見出しの隣に **変更の表示** リンクが表示されます。**変更の表示** をクリックすると、変更されたアイテムのみが表示されます。**変更を非表示** をクリックすると、すべてのアイテムが表示されます。	なし
サービス	デバイスで実行されているサービスのリスト。 このセクションの変更履歴が有効で、セクションの情報が変更されている場合、見出しの隣に **変更の表示** リンクが表示されます。**変更の表示** をクリックすると、変更されたアイテムのみが表示されます。**変更を非表示** をクリックすると、すべてのアイテムが表示されます。	なし

Activities（アクティビティ）グループ

デバイスで実行されるアクションに関する情報。

セクション	説明	データベースフィールド
監視	サーバー監視に関連する情報（サーバー監視が有効で、デバイスのオペレーティングシステムがサポートされている場合）。 オペレーティングシステムがサポートされていない場合、このことがメッセージとして表示されます。 デバイスが監視対象であるが、監視が有効ではない場合、**監視を有効にする** ボタンが表示されます。	なし
アクティブ/一時停止	このデバイスで監視が有効化されているかどうか。	なし
プロファイル	このデバイスに割り当てられている警告基準プロファイル。	なし
メンテナンスウィンドウ	このデバイスに割り当てられているメンテナンスウィンドウ。	なし

セクション	説明	データベースフィールド
レベル/警告	警告のレベルを示すアイコンが含まれた、このデバイスでアクティブな警告。	なし
ラベル	このデバイスに割り当てられたラベル。ラベルを使用して、マシンと資産を整理したり分類したりします。	なし
失敗した管理対象インストール	インストールに失敗した管理対象インストールのリスト。管理対象インストールの詳細を確認するには、**管理対象インストールの詳細** リンクをクリックします。	なし
管理対象インストール リスト	アプライアンスへの次回接続時にデバイスに送信されるようにスケジュールされている管理対象インストールのリスト。	なし
サービスデスクチケット	このデバイスに関連付けられているチケットのリスト。これらは、デバイス所有者に割り当てられたチケットまたはデバイス所有者によって送信されたチケットである場合があります。チケットの詳細を表示するには、チケットID（例えば、TICK: 0032）をクリックします。	なし
SNMPインベントリ設定	このデバイスに関連付けられたSNMP インベントリ設定のリスト。設定の詳細にアクセスしたり、設定を追加したりするには、**関連するSNMP設定の管理** をクリックします。	なし

セキュリティ グループ

パッチ適用およびデバイスの脆弱性に関連する情報。

セクション	説明	データベースフィールド
パッチ適用の検出/デプロイのステータス	デバイス上で検出および展開されたパッチのリスト。 パッチ適用が試行されたにもかかわらず失敗に終わった場合、**試行回数のリセット** をクリックすると、パッチ適用の最大許容試行回数をリセットできます。	なし
脅威レベル5のリスト	デバイス上のアプリケーション、プロセス、スタートアップアイテ	なし

セクション	説明	データベースフィールド
	ム、またはサービスに有害な脅威。	
Windows Feature Update ステータス	デバイス上で検出および展開された Windows Feature Update タスクのリスト。 更新プログラムが試行されたにもかかわらず失敗に終わった場合、**試行回数のリセット** をクリックすると、パッチ適用の最大許容試行回数をリセットできます。	
OVAL脆弱性	このデバイスで実行された OVAL（Open Vulnerability Assessment Language）脆弱性テストの結果。このデバイスで失敗したテストのみがOVAL ID別に示され、「脆弱」としてマークされます。合格したテストはグループ化され、「安全」としてマークされます。	なし
SCAP設定スキャン	このデバイスで実行されたFDCC/SCAP設定スキャンの結果。	なし
Linux パッケージリポジトリ情報	デバイスに関連付けられた Linux パッケージリポジトリへの URL のリスト。	なし
Linux パッケージアップグレードのステータス	デバイス上で検出および展開されたパッチのリスト。 パッチ適用が試行されたにもかかわらず失敗に終わった場合、**試行回数のリセット** をクリックすると、パッチ適用の最大許容試行回数をリセットできます。	なし
Microsoft Defender	Microsoft Defender のコンポーネントとそのプロパティの一覧（概要、マルウェア対策、スパイウェア対策、ウイルス対策、およびウイルス対策ネットワーク検査、リアルタイム保護、改ざん防止）。	なし
Microsoft Defender の脅威履歴	Microsoft Defender で検出された脅威のリスト。各脅威について、リストにはその名前、最初に検出された日時、重大度、脅威が隔離されているかどうか、および脅威が起動されてアクティブであるかどうかが表示されます。その他の詳細については、脅威をクリックし、表示されるダイアログボックスで、脅威のカテゴリ、タイプ、起動ステータス、検出ソース、お	なし

セクション	説明	データベースフィールド
	よび影響を受けるファイルを確認できます。	

Dell Command | Monitor - Monitor グループ

Dell Command | Monitor - Monitor を使用して選択した Dell クライアントシステムに関する追加のインベントリ情報。

セクション	説明	データベースフィールド
警告	DCM ログエントリ。これらは、ファームウェアが検出したハードウェアエラーを示すことがあります。	なし
ハードウェア	詳細なバッテリ仕様と使用率データ、サービスプロセッサの有無と設定、メモリインベントリ、接続された Dell モニタなど、収集された情報。	なし

Dell Command | Monitor を使用してアプライアンスがクエリを実行したクラスおよびプロパティについては、「Dell Command | Monitor について」を参照してください。

Dellアップデート グループ

更新プログラムおよびインベントリに関する情報（ Dellデバイスのみ ）

セクション	説明	データベースフィールド
Dell アップデートの検出と展開のステータス	デバイスで検出および展開された Dell アップデートと、関連するスケジュールのリスト。 更新プログラムが試行されたにもかかわらず失敗に終わった場合、**試行回数のリセット** をクリックすると、更新プログラムの最大許容試行回数をリセットできます。	なし

ログと診断 グループ

アプライアンスレコードに関連する情報。

- **管理サービスログ**: アプライアンス管理サービスの主な役割は、オフラインKScriptを実行することです。管理サービスログには、オフライン KScript を実行するために管理サービスによって実行された
- 手順が表示されます。これらの手順には、依存関係のダウンロードとKBOTSファイルの検証が含まれます。オフラインKScriptの実行時に発生したエラーはすべて管理サービスログに記録されます。
- **ブートストラップログ** : アプライアンスは、初めてチェックインしたデバイスに関するインベントリ情報を得るために、ブートストラップ要求を送信します。この要求に関するログはブートストラップログに表示されます。
- **クライアントログ**: アプライアンスからエージェントに要求を送信することによって、要求インベントリ情報を定期的に取得します。デバイス上でのスクリプトの実行により、インベントリ情報がアプライアンス

に送信され、インベントリがアプライアンスにアップロードされます。エージェントログにはこれらのアクションが表示されます。

- **スクリプトアップデータ**: デバイスから定期的に要求を送信することにより、オフラインKScriptでの変更に関する最新情報を取得します。スクリプトアップデータログには、この情報が表示されます。
- **エージェント不要インベントリステータスメッセージ**：このログには、エージェント不要管理対象デバイスからのインベントリデータの収集と送信に関連するメッセージが表示されます。

セクション	説明	データベースフィールド
エージェントログ	KACE エージェントのログ。	なし
Agent Diagnostic Files（エージェント診断ファイル）	このページで **アクションの選択 > エージェントファイルをアップロードする** を選択してアップロードしたファイル。	なし
ユーザーコンソールのインストールログ	このデバイスにインストールされた**ユーザーコンソール**パッケージに関する詳細。	なし
スクリプトログ	このデバイスで実行された設定ポリシースクリプトと、進行中のスクリプトの使用可能ステータス。	なし
サーバ側のデバイスのログデータ	選択したデバイスのログエントリ。このセクションでは、関連する各ログの最後の 5 つのエントリを示し、既存の問題をトラブルシューティングできるようにします。	なし
デバイスアクティビティ	**Chrome デバイスのみ**。デバイスが最後にアクティブになった日付、デバイスがアクティブになった時間の長さ、およびアクティビティ履歴が表示されます。アクティビティ履歴の各エントリには、日付と長さ、または各ユーザーセッションが表示されます。	なし

資産 グループ

このセクションには、このデバイスに関連付けられている資産の詳細が表示されます。**この資産の編集** リンクをクリックすると、資産情報を編集できます。

セクション	説明	データベースフィールド
資産情報	資産の詳細（レコードの作成日時とレコードの前回更新日時、資産タイプ（デバイスなど）、および資産の名前など）。	なし
バーコード	この資産に関連付けられているバーコード（存在する場合）。	なし

セクション	説明	データベースフィールド
関連する資産	この資産に関連付けられている資産（親資産や子資産など）。	なし
タスク履歴	デバイスで実行されているタスクのリスト。	なし

デバイス詳細の Dell Data Protection | Encryption（DDP|E）および暗号化情報について

ネットワーク内のデバイスに DDP|E クライアントがインストールされている場合、アプライアンスはステータスおよび設定情報を収集して、デバイスの詳細 ページに表示できます。

Windows DDP|E クライアントで設定する必要があるレジストリキー

アプライアンスが Windows DDP|E クライアントから詳細なインベントリを収集できるようにするための要件は、クライアントで DumpXmlInventory キーを設定することです。

キー: HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters
DWORD Value: DumpXmlInventory
Data: 0x1

このレジストリ値を設定すると、DDP|E が inventory.xml ファイルをターゲットデバイスに書き込みます。書き込まれたファイルは、インベントリによって解析されます。詳細については、「Windows DDP|E クライアントデバイスでインベントリ収集を許可するための Dump Inventory レジストリキーの追加」を参照してください。

この要件は、Windows にのみ適用されます。

Dell Data Protection | Encryption（DDP|E）

DDP|E はさまざまなアプリケーションで構成されており、ユーザーは次の操作を実行できるようになります。

- デスクトップ、ラップトップ、および外付けメディアでデータセキュリティリスクを検出します。
- アクセス制御ポリシー、認証、および機密データの暗号化を実施して、これらのデバイス上でデータを保護します。
- 既存のユーザーディレクトリに統合されるコラボレーションツールを使用して、ポリシーに従ってデータを一元管理します。
- キーとデータのリカバリ、自動更新、および保護されているデバイスの追跡をサポートします。

DDP|E 用にサポートされている OS

オペレーティングシステム	バージョン
Windows	7, 8, 8.1
Mac OS X	10.7.5、10.8.3 ～ 10.8.5、10.9.2 ～ 10.9.3

デバイスの詳細 ページに表示される DDP|E 情報

??	??	MACHINE_DDPE
アイテム	説明	データベースフィールド
固有のID	DDP|E サーバーによって使用される DDP|E クライアントの識別。	MCID

??	??	MACHINE_DDPE
アイテム	説明	データベースフィールド
エージェントのバージョン	インストールされている DDP|E クライアントのバージョン。	AGENT_VERSION
サーバーのホスト名	この DDP|E クライアントを管理している DDP|E サーバーのホスト名。	SERVER_HOSTNAME
保護ステータス	値の例として、Protected（保護されている）と Unprotected（保護されていない）があります。値が Locked（ロック済み）または Unknown（不明な）の場合、問題が発生している可能性があります。	PROTECTION_STATUS
最後に生成されたインベントリ	DDP|E クライアントインベントリが最後に発生したときのタイムスタンプ。K1 インベントリと混同しないでください。	PROTECTION_STATUS_UPDATED

デバイスの詳細 ページに表示される DDP|E ボリューム情報

??	??	MACHINE_DDPE_VOLUME
アイテム	説明	データベースフィールド
デバイス	オペレーティングシステムによってレポートされるデバイス / ボリュームの名前。	DEVICE_ID
保護ステータス	DDP|E クライアントでの DDP|E 保護の現在のレベル / ステータスを示します。	PROTECTION_STATUS
保護の理由	DDP|E クライアントで使用される保護の手段。オプションは通常 VendorProtected で、これは DDP|E または BitLocker を示します。	PROTECTION_REASON

BitLocker

BitLocker は、Windows に付属しているディスク全体の暗号化機能です。

BitLocker 用にサポートされている OS

オペレーティングシステム	バージョン
Windows	Vista、7（Enterprise および Ultimate）
Windows	8、8.1（Pro および Enterprise）
Windows Server	2008、2008 R2、2012、2012 R2

デバイスの詳細 ページに表示される BitLocker 情報

?? アイテム	?? 説明	MACHINE_BITLOCKER_VOLUME データベースフィールド
デバイスID	システム上のボリュームの一意の識別子。	DEVICE_ID
永続ボリューム ID	システム上のボリュームの永続的な識別子。	PERSISTENT_VOLUME_ID
保護ステータス	BitLocker がボリュームを保護しているかどうかを示します。 • Protection Off（保護オフ） • Protection On（保護オン） • Protection Unknown（保護不明）	PROTECTION_STATUS
メタデータバージョン	可能な値は次のとおりです。 • 0 • 1 • 2	バージョン
暗号化方式	使用される暗号化のタイプ。例えば、AES-128 です。可能な値は次のとおりです。 • なし • AES-128 with Diffuser • AES-256 with Diffuser • AES-128 • AES-256 • Encrypted（暗号化済み） • 不明	SELF_ENCRYPTION_DRIVE _ENCRYPTION_METHOD（自己暗号化ドライブのみ） ENCRYPTION_METHOD（ソフトウェアベースの暗号化のみ）
ハードウェア暗号化ステータス	**注:** ハードウェア暗号化ステータスプロパティは、Windows 8 以降のシステムでサポートされています。	HARDWARE_ENCRYPTION_STATUS

?? アイテム	?? 説明	MACHINE_BITLOCKER_VOLUME データベースフィールド
	可能な値は次のとおりです。 • 不明 • サポートされていません • No Protection（保護なし） • Uses Software（ソフトウェアを使用） • Uses Hardware（ハードウェアを使用）	
ロックステータス	可能な値は次のとおりです。 • 不明 • Unlocked（ロック解除） • Locked（ロック済み）	LOCK_STATUS
変換ステータス	変換のステータス。可能な値は次のとおりです。 • 不明 • Fully Decrypted（完全復号化） • Fully Encrypted（完全暗号化） • Encryption In Progress（暗号化進行中） • Decryption In Progress（復号化進行中） • Encryption Paused（暗号化一時停止） • Decryption Paused（復号化一時停止）	CONVERSION_STATUS
暗号化率	率として表示される変換の程度。	ENCRYPTION_PERCENTAGE

?? アイテム	?? 説明	MACHINE_BITLOCKER_VOLUME データベースフィールド
消去ステータス	空き領域の消去のステータス。可能な値は次のとおりです。 • 不明 • Free Space Not Wiped（空き領域未消去） • Free Space Wiped（空き領域消去済み） • Free Space Wiping In Progress（空き領域消去中） • Free Space Wiping Paused（空き領域消去ー時停止）	WIPING_STATUS
消去率	率として表示される空き領域消去の程度。	WIPING_PERCENTAGE
Key Protectors（キープロテクタ）	導入されているキープロテクタ。可能な値は次のとおりです。 • 不明 • Trusted Platform Module (TPM)（信頼済みプラットフォームモジュール（TPM）） • External Key（外部キー） • Numerical Password（数値パスワード） • TPM and PIN（TPM および PIN） • TPM and Startup Key（TPM および起動キー） • TPM and PIN and Startup Key（TPM と PIN と起動キー） • Public Key（公開キー） • Passphrase（パスフレーズ） • TPM Certificate（TPM 証明書） • CryptoAPI Next Generation (CNG) Protector（CryptoAPI Next Generation（CNG）プロテクタ）	KEY_PROTECTORS

FileVault 2

FileVault 2 は、Mac OS X に付属しているディスク全体の暗号化機能です。

FileVault 2 用にサポートされている OS

オペレーティングシステム	バージョン
Mac OS X	10.8, 10.9, 10.10

デバイスの詳細 ページに表示される FileVault 2 情報

?? アイテム	?? 説明	MACHINE_FILEVAULT_VOLUME データベースフィールド
有効	FileVault が有効になっているかどうかを示します。	IS_ENABLED
Personal Recovery Key（個人用リカバリキー）	個人用リカバリキーが存在することを示します。	HAS_PERSONAL_RECOVERY_KEY
組織用リカバリキー	企業がプロビジョニングした X.509 ベースの非対称キーペアが存在することを示します。	HAS_INSTITUTIONAL_RECOVERY_KEY
承認されたユーザー	EFI のドライブのロックを解除できるアカウントのリスト。	AUTHORIZED_USERS
変換ステータス	暗号化プロセスのステータス。例として、Pending Conversion（保留中の変換）、Converting（変換中）、Encryption Paused（暗号化一時停止）、Complete（完了）などがあります。	CONVERSION_STATUS
変換率	率として表示される変換の程度。	CONVERSION_PERCENTAGE
暗号化ステータス	暗号化のステータス。例えば、Locked（ロック済み）や Unlocked（ロック解除）などです。	ENCRYPTION_STATUS
暗号化タイプ	使用される暗号化のタイプ。例えば、AES-XTS です。	ENCRYPTION_TYPE
デバイス	システム上のボリュームの一意の識別子。	DEVICE_ID
バージョン		バージョン

Trusted Platform Module (TPM)（信頼済みプラットフォームモジュール（TPM））

TPM は、暗号キーをデバイスに統合してハードウェアを保護する専用のマイクロプロセッサです。

TPM 用にサポートされている OS

オペレーティングシステム	バージョン
Windows	Vista、7、8、8.1
Windows Server	2008、2008 R2、2012、2012 R2

デバイスの詳細 ページに表示される TPM 情報

?? アイテム	?? 説明	MACHINE_TPM データベースフィールド
製造元	TPM チップの製造元。	MANUFACTURER_ID_TEXT
Manufacturer Version（製造元バージョン）	TPM チップのバージョン。	MANUFACTURER_VERSION
製造元バージョン情報	製造元に固有の追加のバージョン情報。	MANUFACTURER_VERSION_INFO
仕様バージョン	TPM がサポートする Trusted Computing Group（TCG）仕様のバージョン。	SPECIFICATION_VERSION
物理プレゼンスバージョン	デバイスがサポートする物理プレゼンスインタフェースのバージョン。物理プレゼンスインタフェースは、物理プレゼンスを必要とするデバイス操作を実行する通信メカニズムです。	PHYSICAL_PRESENCE_VERSION_INFO
TPMを有効にする	TPM 初期化の手順 1。	IS_TPM_ENABLED
TPM アクティブ済み	TPM 初期化の手順 2。	IS_TPM_ACTIVATED
TPM 所有済み	TPM 初期化の手順 3。	IS_TPM_OWNED

Windows DDP|E クライアントデバイスでインベントリ収集を許可するための Dump Inventory レジストリキーの追加

Windows DDP|E クライアントに DumpXmlInventory がない場合、アプライアンスは inventory.xml ファイルにアクセスして関連するフィールド情報を収集することができません。

Dell Data Protection | Encryption は、Windows デバイスにインストールされています。http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers に移動します。

キーを追加するための手順は、エージェント管理対象デバイスとエージェント不要管理対象デバイスとでは異なります。

- エージェント管理対象 Windows デバイスへの DumpXmlInventory レジストリキーの追加
- エージェント不要管理対象 Windows デバイスへの DumpXmlInventory レジストリキーの追加

エージェント管理対象 Windows デバイスへの DumpXmlInventory レジストリキーの追加

アプライアンスが Windows DDP|E クライアントの inventory.xml ファイルからフィールド情報を収集できるようにするには、そのクライアントに DumpXmlInventory を追加する必要があります。

エージェント管理対象 Windows デバイスの場合、アプライアンススクリプト機能からデフォルトのオフライン KScript を使用して、「dump inventory」レジストリキーを設定できます。DDP|E エージェントが詳細なインベントリ XML データをアプライアンスファイルシステムに書き込むようにするには、このキーが必要です。

注: このレジストリキーを設定した後、アプライアンスがインベントリを収集できるようにするには、DDP|E サービスで完全ポリシー更新スケジュールが必要になります。

1. K1000 Enable Detailed DDPE Inventory (Windows) スクリプトの Script Detail（スクリプトの詳細）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
    c. リストから、**K1000 Enable Detailed DDPE Inventory (Windows)** を選択します。
2. 設定セクションで、スクリプトの設定項目を次のように指定します。

オプション	説明
名前	K1000 Enable Detailed DDPE Inventory (Windows)。このデフォルトのスクリプトの名前です。
有効	ターゲットデバイスでスクリプトを実行するには、このチェックボックスをオンにします。スクリプトのテストが完了して、実行準備ができるまで、スクリプトを有効にしないでください。スクリプトはテストラベルに対して有効にしてから、すべてのデバイスに対して有効にします。
タイプ	スクリプトタイプは**オフライン KScripts** です。
ステータス	スクリプトを即座にネットワークにロールアウトできることを示します。ステータスを **本番** に設定します。
説明	デフォルトのスクリプトによって実行されるアクションの簡単な説明が含まれています。
メモ	任意の追加情報を入力します。

3. 展開 セクションで、次の展開オプションを指定します。

オプション	説明
全デバイス	すべてのデバイスに展開します。展開を特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。

オプション	説明
ラベル	指定したラベルに属するデバイスだけに展開を制限します。ラベルを選択するには、**編集** をクリックしてラベルを 展開の制限対象 ウィンドウにドラッグし、**保存** をクリックします。 レプリケーション共有または代替のダウンロード場所が指定されているラベルを選択した場合、デジタル資産は、アプライアンスから直接ダウンロードされるのではなく、指定されたレプリケーション共有または代替のダウンロード場所からコピーされます。 **注:** アプライアンスがKACE代替の場所を使用する前にレプリケーション共有を使用することが明らかになりました。
デバイス	1つまたは複数のデバイスに、展開を制限します。デバイスを検索するには、フィールドに入力し始めます。
オペレーティングシステム	アプリケーションが実行されるオペレーティングシステム。アプリケーションは、選択したオペレーティングシステムがインストールされているデバイスにのみ導入されます。 a. **オペレーティングシステムの管理** をクリックします。 b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**すべて** > **Windows** > **Windows 10** の順に選択し、**x64** を選択します。

4. スケジュール セクションで、次の実行オプションを指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。

オプション	説明
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。

オプション	説明
	詳細については、「タスクスケジュールの表示」を参照してください。

5. Dependencies（依存関係）セクションおよび Tasks（タスク）セクションをスキップします。
6. 次のいずれかを実行します。
   - **今すぐ実行 をクリックすると、すべてのデバイスにスクリプトがすぐにプッシュされます。**

     このオプションの使用には注意が必要です。詳細については、「実行 および 今すぐ実行 コマンドの使用」を参照してください。
   - **保存 をクリックします。**

エージェント不要管理対象 Windows デバイスへの DumpXmlInventory レジストリキーの追加

アプライアンスが Windows DDP|E クライアントの inventory.xml ファイルからフィールド情報を収集できるようにするには、そのクライアントに DumpXmlInventory を追加する必要があります。

エージェント不要管理対象 Windows デバイスの場合、ドメイン内の複数のデバイスにレジストリ設定を展開するには、Windows Server 2008 または 2012 デバイスに新しいグループポリシーオブジェクトを作成する必要があります。

1. Windows Server 2008 または 2012 デバイスで、グループ ポリシー管理コンソール を開きます。
2. **グループ ポリシー オブジェクト** を右クリックし、**新規** をクリックします。
3. 新しい GPO の説明と名前（例えば、Dell Data Protection | Encryption：インベントリレジストリ設定）を指定し、**OK** をクリックします。
4. 新しい GPO を右クリックし、**編集** をクリックします。
5. **コンピュータの構成 > 基本設定 > Windows の設定 > レジストリ** を参照します。
6. **レジストリ** を右クリックし、**新規 > レジストリ項目** を選択します。
7. 全般 タブで、アクション ドロップダウンメニューの **更新** を選択します。
8. ハイブ ドロップダウンリストの **HKEY_LOCAL_MACHINE** を選択します。
9. SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters の キー パス を指定します。
10. DumpXmlInventory の 値 名を指定します。
11. 値の種類 ドロップダウンリストで **REG_DWORD** を選択します。
12. 値 データフィールドに「1」を指定します。
13. 表記 グループの 16 進数 オプションを選択し、**OK** をクリックします。
14. グループ ポリシー管理エディタ を閉じます。

この新しいグループポリシーオブジェクトを特定のドメイン（組織単位など）にリンクできるようになりました。

重要: GPO をすべてのシステムに展開する前に、特定のコンピューターまたはコンピューターのセットで GPO をテストしてください。

デバイス詳細のインテル AMT 情報について

インテル AMT テクノロジ搭載の Intel ベースの Windows デバイスで、アプライアンスは AMT 設定に関する情報を表示できます。

インテル AMT は、Intel ベースのコンピューターデバイスをリモートから管理するためのハードウェアベースのテクノロジです。インテル AMT は、Intel?? vPro??? テクノロジ搭載の Intel?? Core??? プロセッサの機能です。

注: ここで説明するデータ収集は、アプライアンスが Dell Command | Monitor を使用して収集する vPro および AMT データとは別のものです。詳細については、「Dell Command | Monitor について」を参照してください。

インテル AMT リソースおよびアプライアンス要件

Dell Tech Center からの情報については、http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7537.dell-command-intel-vpro-out-of-bandを参照してください。インテル AMT を設定するために必要なコンポーネントが含まれている Intel Setup and Configuration Software（SCS）の情報およびダウンロードリンクについては、http://www.intel.com/content/www/us/en/software/setup-configuration-software.htmlを参照してください。

アプライアンスが AMT デバイス上の完全なインベントリ情報にアクセスするためには、そのデバイスに Intel Management Engine がインストールされている必要があります。Intel からのドライバのダウンロードについては、https://downloadcenter.intel.com/search?keyword=intel+management+engineを参照してください。

インテル AMT 情報

デバイスの詳細 ページに表示される インテル AMT 情報

?? アイテム	?? 説明	MACHINE_INTEL_AMT データベースフィールド
SKU	デバイスの Stock Keeping Unit。可能な値は、 • Full AMT Manageability（完全 AMT 管理性） • Standard Manageability（標準管理性）	SKU
ステータス	AMT がデバイス上に設定されているかどうかを示します。	STATE IS_AMT_CONFIGURED
設定モード	AMT デバイスの現在の設定モード。可能な値は、 • SMB Mode（SMB モード） • エンタープライズモード • なし	CONFIGURATION_MODE
制御モード	AMT デバイスの現在の制御モード。可能な値は、 • Client control Mode（クライアント制御モード） • 管理者制御モード • なし	CONTROL_MODE
ファームウェアバージョン	AMT デバイスのファームウェアのバージョン。	FW_VERSION
MEI ドライバ	MEI ドライバがインストールされ、動作しているかどうかを示し、そうである場合はドライバのバージョンを示します。	IS_MEI_ENABLED MEI_VERSION

デバイスの検出および管理

高度な検索、ラベル、および警告を使用して、インベントリ内のデバイスを検索および管理します。

インベントリ内でのデバイスの検索

高度な検索では、インベントリレコード内の任意のフィールドの値を指定し、それらの値をインベントリ全体で検索できます。

このタイプの検索は、特定のBIOSバージョン、MACアドレス、またはオペレーティングシステムといった具体的な特性でデバイスを検索する場合に便利です。詳細については、「高度なオプションによるページレベルの検索」を参照してください。

特定のデバイスをすばやく検索するために、簡易検索を実行することもできます。例えば、バーコードに特定の文字が含まれるデバイスを検索できます。

通知の使用によるデバイスの検索

デバイスが選択した条件を満たした場合、管理者へEメールメッセージが自動的に送信されるよう通知を設定できます。例えば、デバイスがディスク領域の制限に近づいたときに管理者に通知する場合は、ディスク使用量に基づきEメール通知をセットアップできます。詳細については、「レポート作成 セクションでの通知スケジュールの追加」を参照してください。

組織単位に基づいたデバイスのフィルタリング

LDAPまたはActive Directoryサーバーで見つかった組織単位に基づいてデバイスをフィルタリングするには、LDAPラベルを使用します。詳細については、「LDAPラベルについて」を参照してください。

デバイスのラベル付けによるグループ化

手動ラベル作成とSmart Labelを使用してデバイスをグループ化できます。そうすることにより、グループ化したデバイスに対してソフトウェア更新などのアクションを実行することができます。

ソフトウェアカタログのアプリケーションに関するメータリングを有効にするには、そのアプリケーションがインストールされているデバイスに、メータリングが有効なラベルを適用する必要があります。メータリングの詳細については、ソフトウェアメータリングの使用を参照してください。

手動作成デバイスラベルの追加、適用、および削除

手動作成ラベルは、デバイスへの追加と適用、またはデバイスからの削除が可能です。手動作成ラベルは、デバイスから手動で削除されるまで、そのデバイスに関連付けられます。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**デバイス** をクリックします。
2. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
3. **アクションの選択 > ラベルの追加** を選択します。
4. ラベルの追加 テキストボックスで、ラベルの名前を入力します。

ヒント: ラベル名にはバックスラッシュ（\）を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して（\\）エスケープします。

5. **ラベルの追加** をクリックします。
6. 既存のラベルを適用するには、次の手順を実行します。
   a. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
   b. **アクションの選択 > ラベルの適用** を選択します。
   c. ラベルを これらのラベルを適用 にドラッグし、**ラベルの適用** をクリックします。

   デバイス リストのデバイス名の隣にラベルが表示されます。
7. 手動作成ラベルを削除するには、以下の操作を実行します。
   a. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
   b. **アクションの選択 > ラベルの削除 > Label_Name**を選択します。

   ラベルがデバイスから削除されます。

デバイスに対するSmart Labelの使用

Smart Labelを使用して、特定の条件に基づいてデバイスに対して自動で検索およびラベル付けを実行します。

例えば、特定のオフィス（この例ではSan Franciscoのオフィス）にあるノートPCを追跡するには、まず「San Francisco Office」というラベルを作成します。次に、このオフィスにあるデバイスのIPアドレス範囲（サブネット）に基づいてSmart Labelを作成します。この IP アドレス範囲内にあるデバイスがインベントリに設定されるたびに、「San Francisco Office」という Smart Label が自動的に適用されます。デバイスがIPアドレス範囲外になり、再度インベントリに設定されると、ラベルは自動的に削除されます。

Smart Labelは、アプライアンスがデバイスインベントリを処理するときに、管理対象デバイスに対して適用または削除されます。そのため、デバイスでメータリングを有効化するSmart Labelを作成しても、Smart Labelがデバイスに対して適用されるまでに時間がかかることがあります。また、デバイスがメータリング情報をレポートするまでにも時間がかかる場合があります。デバイスがインベントリ設定され、Smart Labelが適用された後にのみ、Smart Labelの基準に一致するデバイスでメータリングが有効化されます。

詳細については、「Smart Labelの管理」を参照してください。

以下の表に、インベントリ属性に基づいてデバイスに適用できる便利なSmart Labelの例を示します。

サンプルラベル名	サンプル条件
Win7 Low Disk	ハードディスクの空き容量が1 GB未満のWindows 7デバイス
WS2012 No 2916993	修正プログラム2916993がインストールされていないWindows Server 2012デバイス
Building 3	Building 3に配置されていると認識されたIPアドレス範囲内のデバイス
CN Sales	デバイス名に「**sales**」という単語が含まれているデバイス

デバイスでのアクションの実行

デバイスのアクションを使用してデバイス上でアクションをリモートで実行できるのは、これらのプログラムがリモートデバイスにインストールされている場合に限ります。

選択元となるデバイスのアクションの作成が完了しています。デバイスのアクションの追加または編集の詳細については、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。

注: この機能は、Windows デバイスでのみサポートされます。デバイスアクションを実行している Windows デバイスに KACE エージェントバージョン 9.0 以降のエージェントがインストールされ、接続されている必要があります。

注: エージェントを介してデバイスを開始する場合、アクションの実行可能ファイルは %PATH% に配置する必要があります。エージェントは 32 ビットであるため、64 ビットの Windows デバイスでは、%windir%/Wow64 ディレクトリのエイリアスとして %windir%/System32 を使用します。64 ビット Windows システムの %windir%/System32 ディレクトリにあるプログラムを実行する必要がある場合は、%windir%/SysNative 仮想ディレクトリを使用する必要があります。マシンアクションを定義するときは、%windir%/SysNative を %PATH% 環境変数に追加するか、実行可能ファイルの前に %windir%/SysNative を追加して、完全修飾パスを提供することができます。

1. デバイスの デバイスの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**デバイス** をクリックします。
    c. デバイス リストの必要なデバイスを含む行で、チェックボックスをオンにします。
2. アクション ドロップダウンリストからアクションを選択します。

注: デバイスのアクションが作成されていない場合、アクション ドロップダウンリストは表示されません。

ヒント: ユーザーにデバイスを割り当てると（ **アクション**、**割り当て先 の順に選択します** ）、**ユーザーコンソール**の マイデバイス ページで選択したユーザーに対して、割り当てられたすべてのデバイスが表示されます。このユーザーがソフトウェアのダウンロードとインストールを行う場合、必要に応じてターゲットデバイスを選択できます。

手動で追加されたデバイスの表示

手動で追加されたデバイスは、他の管理対象デバイスと共に デバイス リストに表示されます。高度な検索を使用して、デバイス リストをフィルタリングして、手動で追加されたデバイスのみを表示します。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**デバイス** をクリックします。
2. リストをフィルタリングして手動で追加されたデバイスのみを表示するには、以下の操作を実行します。
    a. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
    b. 以下のように、手動で追加されたマシンを検出するために必要な条件を指定します。

オプション	条件
フィールド名	デバイスID情報：インベントリタイプ
演算子	**は**

オプション	条件
値	次のいずれかを選択します。 • **WSAPIエージェント**: API を通じてアップロードされたインベントリ。 • **XMLインポート**: ソフトウェアの詳細 ページでアップロードされたインベントリ。

c. **検索** をクリックします。

手動で追加されたデバイスが表示されます。

インベントリからのデバイスの削除

インベントリに未使用または古くなったデバイスが含まれている場合、それらを手動で削除できます。削除すると、Quest KACEライセンスによって管理が許可されているデバイスの台数からこれらのデバイスが除外されます。

1. デバイス リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**デバイス** をクリックします。
2. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

アプライアンスへの KACE エージェントの登録

アプライアンスは登録プロセスを使用して、リソースへの不正アクセスを防止します。認証された KACE エージェントのみが正常な接続を確立できます。

アプライアンスに接続しようとするすべてのエージェントは、検疫リストに配置されます。エージェントに有効なトークンがある場合、アプライアンスはエージェントを認証し、アプライアンスへのアクセスを自動的に許可します。トークンを持たないエージェントは、システム管理者が接続要求を承認するまで、検疫状態のままになります。

エージェントトークンを作成および管理したり、検疫エージェントからのアプライアンスへの接続要求を管理したりできます。

KACE エージェントトークンの管理

KACE エージェントトークンを使用すると、アプライアンスでエージェントの認証と登録が可能になり、アプライアンスリソースへのアクセスが可能になります。

各トークンは、1 つ以上のエージェントに関連付けることができます。エージェントトークンの詳細 ページを使用して、エージェントトークンを作成または変更します。また、このページでは、特定のトークンを使用してアプライアンスに接続したすべてのデバイスを識別し、選択したトークンを含むエージェントインストーラをダウンロードできます。

有効なトークンがないエージェントが接続を確立するためには、アプライアンス管理者によって承認される必要があります。詳細については、「検疫された KACE エージェントの確認」を参照してください。

1. 次のいずれかを実行します。
   - **アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または、管理ヘッダーに組織メニューを表示 がアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。**
   - **アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。**

   ダッシュボード ページまたは システム概要 ページが表示されます。
2. エージェントトークンの詳細 ページに移動します。
   a. 左のナビゲーションバーで **設定**、**エージェントトークン** の順にクリックします。

   エージェントトークン ページが表示され、すべてのエージェントトークンのリストが表示されます。各トークンについて、トークンステータス、作成者の名前、有効期限（該当する場合）、トークンを使用してエージェントデバイスをアプライアンスに登録する回数、および使用制限（該当する場合）が表示されます。
3. 表示された エージェントトークン リストページで、次の手順のいずれかを実行します。
   - **新しいエージェントトークンを作成するには、アクションの選択 > 新規作成 の順にクリックします。**

     ヒント: 1 つまたは複数のトークンを削除または取り消すには、リストでトークンを選択し、**アクションの選択** メニューから該当するコマンドを使用します。このアクションは、エージェントトークンの詳細 ページでも実行できます。
   - **既存のエージェントトークンを編集するには、リスト内のトークン名をクリックします。**
4. 表示される エージェントトークンの詳細 ページの 設定 で、次の情報を入力します。

オプション	説明
名前	エージェントトークンの名前。特定のエージェント、プラットフォーム、または目的を簡単に認識して関連付けられる名前を選択します。
有効期限	このトークンを期間限定で有効にする場合は、**有効期限を有効にする** を選択し、必要に応じて有効期限の日時を指定します。 指定した日時を変更するには、**クリア** をクリックして、新しい有効期限を入力します。
組織	このトークンを使用する組織の名前。特定の組織を 1 つ選択するか、All Orgs（全組織）を選択してすべての組織に適用できます。 **注:** このフィールドは、**システム管理コンソール**を使用している場合にのみ表示されます。

5. トークンを使用して 1 つまたは複数のエージェントをアプライアンスに登録できる回数を指定する場合は、使用制限 で **使用制限の有効化** を選択し、表示されるフィールドで最大使用数を指定します。

   エージェントの履歴がアプライアンスから削除されない限り、エージェントはアプライアンスに 1 回だけ登録されるため、この数は 1 つまたは複数のエージェントがアプライアンスに登録できる合計回数を表します。
6. **保存** をクリックします。

新しいエージェントトークンを作成した場合は、ページに次の追加セクションが表示されます。情報、エージェントトークンバンドルインストーラ、マシンによるトークンの使用、プロビジョニングスケジュールによるトークンの使用。

7. （**オプション**）以下のセクションの内容を確認します。

セクション	説明
情報	エージェントトークンに関する一般情報（作成日時、最終変更日時、作成者の名前、ステータス、トークン文字列など）。 トークン文字列をクリップボードにコピーするには、トークン フィールドでアイコンをクリックします。対象のデバイスに KACE エージェントをインストールするときにトークン文字列を指定できます。エージェントのインストールの詳細については、「KACE エージェントを手動展開する」を参照してください。
エージェントトークンバンドルインストーラ	サポートされている各オペレーティングシステムの KACE エージェントインストーラへのリンク。各インストーラバンドルには、この エージェントトークンが含まれています。
マシンによるトークンの使用	このエージェントトークンを使用するアプライアンスインベントリ内のデバイスのリスト、およびアプライアンス管理者が各デバイスのアクセスを承認した日時。
プロビジョニングスケジュールによるトークンの使用	このエージェントトークンを使用するプロビジョニングスケジュールのリスト。各エントリについて、リストに IP 範囲とスケジュールが有効かどうかが示されます。

検疫された KACE エージェントの確認

アプライアンスでは、アプライアンスへの接続を要求するすべてのエージェントを追跡します。

デフォルトビューでは、検疫 リストページには、登録待ちのエージェントのみが表示されます。これを使用して、該当するエージェントを確認および登録できます。接続しているエージェントを表示するには、リストフィルタを変更します。

注: 検疫 リストページの、ゾーン 列には、各エージェントが 内部 または 外部 として表示されます。ポート 443 を外部からアプライアンスのポート 52230 にマッピングするようにファイアウォールを設定すると、ファイアウォールからポート 443 に接続するエージェントは、このページで 外部 と表示されます。アプライアンスのポート 443 に直接接続するエージェントは 内部 として表示されます。この機能はオプションですが、アプライアンスが周辺ネットワークでホストされている場合などに使用できます。詳細については、「https://go.kace.com/to/k1000-external-agent-port」を参照してください。

有効なトークンを含むエージェントは自動的に接続されます。トークンの詳細については、「KACE エージェントトークンの管理」を参照してください。

1. 次のいずれかの操作を行って、検疫 リストに移動します。
   - **アプライアンスの組織コンポーネントが有効で、システムレベルの検疫リストにアクセスする必要がある場合：**

     アプライアンスシステム管理コンソール（https://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。次に、**組織** > **検疫** を選択します。

システムレベルの検疫リストには、アプライアンスによって管理されているすべての組織に関連付けられているエージェントが含まれます。

- **アプライアンスで組織コンポーネントが有効化されていない場合、または組織レベル検疫リストにアクセスする場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。次に、インベントリ > 検疫 を選択します。**

  組織レベルの検疫リストには、選択した組織に関連付けられているエージェントのみが含まれます。

検疫 リストページが表示されます。デフォルトでは、リストは 待機中アクション フィルタを使用して、承認が必要なエージェントのみを表示します。さまざまなフィルタを適用して、すべてのアイテム、Approved（承認済み）または Blocked Agents（ブロック済みのエージェント）を表示できます。承認ステータス 列を表示すると、Approved（承認済み）、ブロック済み、および 待機中アクション のエージェントを確認できます。

2. リスト内のアイテムを確認し、必要に応じてエージェントを承認します。

   1 つまたは複数のエージェントを承認するには、リストでエージェントを選択し、**アクションの選択 > 承認** の順にクリックします。必要に応じて、エージェントをブロックまたは削除することもできます。検疫エージェントをブロックすると、検疫 リストページの 待機中アクション ビューからのみ削除されます。通常、承認を検討しないエージェントはブロックできます。ブロックされたエージェントをすべてのビューから削除するには、そのエージェントを削除します。ブロックされたエージェントが再接続を試行すると、待機中アクション ビューに再表示されます。たとえば、外部エージェントからの疑わしいホスト名が表示された場合は、そのエージェントをブロックまたは削除できます。ブロック済みステータスは、ブロックされたデバイスの永続的なリストであり、待機中アクション ビューからは見えない状態になります。このリストは、どの時点でも承認されることを目的としていません。

3. 検疫エージェントの詳細については、次の手順を実行してください。
   a. リストでエージェント名をクリックします。
   b. 表示される 検疫の詳細 ページで、エージェントの詳細を確認します。

      このページには、選択した KACE エージェントの詳細（エージェントがインストールされているデバイスの名前、デバイスの MAC アドレスなど）が表示されます。エージェントがトークンを使用してアプライアンスに接続した場合、トークン名がページに表示されます。このページでは、エージェントの承認、ブロック、または削除もできます。

   c. 完了したら、**キャンセル** をクリックします。
4. **システムレベルのエージェントのみ**。システムレベルのエージェントを特定の組織に関連付ける場合は、リストでその組織を選択し、**アクションの選択 > 組織に割り当て > <組織名>** をクリックします

   選択したエージェントレコードが組織レベルの 隔離 リストページに表示され、必要に応じて、組織の管理者がこのエージェントを確認して登録できるようになります。組織に割り当てられていない状態でエージェントが承認された場合、組織フィルタを使用して、最初のインベントリの後にエージェントを組織に割り当てます。

KACE エージェントのプロビジョニング

エージェントのプロビジョニングは、エージェントを使用してアプライアンスインベントリに追加するデバイスに KACE エージェントをインストールするタスクです。

KACE エージェントについて

KACE エージェントは、デバイスにインストールすることで、インベントリのレポーティングおよびその他の管理機能を可能にするアプリケーションです。

管理対象デバイスにインストールされたエージェントは、エージェントメッセージプロトコルを通じてアプライアンスと通信します。エージェントは、管理対象デバイスからのインベントリ情報の収集や、管理対象デバイスへのソフトウェアの配布などのスケジュール済みタスクを実行します。エージェントとアプライアンス間の通信は、TLS 1.3 プロトコルを使用して暗号化された独自の KACE トンネルを介して行われます。エージェントは、TLS 1.3 暗号化 KACE トンネルを介して暗号化されていないデータを送受信します。

プリンタや、エージェントがサポートしていないオペレーティングシステムを搭載したデバイスなど、エージェントソフトウェアをインストールできないデバイスでは、エージェント不要の管理も使用可能です。詳細については、「エージェント不要の管理の使用」を参照してください。

エージェント設定の変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

KACE エージェントのプロビジョニングの方法

KACE エージェントを管理対象のデバイスに展開する場合、さまざまな方法があります。

- **エージェントのプロビジョニングアシスタントを使用したプロビジョニング**: エージェントのプロビジョニングアシスタントを使用して、Windows、Mac OS X、およびLinuxオペレーティングシステムを搭載したデバイスのプロビジョニングを実行できます。アシスタント内で、アプライアンス GPO プロビジョニングツールを使用してエージェントを Windows デバイスに展開するか、またはオンボードプロビジョニングを使用してエージェントを Windows、Mac OS X、または Linux デバイスに展開するかを選択できます。

  Windowsデバイスの場合は、GPOプロビジョニングツールをお勧めします。これは、このツールを使用すると、ターゲットデバイスで行う必要がある事前設定が最小限になるためです。Active Directory環境が必要です。オンボードプロビジョニングアプローチでは、プロビジョニングを開始する前に、管理対象のデバイスでクライアント側設定を実行する必要があります。

- **手動展開を使用したプロビジョニング**: 手動展開は、エージェントの自動プロビジョニングが現実的でない場合や、E メールまたはログオンスクリプトを使用して KACE エージェントを展開する場合に便利です。

関連トピック

Windows デバイスでの GPO プロビジョニングツールを使用した KACE エージェントのプロビジョニング

オンボードプロビジョニングを使用した KACE エージェントのプロビジョニング

KACE エージェントを手動展開する

ファイル共有を有効にする

エージェントソフトウェアをプロビジョニングするには、ファイル共有を有効にする必要があります。

アプライアンスで組織コンポーネントが有効化されている場合は、システムレベルでのファイル共有の有効化を参照してください。それ以外の場合は、組織コンポーネントが有効になっていない状態でのファイル共有の有効化を参照してください。

システムレベルでのファイル共有の有効化

アプライアンスで組織コンポーネントが有効化されている場合、システムレベルでファイル共有を有効にして、エージェントをプロビジョニングする必要があります。

注: アプライアンスで組織コンポーネントが有効になっていない場合は、組織コンポーネントが有効になっていない状態でのファイル共有の有効化の指示に従ってください。

1. セキュリティ設定 ページに移動します。
   a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。
   b. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。
   c. コントロールパネル で **セキュリティ設定** をクリックします。
2. SAMBA セクションで、各設定を次のように指定します。

オプション	説明
組織コンポーネントが有効になっているアプライアンスの場合： **組織のファイル共有を有効にする**	アプライアンスのクライアント共有を使用して、ファイル（管理対象デバイスにアプリケーションをインストールする際に使用するファイルなど）を保存します。 アプライアンスのクライアント共有は、プロビジョニングサービスで利用可能な組み込みのWindowsファイルサーバーで、ネットワーク上でSambaクライアントを配布するのに役立ちます。Questでは、管理対象デバイス上でアプリケーションのインストールを実行しているときにのみ、このファイルサーバーを有効にすることをお勧めします。
アプライアンスのファイル共有にNTLMv2認証を要求する	アプライアンスファイル共有に対する NTLMv2 認証を有効にします。この設定を有効にした場合は、アプライアンスファイル共有に接続する管理対象デバイスは NTLMv2 をサポートし、NTLMv2 を使用してアプライアンスに対する認証を受ける必要があります。NTLMv2は、NTLMやLANMANよりも安全ですが、非NTLMv2設定の方がより一般的なため、通常、このオプションはオフになっています。このオプションを有効にすると、Samba サーバーで **lanman auth** と **ntlm auth** が無効になります。NTLMv2レベル1～4がサポートされています。NTLM v2 レベル 5 が必要な場合は、KACE エージェントの手動プロビジョニングを検討してください。詳細については、「KACE エージェントを手動展開する」を参照してください。
オフボードファイル共有にNTLMv2を要求する	エージェントのプロビジョニングなど、Samba クライアントを介してサポートされるアプライアンスの特定の機能が、NTLMv2 を使用して強制的にオフボードネットワークファイル共有に対する認証を受けるようにします。NTLMv2は、NTLMやLANMANよりも安全ですが、非NTLMv2設定の方がより一般的なため、通常、このオプションは無効になっています。このオプションを有効にすると、SAMBAクライアント機能の **client ntlmv2 auth** オプションが有効になります。

3. **保存** をクリックします。
4. 要求された場合は、アプライアンスを再起動します。

アプライアンスが再起動したら、組織レベルでファイル共有を有効にします。詳細については、「組織コンポーネントが有効になっている状態での組織レベルのファイル共有の有効化」を参照してください。

組織コンポーネントが有効になっている状態での組織レベルのファイル共有の有効化

アプライアンスで組織コンポーネントが有効化されている場合、組織レベルでファイル共有を有効にして、エージェントをプロビジョニングする必要があります。

組織のファイル共有が有効になっていることを確認します。手順については、システムレベルでのファイル共有の有効化を参照してください。

1. 管理者レベルの 一般設定 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。

c. コントロールパネル で **一般設定** をクリックします。

2. SAMBA共有設定 セクションで、**ファイル共有を有効にする** を選択します。

   ファイル共有が無効になっている場合は、システムレベルで有効にする必要があります。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。

3. **オプション**：ファイル共有ユーザーのパスワードを入力します。
4. **SAMBA設定の保存** をクリックします。
5. 要求された場合は、アプライアンスを再起動します。
6. 複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

組織コンポーネントが有効になっていない状態でのファイル共有の有効化

アプライアンスで組織コンポーネントが有効化されている場合、アプライアンスのセキュリティ設定でファイル共有を有効にして、エージェントをプロビジョニングする必要があります。

1. セキュリティ設定 ページに移動します。

   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

   b. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。

   c. コントロールパネル で **セキュリティ設定** をクリックします。

2. SAMBA セクションで、**ファイル共有を有効にする** を選択します。
3. **オプション**：認証のオプションを選択します。

オプション	説明
アプライアンスのファイル共有にNTLMv2認証を要求する	アプライアンスファイル共有に対する NTLMv2 認証を有効にします。この設定を有効にした場合は、アプライアンスファイル共有に接続する管理対象デバイスは NTLMv2 をサポートし、NTLMv2 を使用してアプライアンスに対する認証を受ける必要があります。NTLMv2は、NTLMやLANMANよりも安全ですが、非NTLMv2設定の方がより一般的なため、通常、このオプションはオフになっています。このオプションを有効にすると、Samba サーバーで **lanman auth** と **ntlm auth** が無効になります。NTLMv2レベル1～4がサポートされています。NTLM v2 レベル 5 が必要な場合は、KACE エージェントの手動プロビジョニングを検討してください。詳細については、「KACE エージェントを手動展開する」を参照してください。
オフボードファイル共有にNTLMv2認証を要求する	エージェントのプロビジョニングなど、Samba クライアントを介してサポートされるアプライアンスの特定の機能が、NTLMv2 を使用して強制的にオフボードネットワークファイル共有に対する認証を受けるようにします。NTLMv2は、NTLMやLANMANよりも安全ですが、非NTLMv2設定の方がより一般的なため、通常、このオプションは無効になっています。このオプションを有効にすると、SAMBAク

オプション	説明
	ライアント機能の **client ntlmv2 auth** オプションが有効になります。

4. **保存** をクリックします。
5. 要求された場合は、アプライアンスを再起動します。

Windows デバイスでの GPO プロビジョニングツールを使用した KACE エージェントのプロビジョニング

Windowsデバイスでのエージェントのプロビジョニング方法として、GPOプロビジョニングツールをお勧めします。これは、このツールを使用すると、ターゲットデバイスで必要となる事前設定が最小化されるためです。

GPO プロビジョニングツールでは、Active Directory?? およびグループポリシーを使用して、インストール設定を配布し、エージェントのインストールを実行します。このツールでは、GPO の作成または既存の GPO の変更を実行して、デバイスが Active Directory で認証されたときに KACE エージェントをインストールします。

ツールが作成または変更プロセスを完了した後に、ターゲットデバイスが初めてグループポリシーを更新すると、新しいグループポリシーのクライアント側拡張dllがこのGPOを適用するデバイスに登録されます。その後、次にデバイスがグループポリシーを更新すると、新たに登録されたクライアント側拡張が Windows でトリガされ、KACE Windows エージェントがインストールされます。

GPOプロビジョニングツールをダウンロードするためのリンクを含むQuestサポート技術情報記事については、https://support.quest.com/kb/133776を参照してください。

エージェントの展開にGPOプロビジョニングツールを使用する準備

GPOプロビジョニングツールを使用してエージェントをWindowsデバイスに展開する前に、このツールを使用するようにシステムが設定されていることを確認する必要があります。

GPOプロビジョニングツールを使用する場合は、次のシステム要件があります。

- **Windows 7 以降**：**リモートサーバー管理ツール**（RSAT）を使用すると、IT 管理者は、Windows 8.1、Windows 8、またはWindows 7 を実行しているコンピューターから、Windows Server 2016、Windows Server 2012 R2、または Windows Server 2012 の役割と機能をリモートで管理できます。

  http://social.technet.microsoft.com/wiki/contents/articles/2202.remote-server-administration-tools-rsat-for-windows-client-and-windows-server-dsforum2wiki.aspx に移動します。
- **.NET Framework 3.5**。
- **Windows Server 2012以降のActive Directoryの機能レベル**。
- **配布共有**: 必ず、すべてのユーザーがアクセスできる共有を使用します。例えば、.msi ファイルを NETLOGON 共有に配置しないようにします。これは、一部のユーザーはこの共有にアクセスできず、アクセスできないと今後のアップグレードが失敗する原因となるためです。この場所は、永続的にアクセス可能な共有である必要があります。インストーラは MSI（Microsoft Installer）ファイルです。ソフトウェアをアンインストールまたはアップグレードするには、MSI が .msi ファイルにアクセスする必要があります。アクセスできない場合、msiexecはアンインストールされません。

アプライアンス GPO プロビジョニングツールを使用した KACE エージェントのプロビジョニング

アプライアンス GPO プロビジョニングツールを使用し、エージェントのプロビジョニングアシスタント内で開始することにより、KACE エージェントを単一のデバイスまたは複数のデバイスにインストールできます。この方法を使用して、Windowsデバイスをプロビジョニングできます。

- Active Directory 環境が必要です。
- ソフトウェアインストールを設定するための適切なアクセス権が必要です。
- エージェントの展開にGPOプロビジョニングツールを使用する準備で説明されているシステム要件を満たしている必要があります。

このタスクを完了するには、アプライアンス GPO プロビジョニングツールを使用して Windows グループポリシー管理コンソールまたは Windows 管理ツールで作業するためにアプライアンスをいったん離れてから、アプライアンスに戻る必要があります。

1. エージェントのプロビジョニングアシスタント に移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**プロビジョニング** の順にクリックします。
    c. プロビジョニング パネルで、**エージェントのプロビジョニングアシスタント** をクリックします。

    エージェントのプロビジョニングアシスタント：手順1/3 ページが表示されます。
2. Windowsグループポリシーを使用してプロビジョニング（ 推奨 ）のチェックボックスをオンにし、**次へ** をクリックして、エージェントのプロビジョニングアシスタント：手順 2/3 ページを表示します。
3. https://support.quest.com/kb/133776 にある、アプライアンス GPO プロビジョニングツールを使用したエージェントの展開に関するサポート技術情報の記事へのリンクをクリックします。

    このサポート技術情報の記事では、GPOプロビジョニングツールのMSIをダウンロードするためのリンクが提供されています。

    このツールをインストールおよび起動する場合、アプライアンスインターフェイスを離れる必要があります。
4. MSIをダウンロードし、起動して、ツールをインストールします。
5. インストールしたツールは **スタート** メニューから起動します。

    この展開ウィザードでは、ソフトウェア展開用にGPOを設定および適用する手順が示されます。可能な場合、ウィザードでは、必要な設定作業を軽減するために、デフォルトを使用することを試みます。

    注: ユーザーに**編集**権限があるGPOのみがツールに表示されます。
6. ツールの作業が完了したら、K1000の エージェントのプロビジョニング：手順 2/3 ページに戻り、**次へ** をクリックします。
7. **終了** を エージェントのプロビジョニング：手順3/3 ページでクリックします。

グループポリシーがこれらのデバイスで更新されると、エージェントはクライアントデバイスにインストールされます。環境に応じて、このインストールは、デバイスの再起動時、またはグループポリシーの90分の更新サイクル後に行われます。

デバイス ページに移動し、エージェントがインストールおよびチェックインされているデバイスの進行状況を追跡します。

オンボードプロビジョニングを使用した KACE エージェントのプロビジョニング

複数のデバイスに KACE エージェントをインストールするには、展開するターゲットとして IP アドレスの範囲を指定します（ オンボードプロビジョニング ）。Windows、Mac OS X、およびLinuxデバイスをオンボードプロビジョニングのターゲットとすることができます。

各ターゲットクライアントデバイスの準備が完了したら、アプライアンスのエージェントのプロビジョニングアシスタントを使用して、デバイスを特定し、プロビジョニングスケジュールを設定します。

KACE エージェントのインストール準備

オンボードプロビジョニングを使用してデバイスに KACE エージェントをインストールする前に、システム要件を確認し、ファイル共有を有効化してデバイスを準備する必要があります。

ファイル共有に関する情報については、ファイル共有を有効にするを参照してください。

KACE エージェントをインストールするためのシステム要件の確認

デバイスに KACE エージェントをインストールする前に、必要なポートがアクセス可能で、管理対象デバイスがシステム要件を満たしていることを確認します。

管理対象デバイスは次のシステム要件を満たし、必要なポートにアクセスできる必要があります。

- 製品マニュアルページで入手可能な技術仕様を参照してください。https://support.quest.com/kace-systems-management-appliance/technical-documents.
- 詳細については、「ポート設定、NTPサービス、およびWebサイトアクセスの検証」を参照してください。

エージェントをインストールしておくためのWindowsデバイスの準備

Windows デバイスに KACE エージェントをインストールする前に、ファイル共有およびユーザーアカウント制御（ UAC ）を適切に設定する必要があります。

- **Windows 7 または Windows 8デバイスの準備**

  デバイスごとに管理者の資格情報を指定します。複数のデバイスに KACE エージェントをインストールするには、管理者の資格情報がすべてのデバイスで同じでなければなりません。

  ユーザーアカウント制御（ UAC ）を設定するには、次のいずれかを実行します。

  - **ユーザーアカウント制御：管理者承認モードですべての管理者を実行** を **無効** に設定します。このオプションを推奨しています。これは、このオプションがより安全で、GPOを使用して一元的に設定できるためです。この設定を見つけるには、「**グループポリシー**」（ **スタート** メニューの プログラムとファイルの検索 フィールドに「secpol.msc」と入力 ）を開いて、**ローカルポリシー > セキュリティオプション**にアクセスします。設定の適用後、デバイスを再起動します。
  - UACを無効にします。Windows 7の場合は、**コントロールパネル > システムとセキュリティ > アクションセンター > ユーザーアカウント制御設定の変更** の順に進みます。Windows 8の場合は、**コントロールパネル > システムとセキュリティ > 管理ツール > ローカルセキュリティポリシー** の順に進み、ローカルポリシー セクションの セキュリティオプション で、「ユーザーアカウントコントロール」のラベルが付いている各アイテムの **無効** を選択します。

  共有の詳細設定 ページで、ネットワーク検出とファイル共有およびプリンタ共有を有効にします。

- **Windowsファイアウォールの準備**

  Windowsファイアウォールを有効にしている場合は、ファイアウォール構成の除外 リストで **ファイルとプリンタの共有** を有効にする必要があります。詳細については、MicrosoftサポートのWebサイトを参照してください。

- **ポートの可用性の確認**

ポート139と445が使用可能かどうかを確認します。

アプライアンスによって、リモートインストールの実行前に、ターゲットデバイスでポート139と445が使用可能かどうかが確認されます。

注: Windowsデバイスの場合、ポート139と445、「ファイルとプリンタの共有」、および管理者の資格情報が必要になるのはエージェントのインストール時のみです。インストール後、これらのポートとサービスは必要に応じて無効にして構いません。継続的な通信には、ポート443が使用されます。

注: インストール後、エージェントはローカルシステムアカウントのコンテキスト内で動作します。これは、Windowsオペレーティングシステムによって使用されるビルトインアカウントです。

単一または複数のデバイスへの KACE エージェントのインストール

エージェントのプロビジョニングアシスタントを使用して、KACE エージェントを単一または複数のデバイスにインストールできます。複数のデバイスにインストールするには、インストールのターゲットとして IP アドレスの範囲を指定します。この方法を使用して、Windows、Mac、またはLinuxデバイスをプロビジョニングできます。

- すべてのターゲットデバイスの準備が完了しています。詳細については、「KACE エージェントのインストール準備」を参照してください。
- エージェントをターゲットデバイスにインストールするために必要な権限を持つ管理者アカウントに関する情報があります。

エージェントのプロビジョニングアシスタントを使用して、プロビジョニングスケジュールを作成して、ネットワーク内のデバイスに KACE エージェントをインストールする方法とタイミングを指定できます。スケジュールに従ったプロビジョニングは、IPアドレス範囲内のデバイスに確実にエージェントをインストールするのに役立ちます。

プロビジョニングスケジュールを追加すると、アプライアンスが指定された IP アドレス範囲のデバイスを定期的にチェックし、必要に応じて KACE エージェントのインストール、再インストール、アンインストールなどを実行するように設定されます。

Windows デバイスをプロビジョニングする場合は、アプライアンス GPO プロビジョニングツールを使用することもできます。このツールを使用すると、ターゲットデバイスで行う必要がある事前設定が最小限になります。詳細については、「Windows デバイスでの GPO プロビジョニングツールを使用した KACE エージェントのプロビジョニング」を参照してください。

1. エージェントのプロビジョニングアシスタント に移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**プロビジョニング** の順にクリックします。
    c. プロビジョニング パネルで、**エージェントのプロビジョニングアシスタント** をクリックします。

    エージェントのプロビジョニングアシスタント：手順1/3 ページが表示されます。
2. IP範囲を使用してプロビジョニング（ Windows、Mac、Linux ）を選択し、**次へ** をクリックして、プロビジョニングスケジュールの詳細 ページを表示します。
3. 設定 セクションで、スケジュールの名前を付け、プロビジョニングを有効化し、プラットフォーム情報を指定します。

オプション	説明
名前	この設定を識別できる一意の名前。この名前が プロビジョニングスケジュール ページに表示されます。

オプション	説明
有効	プロビジョニング済みのスケジュールを有効にします。このチェックボックスがオンになっている場合にのみ、スケジュールが実行されます。
インストール/アンインストール	プロビジョニングスケジュールでエージェントのインストールまたはアンインストールを処理するかどうかを示します。
エージェントトークン	エージェントがアプライアンスへの接続に使用するトークン。既存のエージェントトークンを選択するか、新しいトークンを追加します。 a. エージェントトークンの追加 を選択します。 b. エージェントトークンの追加 ダイアログボックスで、次の情報を指定します。 ◦ **名前**： ◦ **有効期限を有効にする**：このトークンを期間限定で有効にする場合は、このチェックボックスを選択し、必要に応じて有効期限の日時を指定します。指定した日時を変更するには、**クリア** をクリックして、新しい有効期限を入力します。 ◦ **使用制限の有効化**：トークンを使用して 1 つまたは複数のエージェントをアプライアンスに登録できる回数を指定する場合は、このチェックボックスを選択し、表示されるフィールドで最大使用数を指定します。エージェントの履歴がアプライアンスから削除されない限り、エージェントはアプライアンスに 1 回だけ登録されるため、この数は 1 つまたは複数のエージェントがアプライアンスに登録できる合計回数を表します。 c. **保存** をクリックします。 エージェントトークンを選択しない場合は、エージェントが初めてアプライアンスに接続するとき、アプライアンス管理者が接続要求を承認するまで、エージェントトークンは検疫リストに残ります。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。
資格情報	デバイスに接続して、スケジュールで対象となっている特定のプラットフォームに対してコマンドを実行するために必要な資格情報用の行を分離します。最初の列には、オペレーティングシステムが含まれています。2 つ目の列には、インストール対象のエージェントバージョンが配置されています。3 つ目の列には、既存の資格情報を選択するドロップダウンリストが含まれています。**新しい資格情報の追加** を選択して、まだリストにない資格情報を追加できます。

オプション	説明
	詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。

4. 展開 セクションで、スケジュールに含めるデバイスを特定します。

オプション	説明
ターゲットの IP アドレスまたはホスト名	ターゲットデバイスの IP アドレスまたはホスト名のコンマ区切りリスト。ハイフンを使用して個々のIPアドレスクラス範囲を指定します。 **ヒント:** アプライアンスは IPv6（インターネットプロトコルバージョン 6）と IPv4 アドレスの両方をサポートします。 **デバイス選択のヘルプ** リンクを使用して、デバイスを ターゲットのIPアドレスまたはホスト名 リストに追加します。 • **プロビジョニングのIP範囲**：ハイフンを使用して個々のIPアドレスクラス範囲を指定します。例： ◦ 「**IPv6**」：fdef:22b9:e8ae:14a9::1a0:f000-f0aa ◦ 「**IPv4**」: 192.168.2-5.1-200 範囲の指定後、**すべて追加** をクリックします。 • **検出機能からデバイスを選択します**：このドロップダウンリストは、「**検出結果**」から取り込まれます。内容をフィルタリングするには、フィールドに入力し始めます。デバイスを選択して、**すべて追加** をクリックします。

5. スケジュールを実行する時間を設定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0)

オプション	説明
	| | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース ( )**：各フィールドはスペースで区切ります。 • **アスタリスク (*)**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

6. **オプション**：高度な設定 を使用して、次の操作を行います。
   - エージェントを展開するためにアプライアンスが使用するポートをカスタマイズします。
   - エージェントインストーラー用の代替のダウンロード場所を指定します。

     注: Windows 10 などの新しいバージョンの MS Windows では、ファイル共有からのファイルのダウンロードはサポートされていません。これにより、代替の場所 WinRM プロビジョニングが期待どおりに動作しなくなります。
   - Windows デバイスでのエージェントのプロビジョニングに使用する WinRM ポートを指定します。従来の方法で Windows デバイスをプロビジョニングするスケジュールの場合は、WinRM に変更するオ

プションがあります。WinRM 設定の詳細については、「https://support.quest.com/kb/260699/agent-provisioning-with-winrm」を参照してください。

- ログに表示する情報のレベルを選択します。最も重要なメッセージのみを表示するには、緊急 を選択します。すべてのメッセージを表示するには、デバッグ を選択します。その他のオプションには、エラー、警告、通知、情報 などがあります。
- エージェント不要デバイスインベントリのリレーとして使用するデバイスを指定します。検出中にリレーとして使用されるリレーデバイスは、検出結果から新しいデバイスが自動的にプロビジョニングされるとき、エージェント不要インベントリに使用されます。詳細については、「ネットワークの「何をどこで」高速スキャンを実行する検出スケジュールの追加」を参照してください。
- エージェントを完全にアンインストールできるようにします。アンインストール中にKUIDを削除する を選択すると、既存のエージェントがデバイスから削除され、その後に、エージェントが再びインストールされます。この場合、アプライアンスにより資産の新しい KUID が生成され、アプライアンスで新しいデバイスとして表示されます。

7. **今すぐ実行** をクリックして、プロビジョニングスケジュール ページおよび新しい設定を表示します。

   このアプライアンスでは、指定した名前で設定が保存され、ターゲットIPアドレスに対して設定が実行されます。

プロビジョニングスケジュール ページには、スケジュールの開始時刻後に、正常に実行されているインスールの進捗が表示されます。

関連トピック

アプライアンスの電源投入と管理者コンソールへのログイン

Windows デバイスでの GPO プロビジョニングツールを使用した KACE エージェントのプロビジョニング

KACE エージェントを手動展開する

プロビジョニングスケジュールの管理

エージェントのインストールプロセスを合理化するために、デバイスに KACE エージェントをインストールする方法とタイミングを指定した、プロビジョニングスケジュールを追加することができます。プロビジョニングスケジュールは、追加、表示、編集、実行、複製、および削除できます。

プロビジョニングスケジュールの表示、実行、編集、または複製

Provisioning Schedules（プロビジョニングスケジュール）ページでは、プロビジョニングスケジュールのステータスとその他の詳細を表示できます。このページでは、必要に応じてプロビジョニングスケジュールを実行および編集することもできます。

プロビジョニングスケジュールを複製すると、そのプロパティが新しい設定にコピーされます。既存の設定と同様の設定を作成する場合、複製したスケジュールから開始する方が、最初から設定を作成するより早い可能性があります。

1. プロビジョニングスケジュール リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**プロビジョニング** の順にクリックします。
   c. プロビジョニングパネル で **スケジュール** をクリックします。

   リストには次の列が表示されます。

オプション	説明
名前	プロビジョニングスケジュールの名前（プロビジョニングスケジュールの詳細 ページにリンク）。

オプション	説明
対象	設定内のターゲットデバイスの合計数（プロビジョニング結果 ページにリンク）。
実行中	プロビジョニングが実行されているターゲットデバイスの合計数（プロビジョニング結果 ページにリンク）。
保留中	プロビジョニングがまだ開始されていないターゲットデバイスの合計数（プロビジョニング結 」ページにリンク）。
成功	プロビジョニングが成功したターゲットデバイスの合計数（プロビジョニング結果 ページにリンク）。
失敗	プロビジョニングが失敗したターゲットデバイスの合計数（プロビジョニング結果 ページにリンク）。
成功率	プロビジョニングが成功したターゲットデバイスの合計数（パーセント）。
IP範囲	ターゲットデバイスのIPアドレス範囲。
スケジュール	指定したプロビジョニングスケジュール。例：**n**分ごと、**n**時間ごと、なし。
有効	設定が有効か無効かを示します。チェックマークは、プロビジョニングスケジュールが有効になっていることを示します。

2. プロビジョニングスケジュールを実行するには、次の操作を行います。
    a. 実行するスケジュールのチェックボックスをオンにします。
    b. **アクションの選択 > 今すぐ実行** を選択します。
3. スケジュールを編集するには、次の操作を行います。
    a. スケジュールの名前をクリックします。
    b. プロビジョニングスケジュールの プロビジョニングスケジュールの詳細 ページでスケジュールを編集して、**保存** をクリックします。

    詳細については、「単一または複数のデバイスへの KACE エージェントのインストール」を参照してください。
4. スケジュールを複製するには、次の操作を行います。
    a. スケジュールの名前をクリックします。
    b. 高度 セクションで、**複製** をクリックして、新しいスケジュールが「**Schedule Nameのコピー**」として含まれる プロビジョニングスケジュール ページを表示します。

プロビジョニングスケジュールの削除

アプライアンスからスケジュールを削除する場合は、プロビジョニングスケジュールを削除できます。

プロビジョニングスケジュールを削除すると、それらのスケジュールに関連付けられた結果も削除されます。ただし、スケジュールを使用してプロビジョニングされたデバイスは、インベントリから削除されません。

1. プロビジョニングスケジュール リストに移動します。

a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左のナビゲーションバーで **設定**、**プロビジョニング** の順にクリックします。
c. プロビジョニングパネル で **スケジュール** をクリックします。

2. 1つまたは複数のスケジュールの隣のチェックボックスをオンにします。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

プロビジョニング結果の表示

プロビジョニングスケジュールにより実行されたアクションの結果を参照できます。

1. プロビジョニングスケジュール リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**プロビジョニング** の順にクリックします。
   c. プロビジョニングパネル で **スケジュール** をクリックします。
2. 実行中、保留中、成功、または 失敗 列のリンクをクリックします。

   プロビジョニング結果 ページが開き、次のような情報が表示されます。

アイテム	説明
ステータス	アプライアンスとのエージェント接続のステータス。  : エージェント管理対象デバイスがアプライアンスに接続されています。  : エージェント管理対象デバイスがアプライアンスに接続されていません。
スケジュール名	プロビジョニングスケジュールの名前。
IPアドレス	ターゲットデバイスのIPアドレス。
ホスト名	ターゲットデバイスのホスト名。**リモート接続** ボタン  をクリックし、ターゲットデバイスへのリモートデスクトップ接続を開きます（Microsoft Edge のみ）。
結果	前回のプロビジョニングの試行のステータス。
アクション	「**I**」は、インストールの成功を示します。 「**U**」は、アンインストールの成功を示します。
エラー	「TCPポートにアクセスできません」などのエラー。
前回の実行	前回にスケジュールが実行された時間。

3. ターゲットデバイスに関するその他の情報を表示するには、その **IPアドレス** をクリックします。

KACE エージェントのプロビジョニング ページが表示されます。

このページには、最新のプロビジョニングの実行結果が表示されます。表示される内容は、IPアドレス、ポート設定、プロビジョニングの各処理のログ、などの情報です。

4. インベントリ情報を表示するには、**MACアドレス** の隣の **コンピューターインベントリ** リンクをクリックします。

注: **コンピューターインベントリ** リンクは、プロビジョニングプロセスにおいてターゲットデバイスのMACアドレスが現在のインベントリデータに一致した場合にのみ表示されます。詳細については、「MIAデバイスの管理」を参照してください。

エージェント通信の管理

管理対象デバイスにインストールされたエージェントとアプライアンスとの間の通信には、インベントリレポート、警告、パッチ、スクリプト、およびクラッシュログが含まれます。キューに格納された（つまり保留中の）通信を設定および参照できます。

エージェント通信とログ設定の定義

管理対象デバイスにインストールされたエージェントは、定期的にアプライアンスにチェックインし、インベントリのレポート、スクリプトの更新、その他のタスクを実行します。

このセクションでは、エージェント設定の定義（エージェントチェックインの間隔、ユーザーに表示されるメッセージ、ログの保持期間など）を行う方法について説明します。組織が複数ある場合は、それぞれの組織にエージェント設定を個別に定義します。

1. 次のいずれかを実行します。
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから システム を選択します。続いて、組織 をクリックします。組織の情報を表示するには、組織の名前をクリックします。**

     表示される 組織の詳細 ページで、通信とエージェントの設定 セクションを探します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。次に、設定 > プロビジョニング を選択し、プロビジョニング パネルで 通信設定 をクリックします。**

     通信設定 ページが表示されます。
2. 次の設定を指定します。

注: アプライアンスへの負荷を軽減する場合は、エージェントの接続数を 1 時間あたり 500 までに制限します。インベントリ、スクリプト作成、およびメータリング間隔の隣に表示される接続数は、現在の組織のみに適用されます。アプライアンスで組織コンポーネントが有効化されている場合は、すべての組織のエージェント接続の合計数を1時間あたり500より多くしないでください。

オプション	設定案	メモ
エージェントのログ記録	有効	管理対象デバイスにインストールされたエージェントから提供されるスクリプト結果を、アプライアンスが保存するかどうか。エージェントログは、データベース内のディスク領域を最大約1 GB消費します。ディスク領域に問題がない場合は、エージェントのログ記録 を有効にして、エージェント管理対象デバイスのログ情報をすべて保持します。これらのログは、トラブルシューティング時に役立

オプション	設定案	メモ
		ちます。ディスク領域を節約し、エージェント通信を高速化するには、エージェントのログ記録 を無効にします。
エージェントのデバッグトレース	有効	選択した場合、このオプションを使用してエージェントのデバッグトレースを記録できます。この情報を使用すると、管理者はエージェントのパフォーマンスを監視して一般的な問題を診断できます。
エージェントインベントリ	12時間	管理対象デバイスのエージェントがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
エージェント不要インベントリ	1日	エージェント不要デバイスがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
カタログインベントリ	24時間	管理対象デバイスが ソフトウェア カタログ ページにインベントリをレポートする頻度。
メータリング	4時間	管理対象デバイスがアプライアンスにメータリング情報をレポートする頻度。デバイスとアプリケーションに対してメータリングを有効にする必要があります。
スクリプト更新	4時間	管理対象デバイスのエージェントが、管理対象デバイスで有効にされているスクリプトの更新されたコピーを要求する頻度。この間隔はスクリプトの実行頻度に影響を与えません。
最大ダウンロード速度	必要に応じて	必要に応じた最大ダウンロード速度。使用可能なオプションから選択します。
プロセスのタイムアウト	1 時間	エージェントプロセスが終了するまでの最大実行時間。詳細については、https://support.quest.com/kb/177093/how-to-allow-more-time-for-a-kace-script-to-run-before-it-times-out-を参照してください。
起動を待機 タスクを無効にする	無効	選択した場合、このオプションによってエージェントで起動タスクが実行されなくなります。

オプション	設定案	メモ
ログインを待機 タスクを無効にする	無効	選択した場合、このオプションによってエージェントでログインタスクを実行しないようになります。

3. エージェントステータスアイコンの設定 セクションで、各設定を次のように指定します。

オプション	設定案	メモ
デバイスでのエージェントのステータス アイコン	有効	このオプションを選択すると、管理対象デバイス上でエージェントのステータスを表示できます。
デバイスでのエージェントの再通知	有効	このオプションを選択すると、管理対象デバイス上のエージェントのシステムトレイ（Windows）またはメニューバー（Mac OS）を使用したアクティビティを一時停止できます。 **注:** インベントリ、レプリケーションタスク、緊急アラートなど、一部の重要なバックグラウンドタスクは引き続き実行できます。
エージェントの再通知の最大数（1 日あたり）	1 回の再通知	管理対象デバイスで 1 日にエージェントを再通知できる最大回数。
エージェントステータスアイコンのショートカット	必要に応じて	このセクションを使用して、エージェント管理対象デバイスの KACE エージェントメニューにリンクを表示します。最大 10 個のリンクを指定できます。https、ssh、ftp URL など、標準の統一資源位置指定子（URI）リンクがサポートされています。リンクを追加するには、次の手順を実行します。 a. ＋ をクリックします。 b. 表示名 列に、メニューに表示するテキストを入力します。たとえば、マイ FTP リンクなどです。 c. URL 列に、完全修飾 URL アドレスを入力します。例：https://www.quest.com/。URL で

オプション	設定案	メモ
		は、次の置換変数がサポートされています。 ◦ $(KACE_SYS_DIR) ◦ $(KACE_MAC_ADDRESS) ◦ $(KACE_IP_ADDRESS) ◦ $(KACE_SERVER_URL) ◦ $(KACE_SERVER) ◦ $(KACE_COMPANY_NAME) ◦ $(KACE_KUID) ◦ $(KACE_APP_DIR) ◦ $(KACE_DATA_DIR) ◦ $(KACE_AGENT_VERSION) これらの変数およびその他の置換変数の詳細については、「トークン置換変数」を参照してください。 列見出しを使用してリストを並べ替えできます。KACE エージェントメニューには、このページに表示される順序でリンクが表示されます。

注: このセクションで行った変更は、個々のエージェントまたはアプライアンスを再起動した後に、管理対象デバイス上の KACE エージェントがアプライアンスに再接続した後でのみ有効になります。

4. 通知 セクションで、エージェント通信に使用するメッセージを指定します。

オプション	設定案	メモ
エージェントのスプラッシュページのメッセージ	デフォルトのテキストは次の通りです。 **KACE システム管理アプライアンス** は、PC 設定の検証およびソフトウェア更新プログラムの管理を行います。お待ちください…	エージェントがデバイス上でスクリプト実行などのタスクを実行しているときに、ユーザーに表示されるメッセージ。
エージェントのスプラッシュビットマップ	必要に応じて	スプラッシュロゴとして使用する既存の.bmpファイルへのパス。
起動スプラッシュを無効にする	無効	選択した場合、このオプションによってエージェントは起動スプラッシュロゴを表示しなくなります。
ログインスプラッシュを無効にする	無効	選択した場合、このオプションによってエージェントはログインスプラッシュロゴを表示しなくなります。

5. エージェント不要の設定 セクションで、エージェント不要デバイスの通信設定を次のように指定します。

オプション	説明
SSHタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
SNMPタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
再試行回数	接続が試行される回数。
WinRMタイムアウト	アクティビティがない場合、この時間（秒単位）が経過すると接続が切断されます。
VMwareのタイムアウト	VMwareホスト上で実行しているVMware vSphere APIに接続する際の待機時間（秒単位）。

6. アプライアンスで組織コンポーネントが有効になっていない場合は、エージェントタスク 設定を指定します。

   注: アプライアンスで組織コンポーネントが有効になっている場合、エージェントタスク 設定はアプライアンスシステム管理コンソールの 一般設定 ページにあります。

オプション	説明
前回のタスクスループットの更新	この値は、アプライアンスのタスクスループットが最後に更新された日付と時刻を示します。
現在の読み込み平均	このフィールドの値は、任意の時点のアプライアンスに対する負荷を示します。アプライアンスが正常に動作するには、このフィールドの値が0.0と10.0の間になければなりません。
タスクスループット	スケジュール済みタスク（インベントリの収集、スクリプト作成、パッチの更新など）のアプライアンスでの調整方法を制御する値。 **注:** この値は、「現在の読み込み平均」の値が10.0以下で、かつ「前回のタスクスループットの更新」の時間が15分を超える場合にのみ増やすことができます。

7. 重複したマシン検出設定（高度）セクションで、重複するデバイスレコードを防止するために以下のオプションを設定します

   アプライアンスは、既存のインベントリレコード（新規/不明の KUID の使用によって決定される）がないデバイスからインベントリを受信すると、このセクションで選択したデバイスのプロパティをスキャンして、新しいデバイスか既存のデバイスかを判断します。デバイスが既存のインベントリレコードに属していると判断された場合、新しいデバイスレコードは既存のレコードとマージされます。

オプション	説明
既存のマシンレコードを照合する必要がある	次のチェックボックスの 1 つまたは複数を選択して、アプライアンスが重複する可能性のあるデバイ

オプション	説明
	スを識別するために使用するデバイスプロパティを指定します。 • **マシン名** • **BIOSのシリアルナンバー** • **製造元** • **オペレーティングシステムのファミリ**
MAC アドレス	既存のデバイスレコードと照合するマシンレコードに関連付けられている MAC アドレスの番号を指定します。

8. **保存** をクリックします。

   変更は、エージェントがアプライアンスにチェックインするときに有効になります。
9. 複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

関連トピック

アプライアンスログの表示

組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定

エージェントタスクのステータスの表示

現在実行されているタスク、またはエージェント管理対象デバイスでスケジュールされているタスクのステータスを参照できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**サポート** をクリックして、サポート ページを表示します。
3. トラブルシューティングツール セクションで、**エージェントタスクのステータスの表示** をクリックして、エージェントタスク ページを表示します。

   デフォルトでは、「進行中」タスクが表示されます。他のタスクを表示するには、右側のリストの上に表示される 特定基準で表示 ドロップダウンリストから別のフィルタを選択します。タスク情報には、以下が含まれます。

列	説明
デバイス名	タスクのターゲットであるデバイスの名前。
タイプ	タスクのタイプ。アプライアンス設定に応じて、警告、インベントリ、kbot、krashアップロード、スクリプト更新などのタスクタイプが存在します。
開始	タスクの開始時刻。
完了	タスクの完了時刻。

列	説明
次回実行	スケジュールに基づく次のタスク実行時刻。
実行時間	タスクの実行にかかる時間。
タイムアウト	タスクの完了における時間制限。
優先度	タスクの重要度またはランク。

表示されるオプションは、アプライアンスで使用可能なタスクのタイプによって異なります。一般的なオプションは次の通りです。

- **実行準備（接続済み）**：メッセージプロトコルで接続され、実行されようとしているタスク。
- **実行準備**：メッセージプロトコル接続が確立されたときに実行されるようにキューに格納されているタスク。
- **10分を超える**：プロトコル接続を 10 分より長く待っているタスク。

4. デバイスに関する詳細を表示するには、Device Name（デバイス名）列でそのコンピューターの名前をクリックします。

   デバイスの詳細 ページが表示されます。

エージェントコマンドキューの表示

エージェントコマンドキュー リストには、ポップアップや通知などのメッセージが示されます。これらのメッセージは、アプライアンスからエージェントの管理対象デバイスに配布するため、キューに格納されています。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**サポート** をクリックして、サポート ページを表示します。
3. トラブルシューティングツール セクションで、**エージェントコマンドキューの表示** をクリックして、エージェントコマンドキュー ページを表示します。

   エージェントとアプライアンスが常時接続されている場合にのみ、保留のメッセージがこのキューに表示されます。

   注: 保留中の警告は、エージェントとアプライアンスの間に接続がない場合でも エージェントコマンドキュー ページに表示されます。

   エージェントコマンドキュー ページには次のフィールドがあります。

オプション	説明
デバイス名	デバイスの名前。名前をクリックして、デバイスの詳細を表示します。
タイプ[プラグイン、ソース]	メッセージのタイプ（プロセスの実行 など）。
コマンド	メッセージに含まれる内容と情報。

オプション	説明
有効期限	メッセージが期限切れになった日付と時刻。キープアライブ ともいいます。期限切れになったメッセージは、キューから自動的に削除されます。
ステータス	メッセージのステータス（完了、受信済み など）。

関連トピック

管理対象デバイスへの警告のブロードキャスト

エージェントコマンドキューからのメッセージの削除

不要になったメッセージをエージェントコマンドキューから削除できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**サポート** をクリックして、サポート ページを表示します。
3. トラブルシューティングツール セクションで、**エージェントコマンドキューの表示** をクリックして、エージェントコマンドキュー ページを表示します。
4. 1つ以上のメッセージの隣のチェックボックスをオンにします。
5. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

管理対象デバイスでの KACE エージェントの更新

アプライアンスは、毎日午前 3:40 頃に Quest にアクセスして、KACE エージェントのアップデートがあるかどうかを自動的に確認します。また、アプライアンスの再起動時にも必ずQuestでエージェントのアップデートが確認されます。

エージェントのアップデートが使用可能な場合は、アプライアンスがインターネットに接続され、アプライアンス**管理者コンソール**の ホーム ページに警告が表示されていれば、アプライアンスに自動的にダウンロードされます。ただし、展開設定を設定するまで、エージェントのアップデートは管理対象デバイスに自動的に展開されません。警告に含まれるリンクをクリックして、展開設定を設定します。

また、エージェントのソフトウェアアップデートがないか確認し、エージェントのアップデートを手動で取得し、エージェントのアップデート設定をいつでも設定できます。アプライアンスがインターネットに接続されていない場合は、アップデートを手動で取得すると便利です。

KACE エージェントのアップデートの表示

KACE エージェントのアップデートは、**管理者コンソール**で確認できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**アプライアンスの更新**をクリックします。

アプライアンスの更新 ページが表示されます。エージェント セクションに、現在のエージェントバンドルが表示されます。

3. **オプション**：更新をチェックするには：エージェント セクションで、**更新の確認** をクリックします。

   アップデートのチェックが行われ、その結果が ログ ページに表示されます。

エージェントアップデート設定について

エージェントをデバイスにインストールすると、Update Agent Settings（エージェント設定のアップデート）ページで選択したエージェントアップデート設定に基づいて、エージェントが自身を自動的に更新するようになります。これは、エージェントの展開に使用されるプロビジョニング方法（アプライアンスプロビジョニング、GPO ウィザード、その他の GPO 展開、イメージ展開など）に関係なく当てはまります。

複数の組織がある場合は、エージェントのアップデート設定は組織ごとに個別に行います。

1. エージェント設定の更新 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**プロビジョニング** の順にクリックします。
   c. プロビジョニングパネルで **エージェントのアップデート** をクリックします。

   新しいエージェントアップデートが使用可能になると、それが Available Agent Bundle（使用可能なエージェントバンドル）セクションに表示されます。
2. Available Agent Bundle（使用可能なエージェントバンドル）セクションの **適用** をクリックします。

   新しいエージェントバージョン番号が 通知更新 セクションに表示され、エージェント設定 セクションの 有効 チェックボックスがオフになって自動更新が無効になります。これにより、アップデートをシステム全体に展開する前に、選択したデバイスでアップデートをテストできます。
3. 次のエージェントアップデートの設定を確認するか、または指定します。

オプション	説明
有効	次回スケジュールされたインベントリ間隔で、選択したアプライアンスデバイスにアップデートを展開します。アップデートをインストールしない場合には、このチェックボックスをオフにしてください。
修正日	読み取り専用：最新のエージェントバンドルがダウンロードされた時点。
全デバイス	アップデートを、KACE エージェントがインストールされているすべてのデバイスに展開します。このオプションを選択した場合、デバイス および ラベル 要素はページに表示されません。
デバイス	特定のデバイスのみを更新します。フィールドをクリックして表示されるドロップダウンリストでデバイス名を選択するか、デバイス名の最初の数文字を入力してリストを並べ替えます。例えば「Dev」と入力すると、Device-1、Device-2 などの一致するデバイス名が一覧表示されます。このオプションは、**全デバイス** を選択したときには使用できません。
関連づけられたラベルの管理	Edit Labels（ラベルの編集）ダイアログを表示します。ラベルを検索および選択し、選択されたラベルに割り当てられたデバイスを更新します。このオプ

オプション	説明
	ションは、**全デバイス** を選択したときには使用できません。
メモ	任意の追加情報を入力します。

4. **保存** をクリックします。

   次回スケジュールされたインベントリ間隔で、選択したデバイスにアップデートが展開されます。レプリケーション共有を使用し、アプライアンスへのフェールオーバーを選択していない場合は、レプリケーション共有が更新された後で、エージェントが更新されます。
5. テストのため展開を指定のデバイスに制限した場合は、テストが完了したときに、Update Agent Settings（エージェント設定の更新）ページの エージェント設定 セクションで追加のデバイスを選択します。

   次回スケジュールされたインベントリ間隔で、選択したデバイスにアップデートが展開されます。
6. 複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

関連トピック

アイテムのグループを管理するためのラベルのセットアップおよび使用

エージェントのアップデートの手動アップロード

ほとんどの場合、エージェントアップデートは使用可能になると、アプライアンスに自動的にダウンロードされます。ただし、必要に応じて、Quest KACEからアップデートをダウンロードし、アプライアンスにエージェントアップデートを手動でアップロードできます。これは、アプライアンスがインターネットに接続されていない場合や、エージェントアップデートは利用できるもののアプライアンスにまだ自動的にダウンロードされていない場合に便利です。

Quest からエージェント更新をダウンロードするには、**Questサポート**（https://support.quest.com/contact-support）に問い合わせてログイン資格情報を入手する必要があります。

1. アップデートがないか手動で確認するには、アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。

   エージェント セクションに、現在のエージェントバンドルのバージョンが表示されます。
3. エージェント セクションの **更新の確認** をクリックします。

   アップデートのチェックが行われ、その結果が ログ ページに表示されます。
4. アップデートを取得するには、次の手順を実行します。
   a. ログイン資格情報を使用して、Questサポートサイトにログインします：

   https://support.quest.com/kace-systems-management-appliance/download-new-releases.

   b. エージェントアップデートバンドルをダウンロードし、ファイルをローカルに保存します。
5. エージェント設定の更新 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左のナビゲーションバーで **設定**、**プロビジョニング** の順にクリックします。

c. プロビジョニングパネルで **エージェントのアップデート** をクリックします。

6. 次のいずれかを実行します。
   - **新しいアップデートが** Available Agent Bundle **(使用可能なエージェントバンドル) セクションに表示されている場合は、適用 をクリックします。**
   - **アップデートを手動でダウンロードした場合は、**Manually Upload Agent Bundle **(エージェントバンドルの手動アップロード) セクションに移動し、参照 または ファイルの選択 をクリックします。ダウンロードしたファイルを探し、アップロード をクリックします。**

   新しいエージェントバージョン番号が 通知更新 セクションに表示され、エージェント設定 セクションの 有効 チェックボックスがオフになって自動更新が無効になります。これにより、アップデートをシステム全体に展開する前に、選択したデバイスでアップデートをテストできます。
7. エージェント設定 セクションで展開オプションを指定します。詳細については、「エージェントアップデート設定について」を参照してください。
8. 組織が複数ある場合は、組織ごとに6および7を繰り返します。

KACE エージェントを手動展開する

手動の展開は、エージェントの自動プロビジョニングが現実的ではないときや、E メール、ログオンスクリプト、GPO (グループポリシーオブジェクト)、または Active Directory を使用して KACE エージェントを展開するときに便利です。

- **Eメール**: E メールを通じて KACE エージェントを展開するために、次のいずれかの情報を含めて E メールをユーザーに送信します。
  - エージェントのインストールファイル
  - エージェントファイルをダウンロードできるアプライアンスへのリンク
  - 必要なインストールファイルをダウンロードできる、Web上の場所
- **ログオンスクリプト**: ログオンスクリプトを使用すると、ユーザーがデバイスにログオンするときに KACE エージェントを展開できます。ログオンスクリプトを使用する場合は、該当するファイルをアクセス可能なディレクトリにアップロードし、そのファイルを取得するログオンスクリプトを作成します。

エージェントのインストールファイルの取得

エージェントのインストールファイルは、アプライアンスで使用可能です。

Windows、Mac OS X、および Linux デバイス用の KACE エージェントインストーラは、アプライアンスの次のディレクトリにあります。

appliance_hostname\client\agent_provisioning

注: インストーラーにアクセスするには、ファイル共有が有効になっている必要があります。詳細については、「システムレベルでのファイル共有の有効化」を参照してください。

アプライアンスは登録プロセスを使用して、トークンをエージェントに関連付けるか、アプライアンス管理者に接続要求を承認させることによって、認証済みの KACE エージェントがアプライアンスに接続できるようにしま

す。この方法で取得したエージェントインストーラには、有効なトークンは含まれません。次のいずれかのオプションを使用して、エージェントトークンをインストーラに手動で渡すことができます。

- **Windows デバイス：**
  - インストーラを起動するときは、次のパラメータを使用します。HOST=<appliance_hostname> TOKEN=<agent_token>、または：
  - 次の構文を使用して、インストールファイル名を手動で変更します。AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi
- **Windows 以外のデバイス**：
  - インストールファイルを実行する前に KACE_HOST および KACE_TOKEN 環境変数を使用してアプライアンスのホスト名とエージェントトークンを指定します。または、
  - 次の構文を使用して、インストールファイル名を手動で変更します。<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>

エージェントのインストール中に有効なトークン文字列を指定しないと、接続要求があった場合、エージェントが検疫されます。

または、エージェントトークンの詳細 ページから、オペレーティングシステム用のエージェントトークンインストーラバンドルをダウンロードすることもできます。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。

Windows デバイス上で KACE エージェントを手動展開する

インストールウィザード、またはデバイス上でコマンドラインを使用して、Windows デバイスで KACE エージェントを手動で展開できます。

エージェントを手動でインストールする場合には、エージェントの実行可能ファイルを次の場所にインストールする必要があります。

- Windows 32ビットデバイス: C:\Program Files\Quest\KACE\
- Windows 64ビットデバイス：C:\Program Files (x86)\Quest\KACE\

エージェント設定ファイル、ログ、およびその他のデータは次の場所に保存されます。

- Windows 32ビットデバイス: C:\Documents and Settings\All Users\Quest\KACE
- Windows 64ビットデバイス：C:\ProgramData\Quest\KACE

インストールウィザードを使用して KACE エージェントを Windows デバイスに手動展開する

デバイスでインストールウィザードを実行して、KACE エージェントを Windows デバイスに手動展開できます。

1. アプライアンスの次の共有ディレクトリに移動します。

   appliance_hostname\client\agent_provisioning\windows_platform
2. デバイスに ampagent-x.x.xxxxx-x86.msi ファイルをコピーします。
3. そのファイルをダブルクリックしてインストールを開始し、インストールウィザードの手順に従います。
4. エージェントをアプライアンスに登録する場合は、次の手順を実行します。
   - インストーラを起動するときは、次のパラメータを使用します。HOST=<appliance_hostname> TOKEN=<agent_token>、または：
   - 次の構文を使用して、インストールファイル名を手動で変更します。AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi

   エージェントトークン文字列は、エージェントトークンの詳細 ページから取得できます。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。

デバイスの情報がアプライアンスの**インベントリ**に数分以内に表示されます。詳細については、「ソフトウェアページでのアプリケーション管理」を参照してください。

コマンドラインを使用して KACE エージェントを Windows デバイスに手動展開する

Windowsデバイスでコマンドラインからエージェントを展開するには、いくつかの方法があります。

例：

- ログオンスクリプトに含めたバッチファイルで、インストーラー（ msiexec ）を実行し、ホストの値などのさまざまなパラメータを設定します。
- サーバー名に対応する環境変数を設定し、インストーラーを実行します。
- インストーラーの名前を変更します。これにより、インストール中にサーバー名が自動的に設定されます。

次の表に、エージェントの展開に使用するコマンドラインパラメータを示します。

エージェント用のコマンドラインパラメータ

説明	パラメータ
Windowsインストーラーツール	msiexecまたはmsiexec.exe
インストールフラグ	/i **例**： msiexec /i ampagent-6.x.xxxxx-x86
アンインストールフラグ	/x **例**： msiexec /x ampagent-6.x.xxxxx-x86
サイレントインストール	/qn **例**： msiexec /qn /i ampagent-6.x.xxxxx-x86
詳細出力のログ記録	/L*v log.txt **例**： msiexec /qn /L*v C:\temp\log.txt /i ampagent-6.x.xxxxx-x86
ホスト名の自動設定：インストールファイルの名前をサーバーの名前に変更して、自動的にホスト名が設定されるようにします。	rename agent_installer.msi_hostname.msi **例**： msiexec /qn /i ampagent-6.x.xxxxx-x86_kace_sma.example.com.msi
プロパティの設定	PROPERTY=value（ すべて大文字を使用 ） **例**： msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com
サーバー名の設定	set KACE_SERVER=kace_sma_name

説明	パラメータ
	インストールするmsiexecの呼び出しの前に挿入 **例**： set KACE_SERVER=kboxmsiexec /i ampagent-6.x.xxxxx-x86
ログオンまたは起動フックがインストールされないようにし、既存のuserinit.exeファイルを維持	NOHOOKS=1 **例**： msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com NOHOOKS=1
エージェントをインストールするが、サービスを開始しない。これによって、エージェントのイメージを作成して、他のデバイスにクローンを作成できます	CLONEPREP=yes/no **例**： msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com CLONEPREP=yes
ログ生成時のエージェントのデバッグレベルの設定	DEBUG=true/all **例**： msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com DEBUG=true
HTTPS経由でのみ通信するようにエージェントを強制。HTTPSが使用できない場合に、HTTPを使用することはできません	SSLREQUIRED=true **例**： msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com SSLREQUIRED=true

これらの場所の**host**の値に対するシステムフックは、次の順序になります。

1. インストーラーファイル
2. HOST プロパティ値
3. KACE_SERVER（環境変数）
4. amp.confファイル

エージェントをアプライアンスに登録する場合は、次の手順を実行します。

- インストーラを起動するときは、次のパラメータを使用します。HOST=<appliance_hostname> TOKEN=<agent_token>、または：
- 次の構文を使用して、インストールファイル名を手動で変更します。AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi

エージェントトークン文字列は、エージェントトークンの詳細 ページから取得できます。詳細については、以下を参照してください： アプライアンスへの KACE エージェントの登録

注意: ホスト値を空のままにする場合は、環境変数を設定する必要があります。そのようにしないと、エージェントがアプライアンスに接続できなくなります。ホスト名として完全修飾ドメイン名を使用することをお勧めします。

Windows システムトレイを使用して Windows デバイスで KACE エージェントを管理する

Windows システムトレイを使用して、KACE エージェントのステータスの表示、強制的なインベントリ更新、およびエージェント情報の表示ができます。

システムトレイを使用して KACE エージェントのステータスにアクセスするには、エージェントおよび通信設定セクションで **デバイスでのエージェントのステータス** オプションを有効にする必要があります。詳細については、「エージェント通信とログ設定の定義」を参照してください。

1. KACE エージェントが動作しているデバイスの Windows システムトレイで をクリックします。

   アイコンの右下隅にあるインジケータは、エージェントのステータスについて以下が該当するかどうかを示します。

   - : エージェントはアプライアンスに接続されています。
   - : エージェントは再通知設定されています。
   - : エージェントに保留中のアクションがあります。
   - : エージェントはアプライアンスから切断されています。

2. エージェントがアプライアンスに接続されているかどうかを確認するには、メニューの ステータス アイコンを確認します。

   これは、エージェント アイコンに表示されるインジケータと同じで、エージェントが接続されているか、再通知設定されているか、保留中のアクションがあるか、またはアプライアンスから切断されているかを示します。

3. デバイスインベントリを実行するには、メニューで **インベントリ** をクリックします。
4. エージェントを再起動するには、メニューで **エージェントの再起動** をクリックします。
5. 特定の期間にエージェントのアクティビティを一時的に中断するには、**エージェントの再通知** をクリックし、メニューで時間を選択します。エージェントの再通知は、15 分、30 分、1 時間、または 2 時間に設定できます。

   注: エージェントを再通知できるのは、アプライアンスの エージェントおよび通信設定 セクションで **デバイスでのエージェントの再通知** オプションが有効になっていて、再通知の最大数に達していない場合だけです。詳細については、「エージェント通信とログ設定の定義」を参照してください。

   エージェントを再通知しても、デバイス上で実行中のエージェントプロセスは停止しません。エージェントが新しいプロセスを開始できないようにするだけです。設定などの理由でエージェントの再通知ができない場合は、エラーメッセージが表示されます。

6. エージェントデバイスにダウンロードしたパッチをインストールするには、**Deploy staged patches**（ステージングされたパッチの展開 ）をクリックします。

   注: このメニュー項目は、検出、ステージおよびオンデマンド展開パッチまたは Windows 機能スケジュールが、該当するすべてのパッチをエージェントデバイスにダウンロードした場合にのみ表示されます。詳細については、「パッチスケジュールの設定」を参照してください。

7. エージェント関連のリンクにアクセスするには、メニューの **ショートカット** をクリックし、必要に応じてリンクをクリックします。https、ssh、ftp URL など、あらゆる標準の統一資源位置指定子（URI ）リンクがサポートされています。

   このメニュー項目は、システム管理者が 1 つ以上のリンクを指定した場合にのみ表示されます。詳細については、「エージェント通信とログ設定の定義」を参照してください。

   このリンクを使用すると、OS が選択したリソースに関連付けられたアプリケーションが起動します。たとえば、HTTP リンクを開くために、システムはデフォルトのブラウザでリンクを開きます。

8. エージェントアプリケーションの詳細については、**バージョン情報** をクリックしてください。

Linux デバイスでの手動による KACE エージェントの展開およびアップグレード

必要に応じて、Linux デバイスで KACE エージェントを手動で展開およびアップグレードできます。

Linux デバイスで手動により KACE エージェントを展開する

エージェントのインストールファイルをデバイスにコピーし、インストールコマンドを実行して、Linux デバイス上で KACE エージェントを手動で展開できます。

1. KACE エージェントのインストールファイルをデバイスにコピーします。

   詳細については、「エージェントのインストールファイルの取得」を参照してください。

2. エージェントをアプライアンスに登録する場合は、次の手順を実行します。

   - インストールファイルを実行する前に KACE_HOST および KACE_TOKEN 環境変数を使用してアプライアンスのホスト名とエージェントトークンを指定します。または、
   - 次の構文を使用して、インストールファイル名を手動で変更します。<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>

   エージェントトークン文字列は、エージェントトークンの詳細 ページから取得できます。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。

3. **アプリケーション > システムツール** からターミナルウィンドウを開きます。
4. コマンドプロンプトで、サーバーの名前を設定し、エージェントをインストールします。

   sudo KACE_SERVER=kace_sma_name rpm -Uvh ampagent-x.x.xxxxx-x.i386.rpm

   エージェントは次のディレクトリにインストールされます。

   - /opt/quest/kace/bin/（ここに、エージェントの実行可能ファイルがインストールされます）。
   - /var/quest/kace/（ここに、エージェント設定、ログ、およびその他のデータが保存されます）。

デバイスの情報がアプライアンスの**インベントリ**に数分以内に表示されます。詳細については、「ソフトウェアページでのアプリケーション管理」を参照してください。

起動時またはログイン時に KACE エージェントを Linux デバイスに展開する

ユーザーがLinuxデバイスを起動またはLinuxデバイスにログインしたときにエージェントが展開されるようにスケジュールすることができます。

- ルートディレクトリに次のコマンドを追加することにより、ホストの名前を設定します。

  export KACE_SERVER=kace_sma_name

  exportの呼び出しはインストーラーの呼び出しの前に挿入する必要があります。例：export KACE_SERVER=kace_sma_name rpm -Uvh kace_sma_agent-12345.i386.rpm

  これらの場所の**host**の値に対するシステムフックは、次の順序になります。

  1. インストーラーファイル
  2. KACE_SERVER（環境変数）
  3. amp.confファイル

  エージェントをアプライアンスに登録する場合は、次の手順を実行します。

  - インストールファイルを実行する前に KACE_HOST および KACE_TOKEN 環境変数を使用してアプライアンスのホスト名とエージェントトークンを指定します。または、
  - 次の構文を使用して、インストールファイル名を手動で変更します。<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>

  エージェントトークン文字列は、エージェントトークンの詳細 ページから取得できます。詳細については、以下を参照してください： アプライアンスへの KACE エージェントの登録

  注意: ホスト値を空のままにする場合は、環境変数を設定する必要があります。そのようにしないと、エージェントがアプライアンスに接続できなくなります。ホスト名として完全修飾ドメイン名を使用することをお勧めします。

Linux デバイスの KACE エージェントをアップグレードする

Linux デバイスでコマンドを実行して、これらのデバイスの KACE エージェントを手動でアップグレードできます。

1. KACE エージェントのインストールファイルをデバイスにコピーします。詳細については、「エージェントのインストールファイルの取得」を参照してください。
2. エージェントをアプライアンスに登録する場合は、次の手順を実行します。
   - インストールファイルを実行する前に KACE_HOST および KACE_TOKEN 環境変数を使用してアプライアンスのホスト名とエージェントトークンを指定します。または、
   - 次の構文を使用して、インストールファイル名を手動で変更します。<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>

   エージェントトークン文字列は、エージェントトークンの詳細 ページから取得できます。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。
3. **アプリケーション > システムツール** からターミナルウィンドウを開きます。
4. コマンドプロンプトで、次のように入力します。

   rpm -uvh kace_sma_agent-linux_buildnumber.rpm

Linuxデバイス上でのエージェントに関する操作の実行

エージェント管理対象のLinuxデバイスでコマンドを実行して、エージェントに関するさまざまな操作を実行できます。

Linuxデバイス上のエージェントの開始と停止

Linux デバイスでコマンドを実行して、エージェントを開始および停止できます。この手順は、エージェント関連の問題のトラブルシューティングを行う際に役立ちます。

1. **アプリケーション > システムツール** からターミナルウィンドウを開きます。
2. エージェントを開始するには、次のように入力します。

   /opt/quest/kace/bin/AMPTools start
3. エージェントを停止するには、次のように入力します。

   /opt/quest/kace/bin/AMPTools stop

Linuxデバイスからエージェントを手動で削除する

Linuxデバイスでコマンドを実行して、これらのデバイスからエージェントを手動で削除できます。

1. **アプリケーション > システムツール** からターミナルウィンドウを開きます。
2. コマンドプロンプトで、次のように入力します。

   sudo rpm -e ampagent
3. **オプション**：kaceディレクトリを削除します。

   rm -rf /var/quest/kace/

Linuxデバイス上でエージェントが実行中であることを確認する

Linuxデバイスでコマンドを実行して、エージェントが実行中であるかどうかを確認します。

1. **アプリケーション > システムツール** からターミナルウィンドウを開きます。
2. コマンドラインプロンプトで、次のように入力します。

   ps aux | grep AMPAgent

この出力には、次のようにプロセスが動作していることが表示されます。

root 6100 0.0 3.9 3110640 20384 ? Ssl Mar03 0:00 /opt/quest/kace/bin/AMPAgent --daemon

Linuxデバイス上のエージェントのバージョンを表示する

Linuxデバイスでコマンドを実行して、これらのデバイスにインストールされているエージェントのバージョンを確認します。

1. **アプリケーション > システムツール** からターミナルウィンドウを開きます。
2. コマンドプロンプトで、次のように入力します。

   rpm -q ampagent

   バージョン番号が表示されます。

インベントリ情報の収集

インベントリ更新を強制実行して、Linuxデバイス上のインベントリを手動で収集できます。

詳細については、「インベントリ更新の強制実行」を参照してください。

Mac デバイスでの手動による KACE エージェントの展開およびアップグレード

必要に応じて、Macデバイスでエージェントを手動で展開およびアップグレードできます。

このセクションでは、KACE エージェントを Mac OS X デバイスで手動展開する方法について説明します。その他のオプションについては、シェルスクリプトを使用した KACE エージェントの展開で説明しています。

注: 一部のコマンドは **root** として実行する必要があります。
注: 必要に応じて続いて「su」または「sudo」を実行します。

エージェントインストーラを使用して Mac デバイス上で KACE エージェントを展開またはアップグレードする

エージェントのインストールファイルをデバイスにコピーし、インストーラを実行して、Mac デバイス上で KACE エージェントを手動で展開できます。

1. KACE エージェントのインストールファイルをデバイスにコピーします。

   詳細については、「エージェントのインストールファイルの取得」を参照してください。

2. エージェントをアプライアンスに登録する場合は、次の手順を実行します。
   - インストールファイルを実行する前に KACE_HOST および KACE_TOKEN 環境変数を使用してアプライアンスのホスト名とエージェントトークンを指定します。または、
   - 次の構文を使用して、インストールファイル名を手動で変更します。<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>

   エージェントトークン文字列は、エージェントトークンの詳細 ページから取得できます。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。

3. **ampagent-x.x.build_number.dmg** をダブルクリックします。
4. **AMPAgent.pkg**をダブルクリックします。
5. インストーラーの手順に従います。

   アプライアンスの名前を必ず入力してください。

インストーラーによってデバイス上に次のディレクトリが作成されます。

- /Library/Application Support/Quest/KACE/bin（ここに、エージェントの実行可能ファイルがインストールされます）。
- /Library/Application Support/Quest/KACE/data/（ここに、エージェント設定、ログ、およびその他のデータが保存されます）。

ターミナルウィンドウを使用してMacデバイスにエージェントを展開する

エージェントのインストールファイルをデバイスにコピーし、コマンドを実行して、Mac デバイス上で KACE エージェントを手動で展開できます。

1. KACE エージェントのインストールファイルをデバイスにコピーします。

   詳細については、「エージェントのインストールファイルの取得」を参照してください。

2. エージェントをアプライアンスに登録する場合は、次の手順を実行します。
   - インストールファイルを実行する前に KACE_HOST および KACE_TOKEN 環境変数を使用してアプライアンスのホスト名とエージェントトークンを指定します。または、
   - 次の構文を使用して、インストールファイル名を手動で変更します。<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>

   エージェントトークン文字列は、エージェントトークンの詳細 ページから取得できます。詳細については、「アプライアンスへの KACE エージェントの登録」を参照してください。

3. **アプリケーション > ユーティリティ** から、ターミナルウィンドウを開きます。
4. コマンドプロンプトで次のコマンドを入力して、サーバーの名前を設定し、エージェントをインストールします。

   hdiutil attach ./ampagent-x.x.xxxxx-all.dmg

   sudo sh -c 'KACE_SERVER=kace_sma_name installer -pkg /Volumes/Quest_KACE/AMPAgent.pkg -target /'

   hdiutil detach '/Volumes/Quest_KACE'

シェルスクリプトを使用した KACE エージェントの展開

シェルスクリプトを実行して、エージェントをMacデバイスに展開できます。

シェルスクリプトを使用してエージェントを展開するときには、以下のコマンドラインオプションを使用できます。

- hdiutil attach ./ampagent-6.x.xxxxx-all.dmg
- sudo sh -c 'KACE_SERVER=kace_sma_name installer -pkg
- /Volumes/Quest_KACE/AMPAgent.pkg -target /'
- hdiutil detach '/Volumes/Quest_KACE'

> **注:** exportの呼び出しはinstallの呼び出しの前に挿入する必要があります。例：sudo export KACE_SERVER=kace_sma_name installer -pkg '/Volumes/Dell KACE/AMPAgent.pkg' -target /

これらの場所の**host**の値に対するシステムフックは、次の順序になります。

1. インストーラーファイル
2. KACE_SERVER（環境変数）
3. amp.confファイル

エージェントをアプライアンスに登録する場合は、次の手順を実行します。

- インストールファイルを実行する前に KACE_HOST および KACE_TOKEN 環境変数を使用してアプライアンスのホスト名とエージェントトークンを指定します。または、
- 次の構文を使用して、インストールファイル名を手動で変更します。<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>

エージェントトークン文字列は、エージェントトークンの詳細 ページから取得できます。詳細については、以下を参照してください： アプライアンスへの KACE エージェントの登録

シェルスクリプトとコマンドラインの使用に関する情報については、http://developer.apple.comを参照してください。

注意: ホスト値を空のままにする場合は、環境変数を設定する必要があります。そのようにしないと、エージェントがアプライアンスに接続できなくなります。Quest KACEでは、ホスト名として完全修飾ドメイン名を使用することをお勧めします。

Macデバイス上でエージェントに関するその他の操作を実行する

エージェント管理対象のMacデバイスでコマンドを実行して、さまざまな操作を実行できます。

Macデバイス上のエージェントの開始と停止

Mac デバイスでコマンドを実行して、エージェントを開始および停止できます。この手順は、エージェント関連の問題のトラブルシューティングを行う際に役立ちます。

1. **アプリケーション > ユーティリティ** から、ターミナルウィンドウを開きます。
2. 次のように入力します。

   cd "Library/Application Support/Quest/KACE/bin"
3. エージェントを開始するには、次のように入力します。

   ./AMPTools start
4. エージェントを停止するには、次のように入力します。

   ./AMPTools stop

Macデバイスからエージェントを手動で削除する

Macデバイスでコマンドを実行して、これらのデバイスからエージェントを手動で削除できます。

1. **アプリケーション > ユーティリティ** から、ターミナルウィンドウを開きます。
2. 次のように入力します。

   sudo "/Library/Application Support/Quest/KACE/bin/AMPTools" uninstall

エージェントが削除されます。

Macデバイス上でエージェントが実行中であることを確認する

Macデバイスでコマンドを実行して、エージェントが実行中であるかどうかを確認します。

1. **アプリケーション > ユーティリティ** から、ターミナルウィンドウを開きます。
2. 次のコマンドを入力します:

   ps aux | grep AMPAgent

   この出力には、次のようにプロセスが動作していることが表示されます。

   root 2159 0.0 1.1 94408 12044 p2 S 3:26PM 0:10.94 /Library/Application Support/Quest/KACE/AMPAgent

Macデバイス上のエージェントのバージョンを確認する

Macデバイスでコマンドを実行して、これらのデバイスにインストールされているエージェントのバージョンを確認します。

1. **アプリケーション > ユーティリティ** から、ターミナルウィンドウを開きます。
2. 次のコマンドを入力します:

   cat /Library/Application\ Support/Quest/KACE/data/version

   バージョン番号が表示されます。

Macデバイスからインベントリ情報を収集する

インベントリ更新を強制実行して、Macデバイス上の情報を手動で収集できます。

詳細については、「インベントリ更新の強制実行」を参照してください。

メニューバーを使用して、Mac デバイスで KACE エージェントを管理する

Mac メニューバーを使用して、KACE エージェントのステータスの表示、強制的なインベントリ更新、およびエージェント情報の表示ができます。

Mac メニューバーを使用して KACE エージェントのステータスにアクセスするには、エージェントおよび通信設定 セクションで **デバイスでのエージェントのステータス** オプションを有効にする必要があります。詳細については、「エージェント通信と ログ設定の定義」を参照してください。

1. KACE エージェントが動作しているデバイスの Mac メニューバーで をクリックします。

   アイコンの右下隅にあるインジケータは、エージェントのステータスについて以下が該当するかどうかを示します。

   - : エージェントはアプライアンスに接続されています。
   - : エージェントは再通知設定されています。
   - : エージェントに保留中のアクションがあります。
   - : エージェントはアプライアンスから切断されています。

   エージェントメニューが表示されます。
2. エージェントがアプライアンスに接続されているかどうかを確認するには、メニューの ステータス アイコンを確認します。

   これは、エージェント アイコンに表示されるインジケータと同じで、エージェントが接続されているか、再通知設定されているか、保留中のアクションがあるか、またはアプライアンスから切断されているかを示します。
3. デバイスインベントリを実行するには、メニューで **インベントリ** をクリックします。
4. エージェントを再起動するには、メニューで **エージェントの再起動** をクリックします。
5. 特定の期間にエージェントのアクティビティを一時的に中断するには、**エージェントの再通知** をクリックし、メニューで時間を選択します。エージェントの再通知は、15 分、30 分、1 時間、または 2 時間に設定できます。

   注: エージェントを再通知できるのは、アプライアンスの エージェントおよび通信設定 セクションで **デバイスでのエージェントの再通知** オプションが有効になっていて、再通知の最大数に達していない場合だけです。詳細については、「エージェント通信と ログ設定の定義」を参照してください。

   エージェントを再通知しても、デバイス上で実行中のエージェントプロセスは停止しません。エージェントが新しいプロセスを開始できないようにするだけです。設定などの理由でエージェントの再通知ができない場合は、エラーメッセージが表示されます。
6. エージェント関連のリンクにアクセスするには、メニューの **ショートカット** をクリックし、必要に応じてリンクをクリックします。https、ssh、ftp URL など、あらゆる標準の統一資源位置指定子（URI）リンクがサポートされています。

このメニュー項目は、システム管理者が 1 つ以上のリンクを指定した場合にのみ表示されます。詳細については、「エージェント通信とログ設定の定義」を参照してください。

このリンクを使用すると、OS が選択したリソースに関連付けられたアプリケーションが起動します。たとえば、HTTP リンクを開くために、システムはデフォルトのブラウザでリンクを開きます。

7. エージェントアプリケーションの詳細については、**バージョン情報** をクリックしてください。
8. Mac メニューバーからエージェントアプリケーションを削除するには、**終了** をクリックします。

   エージェントアイコンがメニューバーから削除されます。再度表示するには、ログオフしてからログオンします。または、アプリケーション ディレクトリからエージェントを再インストールすることもできます。

エージェントによって収集された情報の表示

エージェントによって収集されたインベントリ情報を デバイスの詳細 ページに表示できます。

詳細については、「インベントリ情報の管理」を参照してください。

エージェント不要の管理の使用

KACE エージェントソフトウェアをデバイス上に展開、維持することなくデバイスを管理する必要がある場合は、エージェント不要デバイス管理を使用します。

エージェント不要デバイス管理について

エージェント不要デバイス管理は、デバイスに KACE エージェントソフトウェアを展開および保守する必要なく、デバイスを管理する方法です。

エージェント不要管理では、SSH、SNMP、およびその他の方法を使用して、プリンタ、ネットワークデバイス、およびストレージデバイスなどのエージェントをインストールできないデバイスに接続し、アプライアンス **管理者コンソール** に収集されたインベントリ情報をレポートします。エージェント不要管理を使用すると、オペレーティングシステムのバージョンおよび配布が KACE エージェントのサポート対象ではない場合や、エージェントをインストールするよりもエージェント不要管理が望ましい場合に有用です。

エージェントデバイスとエージェント不要デバイスでサポートされる機能には、いくつかの相違点があります。詳細については、「各デバイス管理方法で使用可能な機能」を参照してください。

エージェント不要管理でサポートされているオペレーティングシステム

エージェント不要管理は、デバイスのさまざまなオペレーティングシステムをサポートしています。

次の表は、エージェント不要管理でサポートされている、デバイスのオペレーティングシステムを示しています。

オペレーティングシステム
CentOS
Chrome OS
Debian
Fedora
FreeBSD

オペレーティングシステム
Mac OS X
Oracle Enterprise Linux
Red Hat Enterprise Linux*
SUSE*
Solaris
Ubuntu*
Windows
Windows Server

*最新バージョンも KACE エージェントで管理できます。

注: 資産などの非コンピュータデバイス、またはエージェント不要管理でサポートされているオペレーティングシステムを搭載していないデバイスの場合、SNMP（簡易ネットワーク管理プロトコル）OID（オブジェクト識別子）をインベントリ表の特定のフィールドにマップできます。これにより、エージェント不要管理デバイスのインベントリを展開できるように、インベントリに設定する特定のデバイスを指定できます。詳細については、「インベントリに追加する特定の SNMP オブジェクトおよびコンピューター以外のデバイスを特定するための SNMP インベントリ設定の使用」を参照してください。

エージェント管理デバイス上のエージェント不要管理の有効化について

エージェント不要管理は、KACE エージェントがインストールされているデバイスも含めて、検出されたすべてのデバイスで有効化できます。

しかし、1台のデバイス上で、両方の管理方法を使用することはお勧めしません。両方の方法がデバイスで有効になっている場合、両方のデバイスおよびそのソフトウェアは、インベントリリストに2回表示されます。このため、エージェント管理対象デバイス上でエージェント不要管理を有効化することはお勧めしません。

エージェント不要デバイスの管理

KACE エージェントソフトウェアをインストールしないでデバイスを管理するには、検出情報を使用して、またはデバイス接続の詳細を手動で入力することでエージェント不要管理を有効にします。

エージェント不要デバイスで利用可能な機能は、エージェント管理対象デバイスで利用可能な機能とは異なります。詳細については、「各デバイス管理方法で使用可能な機能」を参照してください。

検出情報を使用したエージェント不要管理の有効化

エージェント不要管理は、検出情報を使用して有効にできます。

1. 検出結果 リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**検出結果** をクリックします。
2. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
3. **アクションの選択 > プロビジョニング > エージェント不要：自動** を選択します。

選択したデバイスに対してエージェント不要管理が有効化され、次のアイコンのいずれかがデバイス名の隣に表示されます。

 : デバイスでエージェント不要管理が有効になっています。

 : デバイスに対してエージェント不要管理が有効化されていますが、現在デバイスは到達できません。

デバイスに応じて、アプライアンスはさまざまな接続タイプを使用して、選択したデバイスでコマンドを実行し、インベントリ情報を取得し、デバイスの詳細 ページに情報を表示します。エージェント不要デバイスのインベントリスケジュールに従って、情報は更新されます。詳細については、以下を参照してください。

- インベントリ情報の管理
- 管理対象デバイスでのインベントリデータ収集のスケジュール

デバイス情報の手動入力によるエージェント不要管理の有効化

デバイス情報を手動で入力することで、エージェント不要管理を有効化できます。

接続タイプは、SSH、SNMP、WinRM、VMware から選択できます。WinRMは、Windowsデバイスに対して使用する接続タイプです。

1. デバイス リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. **アクションの選択 > 新規作成 > エージェント不要デバイス** を選択して、エージェント不要デバイス接続の詳細 ページを表示します。
3. 接続のタイプに応じた情報を指定します。
   - **デバイスでSSH接続を設定するには、次の情報を入力します。**

オプション	説明
名前	デバイスのホスト名またはIPアドレス。
資産サブタイプ	資産のサブカテゴリ（ 該当する場合 ）。この情報を使用すると、資産のサブタイプを識別し、管理できます。サブタイプには、コンピュータ、プリンタ、ルーターなどのデバイス資産や、インベントリ内の Windows システム、Mac システム、Linux システムで動作するソフトウェア資産などがあります。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。

オプション	説明
	注: デフォルトのインストールでは、デバイス資産のプリンタデバイスには次の 2 つの資産サブタイプがあります。レーザープリンタ：カラー と レーザープリンタ：モノクロ：これらの各サブタイプは、ほとんどのプリンタに適用される一般的な一連のフィールドを提供します。また、これらの資産のサブタイプに基づいて、一般的な SNMP 対応プリンタモデル用の一連のプリンタテンプレートが付属しています。必要に応じて、これらのテンプレートを編集したり、新規追加したりすることができます。プリンタテンプレートをデバイスに適用するとき、次のインベントリサイクルで、トナーレベルや説明などテンプレートで定義されたデータがプリンタ用に収集されます。詳細については、「プリンタテンプレートについて」を参照してください。
接続タイプ	デバイスに接続してインベントリ情報を取得するために使用する接続方法。この場合はSSHです。
ポート	アプライアンスがデバイスへの接続に使用するポート番号。次のデフォルトポート番号（22）を使用する場合は入力する必要がありません。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。
sudoパスワード	デバイスに接続する権限を持つサービスユーザーアカウント名。サービスアカウントとsudoパスワードの使用は、デバイスへのアクセスにルート資格情報を使用することを避けたい場合に役に立ちます。しかし、デバイスによっては高い特権がある場合にもっと詳細なインベントリ情報を取得できる場合もあります。
オペレーティングシステム	デバイスのオペレーティングシステム。
シェル	接続時に使用するシェル。詳細については、「SSH接続のシェルサポート」を参照してください。
ログレベル	デバイスの詳細 ページに表示される情報のレベル。最も重要なメッセージのみを表示するには、**緊急** を選択します。すべてのメッセージを表示するには、**デバッグ** を選択します。
インベントリを有効にする	インベントリコレクションのオプション。このオプションを選択した場合、エージェント不要デバイスのインベントリスケジュールに従って、デバイスの

オプション	説明
	インベントリ情報が収集されます。このオプションをオフにすると、インベントリ情報は収集されません。しかし、どちらの場合も、エージェント不要デバイスはカウントされます。
DNSサーバ	デバイスのホスト名などの情報を識別する際に使用するDNSサーバーのホスト名。DNSサーバー情報を入力することで、更新時にそのデバイスを既存のインベントリ情報と一致させることができます。デバイスのホスト名またはIPアドレスが変更されたためにアプライアンスがデバイスを検出できない場合、インベントリが失敗します。
リレーデバイス	エージェント不要デバイスインベントリのリレーとして使用するデバイスの名前。 検出中にリレーとして使用されるリレーデバイスは、検出結果から新しいデバイスが自動的にプロビジョニングされるとき、エージェント不要インベントリに使用されます。検出スケジュールの詳細 ページでリレーデバイスを選択することができます。詳細については、「ネットワークの「何をどこで」高速スキャンを実行する検出スケジュールの追加」を参照してください。

- **デバイスでSNMP接続を設定するには、次の情報を入力します。**

オプション	説明
名前	デバイスのホスト名またはIPアドレス。
資産サブタイプ	資産のサブカテゴリ（該当する場合）。この情報を使用すると、資産のサブタイプを識別し、管理できます。サブタイプには、コンピュータ、プリンタ、ルーターなどのデバイス資産や、インベントリ内のWindows システム、Mac システム、Linux システムで動作するソフトウェア資産などがあります。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。

オプション	説明
	注: デフォルトのインストールでは、デバイス資産のプリンタデバイスには次の 2 つの資産サブタイプがあります。レーザープリンタ：カラー と レーザープリンタ：モノクロ：これらの各サブタイプは、ほとんどのプリンタに適用される一般的な一連のフィールドを提供します。また、これらの資産のサブタイプに基づいて、一般的な SNMP 対応プリンタモデル用の一連のプリンタテンプレートが付属しています。必要に応じて、これらのテンプレートを編集したり、新規追加したりすることができます。プリンタテンプレートをデバイスに適用するとき、次のインベントリサイクルで、トナーレベルや説明などテンプレートで定義されたデータがプリンタ用に収集されます。詳細については、「プリンタテンプレートについて」を参照してください。
接続タイプ	デバイスに接続してインベントリ情報を取得するために使用する接続方法。この場合はSNMPです。 SNMP（簡易ネットワーク管理プロトコル）は、ネットワーク上の管理対象デバイスを監視するためのプロトコルです。SNMPを有効化するには、ポート161がアプライアンスとデバイスで開いている必要があります。 SNMPスキャン結果には、すべてのSNMP対応デバイスが含まれます。リモートシェル拡張は、アプライアンスがデバイスに接続し、コマンドを実行し、インベントリとして管理可能な情報をキャプチャすることを可能にします。SNMP のオプションの詳細については、コンピューター以外の SNMP 対応デバイスの検出スケジュールの追加を参照してください。
SNMPバージョン	接続に使用するSNMPバージョン。SNMPv1およびSNMPv2cは、認証と暗号化を使用しません。 SNMP v3では認証アルゴリズムと暗号化アルゴリズムが使用され、SNMP通信のセキュリティ性が向上します。SNMP v3のオプションを設定すると、選択したデバイスでSNMP v3スキャンが実行されます。このスキャンが失敗すると、アプライアンスは、指定した**パブリック文字列**を使用してSNMP v1スキャンを試みます。
読み取りコミュニティ	（SNMP v1、SNMP v2c）照会するコミュニティ文字列です。デフォルトは「**Public**」です。認証が不要な場合のみ、パブリック文字列が必要です。認証が必要なとき、スキャンでは「SNMPを有効にする」と表示され、システムデータは返されません。
資格情報	SNMP v3を使用してデバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** をクリックして、まだ

オプション	説明
	リストにない資格情報を追加します。SNMPv1およびSNMPv2cでは、資格情報は必要ありません。 詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。
インベントリ設定	Brother レーザープリンタ など新しい SNMP エージェント不要デバイスの 1 つ以上のインベントリ設定。色、その他。
インベントリタイプ	インベントリ情報の収集に使用する方法。 • **インベントリ**: IPアドレス、MACアドレス、およびデバイス名などのデバイス情報のサブセットを収集します。 • **インベントリ/ウォーク**: SNMPの完全なウォークを実行してインベントリ情報を収集します。完全なウォーク結果は、デバイスの詳細 ページに表示されます。 **注:** SNMPのインベントリウォークは、Windowsデバイスで英語以外の文字をサポートしていません。英語以外の文字が出現すると、SNMPのインベントリプロセスでエラーが報告され、インベントリ情報のロードが中止されます。
ログレベル	デバイスの詳細 ページに表示される情報のレベル。最も重要なメッセージのみを表示するには、**緊急** を選択します。すべてのメッセージを表示するには、**デバッグ** を選択します。
インベントリを有効にする	インベントリコレクションのオプション。このオプションを選択した場合、エージェント不要デバイスのインベントリスケジュールに従って、デバイスのインベントリ情報が収集されます。このオプションをオフにすると、インベントリ情報は収集されません。しかし、どちらの場合も、エージェント不要デバイスはカウントされます。
DNSサーバ	デバイスのホスト名などの情報を識別する際に使用するDNSサーバーのホスト名。DNSサーバー情報を入力することで、更新時にそのデバイスを既存のインベントリ情報と一致させることができます。デバイスのホスト名またはIPアドレスが変更されたためにアプライアンスがデバイスを検出できない場合、インベントリが失敗します。
リレーデバイス	エージェント不要デバイスインベントリのリレーとして使用するデバイスの名前。 検出中にリレーとして使用されるリレーデバイスは、検出結果から新しいデバイスが自動的にプロビジョニングされるとき、エージェント不要インベントリに使用されます。検出スケジュールの詳細 ページでリレーデバイスを選択することができます。詳細については、「ネットワークの「何をどこで」高

オプション	説明
	速スキャンを実行する検出スケジュールの追加」を参照してください。

- **デバイスでWinRM接続を設定するには、次の情報を入力します。**

オプション	説明
名前	デバイスのホスト名またはIPアドレス。
資産サブタイプ	資産のサブカテゴリ（該当する場合）。この情報を使用すると、資産のサブタイプを識別し、管理できます。サブタイプには、コンピュータ、プリンタ、ルーターなどのデバイス資産や、インベントリ内の Windows システム、Mac システム、Linux システムで動作するソフトウェア資産などがあります。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。 **注:** デフォルトのインストールでは、デバイス資産のプリンタデバイスには次の 2 つの資産サブタイプがあります。レーザープリンタ：カラー と レーザープリンタ：モノクロ：これらの各サブタイプは、ほとんどのプリンタに適用される一般的な一連のフィールドを提供します。また、これらの資産のサブタイプに基づいて、一般的な SNMP 対応プリンタモデル用の一連のプリンタテンプレートが付属しています。必要に応じて、これらのテンプレートを編集したり、新規追加したりすることができます。プリンタテンプレートをデバイスに適用するとき、次のインベントリサイクルで、トナーレベルや説明などテンプレートで定義されたデータがプリンタ用に収集されます。詳細については、「プリンタテンプレートについて」を参照してください。
接続タイプ	Windowsデバイスに接続してインベントリ情報を取得するために使用する接続方法。この場合はWinRMです。
ポート	アプライアンスがデバイスへの接続に使用するポート番号。次のデフォルトポート番号を使用する場合は入力する必要がありません。5985 です。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。

オプション	説明
Kerberosが必要	選択した場合、認証にはKerberosが必要です。Kerberos を使用できない場合に、代替認証として NTLM は使用されません。 Kerberosを使用するには、同じ検出設定でDNS参照を有効にする必要があります。DNS サーバは、ローカルアプライアンスネットワーク設定でも必要になります。
ログレベル	デバイスの詳細 ページに表示される情報のレベル。最も重要なメッセージのみを表示するには、**緊急** を選択します。すべてのメッセージを表示するには、**デバッグ** を選択します。
インベントリを有効にする	インベントリコレクションのオプション。このオプションを選択した場合、エージェント不要デバイスのインベントリスケジュールに従って、デバイスのインベントリ情報が収集されます。このオプションをオフにすると、インベントリ情報は収集されません。しかし、どちらの場合も、エージェント不要デバイスはカウントされます。
DNSサーバ	デバイスのホスト名などの情報を識別する際に使用するDNSサーバーのホスト名。DNSサーバー情報を入力することで、更新時にそのデバイスを既存のインベントリ情報と一致させることができます。デバイスのホスト名またはIPアドレスが変更されたためにアプライアンスがデバイスを検出できない場合、インベントリが失敗します。
インベントリの Hyper-V または Virtual Machine Manager	アプライアンスがエージェント不要管理を使用して Microsoft Hyper-V または System Center Virtual Machine Manager インフラストラクチャをインポートできるようにするには、このオプションを選択します。この機能の詳細については、「Microsoft Hyper-V または System Center Virtual Machine Manager の検出スケジュールの追加」を参照してください。
リレーデバイス	エージェント不要デバイスインベントリのリレーとして使用するデバイスの名前。 検出中にリレーとして使用されるリレーデバイスは、検出結果から新しいデバイスが自動的にプロビジョニングされるとき、エージェント不要インベントリに使用されます。検出スケジュールの詳細 ページでリレーデバイスを選択することができます。詳細については、「ネットワークの「何をどこで」高速スキャンを実行する検出スケジュールの追加」を参照してください。

- **VMware®デバイスを設定するには、次の情報を入力します。**

オプション	説明
名前	ESXiホストまたはvCenterサーバーのホスト名またはIPアドレス。
資産サブタイプ	資産のサブカテゴリ（該当する場合）。この情報を使用すると、VMwareデバイスなどの資産のサブタイプを識別および管理することができます。例えば、ハイパーバイザー（ESXiホスト）です。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。
接続タイプ	VMwareデバイスに接続してインベントリ情報を取得するための接続に使用する接続方法。
VMwareタイプ	VMwareデバイスタイプです。**ESXi** または **vCenter サーバー** です。 **注:** vCenterサーバーデバイスは、デバイスライセンスの合計数にはカウントされません。これは、vCenterサーバーデバイスのインスタンスは、vCenterサーバー、ESXiホスト、およびそれらで実行中の仮想マシンの間の関係を確立するためにのみ使用されるためです。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。読み取り専用のアクセス権を持つアカウントを使用できます。詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。
ログレベル	デバイスの詳細 ページに表示される情報のレベル。最も重要なメッセージのみを表示するには、**緊急** を選択します。すべてのメッセージを表示するには、**デバッグ** を選択します。
インベントリを有効にする	インベントリコレクションのオプション。このオプションを選択した場合、エージェント不要デバイスのインベントリスケジュールに従って、デバイスのインベントリ情報が収集されます。このオプションをオフにすると、インベントリ情報は収集されません。しかし、どちらの場合も、エージェント不要デバイスはカウントされます。
DNSサーバ	デバイスのホスト名などの情報を識別する際に使用するDNSサーバーのホスト名。DNSサーバー情報を入力することで、更新時にそのデバイスを既存のインベントリ情報と一致させることができます。デバイスのホスト名またはIPアドレスが変更されたため

オプション	説明
	にアプライアンスがデバイスを検出できない場合、インベントリが失敗します。

4. **Test Connection**（テスト接続）をクリックします。

   接続ステータスが表示されます。
5. **保存** をクリックします。

   エージェント不要デバイスが追加されました。インベントリを有効にする を選択した場合、エージェント不要デバイスのインベントリスケジュールに従って、インベントリ情報が更新されます。詳細については、「管理対象デバイスでのインベントリデータ収集のスケジュール」を参照してください。

SSH 接続のシェルサポート

オペレーティングシステムは、アプライアンスと管理対象デバイスの間の SSH 接続に使用されるシェルのサポートという点で相違があります。

次の表は、各オペレーティングシステムで SSH 接続に利用可能なシェルを示しています。

オペレーティングシステム別の SSH 接続用シェルのサポート

オペレーティングシステム	デフォルトシェル	サポートされているシェル
CentOS	bash	bash、sh
Debian Linux	bash	bash、sh
Fedora	bash	bash、sh
FreeBSD	csh	bash、csh、sh
Mac OS X	sh	bash、sh
openSUSE/SLES???	bash	bash、sh
Oracle Enterprise Linux	bash	bash、sh
Red Hat?? Enterprise Linux??	bash	bash、sh
Ubuntu	bash	bash、sh

エージェント不要デバイス接続の詳細の編集またはエージェント不要デバイスの削除

必要に応じて、エージェント不要デバイスのデバイス接続の詳細を編集したり、エージェント不要デバイスを削除することができます。

1. デバイス リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。

2. 手動で入力されたエージェント不要デバイスの名前をクリックして、デバイスの詳細 ページを表示します。
3. 概要 セクション内の デバイスエントリタイプ 行で **編集** をクリックして、エージェント不要デバイス接続の詳細 ページを表示します。
4. 次のいずれかを実行します。
   - **必要に応じて接続の詳細を修正し、保存 をクリックします。詳細については、「デバイス情報の手動入力によるエージェント不要管理の有効化」を参照してください。**
   - **デバイスを削除するには、削除 をクリックします。**
   - **KACE Cloud Mobile Device Managed（MDM）に登録されているエージェント不要デバイスの場合、そのデバイスと KACE Cloud MDM の関連付けを削除し、エージェントのみのインベントリレコードに戻すには、エージェント不要統合の削除 をクリックします。**

インベントリに追加する特定の SNMP オブジェクトおよびコンピューター以外のデバイスを特定するための SNMP インベントリ設定の使用

ニーズに合わせてインベントリを展開または制限できるように、インベントリ設定する特定の SNMP（Simple Network Management Protocol）オブジェクトおよびコンピューター以外のデバイスを指定できます。また、アプライアンスでは、資産サブタイプを使用して、SNMP OID（オブジェクト識別子）をアプライアンスインベントリ表の特定のフィールドにマップできます。

重要: SNMP デバイスの場合、デバイスを設定するときに、適切な資産サブタイプを割り当てる必要があります。SNMP 資産サブタイプを設定後に追加または変更することはできません。

SNMP は、アプライアンスエージェント不要インベントリがインベントリのデータを抽出し、アプライアンスに統合するために使用できる方法の 1 つです。アプライアンスでは、RFC1213 MIB（Management Information Base）を主要なデータ収集層として使用します。これは、すべての SNMP 対応デバイスに固有のデータが含まれているためです。すべてのSNMP対応デバイスが、RFC1213データを公開します。詳細については、http://tools.ietf.org/html/rfc1213を参照してください。

アプライアンス SNMP インベントリ設定機能では、追加の OID セットを定義して、標準の RFC1213 データ範囲外のデータをインベントリ中に収集できます。これにより、使用しない場合は各デバイスから収集できるデータ量という点で制限される状態に対して拡張性と堅牢性を即座に実現できます。

関連トピック

資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について

管理者コンソールを使用したオブジェクト識別子（OID）のリストの取得

ベンダー提供の MIB（管理情報ベース）またはオブジェクトに関して一般的に利用可能な MIB がない場合は、アプライアンスを使用してオブジェクト識別子のリストを取得することにより、オブジェクトを調査できます。

OIDの追加セットを定義することにより、標準のRFC1213データ以外のデータをインベントリ時に収集できるようになり、各デバイスから収集できるデータの量を拡大できます。これらのOIDを見つけるには、別の場所で取

得したMIBに対してMIBブラウザを使用します。アプライアンスでは、デバイス検出またはデバイスインベントリを介して SNMP フルウォークを実行できます（これ以外の方法で MIB にアクセスできない場合）。

1. オブジェクトに対してSNMPフルウォークを実行します。
   - **検出スケジュールを使用してスキャンします。詳細については、「ネットワーク上のデバイスの検出」を参照してください。**
   - **インベントリデータ収集を使用してスキャンします。詳細については、「管理対象デバイスでのインベントリデータ収集のスケジュール」を参照してください。**
2. スキャン対象のオブジェクトの デバイスの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
   c. デバイス リストページで、オブジェクトの名前をクリックします。
3. インベントリ セクションの **SNMPデータ** をクリックして、フルウォークの結果を表示します。
4. 関連するOIDをリストから収集します。

OID をアプライアンスインベントリ表のフィールドにマップして、情報がインベントリに統合されるようにします。詳細については、「インベントリ表に存在するフィールドへのオブジェクト識別子のマップ」を参照してください。

インベントリ表に存在するフィールドへのオブジェクト識別子のマップ

資産サブタイプとして作成した特定のフィールドに SNMP OID（オブジェクト識別子）をマップできます。生成される SNMP インベントリ設定を使用することにより、コンピューター以外のデバイスからのデータを含むようにインベントリ情報を拡張できます。

- 関連するOIDが設定に含まれていることの確認が完了しています。
  - ベンダー提供のMIB（管理情報ベース）でMIBブラウザが使用されています。
  - ターゲットオブジェクト上で SNMP の完全なウォークがアプライアンスを使用して実行されており、オブジェクトの デバイスの詳細 ページの インベントリ情報 セクションにある **SNMP データ** に表示される OID が確認されています。詳細については、「ネットワーク上のデバイスの検出」を参照してください。
- インベントリで管理するコンピューター以外のデバイス用に適切な資産サブタイプを作成しました。詳細については、「資産サブタイプの追加と デバイスの詳細 ページの基本設定の選択」を参照してください。

SNMPインベントリ設定 リストページでは、新しいマッピングの作成または既存のマッピングの管理を行うツールを提供しています。

収集する OID データを指定した後で、デバイスの詳細 ページのカテゴリと同じカテゴリからデバイスのサブタイプを選択します。そのカテゴリのプロパティを選択すると、インベントリ表のフィールドにOIDがマップされます。次のスキャン後に、SNMPオブジェクトがデバイスインベントリに表示されます。

例えば、手動または検出スケジュールを介して追加されたプリンタがインベントリに存在する場合、SNMP インベントリ設定を使用して、プリンタのカートリッジインクレベルがアプライアンスに報告されるようにすることができます。この場合、Toner Level という名前のフィールドでデバイスのサブタイプとして作成した プリンタ を資産サブタイプに使用します。

1. SNMPインベントリ設定 リストページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**SNMPインベントリ設定** をクリックします。

2. **アクションの選択 > 新規作成** を選択します。
3. 名前 フィールドに設定の名前を入力します。

重要: SNMP デバイスの場合、デバイスを設定するときに、適切な資産サブタイプを割り当てる必要があります。SNMP デバイスサブタイプを設定後に追加または変更することはできません。

4. インベントリに設定するデバイスのタイプを識別する資産サブタイプを選択します。
5. OID をアプライアンスインベントリフィールドにマップするには、次の手順を実行します。
   a. 追加 ボタンをクリックします＋ をクリックします。

      見出しの下に新しい行が表示されます。

   b. オブジェクト識別子（ OID ）の下のテキストボックスにOIDを入力します。
   c. カテゴリ の下のドロップダウンリストからカテゴリを選択します。

      このカテゴリは、Asset Subtype Detail（ 資産サブタイプの詳細 ）ページで識別されたものと一致します。

   d. プロパティ の下のドロップダウンリストからプロパティを選択します。

      表示されるプロパティは、選択したサブタイプおよびカテゴリによって異なります。

   e. 行の最後で **保存** をクリックします。
6. 目的に応じて必要なだけのOIDをマップして、ページの左下にある **保存** をクリックします。

設定をオブジェクトに適用します。詳細については、「デバイスへのSNMPインベントリ設定の適用」を参照してください。

デバイスへのSNMPインベントリ設定の適用

SNMPインベントリ設定をデバイスに適用して、そのデバイスの次のスキャン時に追加データを収集できます。

設定の構成が完了しています。詳細については、「インベントリ表に存在するフィールドへのオブジェクト識別子のマップ」を参照してください。

注: SNMP インベントリ設定は、SNMP 管理対象エージェント不要デバイスにのみ適用できます。

1. デバイス ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、デバイス ページを表示します。
2. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
3. **アクションの選択 > SNMP設定の適用** を選択して、SNMP設定の適用 ダイアログを表示します。
4. 適用する設定を これらのSNMP設定を適用 ボックスにドラッグします。

   特定の設定を検索するには、名前を SNMP設定の検索 フィールドに入力します。
5. **SNMP設定の適用** をクリックします。

   設定が適用された後に、デバイス リストページが再び表示されます。

デバイスについての情報は、次の定期的にスケジュールされたレポート時間または強制的なインベントリ更新の後に表示されます。

関連トピック

管理対象デバイスでのインベントリデータ収集のスケジュール

インベントリ更新の強制実行

プリンタテンプレートについて

アプライアンスには、一般的な SNMP (簡易ネットワーク管理プロトコル) プリンタモデル用の一連のプリンタテンプレートも付属しています。必要に応じて、これらの SNMP 設定をプリンタデバイスに適用することができます。

SNMP インベントリ設定 リストページには、使用可能なプリンタテンプレートが表示されます。プリンタテンプレートをデバイスに適用するとき、次のインベントリサイクルで、トナーレベルや説明などテンプレートで定義されたデータがプリンタ用に収集されます。

デフォルトのインストールには、以下のレーザープリンタ用の一連のテンプレートが含まれており、モノクロおよびカラープリンタに対応するために、ブランドごとに 2 つのバリエーションがあります。Brother、Canon、HP、Lexmark、および Xerox.

必要に応じて、これらのテンプレートを編集または削除することができます。プリンタテンプレートを作成または編集するには、関連付けられた資産サブタイプとして存在するフィールドに関連する SNMP OID (オブジェクト識別子) が必要です。アプライアンスには、トナーレベルなどプリンタ固有のフィールドを取得する 2 つの資産サブタイプが付属しています。レーザープリンタ：カラー と レーザープリンタ：モノクロ：OID のマッピングの詳細については、「インベントリ表に存在するフィールドへのオブジェクト識別子のマップ」を参照してください。資産サブタイプの詳細について、および SNMP 設定との関連を確認するには、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。

管理者コンソールでの、または API を使用したデバイスの手動追加

管理者コンソール内で、またはインベントリ API (アプリケーションプログラミングインターフェイス) を使用して、デバイスをインベントリに手動で追加できます。

デバイスの手動追加は、デバイス情報を追跡したいものの、KACE エージェントをインストールしたり、エージェント不要管理を使用したりしてデバイスを管理することは希望しない場合に便利です。

手動で追加したデバイスのインベントリは、手動で更新またはアップロードする必要があります。手動追加のデバイスから、スケジュール済みのインベントリ更新がアプライアンスに配信されることはありません。

デバイスの管理について

デバイスの管理とは、ネットワーク上のデバイスに関する情報をアプライアンスを使用して収集し保持するプロセス、およびデバイスのステータス監視とレポート作成などのタスクを実行するプロセスのことです。

アプライアンスインベントリにデバイスを追加するには、次の手順を実行します。

- **デバイスに KACE エージェントをインストールします。**デバイスにエージェントがインストールされて、エージェントによってインベントリがアプライアンスにレポートされると、それらのデバイスが自動的にインベントリに追加されます。詳細については、「KACE エージェントのプロビジョニング」を参照してください。
- **デバイスでエージェント不要管理を有効にします。**エージェント不要管理は、サポート対象外のオペレーティングシステムを持つデバイスなど、デバイスに KACE エージェントをインストールできない場合に特に役立ちます。詳細については、「エージェント不要デバイスの管理」を参照してください。
- **デバイスのインベントリ情報を手動でアップロードします。**詳細については、「管理者コンソールでの、または API を使用したデバイスの手動追加」を参照してください。

注: 製品ライセンス契約に従い、管理対象コンピュータ、資産、監視対象サーバに分類された、指定された数のデバイスを管理できます。デバイスがMIA (未同期) となっている場合や既に使用されなくなった場合であっても、ライセンス数にカウントされます。手動で、またはAPIを通じてインベントリに追加されたデバイスは、ライセンス数にカウントされません。詳細については、「製品ライセンス情報の表示」を参照してください。

デバイスで使用可能な機能に関する情報は、「各デバイス管理方法で使用可能な機能」を参照してください。

インベントリ設定に対する変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

インベントリの変更履歴について

デバイスの変更履歴は、最初のレポート作成時に収集された情報に変更が加えられたときに初めて記録されます。

管理対象デバイスによってアプライアンスにインベントリが初めてレポートされたときに、その情報がベースラインレポートとして考慮されます。そのため、その情報は変更履歴に記録されません。

管理者コンソールを使用して手動でデバイスを追加

デバイスの詳細 ページでデバイス情報を入力して、アプライアンスインベントリにデバイスを手動で追加できます。

手動により追加されたレコードは、アプライアンスまたはエージェントからアクセスまたは変更できません。このため、手動により追加されたレコードのフィールドは、管理者が手動で行う場合のみ更新できます。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. **アクションを選択 > 新規作成 > 手動登録デバイス** を選択して、デバイスの詳細 ページを表示します。
3. 次のいずれかを実行します。
    - device.xmlのインポート **で、ファイルの選択 をクリックして、デバイスのインベントリ情報が含まれたXMLファイルを検索およびインポートします。Windowsに有効なXMLスキーマおよび管理者コンソールを使用した XML ファイルのアップロードを参照してください。**

      概要 セクションで、デバイスの 名前 を入力して、手順10にスキップします。
    - 概要 **セクションで、次の情報を入力します。**

アイテム	説明	データベースフィールド
システム名	デバイスのホスト名またはIPアドレス。	名前
システムの説明	デバイスの説明。	SYSTEM_DESCRIPTION
モデル	デバイスモデル。	CS_MODEL
シャーシタイプ	デバイスのタイプ（デスクトップ、ノートPCなど）。	CHASSIS_TYPE
IPアドレス	デバイスのIPアドレス。	IP

アイテム	説明	データベースフィールド
MAC	デバイスのメディアアクセス制御（MAC）アドレス番号。	MAC
OS 名	デバイスのオペレーティングシステム（Windows、Mac OS X、またはLinuxなど）。	OS_NAME
サービスパック	サービスパックのバージョン番号（Windowsのみ）。	SERVICE_PACK
デバイスのタイムゾーン	デバイスにインストールされている KACE エージェントは、このタイムゾーンを使用します。	TZ_AGENT
ユーザー	このデバイスに関連付けられているユーザー。	ユーザー
ドメイン	デバイスのドメイン。	CS_DOMAIN
メモ	任意の追加情報を入力します。	NOTES

4. ハードウェア セクションで、次の情報を入力します。

アイテム	説明	データベースフィールド
RAMの最大容量	使用可能なランダムアクセスメモリ（RAM）の最大容量。	RAM_MAX
RAMの合計	デバイス上のランダムアクセスメモリ（RAM）の合計容量。	RAM_TOTAL
使用中のRAM	デバイスで使用中のランダムアクセスメモリ（RAM）の容量。	RAM_USED
システム製造元	デバイスの製造元。	CS_MANUFACTURER
システムモデル	デバイスモデル。	CS_MODEL
サービスタグ	デバイスサービスの識別に使用される情報。	SERVICE_TAG
資産タグ	デバイスハードウェアの識別に使用される情報。	ASSET_TAG
マザーボードプライマリバス	メインのバス。	MOTHERBOARD_PRIMARY_BUS
マザーボードセカンダリバス	周辺のバス。	MOTHERBOARD_SECONDARY_BUS
アーキテクチャ	デバイスのオペレーティングシステムのアーキテクチャ（x86、x64など）。	SYS_ARCH

アイテム	説明	データベースフィールド
仮想デバイス	仮想デバイス（VMwareプラットフォームで実行されているデバイスなど）の識別に使用されます。物理デバイス（ノートPC、サーバーなど）には表示されません。	VIRTUAL
プロセッサ	CPUの数、タイプ、および製造元。	PROCESSORS
CD/DVDドライブ	デバイスにインストールされたCD-ROMおよびDVD-ROMドライブの設定。	CDROM_DEVICES
サウンドデバイス	デバイス上のオーディオデバイスに関する情報。	SOUND_DEVICES
モニタ	デバイスに接続されているモニタのタイプおよび製造元。仮想デバイスの場合、このフィールドは表示されません。	MONITOR
ビデオコントローラー	デバイス上のビデオコントローラーに関する情報。	VIDEO_CONTROLLERS
BIOS名	BIOS名。	BIOS_NAME
BIOSのリリース日	BIOSのバージョンがリリースされた日。	BIOS_RELEASE_DATE
BIOSバージョン	BIOSのバージョン。	BIOS_VERSION
BIOS製造元	BIOSの製造元。	BIOS_MANUFACTURER
BIOSの説明	BIOSの説明。	BIOS_DESCRIPTION
BIOSの識別コード	BIOSの識別コード。	BIOS_IDENTIFICATION_CODE
BIOSのシリアルナンバー	BIOSのシリアルナンバー。	BIOS_SERIAL_NUMBER

5. プリンタ セクションで、デバイスに関連するプリンタ情報を指定します。
6. エージェント セクションで、デバイスにインストールされた KACE エージェントのバージョン番号を指定します。
7. ユーザー セクションで、ユーザー情報を指定します。

アイテム	説明	データベースフィールド
ログに記録されたユーザー	デバイスに現在ログインしているユーザー。このエントリには、ユーザー名と、そのユーザーが属しているドメインが含まれます。	USER_LOGGED

アイテム	説明	データベースフィールド
ユーザーフルネーム	デバイスを所有しているユーザーのフルネーム。	USER_FULLNAME
ユーザードメイン	ユーザーが属しているドメイン。	USER_DOMAIN
最新のユーザー	前回デバイスにログインしたユーザーの名前。一部のデバイスは複数のユーザーが利用している場合があります。	ユーザー

8. オペレーティングシステム セクションで、デバイスにインストールされているオペレーティングシステムに関する情報を指定します。

アイテム	説明	データベースフィールド
オペレーティングシステムのバージョン	オペレーティングシステムのバージョン番号。	OS_VERSION
オペレーティングシステムのビルドのバージョン	オペレーティングシステムのビルド番号。	OS_BUILD
数値	オペレーティングシステムの番号。	OS_NUMBER
オペレーティングシステムのメジャーバージョン	オペレーティングシステムのメジャーバージョンを識別する番号。	OS_MAJOR
オペレーティングシステムのマイナーバージョン	オペレーティングシステムのマイナーバージョンを識別する番号。	OS_MINOR
マイナーバージョン (2)	追加のオペレーティングシステムのバージョン情報。	OS_MINOR2
Internet Explorerのバージョン	デバイスにインストールされているInternet Explorerのバージョン。	IE_VERSION
.NETのバージョン	デバイスにインストールされている.NETのバージョン。	DOT_NET_VERSIONS
オペレーティングシステムのアーキテクチャ	デバイスのオペレーティングシステムのアーキテクチャ (x86、x64 など) 。	OS_ARCH
オペレーティングシステム OS 名	デバイスのオペレーティングシステムの名前。	OS_NAME
Edge のバージョン	デバイスにインストールされている Microsoft Edge のバージョン。	EDGE_VERSION
ファミリ	オペレーティングシステムの製品ファミリ。	OS_FAMILY

アイテム	説明	データベースフィールド
サービスパック		
オペレーティングシステムのインストール日	オペレーティングシステムがインストールされた日付。	OS_INSTALLED_DATE
前回のスタートアップ	前回オペレーティングシステムがシャットダウンされた日時。	LAST_REBOOT
前回のシステムシャットダウン	前回オペレーティングシステムがシャットダウンされた日時。	LAST_SHUTDOWN
前回の再起動からの稼働時間	オペレーティングシステムの稼働時間。	LAST_REBOOT
ドメイン	デバイスのドメイン。	CS_DOMAIN
システムディレクトリ	システムディレクトリの場所。	SYSTEM_DIRECTORY
レジストリサイズ	レジストリのサイズ。	REGISTRY_SIZE
レジストリの最大サイズ	レジストリの最大サイズ。	REGISTRY_MAX_SIZE
WMIのステータス	Windows Management Instrumentation（WMI）サービスのステータス（Windowsデバイスのみ）。	WMI_STATUS

9. **保存** をクリックします。

   手動で追加したデバイスのアイコンが **デバイス** ページのデバイスの ステータス 列に表示されます  。
   手動で追加したデバイスのインベントリは、手動で更新する必要があります。

APIを使用したデバイスの手動追加

XML ファイルを作成し、そのファイルを API（アプリケーションプログラミングインターフェイス）を使用してアプライアンスにアップロードすることで、デバイスを手動でアプライアンスに追加することができます。この方法でデバイスを追加すると、セキュリティ上の理由から KACE エージェントを実行できないデバイスや、LAN（ローカルエリアネットワーク）に接続してインベントリをレポートできないデバイスにとって役立ちます。

このセクションのサンプルスクリプトを手本にしてXMLファイルを作成できます。

API を通じてインベントリに追加されたデバイスは、ライセンス制限にカウントされません。詳細については、「製品ライセンス情報の表示」を参照してください。

API を通じてアップロードされたアプリケーションインベントリは ソフトウェア ページには表示されますが、ソフトウェアカタログ ページには表示されません。詳細については、以下を参照してください。

- ソフトウェア ページでのアプリケーション管理
- ソフトウェアカタログインベントリの管理

注: インベントリAPIは、アプライアンスの設定に応じて、HTTP通信およびHTTPS通信をサポートします。インベントリ情報をアップロードするには、以下のURLを使用します。http://**appliance_hostname**/service/wsapi.php。ここで、**appliance_hostname** は、アプライアンスのホスト名です。

APIを使用したインベントリ情報の送信

APIを使用してインベントリを送信するには、最初にインベントリ情報が含まれるXMLファイルを生成する必要があります。

例については、次を参照してください。

- Windowsに有効なXMLスキーマ
- WindowsデバイスでのXMLスキーマの使用例
- LinuxおよびMacデバイスに有効なXMLスキーマ

必要なコンテンツが含まれているXMLファイルを生成したら、APIを使用してインベントリを送信できます。

1. （必須）セッションキーを要求します。

   要求を送信する際、本文に「keyreq=true」を含めると、応答でセッション文字列が返されます。

2. （必須）認証トークンを構成します。
   a. 次のようなauth文字列を構成します。

   session_string + '|' + MD5 of API password

   b. auth文字列でMD5を実行します。
3. （新しいデバイスの場合に必須）デバイスのUUIDを要求します。

   要求を送信する際、本文に「req=newuuid&key=$auth」を含めると、応答で UUID が返されます。

4. （必須）インベントリXMLデータを送信します。

   要求を送信する際、本文のGET行とインベントリXMLに「req=loadxml&key=$auth&KUID=$uuid&version=6.0」を含めます。

   詳細については、「サンプルPerlスクリプト」を参照してください。

サンプルPerlスクリプト

Perlスクリプトを使用して、デバイスのインベントリ情報が含まれたXMLファイルをアプライアンスにアップロードできます。

以下は、ユーザーによって作成された XML ファイルをアプライアンスにアップロードするサンプル Perl スクリプトです。このスクリプトの使用については、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。

```
#!/usr/bin/perl
use strict;
use warnings;
use WWW::Curl::Easy;
use XML::Simple;
use Data::Dumper;
use Digest::MD5 qw(md5 md5_hex md5_base64);
   # Curl出力ハンドラ ...
   my $response;
   sub write_data($$$$) {
      $response = shift;
      return length($response);
   }
   # ----------------------------------------------------
   #アプライアンス設定 ...
   # ----------------------------------------------------
```

```
my $password = "xxx"; # password set in Settings -> Security Settings
my $host = "hostname";       # hostname or IP address here
my $http = "https";        # HTTP or HTTPS
# ------------------------------------------------------------
# XMLパッケージの構築 ...
# ------------------------------------------------------------
my $simple = new XML::Simple(keeproot => 1, forcearray => 1);
my $data = $simple->XMLin("machine.xml");
my $uuid = $data->{MachineStruct}->[0]->{MAC}->[0];
# ------------------------------------------------------------
# CURLスタッフの設定 ...
# ------------------------------------------------------------
my $url = "$http://$host/service/wsapi.php";
my $ch = WWW::Curl::Easy->new;
$ch->setopt(CURLOPT_URL, $url);  # set url to post to
$ch->setopt(CURLOPT_SSL_VERIFYPEER, 0);  # ok for self-signed ca
$ch->setopt(CURLOPT_VERBOSE, 0);
$ch->setopt(CURLOPT_WRITEFUNCTION, \&write_data); # return into a variable
$ch->setopt(CURLOPT_HEADER, 0);
$ch->setopt(CURLOPT_TIMEOUT, 40);  # times out after 4s
$ch->setopt(CURLOPT_POST, 1);
$ch->setopt(CURLOPT_COOKIEFILE, '/tmp/cookiefile.txt');
# ------------------------------------------------------------
#手順 1 - アプライアンスからのセッションの要求 ...
# ------------------------------------------------------------
$ch->setopt(CURLOPT_POSTFIELDS, "keyreq=true"); # add POST fields
my $out = $ch->perform;
if ( $out != 0 ) {
        die ("Error: $out " .
        $ch->strerror($out).
        " " .
        $ch->errbuf."\n");
}
my $sess = $response;
# ------------------------------------------------------------
#手順2 - 認証トークンの構築...
# ------------------------------------------------------------
my $auth = md5_hex("$sess|".md5_hex($password));
# ------------------------------------------------------------
#手順 3 - アプライアンスのからの新規 UUID の要求（ 新しいデバイスレコードを
#        作成する場合。 既存のデバイスを編集する場合は、
#        XMLでUUIDが設定されていることを要確認 ）...
# ------------------------------------------------------------
if ( 1 ) {
        print "Using UUID From XML File: $uuid\n";
} else {
        $ch->setopt(CURLOPT_POSTFIELDS,"req=newuuid&key=$auth");
        $out = $ch->perform;
        if ( $out != 0 ) {
             die ("Error: $out " .
                  $ch->strerror($out).
                  " " .
                  $ch->errbuf."\n");
        }
        $uuid = $response;
        $data->{MachineStruct}->[0]->{MAC}->[0] = $uuid;
        $data->{MachineStruct}->[0]->{NAME}->[0] = "WSAPI-" .$uuid;
        print "Created New UUID: $uuid\n";
        }
#シンプルなXMLハッシュをXML文字列に変換 ...
```

```
my $xml = $simple->XMLout(
        $data,
        KeepRoot => 1,
        NoAttr => 1,
);
# -----------------------------------------------------
#手順 4 - アプライアンスへの XML の送信 ...
# -----------------------------------------------------
my @curlHeader = ("Content-Type: text/xml");
$url = "$http://$host/service/wsapi.php?req=loadxml&key=$auth&KUID=$uuid&version=6.0";
$ch->setopt(CURLOPT_URL, $url); # set url to post to
$ch->setopt(CURLOPT_HTTPHEADER, \@curlHeader);
$ch->setopt(CURLOPT_POSTFIELDS, $xml);
$out = $ch->perform;
if ( $out != 0 ) {
        die ("Error: $out " .$ch->strerror($out)." " .$ch->errbuf."\n");
}
print "Loaded $uuid to the appliance ($host)\n";
```

Windowsに有効なXMLスキーマ

Windowsデバイスのインベントリ情報のアップロードに使用されるファイルは、有効なXMLスキーマに従っている必要があります。

以下は、Windowsデバイスに有効なXMLスキーマの例です。

```
<?xml version="1.0" encoding="utf-8"?>
<MachineStruct xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="">
  http://www.w3.org/2001/XMLSchema-instance"
<NAME>@@__m_computerSystemName__@@</NAME>
<IP>@@__m_IPAddress__@@</IP>
<MAC>@@__m_versionKaceId__@@</MAC>
<OS_NAME>@@__m_operatingSystemCaption__@@</OS_NAME>
<OS_NUMBER>@@__m_operatingSystemVersion__@@</OS_NUMBER>
<OS_MAJOR>@@__m_operatingSystemVersionMajor__@@</OS_MAJOR>
<OS_MINOR>@@__m_operatingSystemVersionMinor__@@</OS_MINOR>
<SERVICE_PACK>@@__m_operatingSystemCsdVersion__@@</SERVICE_PACK>
<USER>@@__m_userAccountName__@@</USER>
<USER_FULLNAME>@@__m_userAccountFullName__@@</USER_FULLNAME>
<DOMAIN>@@__m_computerSystemDomain__@@</DOMAIN>
<OS_VERSION>@@__m_operatingSystemVersion__@@</OS_VERSION>
<OS_BUILD>@@__m_operatingSystemBuildNumber__@@</OS_BUILD>
<OS_INSTALLED_DATE>@@__m_operatingSystemInstallDate__@@</OS_INSTALLED_DATE>
<LAST_REBOOT>@@__m_operatingSystemLastBootupTime__@@</LAST_REBOOT>
<LAST_SHUTDOWN>@@__m_operatingSystemLastBootupTime__@@</LAST_SHUTDOWN>
<UPTIME>@@__m_operatingSystemUptime__@@</UPTIME>
<SYSTEM_DIRECTORY>@@__m_operatingSystemWindowsDirectory__@@</SYSTEM_DIRECTORY>
<SYSTEM_DESCRIPTION>@@__m_operatingSystemDescription__@@</SYSTEM_DESCRIPTION>
<RAM_TOTAL>@@__m_physicalMemoryTotalSize__@@</RAM_TOTAL>
<RAM_USED>@@__m_operatingSystemUsedPhysicalMemory__@@</RAM_USED>
<CS_MANUFACTURER>@@__m_computerSystemManufacturer__@@</CS_MANUFACTURER>
<CS_MODEL>@@__m_computerSystemModel__@@</CS_MODEL>
<CHASSIS_TYPE>@@__m_systemEnclosureChassisType__@@</CHASSIS_TYPE>
<TZ_AGENT>@@__m_versionTimeZone__@@</TZ_AGENT>
<USER_LOGGED>@@__m_computerSystemUserName__@@</USER_LOGGED>
<CS_DOMAIN>@@__m_computerSystemDomain__@@</CS_DOMAIN>
<USER_NAME>@@__m_userAccountName__@@</USER_NAME>
<USER_DOMAIN>@@__m_userAccountDomain__@@</USER_DOMAIN>
<BIOS_NAME>@@__m_biosName__@@</BIOS_NAME>
<BIOS_VERSION>@@__m_biosVersion__@@</BIOS_VERSION>
<BIOS_MANUFACTURER>@@__m_biosManufacturer__@@</BIOS_MANUFACTURER>
```

```
<BIOS_DESCRIPTION>@@__m_biosDescription__@@</BIOS_DESCRIPTION>
<BIOS_SERIAL_NUMBER>@@__m_biosSerialNumber__@@</BIOS_SERIAL_NUMBER>
<MOTHERBOARD_PRIMARY_BUS>@@__m_motherboardDevicePrimaryBusType__@@
 </MOTHERBOARD_PRIMARY_BUS>
<MOTHERBOARD_SECONDARY_BUS>@@__m_motherboardDeviceSecondaryBusType__@@
 </MOTHERBOARD_SECONDARY_BUS>
<PROCESSORS>CPU Chip Count: @@__m_processorCount__@@
CPU Core Count: @@__m_processorCoreCount__@@
@@__m_processorList__@@ </PROCESSORS>
<SOUND_DEVICES>@@__m_soundDeviceDescription__@@</SOUND_DEVICES>
<CDROM_DEVICES>@@__m_CDROMDeviceName__@@</CDROM_DEVICES>
<VIDEO_CONTROLLERS>@@__m_videoControllerName__@@</VIDEO_CONTROLLERS>
<REGISTRY_SIZE>@@__m_registryCurrentSize__@@</REGISTRY_SIZE>
<REGISTRY_MAX_SIZE>@@__m_registryMaximumSize__@@</REGISTRY_MAX_SIZE>
<DISK_DRIVES>
@@__m_logicalDiskDriveList__@@ </DISK_DRIVES>
<NETWORK_INTERFACES>
@@__m_networkAdapterConfigurationList__@@ </NETWORK_INTERFACES>
<PRINTERS>@@__m_printerList__@@</PRINTERS>
<STARTUP_PROGRAMS>
@@__m_startupProgramsList__@@ </STARTUP_PROGRAMS>
<PROCESSES>
@@__m_processList__@@ </PROCESSES>
<NT_SERVICES>
@@__m_servicesList__@@ </NT_SERVICES>
<INSTALLED_software>
@@__m_installedProgramsList__@@ </INSTALLED_software>
<CLIENT_VERSION>@@__m_appVersion__@@</CLIENT_VERSION>
</MachineStruct>
```

Windowsデバイスでの XMLスキーマの使用例

Windowsデバイスの有効なXMLスキーマに適合するファイル例を表示できます。

以下は、Windowsに有効なXMLスキーマに示されているスキーマを使用した有効な XML の例です。

```
<?xml version="1.0" encoding="utf-8"?>
<MachineStruct xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <NAME>TestComputer</NAME>
  <IP>10.10.10.10</IP>
  <MAC>F1234567-C2D2-4055-85BB-294E6A3D22D9</MAC>
  <OS_NAME>Microsoft Windows 7 Professional</OS_NAME>
  <OS_NUMBER>6.1.7601.17514</OS_NUMBER>
  <OS_MAJOR>6</OS_MAJOR>
  <OS_MINOR>1</OS_MINOR>
  <SERVICE_PACK>Service Pack 1</SERVICE_PACK>
  <USER>Administrator</USER>
  <USER_FULLNAME>Tom Silver</USER_FULLNAME>
  <DOMAIN>WORK</DOMAIN>
  <OS_VERSION>6.1.7601</OS_VERSION>
  <OS_BUILD>17514</OS_BUILD>
  <OS_INSTALLED_DATE>2017-08-30 14:22:39 -0400</OS_INSTALLED_DATE>
  <LAST_REBOOT>2017-08-30 14:25:05 -0400</LAST_REBOOT>
  <LAST_SHUTDOWN>2017-08-30 14:25:05 -0400</LAST_SHUTDOWN>
  <UPTIME>4 days </UPTIME>
  <SYSTEM_DIRECTORY>C:\WINDOWS</SYSTEM_DIRECTORY>
  <SYSTEM_DESCRIPTION>Windows 7 Machine</SYSTEM_DESCRIPTION>
  <RAM_TOTAL>512.00MB</RAM_TOTAL>
  <RAM_USED>180MB</RAM_USED>
  <CS_MANUFACTURER>VMware, Inc.</CS_MANUFACTURER>
```

```
  <CS_MODEL>VMware Virtual Platform</CS_MODEL>
  <CHASSIS_TYPE>Other</CHASSIS_TYPE>
  <USER_LOGGED>Tom</USER_LOGGED>
  <CS_DOMAIN>WORK</CS_DOMAIN>
  <USER_NAME>Administrator</USER_NAME>
  <USER_DOMAIN>Work</USER_DOMAIN>
  <BIOS_NAME>PhoenixBIOS 4.0 Release 5.5     </BIOS_NAME>
  <BIOS_VERSION>INTEL  - 6040000</BIOS_VERSION>
  <BIOS_MANUFACTURER>Phoenix Technologies LTD</BIOS_MANUFACTURER>
  <BIOS_DESCRIPTION>PhoenixBIOS 4.0 Release 5.5  </BIOS_DESCRIPTION>
  <BIOS_SERIAL_NUMBER>VMware-56 4d bd d3 5e 4f a5 4e-6a ce a0 d3 39 bd ae 02
    </BIOS_SERIAL_NUMBER>
  <MOTHERBOARD_PRIMARY_BUS>PCI</MOTHERBOARD_PRIMARY_BUS>
  <MOTHERBOARD_SECONDARY_BUS>ISA</MOTHERBOARD_SECONDARY_BUS>
  <PROCESSORS>CPU Chip Count: 1
CPU Core Count: 0
CPU0: Intel Celeron processor (0 cores)  </PROCESSORS>
  <SOUND_DEVICES>Creative AudioPCI (ES1371,ES1373) (WDM)
</SOUND_DEVICES>
  <CDROM_DEVICES>TSSTcorp DVD+-RW TS-U633F
</CDROM_DEVICES>
  <VIDEO_CONTROLLERS>VMware SVGA II
</VIDEO_CONTROLLERS>
  <REGISTRY_SIZE>1MB</REGISTRY_SIZE>
  <REGISTRY_MAX_SIZE>86MB</REGISTRY_MAX_SIZE>
  <DISK_DRIVES>
    <DiskDrive>
      <NAME>Drive C: (Physical Disk) FileSystem: NTFS Used: 2.08GB Total: 39.99GB</NAME>
      <DISK_SIZE>39.9906</DISK_SIZE>
      <DISK_USED>2.07966</DISK_USED>
      <DISK_FREE>37.9109</DISK_FREE>
      <PERCENT_USED>5.2</PERCENT_USED>
    </DiskDrive>
  </DISK_DRIVES>
  <NETWORK_INTERFACES>
    <NetworkInterface>
      <NIC>AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler
Miniport</NIC>
      <MAC>00:0C:29:BD:AE:03</MAC>
      <IP>192.168.220.132</IP>
      <DHCP_ENABLED>True</DHCP_ENABLED>
    </NetworkInterface>
  </NETWORK_INTERFACES>
  <PRINTERS></PRINTERS>
  <STARTUP_PROGRAMS>
    <StartupProgram>
      <NAME>desktop</NAME>
    </StartupProgram>
    <StartupProgram>
      <NAME>VMware Tools</NAME>
      <COMMAND_EXE>C:\Program Files\VMware\VMware Tools\VMwareTray.exe</COMMAND_EXE>
      <COMMAND_ARGS />
      <FILE_INFO>
        <FILE_NAME>VMwareTray.exe</FILE_NAME>
        <FILE_DESCRIPTION>VMware Tools tray application</FILE_DESCRIPTION>
        <FILE_VERSION>8.4.6.16648</FILE_VERSION>
        <PRODUCT_NAME>VMware Tools</PRODUCT_NAME>
        <PRODUCT_VERSION>8.4.6 build-385536</PRODUCT_VERSION>
        <COMPANY_NAME>VMware, Inc.</COMPANY_NAME>
      </FILE_INFO>
```

```
  </StartupProgram>
  <StartupProgram>
    <NAME>VMware User Process</NAME>
    <COMMAND_EXE>C:\Program Files\VMware\VMware Tools\VMwareUser.exe</COMMAND_EXE>
    <COMMAND_ARGS />
    <FILE_INFO>
      <FILE_NAME>VMwareUser.exe</FILE_NAME>
      <FILE_DESCRIPTION>VMware Tools Service</FILE_DESCRIPTION>
      <FILE_VERSION>8.4.6.16648</FILE_VERSION>
      <PRODUCT_NAME>VMware Tools</PRODUCT_NAME>
      <PRODUCT_VERSION>8.4.6 build-385536</PRODUCT_VERSION>
      <COMPANY_NAME>VMware, Inc.</COMPANY_NAME>
    </FILE_INFO>
  </StartupProgram>
</STARTUP_PROGRAMS>
<PROCESSES>
  <MachineProcess>
    <NAME>konea.exe</NAME>
    <COMMAND_EXE>C:\Program Files (x86)\Quest\KACE\konea.exe</COMMAND_EXE>
    <COMMAND_ARGS/>
    <FILE_INFO>
      <FILE_NAME>konea.exe</FILE_NAME>
      <FILE_DESCRIPTION>konea</FILE_DESCRIPTION>
      <FILE_VERSION>255.239.6</FILE_VERSION>
      <PRODUCT_NAME>KACE Agent</PRODUCT_NAME>
      <PRODUCT_VERSION>255.239.6</PRODUCT_VERSION>
      <COMPANY_NAME>Quest Software Inc.</COMPANY_NAME>
    </FILE_INFO>
  </MachineProcess>
</PROCESSES>
<NT_SERVICES>
  <NtService>
    <NAME>Alerter</NAME>
    <DISPLAY_NAME>Alerter</DISPLAY_NAME>
    <STATUS>SERVICE_STOPPED</STATUS>
    <STARTUP_TYPE>SERVICE_DISABLED</STARTUP_TYPE>
    <DESCRIPTION />
    <LOGON_AS_USER>NT AUTHORITY\LocalService</LOGON_AS_USER>
    <CAN_INTERACT_WITH_DESKTOP>False</CAN_INTERACT_WITH_DESKTOP>
    <COMMAND_EXE>C:\WINDOWS\system32\svchost.exe</COMMAND_EXE>
    <COMMAND_ARGS> -k LocalService</COMMAND_ARGS>
    <FILE_INFO>
      <FILE_NAME>svchost.exe</FILE_NAME>
      <FILE_DESCRIPTION>Generic Host Process for Win32 Services</FILE_DESCRIPTION>
      <FILE_VERSION>6.1.7600.16385 (win7_rtm.090713-1255)</FILE_VERSION>
      <PRODUCT_NAME>Microsoft?? Windows?? Operating System</PRODUCT_NAME>
      <PRODUCT_VERSION>6.1.7600.16385</PRODUCT_VERSION>
      <COMPANY_NAME>Microsoft Corporation</COMPANY_NAME>
    </FILE_INFO>
  </NtService>
</NT_SERVICES>
<INSTALLED_software>
  <software>
    <DISPLAY_VERSION>5.2.38916</DISPLAY_VERSION>
    <HELP_LINK />
    <README />
    <INSTALL_DATE>20170830</INSTALL_DATE>
    <PUBLISHER>Quest Software Inc.</PUBLISHER>
    <UNINSTALL_STRING />
    <URLINFO_ABOUT />
```

```
    <DISPLAY_NAME>Quest KACE Agent</DISPLAY_NAME>
  </software>
 </INSTALLED_software>
 <CLIENT_VERSION>8.0.xxxxx</CLIENT_VERSION>
</MachineStruct>
```

LinuxおよびMacデバイスに有効なXMLスキーマ

LinuxおよびMacデバイスのインベントリ情報のアップロードに使用されるファイルは、有効なXMLスキーマを使用する必要があります。

以下は、LinuxおよびMacデバイス向けのXMLスキーマの例です。

```
<?xml version="1.0" encoding="utf-8"?>
        <MachineStruct>
            <NAME>@@__m_versionHostName__@@</NAME>
            <CLIENT_VERSION>@@__m_appVersion__@@</CLIENT_VERSION>
            <IP>@@__m_IPAddress__@@</IP>
            <MAC>@@__m_versionKaceId__@@</MAC>
            <OS_NAME>@@__m_operatingSystemCaption__@@</OS_NAME>
            <OS_NUMBER>@@__m_operatingSystemVersion__@@</OS_NUMBER>
            <OS_MAJOR>@@__m_operatingSystemVersionMajor__@@</OS_MAJOR>
            <OS_MINOR>@@__m_operatingSystemVersionMinor__@@</OS_MINOR>
            <SERVICE_PACK></SERVICE_PACK>
            <INSTALL_DATE></INSTALL_DATE>
 <OS_ARCH>@@__m_operatingSystemOSArchitecture__@@</OS_ARCH>
            <OS_FAMILY>@@__m_operatingSystemOSFamily__@@</OS_FAMILY>
            <OS_VERSION>@@__m_operatingSystemVersion__@@</OS_VERSION>
            <OS_BUILD>@@__m_operatingSystemBuildNumber__@@</OS_BUILD>
            <DOMAIN>@@__m_userAccountDomain__@@</DOMAIN>
            <CS_DOMAIN>@@__m_userAccountDomain__@@</CS_DOMAIN>
 <LAST_REBOOT>@@__m_operatingSystemLastBootupTime__@@</LAST_REBOOT>
            <TZ_AGENT>@@__m_versionTimeZone__@@</TZ_AGENT>
            <UPTIME>@@__m_operatingSystemUptime__@@</UPTIME>
 <RAM_TOTAL>@@__m_operatingSystemTotalVisibleMemorySize__@@</RAM_TOTAL>
 <RAM_USED>@@__m_operatingSystemUsedPhysicalMemory__@@</RAM_USED>
            <CS_MANUFACTURER>@@__m_biosManufacturer__@@</CS_MANUFACTURER>
            <CS_MODEL></CS_MODEL>
            <USER_LOGGED>@@__m_userAccountName__@@</USER_LOGGED>
            <USER>@@__m_userAccountName__@@</USER>
            <USER_NAME>@@__m_userAccountName__@@</USER_NAME>
            <USER_FULLNAME>@@__m_userAccountFullName__@@</USER_FULLNAME>
            <USER_DOMAIN>@@__m_userAccountDomain__@@</USER_DOMAIN>
            <BIOS_NAME>@@__m_biosName__@@</BIOS_NAME>
            <BIOS_VERSION>@@__m_biosVersion__@@</BIOS_VERSION>
            <BIOS_MANUFACTURER>@@__m_biosManufacturer__@@</BIOS_MANUFACTURER>
            <BIOS_DESCRIPTION>@@__m_biosName__@@</BIOS_DESCRIPTION>
    <BIOS_SERIAL_NUMBER>@@__m_biosSerialNumber__@@</BIOS_SERIAL_NUMBER>
            <MOTHERBOARD_PRIMARY_BUS></MOTHERBOARD_PRIMARY_BUS>
            <MOTHERBOARD_SECONDARY_BUS></MOTHERBOARD_SECONDARY_BUS>
            <PROCESSORS>@@__m_processorList__@@</PROCESSORS>
            <SOUND_DEVICES>@@__m_soundDeviceDescription__@@</SOUND_DEVICES>
            <CDROM_DEVICES>@@__m_CDROMDeviceName__@@</CDROM_DEVICES>
            <MONITOR>@@__m_desktopMonitorDescription__@@</MONITOR>
 <VIDEO_CONTROLLERS>@@__m_videoControllerName__@@</VIDEO_CONTROLLERS>
            <DISK_DRIVES>
@@__m_logicalDiskDriveList__@@</DISK_DRIVES>
   <NETWORK_INTERFACES>
@@__m_networkAdapterConfigurationList__@@</NETWORK_INTERFACES>
    <PRINTERS>@@__m_printerList__@@</PRINTERS>
    <STARTUP_PROGRAMS>
```

```
@@__m_startupProgramsList__@@</STARTUP_PROGRAMS>
    <PROCESSES>
@@__m_processList__@@</PROCESSES>
    <INSTALLED_software>
@@__m_installedProgramsList__@@</INSTALLED_software>
  </MachineStruct>
```

管理者コンソールを使用した XML ファイルのアップロード

管理者コンソールを使用して、デバイスのインベントリ情報が含まれた XML ファイルをアップロードできます。このタイプの情報は、手動インベントリ情報と呼ばれます。

KACE エージェントが、インベントリ情報が追加されたデバイスにインストールされています。

インベントリに追加されるデバイスで XML ファイルを作成し、アプライアンスに移動してこのファイルをアップロードします。

手動インベントリ情報は ソフトウェア ページに表示されますが、ソフトウェアカタログ ページには表示されません。詳細については、以下を参照してください。

- ソフトウェア ページでのアプリケーション管理
- ソフトウェアカタログインベントリの管理

1. 情報が含まれるXMLファイルを生成します。
    a. KACE エージェントがインストールされているデバイス上で、コマンドプロンプトまたはターミナルウィンドウを開きます。
    b. Quest KACEのインストールディレクトリに移動します。

    例：

    - Windows 32ビットシステム：C:\Program Files\Quest\KACE
    - Windows 64ビットシステム：C:\Program Files (x86)\Quest\KACE
    - Mac OS Xシステム：/Library/Application Support/Quest/KACE/bin
    - Linuxシステム：/opt/quest/kace/bin

    c. 次のコマンドを入力します:

    KInventory -machine -output **filename**

    ここでの**filename**は、作成するXMLファイルへのパスです。パスにスペースが含まれる場合は、二重引用符でパス全体を囲みます。

    エージェントでインベントリデータが収集され、XMLファイルが生成されます。
2. アプライアンスの管理者コンソールで、デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
3. **アクションの選択 > 新規作成 > 手動登録デバイス** を選択して、デバイスの詳細 ページを表示します。
4. Import Device（ デバイスのインポート ）で、**参照** をクリックします。
5. ファイルを選択し、**開く** または **選択** をクリックします。
6. **保存** をクリックします。

デバイスの情報がインベントリに追加されます。XMLファイルをアップロードした場合、アプライアンスによりページ上の他のすべての情報が無視され、インベントリ情報にXMLファイルが使用されます。

インベントリ更新の強制実行

定期的にスケジュールされたレポート時間とは別に、管理対象デバイスでインベントリ情報を強制的に更新することができます。

インベントリ更新を強制的に実行するには、以下の条件の1つが満たされている必要があります。

- KACE エージェントがデバイスにインストールされており、アプライアンスとデバイス間にアクティブなメッセージプロトコル接続が確立している。
- エージェント不要管理がデバイスで有効化されている。

エージェント管理対象デバイスまたはエージェント不要管理デバイスのいずれでもないデバイスでは、更新を強制的に実行することはできません。

選択したデバイスに関連付けられている管理対象インストールは、指定したソフトウェアパッケージがソフトウェアカタログに含まれているかソフトウェアリストに含まれているかにかかわらず、常に順番に展開されます。

アプライアンスでのインベントリ更新の強制実行

アプライアンスの**管理者コンソール**を使用して、デバイスでのインベントリのレポートを強制的に実行できます。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. インベントリを更新するデバイスの隣のチェックボックスをオンにします。

    アプライアンスに過度の負荷がかからないようにするには、一度に更新するデバイスの数を50台未満にします。
3. **アクションの選択 > 強制的なインベントリ更新** を選択します。

インベントリ情報が更新されます。

Windowsデバイスでのインベントリ更新の強制実行

Windowsデバイスでコマンドを実行して、これらのデバイスでのインベントリのレポートを強制的に実行できます。

1. Windowsデバイスにログインし、コマンドプロンプトを開きます。
2. 以下のいずれかのディレクトリに移動します。
    - 32ビットシステムの場合：C:\Program Files\Quest\KACE\
    - 64ビットシステムの場合：C:\Program Files (x86)\Quest\KACE\

    注: Windows Vista以降では、コマンドを実行する際、「管理者として実行」を使用します。
3. 次のコマンドを入力します:

    runkbot 4 0

インベントリ情報が更新されます。

Mac OS Xデバイスでのインベントリ更新の強制実行

Mac OS Xデバイスでコマンドを実行して、これらのデバイスでインベントリのレポートを強制的に実行できます。

1. Mac OS X デバイスにログインし、**アプリケーション > ユーティリティ** からターミナルを開きます。
2. 以下のディレクトリに移動します。

   /Library/Application Support/Quest/KACE/bin/
3. 次のコマンドを入力します:

   sudo ./runkbot 2 0

インベントリ情報が更新されます。

Linuxデバイスでのインベントリ更新の強制実行

Linuxデバイスでコマンドを実行して、これらのデバイスでインベントリのレポートを強制的に実行できます。

1. Linux デバイスにログインし、**アプリケーション > システムツール** からターミナルを開きます。
2. 以下のディレクトリに移動します。

   /opt/quest/kace/bin/
3. 次のコマンドを入力します:

   sudo ./runkbot 2 0

インベントリ情報が更新されます。

MIAデバイスの管理

管理下に置かれているが、過去1〜90日以内にアプライアンスと通信していないデバイスは、MIA（未同期）または接続不能とみなされます。必要に応じて、MIAデバイスの設定項目を指定し、MIAデバイスを管理できます。

注: 製品ライセンス契約に従い、管理対象コンピュータ、監視対象デバイス、および資産に分類された、指定された数のデバイスを管理できます。デバイスがMIA（未同期）となっている場合や既に使用されなくなった場合であっても、ライセンス数にカウントされます。手動で、またはAPIを通じてインベントリに追加されたデバイスは、ライセンス数にカウントされません。詳細については、「製品ライセンス情報の表示」を参照してください。

注: ライセンスの上限を増やす方法については、次のQuestのウェブサイトを参照してください：https://quest.com/buy.

MIA設定項目の設定

MIAデバイスが指定された日数の間にチェックインしなかった場合、MIAデバイスが自動的にインベントリから削除されるようにアプライアンスを設定できます。MIAデバイスの自動削除により、MIAデバイスを手動で削除する必要性を軽減できます。

MIA デバイスを削除するプロセスは、毎日午前 3 時 45 分に実行されます。1 回の実行で最大 100 台のデバイスを削除できます。削除するMIAデバイスが100台を超えている場合や、デバイスを今すぐ削除する必要がある場合は、デバイスを手動で削除することを検討してください。

1. デバイス リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。

2. **アクションの選択 > MIA設定項目の設定** を選択して、MIA設定 ページを表示します。
3. 次の情報を入力します。

オプション	説明
MIAデバイスを自動的に削除	指定された期間の経過後、MIA（未同期）となっている管理対象デバイスをアーカイブまたは削除します。MIデバイスが自動的にアーカイブまたは削除されないようにするには、このチェックボックスをオフにします。
n 日後	MIAデバイスの自動削除 が選択されている場合にMIAデバイスがインベントリに保持される日数。指定された日数の間にアプライアンスと通信しない管理対象デバイスは、指定されたとおり自動的に削除またはアーカイブされます。
MIA資産デバイスをアーカイブ	このオプションを選択すると、指定した日数の経過後にMIAデバイスがアーカイブされます。
MIAデバイスを削除	このオプションを選択すると、指定した日数の経過後にMIAデバイスが永続的に削除されます。

4. **保存** をクリックします。

   デバイスは、毎日 03:45 に削除プロセスが実行されると削除されます。プロセスは 1 回の実行で最大 100 台のデバイスを削除できます。

削除するMIAデバイスが100台を超えている場合や、デバイスを今すぐ削除する必要がある場合は、デバイスを手動で削除することを検討してください。詳細については、「MIAデバイスの手動削除」を参照してください。

MIAデバイスへのラベルの適用

ラベルを使用して、MIAデバイスをグループで管理できます。

1. デバイス リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. **オプション**：MIAデバイスを表示するには、次の操作を実行します。右側の表の上に表示される 特定基準で表示 ドロップダウンリストから **MIA** を選択して、デバイスで実行できなかった同期の回数または実行できなかった日数を選択します。
3. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
4. **アクションの選択 > ラベルの適用** を選択して、ラベルの適用 ダイアログを表示します。
5. ラベルを検索するか、またはリストされているラベルを これらのラベルを適用 にドラッグして、**ラベルの適用** をクリックします。

MIAデバイスの手動削除

必要に応じてMIAデバイスを手動で削除できます。

MIAデバイスが自動で削除されるようにアプライアンスを設定するには、MIA設定項目の設定を参照してください。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. **オプション**：MIAデバイスを表示するには、次の操作を実行します。右側の表の上に表示される 特定基準で表示 ドロップダウンリストから **MIA** を選択して、デバイスで実行できなかった同期の回数または実行できなかった日数を選択します。
3. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
4. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

インベントリに表示されないデバイスのトラブルシューティング

インベントリにエージェント管理対象デバイスが表示されない場合は、エージェントとアプライアンスの設定を確認します。

デフォルトでは、管理対象デバイスにインストールされている KACE エージェントは、ポート 80 および 443 上で HTTP を使用することにより、アプライアンスと通信します。ネットワーク接続は正常に動作しているにもかかわらず、新たにインストールされたエージェントがアプライアンスに接続されない場合、DNS のデフォルトの kbox ホスト名に問題がある可能性があります。

1. ホスト名またはIPアドレスを正しく指定して、エージェントをインストールします。

    Windows

    msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=my_kace_sma

    Mac OS X

    hdiutil attach ampagent-6.x.xxxxx-all.dmg
    sudo sh -c 'KACE_SERVER=my_kace_sma installer -pkg /Volumes/Quest_KACE/AMPAgent.pkg
     -target /'
    hdiutil detach /Volumes/Quest_KACE

    Linux（RHELおよびSLES）

    export KACE_SERVER=my_kace_sma
    export KACE_SERVER=my_kace_smasudo rpm -ivh ampagent-6.x.xxxxx.xxxx.xx.rpm
2. インストール済みのデバイスのサーバー名を修正するには、AMPToolsユーティリティを使用します。

    Windows

    32ビットシステム："C:\Program Files\Quest\KACE\AMPTools" host=my_kace_sma

    64ビットシステム："C:\Program Files (x86)\Quest\KACE\AMPTools" host=my_kace_sma

    Mac OS X

    /Library/Application\ Support/Quest/KACE/bin/AMPTools host=my_kace_sma

    Linux

/opt/quest/kace/bin/AMPTools host=my_kace_sma

3. アプライアンスに対して ping を実行できることと、Web ブラウザで http://**appliance_hostname** を指定して、アプライアンスに接続できることを確認します。
4. インターネットオプションがプロキシを使用するように設定されていないことを確認します。ローカルネットワークまたは **appliance_hostname** に対してプロキシが除外されていることを確認します。
5. ファイアウォールやスパイウェア対策アプリケーションが、アプライアンスと、次のようなエージェントコンポーネントとの間の通信をブロックしていないことを確認します。

各オペレーティングシステム用の KACE エージェントコンポーネント

オペレーティングシステム	エージェントコンポーネント
Windows	ACUConfig.exe AMPAgent.exe AMPKickstart.exe AMPTools.exe AMPWatchDog.exe Inventory.exe KCopy.exe KDeploy.exe KInventory.exe konea.exe kpatch.exe KSWMeterSvc.exe KUserAlert.exe runkbot.exe
Mac OS XとLinux	AMPAgent AMPAgentBootup AMPctl AMPTools AMPWatchDog インベントリ KBoxClient KCopy KDeploy KInventory konea kpatch KSWMeterSvc KUpdater KUserAlert runkbot

6. 次のプロセスが実行されていることを確認します。
   - **Windows: AMPAgent.exe、AMPWatchDog.exe、konea.exe.**
   - **Mac および Linux：AMPAgent、konea。**

これらの事項を確認しても、エージェントがアプライアンスに接続されない場合は、**Questサポート**（https://support.quest.com/contact-support）に連絡してください。

Dell保証情報の取得

アプライアンスで定期的に実行されるバックグラウンドサービスによって、アプライアンスインベントリ内のDell 製デバイスの Dell 保証情報が収集および更新されます。

このサービスは4時間ごとに実行されます。組織が複数ある場合は、サービスがラウンドロビン方式でそれぞれの組織を選択し、組織あたり約100台のデバイスの保証情報を収集します。時間と共に、すべてのDell製デバイスの保証情報が収集および更新されます。

Dell保証情報は任意の時間に更新でき、レポートを実行して保証情報を追跡することができます。

注: Dell保証情報は、インベントリ内のDellコンピューターにのみ適用可能です。また、アプライアンスが次のドメインにアクセスして保証情報を収集できる必要があります。**api.dell.com**。詳細については、「アプライアンスから必要な Web サイトへのアクセスの許可」を参照してください。

1台のDell製デバイスに対するDell保証情報の即時取得

インベントリにある任意の管理対象 Dell デバイスの保証情報は、**管理者コンソール**から取得できます。

Dell製デバイスが多数ある場合、アプライアンスのバックグラウンドサービスを通じて保証情報を更新すると時間がかかることがあります。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. デバイスのリストで、Dell製デバイスの名前をクリックして、デバイスの詳細 ページを表示します。
3. インベントリ情報セクションで、**ハードウェア** を展開します。

    デル保証情報は、Dell Service Information（デルサービスの情報）セクションの下に表示されます。
4. **更新** をクリックします。

保証情報が即座に更新されます。

Dell保証の更新

Dell Supportウェブサイトにアクセスして、インベントリ内のデル製デバイスに関する保証を更新できます。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. デバイスのリストで、Dell製デバイスの名前をクリックして、デバイスの詳細 ページを表示します。
3. インベントリ情報セクションで、**ハードウェア** を展開します。
4. Dellサービスの情報 セクションで**support.dell.com**のリンクを選択します。

Dell Supportウェブサイトに移動し、ここで期限切れの保証を更新したり、追加情報を確認したりできます。

Dell保証レポートの実行

インベントリにある Dell デバイスの保証状況を示すレポートを実行できます。アプライアンスで組織コンポーネントが有効化されている場合は、これらのレポートを組織レベルとシステムレベルで実行できます。

1. レポート リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**レポート作成** をクリックして、**レポート** をクリックします。
2. 右側の表の上に表示される特定基準で表示 ドロップダウンリストから、**デルの保証** を選択して、Dell保証レポートを表示します。
3. レポートの生成 列で、レポートを実行するレポートタイプをクリックします。

    詳細については、「レポートについて」を参照してください。

ソフトウェア ページでのアプリケーション管理

管理対象デバイスで見つかったアプリケーションは、ソフトウェア ページにリストされます。

ソフトウェア ページについて

ソフトウェア ページには、管理対象デバイスにインストールされたすべてのアプリケーションと、手動でインベントリに追加されたか、インベントリAPIを使用してアップロードされたすべてのアプリケーションが表示されます。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織ごとにアプリケーションを個別に管理します。

ソフトウェア ページからアクセスできる情報と機能は、ソフトウェアカタログ ページからアクセスできる情報と機能とは異なります。詳細については、「ソフトウェア ページと ソフトウェアカタログ ページの相違点」を参照してください。

ソフトウェア ページインベントリのアイテムの表示

インベントリに追加されたアイテムを ソフトウェア ページで表示できます。アプライアンス上で組織コンポーネントが有効化されている場合は、組織ごとに ソフトウェア ページインベントリを個別に表示できます。

1. ソフトウェア リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。

インベントリ設定に対する変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

ソフトウェア ページインベントリ内のアプリケーションの追加と削除

管理対象デバイスがインベントリ情報をアプライアンスにアップロードすると、アプリケーションは自動的に ソフトウェア ページインベントリに追加されます。さらに、必要に応じてアプリケーションを ソフトウェア ページに手動で追加することもできます。

ソフトウェア ページインベントリへのアプリケーションの手動による追加

必要に応じて、アプリケーションを ソフトウェア ページインベントリに手動で追加できます。

通常は、手動でアプリケーションをアプライアンスに追加することにより、アプリケーションが自動的にアプライアンスインベントリに追加されるのが最善の方法です。しかし、現在、管理対象デバイスにインストールされていないアプリケーションを追加する場合は、手動によるアプリケーションの追加が役に立ちます。アプリケーションを手動で追加し、管理対象インストールを作成して、管理対象デバイスに展開できます。

アプリケーションを手動で追加する場合、アプリケーションに関する情報が最新の状態で保たれ、かつエージェントがチェックインするたびにパッケージが再インストールされないように、カスタムインベントリルールの追加が必要になることがあります。詳細については、カスタムインベントリルールの記述を参照してください。

ヒント: 手動で追加されたアプリケーションは ソフトウェア ページには表示されますが、ソフトウェアカタログ ページには表示されません。アプリケーションを ソフトウェアカタログ ページに手動で追加できません。

1. ソフトウェアの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. 次の一般情報を入力します。「名前」、「バージョン」、および「発行元」。

    ダウンストリームへのレポート処理が適切に実行されるように、この情報がソフトウェアインベントリ全体で整合するようにします。
3. 次の情報を入力します。

オプション	説明
ラベルへの割り当て	（ オプション ）アイテムに関連付けられるラベル。
メモ	任意の追加情報を入力します。

オプション	説明
サポートされているオペレーティングシステム	アプリケーションが実行されるオペレーティングシステム。アプリケーションは、選択したオペレーティングシステムがインストールされているデバイスにのみ導入されます。 a. **オペレーティングシステムの管理** をクリックします。 b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**すべて > Windows > Windows 10** の順に選択し、**x64** を選択します。
カスタムインベントリルール	（オプション）アプリケーションに適用されるカスタムインベントリルール。カスタムインベントリルールを使用すると、デバイス上のアプリケーションおよび他のアイテムを検出したり、レポート目的で詳細を取得したりできます。 例えば、アプライアンスでは、デバイス上にアプリケーションが存在するかどうかを確認してから、アプリケーションが展開されます。にもかかわらず、インストールされているプログラムが プログラムの追加と削除 またはレジストリの標準領域に登録されていない場合があります。そのような場合、アプライアンスは、管理者からの追加の情報なしでは、アプリケーションの存在を検出できないことがあります。そのため、デバイスが接続されるたび、アプライアンスでインストールが繰り返される場合があります。カスタムインベントリルールを使用すると、このようなことを回避できます。 次のルールを使用して、デバイスにインストールされているNetwork Associates VirusScanのバージョンが展開前の所定のバージョンよりも新しいことを確認します。 RegistryValueGreaterThan(HKEY_LOCAL_MACHINE\Software\Network Associates\TVD\Shared Components\VirusScan Engine\4.0.xx,szDatVersion,4.0.44) 詳細については、「デバイス（カスタムインベントリフィールド）からの値の取得」を参照してください。

4. ファイルのアップロードと関連付け の隣にある **参照** または **ファイルの選択** をクリックしてファイルを参照し、**開く** または **選択** をクリックします。

管理対象インストールまたはファイル同期によってアプリケーションを配布するには、そのアプリケーションに実際のアプリケーションファイルを関連付ける必要があります。

5. ファイルがレプリケーション共有にコピーされないようにするには、**関連付けられたファイルを複製しない** を選択します。

   これは、ソフトウェアスイートなど、ユーザーにレプリケーション共有にインストールしてほしくない大きいファイルに役立ちます。

6. **オプション**：ソフトウェアの カテゴリ と 脅威レベル を設定します。
7. **保存** をクリックします。

関連トピック

ソフトウェア脅威レベルとカテゴリの使用

アプリケーションの削除

ソフトウェア ページからアプリケーションを削除すると ソフトウェア ページインベントリからも削除され、アプリケーションに関連付けられた管理対象インストールまたはファイル同期も削除されます。

ただし、削除したアプリケーションが管理対象デバイスにインストールされている場合、デバイスがインベントリ情報を更新したときに、それらのアプリケーションのレコードが新しいIDで再作成されます。ただし、削除されたアプリケーションに関連付けられた管理対象インストールとファイル同期は再作成されません。

1. ソフトウェア リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。
2. 1つまたは複数のアプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

ソフトウェア資産の作成

ソフトウェア ページに表示されるアプリケーションのライセンスコンプライアンスを設定するには、最初にそのアプリケーションのソフトウェア資産を追加する必要があります。ソフトウェア資産を作成したら、ライセンス資産と関連付けることができます。

アプライアンスに自動または手動で追加されたアプリケーションの資産を作成できます。

注: ソフトウェアカタログ ページのアプリケーションにライセンスコンプライアンスを設定する場合には、ソフトウェア資産は必要ありません。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のソフトウェア資産を個別に作成します。

インベントリ セクションにおけるソフトウェア資産の追加

ソフトウェア リストの インベントリ セクションのアプリケーションを選択することにより、1 つまたは複数のアプリケーションのソフトウェア資産を追加できます。

資産 セクションでソフトウェア資産を追加することもできます。詳細については、「資産 セクションにおけるソフトウェア資産の追加」を参照してください。

1. ソフトウェア リストに移動します。

a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。

2. 1つまたは複数のアプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択 > 資産の作成** を選択します。

資産が作成され、それらが 資産 ページに表示されます。

資産 セクションにおけるソフトウェア資産の追加

資産 セクションでは、一度に 1 つずつソフトウェア資産を追加することができます。

インベントリ セクションでソフトウェア資産を追加することもできます。詳細については、「インベントリ セクションにおけるソフトウェア資産の追加」を参照してください。

1. 資産 リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
2. **アクションの選択 > 新規作成 > ソフトウェア** を選択して、ソフトウェア資産の詳細 ページを表示します。
3. 以下の要領で、資産フィールドに必要事項を入力します。
   a. 名前 フィールドに、資産の名前を入力します。

   例えば、「Office Pro SW Asset」と入力します。

   b. **オプション**：ソフトウェア フィールドで、資産に関連付けるアプリケーションの名前を選択します。アイテムを検索するには、フィールドに入力し始めます。
   c. **オプション**：ソフトウェアラベル フィールドで、ラベルの選択 ドロップダウンリストからラベルを選択します。Smart Labelを作成していない場合、このリストには項目が表示されません。ラベルリストを絞り込むには、ラベル名の数文字を フィルタ フィールドに入力します。
4. **保存** をクリックします。

資産 ページに新しい資産が表示されます。

アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択

管理対象インストールまたは**ユーザーコンソール**ダウンロードを使用して管理対象デバイスにアプリケーションを配布するには、適切なデジタル資産をアプリケーションに添付する必要があります。デジタル資産は、展開に必要なファイルです（インストーラなど）。また、アプリケーションに対してサポートされているオペレーティングシステムを選択する必要があります。これらのタスクは、ソフトウェア 詳細ページで実行します。

複数のファイルをアプリケーションに関連付けるには、そのファイルを含むZIPファイルを作成し、その結果生成されたアーカイブファイルをアプリケーションに関連付けます。

ヒント: デジタル資産は、ソフトウェア ページに表示されているアプリケーションには添付できますが、ソフトウェアカタログ ページのアイテムに添付することはできません。

1. ソフトウェアの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。

c. ソフトウェアアプリケーションの名前をクリックします。

2. 次のいずれかを実行します。

- ファイルのアップロードと関連付け **の隣に表示されている 参照 または ファイルの選択 をクリックします。**
- Upload and Associate Client Drop File **(クライアントドロップファイルのアップロードと関連付け) の隣に表示されている 参照 または ファイルの選択 をクリックします。このオプションが使用可能になるのは、ファイルをアプライアンスまたは組織のクライアントドロップの場所にコピーし、かつそれらのファイルの大きさがアプライアンスの** Client Drop File Size Filter **(クライアントドロップファイルサイズフィルタ) または組織の Client Drop Size (クライアントドロップサイズ) に指定されているサイズよりも大きい場合のみです。アプライアンス上で組織コンポーネントが有効化されている場合は、選択した組織のみがファイルを使用できます。複数の組織がファイルを使用できるようにするには、組織ごとにファイルをクライアントドロップの場所にコピーします。**アプライアンスクライアントドロップの場所へのファイルのコピー.

3. アップロードするファイルを指定して、**開く** または **選択** をクリックします。
4. Supported Operating Systems (サポートされているオペレーティングシステム) セクションで、アプリケーションをインストールできるオペレーティングシステムを選択します。

a. **オペレーティングシステムの管理** をクリックします。

b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。

表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。

ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**すべて > Windows > Windows 10** の順に選択し、**x64** を選択します。

注: オペレーティングシステムを選択していない場合は、アプリケーションを管理対象デバイスに配布することはできません。管理対象インストールなどの展開を作成できますが、それらを展開できるのはサポートされているオペレーティングシステムについて正しい情報が提供されている場合に限られます。

5. 必要に応じてその他の詳細を修正し、**保存** をクリックします。

注: Software Detail (ソフトウェアの詳細) ページの下部にある表に、ソフトウェアがインストールされているデバイスが表示されます。

アプライアンスクライアントドロップの場所へのファイルのコピー

アプリケーションファイルやバックアップファイルなどの大規模ファイルをアプライアンス上のクライアントドロップの場所にコピーすることで、それらのファイルをアプライアンスにアップロードできます。大規模ファイルの場合、**管理者コンソール**でデフォルトの HTTP メカニズムを使用してファイルをコピーするとブラウザがタ

イムアウトする場合があるため、代わりにクライアントドロップの場所へのファイルのアップロードを使用します。

- ファイル共有（Samba）を有効化します。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。
- アプライアンス上で組織コンポーネントが有効化されている場合は、組織ごとにファイル共有を有効にします。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。
- アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンスの Client Drop File Size Filter（クライアントドロップファイルサイズフィルタ）設定を設定します。詳細については、「組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定」を参照してください。
- アプライアンス上で組織コンポーネントが有効化されている場合は、組織ごとにクライアントドロップサイズ設定を設定します。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。

1. ファイルシステムナビゲータで、アプライアンス上のクライアントドロップの場所に移動します。
   - **Windows エクスプローラで、アプライアンスホスト名または IP アドレスを使用した UNC パスを入力します。例：\\kbox\clientdrop。2 つのバックスラッシュを使用して、場所が Samba パスであることを示します。**
   - **Mac OS X の場合、実行 > サーバーに接続 を選択し、**Server Address**（サーバーアドレス）フィールドに SMB アドレスを入力します。**
   - **Linux の場合、検索 を選択し、SMB アドレスを入力します。**

   client Share フォルダおよび clientdrop Share フォルダが表示されます。

   注: 組織コンポーネントが有効になっている場合は、各組織がそれぞれ別個のクライアントドロップの場所を持ちます。例：
   - ORG1： clientdrop
   - ORG2： clientdrop_2
   - ORG3： clientdrop_3
2. 要求された場合は、クライアントドロップの場所のログイン資格情報を指定します。これらの資格情報は、アプライアンスセキュリティ設定に指定されています。詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。

   ヒント: Windows デバイスから接続している場合は、Username（ユーザー名）フィールドに「\admin」と入力します。これにより、認証時に workgroup\admin または domain\admin が使用されないようにすることができます。
3. ファイルをクライアントドロップの場所にコピーします。アプライアンス上で組織コンポーネントが有効化されている場合は、ファイルを選択する組織のクライアントドロップの場所にファイルをコピーします。

   使用できるファイルは次のとおりです。

   - **アプリケーションファイル**：ファイルの大きさが Client Drop File Size Filter（クライアントドロップファイルサイズフィルタ）でアプライアンス用に設定されたサイズよりも大きいか、またはクライアントドロップサイズで組織用に設定されたサイズよりも大きい場合は、Software Detail（ソフトウェア詳細）ページでファイルを選択できます。アプライアンス上で組織コンポーネントが有効化されている場合は、選択した組織のみがファイルを使用できます。複数の組織がファイルを使用できるようにするには、組織ごとにファイルをクライアントドロップの場所にコピーします。
   - **アプライアンスバックアップファイル**：クライアントドロップの場所に配置されるアプライアンスバックアップファイルは、アプライアンスバックアップファイルとして自動的に識別され、5 分以内に バックアップ設定 ページで選択できるようになります。

Software Detail（ソフトウェア詳細）ページで選択したアプリケーションファイルをアップロードしている場合は、Client Drop（クライアントドロップ）の場所フィルタ設定を確認します。このフィルタ設定によって、ファイルがそれぞれのサイズに基づいて Software Detail（ソフトウェア詳細）ページに表示されるかどうかが決まり

ます。組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定または組織の追加または編集を参照してください。

ソフトウェア脅威レベルとカテゴリの使用

脅威レベルおよびカテゴリを使用して、アプリケーションの相対的な安全性を示し、アプリケーションを分類できます。

この情報は、追跡目的のためにのみ使用可能になっています。アプライアンスが、脅威レベルまたはカテゴリに基づきポリシーを強制することはありません。

ソフトウェアカテゴリは、ソフトウェアドライバまたはセキュリティアプリケーションなど特定のグループに属するソフトウェアを分類します。ソフトウェア ページにリストされたアプリケーションについては、カテゴリは手動で割り当てられます。ソフトウェアカタログ ページにリストされたアプリケーションについては、ソフトウェアカテゴリはアプリケーションに自動的に割り当てられます。

アプリケーションへの脅威レベルの割り当て

ソフトウェア ページにリストされたアプリケーションに脅威レベルを割り当てることができます。ソフトウェアカタログ ページにリストされたアイテムには脅威レベルを割り当てることはできません。

1. ソフトウェア リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。
2. 1つまたは複数のアプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択 > 脅威レベルの設定** を選択して、脅威レベルを選択します。

アプリケーションへのカテゴリの割り当て

ソフトウェア ページにリストされたアプリケーションにカテゴリを割り当てることができます。ソフトウェアカタログ ページにリストされたアプリケーションには、カテゴリが自動的に割り当てられます。

1. ソフトウェア リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。
2. 1つまたは複数のアプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択 > カテゴリの設定** を選択して、カテゴリを選択します。

アプリケーションの検索とラベル作成

高度な検索とラベルを使用して、ソフトウェアインベントリを管理できます。

高度な検索を使用したアプリケーションの検索について

高度な検索を使用すると、ソフトウェアインベントリに表示されているフィールドごとに値を指定し、その特定の値または値の組み合わせをインベントリ全体で検索できます。

例えば、高度な検索を使用して、特定のオペレーティングシステムに特定のアプリケーションがインストールされているデバイスを検索できます。詳細については、「高度なオプションによるページレベルの検索」を参照してください。

ソフトウェアラベルの手動追加

必要に応じて、インベントリ セクションにラベルを手動で追加することができます。これは、ラベルをソフトウェアアプリケーションに手動で適用してこれらのアプリケーションをグループ化する場合に役立ちます。

1. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. 次のいずれかを実行します。
   - **インベントリ > ソフトウェア の順に選択して**、ソフトウェア **ページを表示します。**
   - **インベントリ > ソフトウェアカタログ の順に選択して**、ソフトウェアカタログ **ページを表示します。**
3. **アクションの選択 > ラベルの追加** を選択します。
4. ラベルの追加 ウィンドウで、ラベルの名前を入力します。

   ヒント: ラベル名にはバックスラッシュ (\ ) を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して (\\ ) エスケープします。
5. **保存** をクリックします。

ソフトウェアへのラベルの手動による適用または削除

必要に応じて、アプライアンスインベントリ内のソフトウェアに対してラベルを手動で適用または削除することができます。

ラベルを手動で追加します。詳細については、「ソフトウェアラベルの手動追加」を参照してください。

1. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. 次のいずれかを実行します。
   - **インベントリ > ソフトウェア の順に選択して**、ソフトウェア **ページを表示します。**
   - **インベントリ > ソフトウェアカタログ の順に選択して**、ソフトウェアカタログ **ページを表示します。**
3. 1つまたは複数のアプリケーションの隣のチェックボックスをオンにします。
4. 次のいずれかを実行します。
   - **アクションの選択 > ラベルの適用 を選択して、適用するラベルを選択します。**
   - **アクションの選択 > ラベルの削除 を選択して、削除するラベルを選択します。**

ラベルの詳細については、手動ラベルの管理を参照してください。

ソフトウェアSmart Labelの追加

必要に応じて、ソフトウェア ページでソフトウェアSmart Labelを追加できます。これは、Smart Labelの条件を満たしているかどうかに基づいてアプリケーションを自動的にグループ化する場合に役立ちます。

例えば、Smart Labelを使用して、特定のベンダーから購入したアプリケーションのすべてのコピーをグループ化することができます。ラベルは、特定のベンダーから購入済みのアプリケーション、および今後購入する可能性のあるアプリケーションに自動的に適用されます。詳細については、「Smart Labelの管理」を参照してください。

注: Smart Labelは、ソフトウェアカタログ ページのアプリケーションには適用できません。

1. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **インベントリ > ソフトウェア** の順に選択して、ソフトウェア ページを表示します。
3. 右側のアプリケーションリストの上にある **Smart Label** タブをクリックして、Smart Label パネルを表示します。

4. 次のように、特定のベンダーからのアプリケーションを検出するために必要な条件を指定します。

   ベンダー連絡先 | 次の値を含む | Smith
5. **テスト** をクリックします。

   指定した条件と一致するアイテムが表示されます。
6. 目的の結果が得られるまで、必要に応じて条件を調整します。
7. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。
   - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

     注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。
   - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。

8. **Create** をクリックします。

アプリケーションが インベントリ > ソフトウェア ページで更新されると、指定された条件をアプリケーションが満たしているかどうかに基づいて、Smart Labelがアプリケーションに対して自動的に適用または除去されます。

ITNinjaフィードの管理

ITNinja フィードを使用すると、ITNinja からのシステム管理コンテンツを**管理者コンソール**に表示できます。データ共有設定を変更して、ITNinjaフィードを有効化または無効化します。

Quest KACEがスポンサーとなっているITNinja.com（以前のAppDeploy.com）は、ITに焦点を絞った製品不問のコミュニティウェブサイトです。このサイトは、ITプロフェッショナルが、システム管理に関連する情報を共有したり、質問したりする主要なインターネットサイトになっています。このWebサイトでは、質疑応答セクションとブログプラットフォームを提供しています。匿名の使用率データを ITNinja と共有することを選択すると、ITNinja フィードが**管理者コンソール**のソフトウェア、管理対象インストール、ファイル同期などの詳細ページに表示されます。フィードは ソフトウェアカタログ の詳細ページでは利用できません。詳細については、「ITNinjaフィードの有効化」を参照してください。

ITNinjaフィードの有効化

ITNinjaフィードを有効にするには、匿名の使用率データをQuestと共有するようにアプライアンス設定を構成します。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **一般設定** をクリックします。
3. Questとのデータの共有 セクションで、ハードウェア、ソフトウェア、およびアプライアンスの使用率サマリデータをデルと共有する と 使用率の詳細データとクラッシュレポート（ITNinjaコミュニティの機能を使用するために必要）を共有する のチェックボックスをオンにします。
4. **保存** をクリックします。

アプライアンスの一般設定の詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。

ITNinja情報の表示

ITNinja フィードを有効にすると、**管理者コンソール**の「管理対象インストール」、「ファイル同期」、および「ソフトウェア」の詳細ページに関連する ITNinja 情報を表示できます。

詳細については、「ITNinjaフィードの有効化」を参照してください。

注: ITNinja 情報は、ソフトウェア ページのソフトウェアでは利用できますが、ソフトウェアカタログ ページのソフトウェアでは利用できません。

ソフトウェアのITNinja情報の表示

ITNinja 情報は、Software Detail（ソフトウェア詳細）ページで確認できます。

ITNinjaフィードを有効にする必要があります。詳細については、「ITNinjaフィードの有効化」を参照してください。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **インベントリ > ソフトウェア** の順に選択して、ソフトウェア ページを表示します。
3. アプリケーションの名前をクリックして、ソフトウェアの詳細 ページを表示します。
4. ITNinja セクションまでスクロールします。

管理対象インストールのITNinja情報の表示

管理対象インストールのITNinja情報を表示できます。

ITNinjaフィードを有効にする必要があります。詳細については、「ITNinjaフィードの有効化」を参照してください。

1. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **配布** をクリックして、管理対象インストール ページを表示します。
3. 管理対象インストールの名前をクリックして、管理対象インストールの詳細 ページを表示します。
4. ITNinja セクションまでスクロールします。

ファイル同期のITNinja情報の表示

ファイル同期のITNinja情報を表示できます。

ITNinjaフィードを有効にする必要があります。詳細については、「ITNinjaフィードの有効化」を参照してください。

1. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **配布 > ファイル同期** を選択して、ファイル同期 ページを表示します。
3. ファイル同期の名前をクリックして、ファイル同期の詳細 ページを表示します。
4. ITNinja セクションまでスクロールします。

ITNinjaフィードの無効化

管理者コンソールに ITNinja フィードを表示しないようにするには、Quest とデータを共有するアプライアンス設定を変更します。これにより、ITNinjaフィードが無効になります。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **一般設定** をクリックします。
3. Questとのデータの共有 セクションで、使用率の詳細データと… チェックボックスをオフにします。
4. **保存** をクリックします。

アプライアンスの一般設定の詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。

ソフトウェアカタログインベントリの管理

管理対象デバイス上に存在すると識別され、ソフトウェアカタログの定義に一致したアプリケーションは、ソフトウェアカタログインベントリと呼ばれます。

ソフトウェアカタログについて

ソフトウェアカタログは、60,000超のWindowsとMacのアプリケーションおよびソフトウェアスイートに関する標準化された情報を格納しているデータベースです。カタログの情報には、各アプリケーションまたはスイートの名前、バージョン、発行元、カテゴリ、およびアプリケーションまたはスイートを実行するオペレーティングシステムが含まれます。

ソフトウェアカタログは、バージョン 5.5 以降を実行するすべての KACE SMA で使用可能です。このカタログは、Questによって継続的に更新および管理が行われて、最新の状態に保たれており、包括性と正確性が確保されています。

エージェントバージョン5.5以降を実行する管理対象デバイスがアプリケーションインベントリをレポートするときに、そのインベントリ情報がソフトウェアカタログのアイテムと比較されます。その後、標準化されたアプリケーションインベントリ情報が ソフトウェアカタログ タブに表示されます。

ソフトウェアカタログにより、以下が可能になります。

- デバイスにインストールされたソフトウェアの識別と、そのソフトウェアに関する標準化された情報の表示。詳細については、「ソフトウェアカタログ情報の表示」を参照してください。
- メータリングの有効化による、ソフトウェアの使用状況に関する詳細情報の収集。詳細については、「ソフトウェアメータリングの使用」を参照してください。
- ライセンス情報とソフトウェアカタログのソフトウェアとの関連付け。これにより、デバイスのソフトウェアライセンスコンプライアンスとライセンス使用率を監視できます。詳細については、「ソフトウェアカタログ インベントリのライセンス資産の追加」を参照してください。
- ソフトウェアを識別して「不許可」としてマーク付けする。これにより、「不許可」としてマーク付けされたソフトウェアの使用を防止できます。詳細については、「アプリケーション制御の使用」を参照してください。

このカタログには、WindowsおよびMacのオペレーティングシステムのみで動作するように設計されたソフトウェアに関する情報が含まれています。Linuxおよびその他のサポートされていないオペレーティングシステム上で動作するよう設計されたソフトウェアは、このカタログには含まれていません。

アプリケーションの分類

ソフトウェアカタログ ページに表示されるアプリケーションは、検出済み、未検出（カタログ登録済み）、およびカタログ未登録に分類されます。この分類により、アプリケーションに対して実行できるアクションの種類と取得可能な情報のタイプが決まります。

検出されたアプリケーション

検出されたアプリケーションはアプライアンスインベントリ内で実行可能で、ソフトウェアカタログに定義されたアプリケーションと一致します。検出されたアプリケーションおよびスイートに対して、メータリングの有効化や「不許可」としてのマーク付けを行ったり、ライセンス情報の追加を行うことができます。また、検出されたアプリケーションのリストをCSV形式でエクスポートすることもできます。検出されたアプリケーションのリスト、カタログ未登録のリスト、ローカルカタログ登録済みのリストはエクスポートできますが、ソフトウェアカタログ全体のエクスポートはできません。

未検出のアプリケーション

アプライアンスインベントリ内には存在せず、Quest KACE ソフトウェアカタログには存在するアプリケーションは、未検出のアプリケーションと呼ばれます。未検出のアプリケーションに対してメータリングを有効化し、「不許可」としてマーク付けを行い、ライセンス情報の追加を行うことができます。ただし、ローカルのアプライアンスインベントリで検出されなかったアプリケーションであるため、未検出のアプリケーションのリストをCSV 形式でエクスポートすることはできません。

カタログ未登録のアプリケーション

カタログ未登録のアプリケーションは、アプライアンスインベントリには存在するが、ソフトウェアカタログには表示されない実行可能ファイルです。ソフトウェアカタログ ページでは、「カタログ未登録」としてリストされたアプリケーションを表示できます。ただし、カタログ未登録のアプリケーションのメータリングの有効化、「不許可」としてのマーク付け、およびライセンス情報の追加を行うことはできません。

カタログ未登録のアプリケーションに対してメータリング、「不許可」としてのマーク付け、またはライセンス情報との関連付けを行うには、カタログ未登録のアプリケーションをローカルまたはパブリックのソフトウェアカタログに追加する必要があります。詳細については、「ソフトウェアカタログへのアプリケーションの追加」を参照してください。

注: カタログ未登録のアプリケーションに対してデータの保持が無効になっている場合、カタログ未登録のアプリケーションリストは空になります。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。

カタログ登録済みのアプリケーションについて

カタログ登録済みのアプリケーションは、公式のソフトウェアカタログデータベースに登録されている実行可能ファイルです。これには、アプライアンスインベントリに表示されるアプリケーション（検出されたアプリケーション）と、このインベントリに表示されないアプリケーション（未検出のアプリケーション）の両方が含まれます。

ローカルカタログ登録済みのアプリケーションについて

公式版のソフトウェアカタログになく、アプライアンス上のローカル版のカタログに追加されたアプリケーションは、ローカルカタログ登録済みのアプリケーションと呼ばれます。

不許可のアプリケーションについて

不許可のアプリケーションとは、ソフトウェアカタログ ページで「不許可」としてマーク付けされたアプリケーションです。

WindowsおよびMacのアプリケーションでは、検出済み、未検出、またはローカルカタログ登録済みアプリケーションのいずれかに分類されている場合のみ、「不許可」としてマーク付けできます。カタログ未登録のアプリケーションは、ソフトウェアカタログに追加されない限り、「不許可」としてマーク付けすることはできません。「不許可」としてマーク付けされているアプリケーションは、アプリケーション制御対応のラベルがデバイスに適用されている場合、管理対象デバイス上でのアクセスをブロックまたはを拒否することができます。

詳細については、「アプリケーション制御の使用」を参照してください。

アプリケーションのカテゴリ

ソフトウェアカタログのアプリケーションは、生産性アプリケーション、ウイルス対策ユーティリティなど、複数のカテゴリにグループ化されます。

これらのカテゴリは、レポート作成とライセンスコンプライアンスにおいて有用です。オペレーティングシステム カテゴリのアプリケーションはメータリングできません。

ソフトウェアカタログの情報が収集される仕組み

指定された間隔で、管理対象デバイスにインストールされているすべての実行可能ファイルに関する情報が収集されます。この情報には、実行可能ファイルの発行元、公開日、ファイルサイズ、およびレジストリ情報が含まれます。

この情報はソフトウェアカタログ内の情報と比較され、検出されたアプリケーションが登録済みであるか、未登録であるかが判別されます。詳細については、「メータリングおよびインベントリコレクションの間隔のスケジュール」を参照してください。

ソフトウェアカタログが組織コンポーネントと共に使用される仕組み

アプライアンスにはそれぞれ 1 つのソフトウェアカタログがあります。アプライアンス上で組織コンポーネントが有効化されている場合、そのアプライアンスにインストールされたものと同じソフトウェアカタログが、すべての組織で使用されます。また、ローカルカタログ登録済みのアプリケーションは、すべての組織で使用できます。

ただし、カタログ未登録のアプリケーション、およびメータリングやライセンス設定などの設定は、組織固有のものとなります。例えば、ある組織でアプリケーションのメータリングを有効化した場合、有効化の対象となるのはその組織のみです。メータリングなどの設定は各組織で個別に有効化します。

同様に、検出されたアプリケーションも組織固有のものとなります。アプリケーションが組織のインベントリで検出された場合にのみ、そのアプリケーションは「検出済み」としてマーク付けされます。

ソフトウェアカタログの情報がローカライズされる仕組み

ソフトウェアカタログのアプリケーションカテゴリは、アプライアンスのロケール設定と一致するようにローカライズされます。ただし、アプリケーション名（Microsoft Excelなど）は各国語環境に変更されません。

ソフトウェアカタログを改善する方法

ソフトウェアカタログは継続的に、新しい情報またはアプリケーションが使用可能になった場合と、カタログ登録要求を受け取った場合に更新されます。アプライアンスインベントリ情報を Quest KACE および ITNinja コミュニティと共有することによって、カタログの改善に役立てることができます。

Quest KACEカタログチームはこの情報を使用して、新しいアプリケーションを特定し、アプリケーションの名前とバージョンを標準化します。詳細については、「データ共有の基本設定の構成」を参照してください。

ソフトウェア ページと ソフトウェアカタログ ページの相違点

ソフトウェア ページと ソフトウェアカタログ ページは、両方とも管理対象デバイスによってレポートされたアプリケーション情報を使用します。ただし、これら2つのページは別個のインベントリシステムを表し、各システムでソフトウェア管理タスクの実行方法が異なります。

ソフトウェア ページにある情報の管理の詳細については、ソフトウェア ページでのアプリケーション管理を参照してください。次の表では、ソフトウェア ページと ソフトウェアカタログ ページを比較しています。

タスク	ソフトウェア ページ	ソフトウェアカタログ ページ
インベントリコレクションプロセス	アプライアンスバージョン 5.4 で使用できる古いバージョンのインベントリコレクションプロセスを使用します。エージェントバージョン 5.4 以前を実行している管理対象デバイスは、ソフトウェア ページに対してのみインベントリをレポートし、ソフトウェアカタログ ページにはインベントリをレポートしません。 エージェントバージョン 5.5 以降を実行している管理対象デバイス	アプライアンスバージョン 5.5 で導入されたインベントリコレクションプロセスを使用します。このプロセスは、管理対象デバイスにインストールされているすべての実行ファイルに関する情報を収集します。 ソフトウェアカタログ ページにインベントリをレポートするには、管理対象デバイスでエージェントバージョン 5.5 以降を実行している必要があります。

タスク	ソフトウェア ページ	ソフトウェアカタログ ページ
	は、ソフトウェア ページと ソフトウェアカタログ ページの両方に対してインベントリをレポートします。	
ソフトウェアインベントリ情報の表示	ソフトウェア ページには、管理対象デバイスで検出されたか、手動または WSAPI を通じてアプライアンスインベントリに追加されたすべてのアプリケーションに関する情報が表示されます。	ソフトウェアインベントリ情報は、ソフトウェアカタログ ページで次のように表示されます。 • **検出済み**: ソフトウェアカタログのアプリケーション情報と一致する、管理対象デバイスにインストールされたアプリケーション。 • **未検出**: 管理対象デバイスにインストールされていない、ソフトウェアカタログのアプリケーション。 • **カタログ未登録**: 管理対象デバイスにインストールされているが、ソフトウェアカタログにないアプリケーション。 手動または WSAPI を使用してアプライアンスに追加されたインベントリ情報は、ソフトウェアカタログ ページには表示されません。
アプリケーションメータリング	使用できません。	ソフトウェアカタログ ページまたは Software Catalog Detail（ソフトウェアカタログの詳細）ページで各アプリケーションに対して個別に有効化されます。
アプリケーションのライセンス情報の追跡	アプリケーションのソフトウェア資産およびライセンス資産を作成することによって有効化。ライセンス情報は、ライセンスコンプライアンスダッシュボードウィジェットに表示されます。Licence Compliance（ライセンスコンプライアンス）ページには表示されません。	ライセンス資産を作成し、ソフトウェアカタログのアプリケーションに関連付けることによって有効化。ライセンス情報は、Licence Compliance（ライセンスコンプライアンス）ページとライセンスコンプライアンスダッシュボードウィジェットの両方に表示されます。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンスについて」を参照してください。
アプリケーションへの「不許可」のマーク付け	使用できません。	Software Catalog Detail（ソフトウェアカタログの詳細）ページで設定されるフラグとして使用できます。詳細については、「アプリケーションおよびスイートへの「不許可」のマーク付け」を参照してください。

タスク	ソフトウェア ページ	ソフトウェアカタログ ページ
アプリケーションへのデジタル資産の追加	ソフトウェアの詳細 ページで実行できます。デジタル資産は、管理対象デバイスにソフトウェアを展開する際に使用されます。詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。	使用できません。
管理対象インストールまたはファイル同期でのソフトウェアの配布	デジタル資産が関連付けられたアプリケーションで使用できます。詳細については、「ソフトウェアの配布とWake On LANの使用」を参照してください。	使用できません。
ITNinjaのヒントと情報の表示	Software Detail（ソフトウェアの詳細）ページで実行できます。詳細については、「ITNinjaフィードの管理」を参照してください。	使用できません。
ライセンスの概要情報の表示	ダッシュボード ページの ライセンスコンプライアンス および ソフトウェアライセンス設定 グラフで確認できます。詳細については、「ダッシュボードのウィジェットについて」を参照してください。	ダッシュボード ページの ライセンスコンプライアンス および ソフトウェアライセンス設定 グラフで確認できます。詳細については、「ダッシュボードのウィジェットについて」を参照してください。
ソフトウェアの脅威レベルの設定	ソフトウェア リストで実行できます。詳細については、「ソフトウェア脅威レベルとカテゴリの使用」を参照してください。	使用できません。
ソフトウェアカテゴリの設定	Software Detail（ソフトウェアの詳細）ページで実行できます。詳細については、「アプリケーションへのカテゴリの割り当て」を参照してください。	Quest KACEソフトウェアカタログチームにより定義済みです。

ソフトウェアカタログ情報の表示

アプリケーション情報は、ソフトウェアカタログ ページで表示できます。

検出されたアプリケーションと未検出のアプリケーションのリスト表示

ソフトウェアカタログ リストで、検出されたアプリケーションと未検出アプリケーションを表示できます。

検出されたアプリケーションはインベントリ内で実行可能で、ソフトウェアカタログに定義されたアプリケーションと一致します。検出されたアプリケーションおよびスイートに対して、メータリングの有効化や「不許可」としてのマーク付けを行ったり、ライセンス情報の追加を行うことができます。また、検出されたアプリ

ケーションのリストをCSV形式でエクスポートすることもできます。検出されたアプリケーションのリスト、カタログ未登録のリスト、ローカルカタログ登録済みのリストはエクスポートできますが、ソフトウェアカタログ全体のエクスポートはできません。

インベントリ内に存在せず、Quest KACE ソフトウェアカタログに存在するアプリケーションは、未検出のアプリケーションと呼ばれます。未検出のアプリケーションに対してメータリングを有効化し、「不許可」としてマーク付けを行い、ライセンス情報の追加を行うことができます。ただし、ローカルのインベントリで検出されなかったアプリケーションであるため、未検出のアプリケーションのリストを CSV 形式でエクスポートすることはできません。

1. ソフトウェアカタログ リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. **検出済み** タブをクリックします。

    リストをフィルタリングして、検出済みとして分類されたアプリケーションのみを表示します。検出されたアプリケーションの情報には、次のものが含まれます。

アイテム	説明
名前	アプリケーションの名前およびバージョン。アプリケーションがスイートの場合は、名前が太字で表示されます。例： **Microsoft Office 2010 Professional**。
発行元	アプリケーションの発行元。この情報は、レポート作成が正確に行われるように標準化されます。例えば、「Microsoft Corp.」と「Microsoft Inc.」は、どちらも「Microsoft Corporation」としてレポートされます。
カテゴリ	ソフトウェアカタログチームによって確立されたアプリケーションのカテゴリ。
インストール済み	アプリケーションをインストールしている管理対象デバイスの数。数字をクリックして、デバイスの情報を表示します。
ライセンス	アプリケーションの使用可能なライセンスの数。この情報は、アプリケーションにライセンス資産が関連付けられている場合にのみ使用可能です。詳細については、「ソフトウェアカタログ インベントリのライセンス資産の追加」を参照してください。
過不足数	使用されていない残りのライセンスの数。この情報は、アプリケーションにライセンス資産が関連付けられている場合にのみ使用可能です。
最近追加	過去7日間でアプリケーションが追加されたデバイスの数。

アイテム	説明
最近削除	過去7日間でアプリケーションが削除されたデバイスの数。

3. **未検出** タブをクリックします。

   リストをフィルタリングして、未検出として分類されたアプリケーションのみを表示します。未検出アプリケーションの情報には、次のものが含まれます。

アイテム	説明
名前	アプリケーションの名前およびバージョン。アプリケーションがスイートの場合は、名前が太字で表示されます。例： **Microsoft Office 2010 Professional**。
発行元	アプリケーションの発行元。この情報は、レポート作成が正確に行われるように標準化されます。例えば、「Microsoft Corp.」と「Microsoft Inc.」は、どちらも「Microsoft Corporation」としてレポートされます。
カテゴリ	ソフトウェアカタログチームによって確立されたアプリケーションのカテゴリ。
プラットフォーム	アプリケーションの動作対象オペレーティングシステム。例えば、「Windows」などです。

4. ライセンスコンプライアンス ページまたは選択したレポートからソフトウェアカタログアイテムを含めたり除外するには、リストでそのアイテムを選択し、**アクションの選択** をクリックして、必要に応じて次のオプションのいずれかを選択します。
   - **ライセンスコンプライアンスから除外**
   - **ライセンスコンプライアンスに含める**
   - **レポートから除外**
   - **レポートに含める**
5. 追加の詳細情報を表示するには、アプリケーション名をクリックします。

   詳細については、「ソフトウェアカタログのアプリケーションの詳細の表示」を参照してください。

ヒント: ソフトウェアカタログ ページでは、「高度な検索」および「高度な検索」の条件に基づくカスタムビューを使用してアプリケーションを検索できます。詳細については、「高度なオプションによるページレベルの検索」を参照してください。

カタログ未登録アプリケーションのリストの表示

ソフトウェアカタログ リストで、カタログ未登録アプリケーションを表示できます。

カタログ未登録のアプリケーションは、アプライアンスインベントリには存在するが、ソフトウェアカタログには表示されない実行可能ファイルです。ソフトウェアカタログ リストでは、「カタログ未登録」としてリストされたアプリケーションを表示できます。ただし、カタログ未登録のアプリケーションのメータリングの有効化、「不許可」としてのマーク付け、およびライセンス情報の追加を行うことはできません。カタログ未登録のアプリケーションに対してメータリング、「不許可」としてのマーク付け、またはライセンス情報との関連付けを行うには、カタログ未登録のアプリケーションをローカルまたはパブリックのソフトウェアカタログに追加する必要があります。

カタログ未登録のアプリケーションに関して取得可能な情報は、パブリック版のソフトウェアカタログにタイトルがリストされたアプリケーションの取得可能な情報とは異なります。例えば、カタログ登録済みアプリケーションの取得可能な情報の一部が、カタログ未登録のアプリケーションでは取得できない場合があります。カタログ未登録のアプリケーションで取得可能な情報は、管理対象デバイスによって収集された情報に限られます。

1. ソフトウェアカタログ リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. **カタログ未登録** タブをクリックします。

    リストをフィルタリングして、カタログ未登録として分類されたアプリケーションのみを表示します。カタログ未登録のアプリケーションの取得可能な情報には、次のものが含まれます。

アイテム	説明
名前	アプリケーションの名前およびバージョン。
インストール済み	アプリケーションをインストールしている管理対象デバイスの数。
ファイル名	アプリケーションの実行可能ファイルの名前。
ファイルのバージョン	アプリケーションのバージョン番号。
発行元	アプリケーションの発行元。

3. ライセンスコンプライアンス ページまたは選択したレポートからソフトウェアカタログアイテムを含めたり除外するには、リストでそのアイテムを選択し、**アクションの選択** をクリックして、必要に応じて次のオプションのいずれかを選択します。
    - **ライセンスコンプライアンスから除外**
    - **ライセンスコンプライアンスに含める**
    - **レポートから除外**
    - **レポートに含める**
4. 追加の詳細情報を表示するには、アプリケーション名をクリックします。

    詳細については、「ソフトウェアカタログのアプリケーションの詳細の表示」を参照してください。

ローカルカタログ登録済みアプリケーションのリストの表示

高度な検索を使用して、ソフトウェアカタログ ページを並べ替えて、ローカルバージョンのソフトウェアカタログに追加されたアプリケーションを表示できます。

公式版のソフトウェアカタログになく、アプライアンス上のローカル版のカタログに追加されたアプリケーションは、ローカルカタログ登録済みのアプリケーションと呼ばれます。ローカルカタログ登録済みのアプリケーションには、メータリング、「不許可」としてのマーク付け、およびライセンス資産との関連付けを行うことができます。

1. ソフトウェアカタログ リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。

2. 右側のリストの上にある **高度な検索** タブをクリックして、以下のように、ローカルカタログ登録済みのアプリケーションを表示するために必要な条件を指定します。

   ソフトウェアカタログ: ローカルカタログのみ | is | True

3. **検索** をクリックします。

   リストをフィルタリングして、ローカルカタログ登録済みのアプリケーションのみを表示します。ローカルカタログ登録済みのアプリケーションの取得可能な情報には、次のものが含まれます。

アイテム	説明
名前	アプリケーションの名前およびバージョン。アプリケーションがスイートの場合は、名前が太字で表示されます。例： **Microsoft Office 2010 Professional**。
タイプ	ソフトウェアカタログにないアプリケーションの分類ローカルカタログ登録済みのアプリケーションは検出済みに分類されます。
インストール済み	アプリケーションをインストールしている管理対象デバイスの数。
発行元	アプリケーションの発行元。この情報は、レポート作成が正確に行われるように標準化されます。例えば、「Microsoft Corp.」と「Microsoft Inc.」は、どちらも「Microsoft Corporation」としてレポートされます。
カテゴリ	ソフトウェアカタログチームによって確立されたアプリケーションのカテゴリ。
プラットフォーム	アプリケーションの動作対象オペレーティングシステム。例えば、「Windows」などです。

4. 追加の詳細情報を表示するには、アプリケーション名をクリックします。

   詳細については、「ソフトウェアカタログのアプリケーションの詳細の表示」を参照してください。

ソフトウェアカタログのアプリケーションの詳細の表示

検出済み、未検出、カタログ未登録、およびローカルカタログ登録済みのスイートおよびアプリケーションの詳細を表示できます。

カタログ未登録のアプリケーションの詳細を表示するには、カタログ未登録のアプリケーションのデータ保持を有効にする必要があります。データ保持が無効になっている場合は、カタログ未登録のアプリケーションの詳細を表示できません。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。

ヒント: ライセンスコンプライアンスについては、ライセンスコンプライアンス ページに移動してください。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンス情報の表示」を参照してください。

1. ソフトウェアカタログ リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。

2. スイートまたはアプリケーションの名前をクリックして、ソフトウェアカタログの詳細 ページを表示します。

このページには次のような情報が表示されます。

アイテム	説明
概要	
不許可	スイートまたはアプリケーションが「不許可」としてマーク付けされているかどうかを示します。アプリケーションを「不許可」としてマーク付けすると、アプリケーションがエージェント管理対象デバイスで実行されないようになります。
メータリング有効	スイートまたはアプリケーションのメータリングが有効になっているかどうかを示します。アプリケーションのメータリングが有効になっている場合は、メータリングも有効になっているエージェント管理対象デバイスについて使用率データが収集されます。詳細については、「デバイスとアプリケーションに対するメータリングの有効化および設定」を参照してください。
インストール済み	スイートまたはアプリケーションをインストールしているエージェント管理対象デバイスの数。
ライセンス	スイートまたはアプリケーションに関連付けられたライセンス資産の数。
期限切れライセンス	スイートまたはアプリケーションに関連付けられた期限切れライセンス資産の数。
ライセンスコンプライアンスから除外	ライセンスコンプライアンス ページにスイートまたはアプリケーションを表示するかどうかを示します。
レポートから除外	選択したレポートにスイートまたはアプリケーションを表示するかどうかを示します。
プロパティ	
発行元	スイートまたはアプリケーションの発行元。この情報は、レポート作成が正確に行われるように標準化されます。例えば、「Microsoft Corp.」と「Microsoft Inc.」は、どちらも「Microsoft Corporation」としてレポートされます。
プラットフォーム	スイートまたはアプリケーションの動作対象オペレーティングシステム。例えば、「Windows」などです。

アイテム	説明
ソフトウェアタイプ	スイートまたはアプリケーションが Microsoft Word などの個別のアプリケーションであるか、Microsoft Office などのアプリケーションのスイートであるかを示します。
発行元のライセンスタイプ	推奨されるスイートまたはアプリケーションのライセンスタイプ。
カテゴリ	ソフトウェアカタログチームが作成した、スイートまたはアプリケーションのカテゴリ。 ローカルカタログ登録済みのアプリケーションの場合、カタログ登録要求が送信されたときに指定されます。
アプリケーション ID またはスイート ID	スイートまたはアプリケーションを識別するコード。
一般向け	スイートまたはアプリケーションがお客様に最初にリリースされた日付。
ライフサイクル終了	スイートまたはアプリケーションのサポートが終了した日付。
MSRP（$）	スイートまたはアプリケーションの製造元希望小売価格。
メータリングを有効化	スイートまたはアプリケーションのメータリングが有効化された日付と時刻。
インストール済みバージョンまたはインストール済みアプリケーション	
ファイル名	アプリケーションの場合、実行可能ファイルの名前。
製品名	スイートの場合、スイート名。
バージョン	スイートまたはアプリケーションに関連付けられたバージョン番号。
カテゴリ	ソフトウェアカタログチームが作成した、スイートまたはアプリケーションのカテゴリ。 ローカルカタログ登録済みのアプリケーションの場合、カタログ登録要求が送信されたときに指定されます。
言語	スイートまたはアプリケーションの対象言語。例えば、英語などです。特定の言語向けに設計されていないアプリケーションは、「言語非依存」に指定されます。

アイテム	説明
インストール済み	スイートまたはアプリケーションがインストールされた管理対象デバイスの数。数字をクリックして、デバイスの情報を表示します。
App-V	アプリケーションをデバイスにインストールせずにそれらのアプリケーションを管理するMicrosoft Application Virtualization（App-V）を参照してください。
関連付けられたファイル	選択したバージョンに関連付けられており、ソフトウェアカタログに添付された1つまたは複数のファイル。ファイルを添付するには、＋をクリックし、ファイルの場所を選択します。必要に応じて、添付ファイルを編集または削除することができます。 • ファイルをソフトウェアバージョンに関連付けるには、ファイルブラウザを使用してファイルに移動します。 • または、大きいファイルの場合は、SAMBA共有を使用します。 • ファイルに関するメモを提供します。例えば、スクリプトホスト5.8 - 8.6またはスクリプトホスト5.8 - x64などです。 • ファイルをレプリケーション共有にコピーするには、**関連付けられたファイルの複製**チェックボックスをオンにしていることを確認します。
複製日	ファイルがレプリケーション共有にコピーされているかどうかを示します。
メモ	添付ファイルについてのメモ（入力されている場合）。
ライセンス	スイートまたはアプリケーションにライセンス資産が追加されている場合にのみ使用可能です。
名前	ライセンス名（「**Office Professional PO #1234**」など）。これは資産を検索するために使用される名前です。1つのアプリケーションに対して複数のライセンスを関連付ける場合は、注文書番号または購入日を追加しておくと効果的です。
数	ライセンスによって許諾されるインストール数またはシート数。例えば、「50」と表示されます。
モード	ライセンス資産のモード。モードは、**管理者コンソール**の ダッシュボード に表示される「ライセンスコンプライアンス」グラフで使用されます。Asset Detail（資産詳細）ページで無視にマーク付けされた値は、100% の使用レベルで表示されます。

アイテム	説明
キー、単価、有効期限	ライセンスに関する追加の情報。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
ベンダー	スイートまたはアプリケーションに関連付けるベンダー資産の名前。ベンダー資産を追加していない場合は、ベンダー ドロップダウンリストに何も表示されません。ベンダーを検索するには、リストに入力を開始します。
注文番号	ライセンスに関連付けられた注文書番号。
購入日	ライセンスを取得した日付。フィールド内をクリックし、カレンダーで日付を選択します。
メータリング	
前回使用日（日前）	過去 24 時間にスイートまたはアプリケーションを起動した管理対象デバイスの数。
1〜7	過去 7 日間にスイートまたはアプリケーションを起動した管理対象デバイスの数。
8〜30	8 日前から 30 日前の間にスイートまたはアプリケーションを起動した管理対象デバイスの数。
31〜90	31 日前から 90 日前の間にスイートまたはアプリケーションを起動した管理対象デバイスの数。
未使用	過去 90 日間にスイートまたはアプリケーションを起動しなかった管理対象デバイスの数。

ソフトウェアカタログへのアプリケーションの追加

Questは、その広範なデータウェアハウスを確認し、必要に応じて新しいアプリケーションをソフトウェアカタログに自動的に追加します。あるアプリケーションがまだカタログに表示されていない場合は、Questカタログチームにカタログ登録要求を送信して検討を依頼することができます。

カタログ登録要求は、ソフトウェアカタログに含まれていないアプリケーション（カタログ未登録）をパブリックのソフトウェアカタログに追加するよう要求するために送信できるフォームです。Questがカタログ登録要求を受け取ると、その要求が評価され、アプリケーションを公開ソフトウェアカタログに含めるべきかどうかが決定されます。さらに、カタログ登録要求が送信されると、アプリケーションが自動的にアプライアンス上のローカル版のソフトウェアカタログに追加されます。

組織でのみ使用するアプリケーションがあり、それらをパブリックのソフトウェアカタログに追加しない場合は、代わりにローカル版のソフトウェアカタログに追加します。詳細については、「カタログ登録要求の送信」を参照してください。

カタログ登録要求の送信によるローカルのソフトウェアカタログへの自動的なアプリケーションの追加

アプリケーションのカタログ登録要求を送信すると、即時にアプライアンスのローカル版のソフトウェアカタログにアプリケーションが自動的に追加されます。

その後、そのアプリケーションはローカルカタログ登録済みのアプリケーションとなり、そのアプリケーションに対してメータリング、「不許可」としてのマーク付け、およびライセンス資産との関連付けを行うことができます。

アプライアンスで組織コンポーネントが有効化されている場合は、任意の組織からカタログ登録要求を送信できます。タイトルは即時にローカルのアプライアンスソフトウェアカタログに追加されます。これはすべての組織で使用できます。

重要: カタログ登録要求は、カタログ未登録のアプリケーションのデータ保持が組織に対して有効である場合にのみ送信できます。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。

ローカルカタログ登録済みのアプリケーションがカタログ登録済みのアプリケーションに変更される仕組み

ローカルカタログ登録済みのアプリケーションは、パブリック版のソフトウェアカタログに追加されると、カタログ登録済みのアプリケーションに変更されます。

ローカルカタログ登録済みのアプリケーションは、次の場合にパブリック版のソフトウェアカタログに追加されます。

- お客様が、Quest KACEカタログチームにカタログ登録要求を送信し、アプリケーションのソフトウェアカタログ登録が許可された場合。
- 別のお客様が、Quest KACEカタログチームにカタログ登録要求を送信し、アプリケーションのソフトウェアカタログ登録が許可された場合。
- ソフトウェアカタログチームが率先してアプリケーションをソフトウェアカタログに追加した場合。

アプリケーションが登録されているソフトウェアカタログがアプライアンスで更新された場合、アプリケーションの名前が変更されることがあります。例えば、カタログ登録済みアプリケーションの特性（実行ファイルの名前、ファイルサイズ、バージョンなど）が、ローカルカタログ登録済みアプリケーションの特性と一致する場合、ローカルの情報は、カタログの情報に置き換えられます。アプリケーションの名前は一致するが、ファイルサイズなどの情報が大きく異なる場合、ローカルカタログの情報が置き換えられずに、新しいアプリケーションが追加されます。

つまり、パブリックのソフトウェアカタログの情報は、常にローカルカタログの情報よりも優先されます。パブリックのソフトウェアカタログのアプリケーションと一致するローカルカタログのアプリケーションは、パブリックのソフトウェアカタログのエントリに置き換えられます。ただし、これによって、アプリケーションに追加した情報（ライセンス情報など）が影響を受けることはありません。メータリングや「不許可」などの設定が変更されることもありません。

ローカルカタログ登録済みのアプリケーションがソフトウェアカタログに追加されたときにカスタムの名前が解決される仕組み

アプリケーション名は、カスタムアプリケーションがパブリックのソフトウェアカタログに追加されると標準化される場合があります。

ローカルのアプリケーションにカスタムの名前を使用している場合、そのアプリケーションがパブリックのソフトウェアカタログに追加されたときに、カスタムの名前が標準の名前に置き換えられます。例えば、**Updater** と

いう名前のアプリケーションがパブリックのカタログになかった場合、そのアプリケーションのローカルエントリを作成できます。そのアプリケーションに **MyUpdater** と名前を付けることができます。そのアプリケーションは、ローカルのカタログで **MyUpdater** として表示されます。ただし、その後、そのアプリケーションがパブリックのカタログに追加され、正式名称が決定して **RealTime Updater** という名前が付けられた場合、パブリックのカタログが更新されたときに **MyUpdater** という名前が **RealTime Updater** に置き換えられます。この名前変更によって、メータリング、ライセンス、または履歴の設定が影響を受けることはありません。ただし、以前のアプリケーション名に基づいたカスタムビューまたは検索条件がある場合、そのビューまたは検索条件を引き続き使用するには、それらを更新する必要があります。

カタログ登録要求の送信

必要に応じて、カタログ未登録のアプリケーションのカタログ登録要求を送信することができます。要求は継続的に処理されて、Quest KACEソフトウェアカタログチームの独自の判断で許可または拒否されます。

カタログ未登録のソフトウェアのデータ保持が有効になっています。データ保持が無効になっている場合は、カタログ登録要求を送信できません。詳細については、「管理者レベルまたは組織固有の一般設定項目の設定」を参照してください。

既にカタログに登録されているアプリケーションの実行可能サポートファイルなど、一部のアプリケーションはカタログに登録することができません。また、カタログ未登録のアプリケーションに複数のバージョンがある場合、バージョンごとに個別にカタログ登録要求を送信する必要があります。複数の実行可能ファイルと1つのカタログ登録要求を関連付けることはできません。

ヒント: インベントリデータを Quest と共有することによって、カタログ登録要求のプロセスの改善に役立てることができます。ソフトウェアカタログチームはこのデータを使用して、新しいアプリケーションを特定し、アプリケーションの名前とバージョンを標準化します。詳細については、「データ共有の基本設定の構成」を参照してください。

1. ソフトウェアカタログ リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. 左側のリストの上にある**カタログ未登録** タブをクリックします。
3. アプリケーション名をクリックして、ソフトウェアの詳細 ページを表示します。
4. **カタログに追加** をクリックして、カタログに追加 フォームを表示します。
5. 次の情報を入力します。

オプション	説明
ソフトウェアタイトル	アプリケーションの識別に使用する名前。詳細については、「ローカルカタログ登録済みのアプリケーションがソフトウェアカタログに追加されたときにカスタムの名前が解決される仕組み」を参照してください。
カテゴリ	アプリケーションのカテゴリ。カテゴリはアプリケーションを整理および管理する場合に便利です。

6. 次のように、共有オプションを選択し、連絡先情報を指定します。

オプション	説明
共有	カタログ登録オプション： • **Add software title to this appliance and share with the Quest KACE catalog**（ このアプライアンスにソフトウェアタイトルを追

オプション	説明
	加して Quest KACE カタログと共有する）：Questに要求を送信し、ローカル版のソフトウェアカタログにタイトルを追加します。 • **Add software title to this appliance only**（このアプライアンスのみにソフトウェアタイトルを追加する）：ローカル版のソフトウェアカタログにタイトルを追加しますが、Quest KACEソフトウェアカタログにはタイトルを送信しません。
連絡先の詳細	お客様の連絡先情報を入力します。ソフトウェアカタログチームは、要求に関して質問がある場合にこの情報を使用してお客様に連絡します。

7. **保存** をクリックします。

カタログ登録要求がQuestに送信されます。**Software Catalog Detail**（ソフトウェアカタログの詳細）ページにローカルソフトウェアカタログから削除 というボタンが表示されます。カタログ登録要求がパブリックのソフトウェアカタログに追加され、アプライアンスでカタログが更新されると、**ソフトウェアカタログの詳細** ページのローカルソフトウェアカタログから削除 ボタンが表示されなくなります。カタログ登録要求の追跡は、現在利用できません。

注: パブリックのカタログに追加されるタイトルの情報は、最初に送信された情報とは異なる場合があります。これは、タイトルがパブリックのカタログに追加される際に標準化されることが原因です。

カタログ登録要求のキャンセルおよびローカルカタログ登録の削除

一定の条件が満たされている場合は、カタログ登録要求をキャンセルし、ローカルのソフトウェアカタログからアプリケーションを削除することができます。

- アプリケーションにライセンス資産が関連付けられていない。カタログからアプリケーションを削除する前に、ライセンス資産からアプリケーションを削除する必要があります。
- アプリケーションがソフトウェアカタログチームに許可されていない、またはパブリックのカタログに追加されなかった。例えば、要求を送信し、同じ日にその要求をキャンセルした場合、ソフトウェアカタログチームがその要求を許可している可能性が低くなるため、要求がキャンセルされる可能性があります。ただし、要求を送信し、数日または数週間後にその要求をキャンセルした場合、ソフトウェアカタログチームが既に要求を許可し、パブリックのソフトウェアカタログにそのタイトルが含まれている可能性があります。この場合、カタログ登録要求はキャンセルできません。

削除できるのは、ローカルカタログ登録済みのアプリケーションのみです。カタログ登録済みのアプリケーションをカタログから削除することはできません。

1. ソフトウェアカタログ リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. アプリケーション名をクリックして、ソフトウェアカタログの詳細 ページを表示します。
3. アプリケーションがライセンス資産に関連付けられている場合は、次の手順を実行します。
   a. Software Catalog Detail（ソフトウェアカタログの詳細）ページの ライセンス セクションで、ライセンス資産の名前をクリックして、License Asset Detail（ライセンス資産の詳細）ページを表示します。

b. カタログ登録済みソフトウェアへの適用 フィールドで、アプリケーションの名前を選択し、**削除** をクリックします。
c. **保存** をクリックします。

4. ソフトウェアカタログの詳細 ページに戻ります。
5. **ローカルソフトウェアカタログから削除** をクリックします。

ローカル版のソフトウェアカタログからタイトルが削除され、**Software Catalog Detail**（ソフトウェアカタログの詳細）ページに カタログに追加 ボタンが表示されます。

ソフトウェアカタログのアプリケーションに関するライセンス資産の管理

ライセンス資産は、ソフトウェアカタログのアイテムと ソフトウェア ページにリストされたアイテムのいずれかと関連付けることができます。ただし、ソフトウェアカタログのアイテムと ソフトウェア ページのアイテムの両方を同時に関連付けることはできません。

既存のライセンス資産がある場合、それらのライセンス資産を ソフトウェア ページのアイテムから ソフトウェアカタログ ページのアイテムに移行することができます。これにより、ソフトウェアカタログで使用可能な機能（ライセンスコンプライアンスなど）を利用できるようになります。詳細については、「ソフトウェアカタログのアプリケーションへのライセンス資産の移行」を参照してください。

ソフトウェアカタログ インベントリのライセンス資産の追加

アプリケーションのライセンス資産をソフトウェアカタログインベントリに追加できます。ライセンス資産を追加すると、ライセンスコンプライアンス リストおよびライセンスコンプライアンス ダッシュボード ウィジェットにライセンスコンプライアンス情報を表示できます。

ソフトウェアカタログのアプリケーションは、検出済み、未検出、Locally Cataloged（ローカルカタログ登録済み）のいずれかに分類する必要があります。カタログ未登録 に分類されたアプリケーションのライセンス資産を追加することはできません。

ライセンス資産をアプリケーションに関連付けると、Software Catalog Detail（ソフトウェアカタログの詳細）ページにライセンス情報を表示することもできます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のライセンス情報を個別に管理します。

ヒント: 複数のアプリケーションのライセンス資産を一度に追加するには、その情報をスプレッドシートまたは CSV ファイルからインポートできます。詳細については、「例：作成済みスプレッドシートからのライセンスデータのインポート」を参照してください。

1. ソフトウェアカタログ リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. アプリケーションの名前をクリックして、ソフトウェアカタログの詳細 ページを表示します。
3. ページの一番下付近で **新しいライセンスの追加** をクリックして、ライセンス資産詳細 ページを表示します。
4. ライセンス資産の詳細 ページの 全般 タブで次の情報を入力します。

オプション	説明
サブタイプ	ライセンスに関連付ける資産サブタイプ。詳細については、「資産サブタイプ、カスタムフィールド、

オプション	説明
	およびデバイス詳細基本設定について」を参照してください。
資産ステータス	ライセンスステータス（該当する場合）。デフォルトの資産ステータス、またはカスタムの資産ステータスを選択できます（存在する場合）。アプライアンスのデフォルトのインストールには、以下の資産ステータスが含まれます。 • **アクティブ**：展開済み、アクティブ、または使用中である任意の資産。 • **廃棄済み**：利用できなくなった資産。 • **期限切れ**：期限切れのソフトウェアライセンスまたは契約資産。 • **在庫**：最近受け取った資産。 • **不在**：場所を特定できない資産。 • **修復**：修復されている資産。 • **予約済み**：特定の人または用途のために確保されている資産。 • **廃止**：ライフサイクル終了状態に達した、または使用されなくなった資産。 • **盗難**：盗難されたとして報告された資産。 詳細については、「資産のライフサイクル設定の表示と設定」を参照してください。
場所	資産がある場所の名前。詳細については、「場所の管理」を参照してください。
名前	ライセンス名（「**Office Professional PO #1234**」など）。これは資産を検索するために使用される名前です。1 つのアプリケーションに複数のライセンスを関連付ける場合は、それらのライセンスを区別するために、以下のフィールドに注文書番号または購入日を指定します。
ライセンス数	ライセンスによって許諾されるインストール数またはシート数。例えば、「50」と表示されます。
カタログ登録済みソフトウェアへの適用	ライセンスを適用する、ソフトウェアカタログインベントリ内のアプリケーション。必要に応じて、ソフトウェアカタログの複数のアプリケーションにライセンス資産を関連付けることができます。ただし、ライセンス資産を同じアプリケーションの複数のバージョンに関連付ける必要はありません。アップグレードおよびダウングレードをサポートするためにアプライアンスがこれを自動的に行うからです。ライセンス情報を追加するときに、現在のバージョンをライセンス資産に関連付けるだけです。 また、Microsoft Office や Adobe Acrobat などの別の発行元からアプリケーションを同じライセンス資産に割り当てた場合は、ライセンス資産に指定されて

オプション	説明
	いるシートの総数が各アプリケーションに割り当てられます。例えば、ライセンス資産に 100 個のシートがある場合、Microsoft Office と Adobe Acrobat の両方に 100 個のシートが割り当てられます。
ソフトウェアへの適用	このフィールドは空白のままにします。ソフトウェアカタログ インベントリと ソフトウェア ページインベントリのアプリケーションに対して、同時に1つのソフトウェアライセンスを関連付けることはできません。カタログ登録済みソフトウェアに対してライセンス資産を作成する方法の詳細については、ソフトウェア ページインベントリのライセンス資産の追加を参照してください。
ライセンスモード	ライセンス資産のモード。ライセンスを必要とし、ライセンスコンプライアンス ページにライセンス使用率情報を表示するアプリケーションの場合、Enterprise（エンタープライズ）または Unit License（ユニットライセンス）のいずれかを選択します。 **注:** ライセンスコンプライアンスでは、Not Specified（指定なし）、Client License（クライアントライセンス）、サブスクリプション、Shareware（シェアウェア）、Freeware（フリーウェア）、OpenSource（オープンソース）、No Licensing（ライセンスなし）、Site License（サイトライセンス）などほとんどのモードが使用されません。 ライセンスモードは、**管理者コンソール**の次のセクションで使用されます。 • ライセンスコンプライアンス リスト。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンス情報の表示」を参照してください。 • Dashboard（ダッシュボード）に表示されるライセンスコンプライアンス グラフ。Asset Detail（資産詳細）ページで無視にマーク付けされた値は、100% の使用レベルで表示されます。詳細については、「ダッシュボードのウィジェットについて」を参照してください。

5. **次へ** をクリックします。
6. ライセンス資産の詳細 ページの 購入 タブで次の情報を入力します。

オプション	説明
契約	ライセンスに関連付けられている契約資産。
カタログ登録済みソフトウェアへの適用	ライセンスを適用する、ソフトウェアカタログインベントリ内のアプリケーション。必要に応じて、ソフトウェアカタログの複数のアプリケーションにライセンス資産を関連付けることができます。ただし、ライセンス資産を同じアプリケーションの複数

オプション	説明
	のバージョンに関連付ける必要はありません。アップグレードおよびダウングレードをサポートするためにアプライアンスがこれを自動的に行うからです。ライセンス情報を追加するときに、現在のバージョンをライセンス資産に関連付けるだけです。 また、Microsoft Office や Adobe Acrobat などの別の発行元からアプリケーションを同じライセンス資産に割り当てた場合は、ライセンス資産に指定されているシートの総数が各アプリケーションに割り当てられます。例えば、ライセンス資産に 100 個のシートがある場合、Microsoft Office と Adobe Acrobat の両方に 100 個のシートが割り当てられます。
プロダクトキー	ライセンスに関連付けられているプロダクトキー。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
単価	ライセンスに関連付けられている単価。ライセンス資産タイプについて取得可能なデフォルト情報は、修正および編集可能です。
ベンダー	アプリケーションに関連付けるベンダー資産の名前。ベンダー資産を追加していない場合は、Vendor（ベンダー）ドロップダウンリストに何も表示されません。ベンダーを検索するには、リストに入力を開始します。 **注:** ライセンスコンプライアンス情報が不正確になることがあるため、単一のソフトウェアライセンス資産に複数のベンダーを割り当てることはお勧めしません。
注文書番号	ライセンスに関連付けられた注文書番号。
購入日	購入した日付。フィールド内をクリックし、カレンダーで日付を選択します。
購入	このライセンスに関連付けられている購入レコードを 1 つ以上選択します。詳細については、「購入レコードの管理」を参照してください。

7. **次へ** をクリックします。
8. ライセンス資産の詳細 ページの メンテナンス タブで次の情報を入力します。

オプション	説明
アップグレード権を含む	ライセンスにアップグレード権が含まれるかどうかを示します。アップグレード権とは、ライセンス済みソフトウェアの新しいバージョンが利用可能になったときに、その新しいバージョンにアップグレードできる資格があることを意味します。詳細については、「ライセンスのアップグレードについて」を参照してください。次のいずれかのオプションを選択します。 • **はい**: アップグレード権は、選択したソフトウェアの既存のライセンス数と、それと同

オプション	説明
	ーのソフトウェアで利用可能な、より新しいバージョンのライセンス数を比較することによって計算されます。 • **はい - リストから選択**: アップグレード権を付与するソフトウェアバージョンを1つまたは複数選択します。アップグレードソフトウェアリスト の下で、**追加するカタログ登録済みソフトウェアの選択** をクリックします。選択したソフトウェアにおいて、ライセンスをアップグレードすることが可能なより新しいバージョンのリストが表示されます。リスト内のエントリを選択すると、選択した内容が アップグレードソフトウェアリスト ボックスに表示されます。必要に応じて、1つまたは複数のバージョンを追加できます。リストからアイテムを削除するには、アップグレードソフトウェアリスト ボックスでそのアイテムを選択して、**削除** をクリックします。 • **いいえ**: 選択したソフトウェアにアップグレード権を付与しない場合は、このオプションを選択します。
Includes Maintenance（メンテナンスを含む）	ライセンスがユーザーにアプリケーションのインストールバージョンをアップグレードする権利を与えているかどうか。詳細については、「ソフトウェアカタログのアプリケーションに関するライセンスコンプライアンスについて」を参照してください。
有効期限日	ライセンスにメンテナンスが含まれている場合は、メンテナンス期間の有効期限。 アプライアンスライセンスコンプライアンス機能は、アプリケーションリリース日などソフトウェアカタログ情報を利用します。メンテナンス期間中に新規アプリケーションバージョンをリリースした場合、そのバージョンは自動的にこのライセンス資産の対象範囲になります。
ダウングレード権を含む	ライセンスにダウングレード権が含まれるかどうかを示します。ダウングレード権とは、ソフトウェアの新しいバージョンを同じソフトウェアの古いバージョンにダウングレードするライセンスを適用する資格があることを意味します。詳細については、「ライセンスのダウングレードについて」を参照してください。次のいずれかのオプションを選択します。 • **はい**: ダウングレード権は、選択したソフトウェアの既存のライセンス数と、それと同一のソフトウェアで利用可能な、より古いバージョンのライセンス数を比較することによって計算されます。 • **はい - リストから選択**: ダウングレード権を付与するソフトウェアバージョンを1つまたは複数選択します。ダウングレードソフトウェアリスト の下で、**追加するカタログ登録済みソ**

オプション	説明
	フトウェアの選択 をクリックします。ライセンスをダウングレードすることが可能な、選択したソフトウェアのより古いバージョンのリストが表示されます。リスト内のエントリを選択すると、選択した内容が ダウングレードソフトウェアリスト ボックスに表示されます。必要に応じて、1つまたは複数のバージョンを追加できます。リストからアイテムを削除するには、ダウングレードソフトウェアリスト ボックスでそのアイテムを選択して、**削除** をクリックします。 • **いいえ**: 選択したソフトウェアにダウングレード権を付与しない場合は、このオプションを選択します。

9. **次へ** をクリックします。
10. ライセンス資産の詳細 ページの 関連 タブで次の情報を入力します。

オプション	説明
部門	アプリケーションを所有するビジネスグループまたは部門。
コストセンター	アプリケーションを所有する部門に関連付けられたコストセンター。
承認されたデバイス	ライセンスの使用を承認されたデバイス。この情報は、ライセンスコンプライアンスレポートの作成に使用されます。例えば、対象のアプリケーションをインストールしたデバイスが、承認されたデバイスのリストに存在しない場合、それらのデバイスは「未承認のソフトウェアインストール」というタイトルのレポートで報告されます。ただし、アプライアンスは、ライセンスコンプライアンスを強制しません。例えば、ライセンスが期限切れであったり、コンプライアンスから外れていたとしても、管理対象デバイスへのアプリケーションのインストールがアプライアンスによって阻止されることはありません。
バーコード	必要に応じて、このライセンスに関連付けられたバーコードを追加または編集します。詳細については、「資産へのバーコードの追加」を参照してください。

11. **次へ** をクリックします。
12. ライセンス資産の詳細 ページの カスタム タブで、追加のカスタムデータを入力します。ビジネス目標に合わせて、ライセンス資産タイプを修正し、必要な数のフィールドを追加することができます。詳細については、「資産タイプの追加またはカスタマイズ」を参照してください。
13. **次へ** をクリックします。
14. ライセンス資産の詳細 ページの メモ タブで、次の情報を入力します。

オプション	説明
メモ	任意の追加情報を入力します。

オプション	説明
ライセンステキスト	ライセンスナンバーなどライセンスに関する補足情報。

15. **保存** をクリックします。

    ライセンス ページに新しいライセンス資産が表示されます。ライセンス数 の数値は、資産を更新するまでは変更されません。ただし、対象のソフトウェアをインストールされた管理対象デバイスがアプライアンスにチェックインすると、インストール済み 列の数値が変更されます。これにより、購入およびインストール済みのライセンス数を追跡できます。

次のオプションのタスクを実行します。

- ソフトウェアカタログインベントリに対するメータリングを有効化します。メータリングが有効になっているときは、過去 90 日にアプリケーションが使用されていたかどうかが ライセンスコンプライアンス ページに表示されます。詳細については、「ソフトウェアメータリングについて」を参照してください。
- ライセンス使用率警告しきい値を設定します。これらのしきい値は、ライセンスコンプライアンス ダッシュボード ウィジェットでライセンスコンプライアンスの問題を識別するために使用されます。

ソフトウェアカタログのアプリケーションへのライセンス資産の移行

既存のライセンス資産がある場合に、ライセンス資産を ソフトウェア ページのアプリケーションから ソフトウェアカタログ ページのアプリケーションに移行または転送することができます。これにより、ソフトウェアカタログで使用可能な拡張機能を利用できるようになります。

ライセンスを移行するには、ソフトウェア リストのアプリケーションから、ライセンスの割り当てを ソフトウェアカタログ リストのアプリケーションに変更します。

ライセンス資産は、ソフトウェアカタログ リストのアプリケーションと ソフトウェア リストのアプリケーションのいずれかと関連付けることができます。ただし、両方のタイプのアプリケーションと同時に関連付けることはできません。

1. 資産 リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
2. ソフトウェア リストのアプリケーションに関連付けられているライセンスの名前をクリックして、License Asset Detail（ ライセンス資産の詳細 ）ページを表示します。

    ソフトウェアカタログアイテムに適用するためにライセンスを転送する必要があることを示す注意書きがセクション上部に表示されます。
3. セクション上部で、**今すぐ転送** をクリックします。
4. Applies to Cataloged Software（ カタログ登録済みソフトウェアへの適用 ）セクションで、ライセンスと関連付けるアプリケーションを選択します。
5. ページの一番下で **保存** をクリックします。

管理対象インストールとカタログ登録済みソフトウェアの関連付け

1 つまたは複数の管理対象インストールをソフトウェアカタログアイテムに追加して、エンドユーザーデバイスへのこれらのアプリケーションの展開を管理できます。

1. ソフトウェアカタログ リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. アプリケーションの名前をクリックして、ソフトウェアカタログの詳細 ページを表示します。
3. ページの下方で、次のいずれかのボタンをクリックします。
    - 管理対象インストールを使用して選択したソフトウェアカタログをインストールするには、**新しい管理対象インストールの追加**。
    - 管理対象インストールを使用して選択したソフトウェアカタログをアンインストールするには、**新しい管理対象アンインストールの追加**。
4. 表示される 管理対象インストールの詳細 ページで、該当する詳細を指定します。詳細は、以下のセクションを参照してください。
    - Windowsデバイス用の管理対象インストールの作成
    - Mac OS Xデバイス用の管理対象インストールの作成
    - RPMファイル用の管理対象インストールの作成

ソフトウェアメータリングの使用

KACE アプライアンスを使用してソフトウェアメータリング情報を管理できます。

ソフトウェアメータリングについて

ソフトウェアメータリングにより、管理対象のWindowsデバイスおよびMacデバイス上での、アプリケーションのインストール状況および使用状況に関する情報を収集することができます。

情報収集には、Bingトラベルなどの Windowsストアのアプリケーションが含まれます。Linuxなど他のオペレーティングシステムにインストールされたアプリケーションに対しては、メータリングを使用できません。メータリングは、ソフトウェアカタログで「検出済み」および「未検出」と表示されているアプリケーション、およびローカルカタログに登録されているアプリケーションに対して有効にすることができます。オペレーティングシステムソフトウェア、サポートされないオペレーティングシステム（ Linuxなど ）にインストールされたアプリケーション、またはソフトウェアカタログ内で「カタログ未登録」としてリストされているアプリケーションに対しては、メータリングを有効にできません。

クラシックメータリングについて

クラシックメータリングは、バージョン 5.5 より前のアプライアンスで提供されていたメータリングシステムです。5.4 以下のバージョンからバージョン 5.5 にアップグレードした場合でも、アップグレード前にメータリングを有効にしていた場合は、引き続き、5.5 リリースでクラシックメータリングにアクセスすることができます。

ただし、クラシックメータリングよりも詳細な情報を提供するソフトウェアカタログのメータリングシステムが、クラシックメータリングに代わって6.0リリースで導入されました。クラシックメータリングは、バージョン6.0以降では使用できなくなりました。

メータリング情報について

アプリケーションのメータリングを有効にすると、アプリケーションがインストールされているデバイスもメータリングが有効な場合は、それらのデバイスの情報が収集されます。

次の情報が収集されます。

- バージョン情報
- スイートに関する情報
- インストール数
- 使用および起動に関する情報

詳細については、「ソフトウェアカタログのメータリング情報の表示」を参照してください。

また、メータリング情報を収集する頻度およびメータリング情報を保持する時間の長さを設定できます。詳細については、「ソフトウェアカタログのアプリケーションに対するメータリングのオプション設定」を参照してください。

メータリング情報を収集するスクリプトについて

ソフトウェアメータリングサービスは、KACE エージェントにバンドルされており、管理対象デバイスにインストールされています。メータリングを有効にすると、スクリプトが実行され、メータリング情報が収集されます。

これらの収集スクリプトは、オペレーティングシステムによって異なります。

- **Windows**: Windowsデバイスでのメータリングは、WMI（Windows Management Instrumentation）イベントを使用してWindows資産を監視するイベントドリブン方式のプロセスです。
- **Mac**: Macデバイスのメータリングスクリプトは、NSWorkspaceの通知センターを使用して、プロセスのイベントを非同期的に識別します。

アプリケーションファイル名、バージョン、ファイルサイズなどの情報が、「ソフトウェアカタログ」の情報と比較され、アプリケーションが識別されます。

スイートのメータリング方法

Microsoft Officeなどのスイートに対してメータリングが有効になっている場合、システムは、メータリングが有効になっている管理対象デバイスで、スイートのアプリケーションが実行されているかどうかを判断するためにチェックを行います。スイート全体、および各アプリケーションの使用率情報がレポートされます。

スイートのいずれかのアプリケーションがインストールされている管理対象デバイス（プログラムの追加と削除のエントリによって判定）は、スイートがインストールされているデバイスとしてカウントされます。スイート内のすべてのアプリケーションがデバイスにインストールされていなくても、スイートがインストールされているデバイスとしてカウントされます。

スイートに対してメータリングが有効化されていると、スイートに含まれる各アプリケーションもメータリングすることができます。スイートに含まれるアプリケーションごとにメータリングを有効または無効にすることはできません。

デバイスとアプリケーションに対するメータリングの有効化および設定

ソフトウェアカタログのアプリケーションに関するメータリング情報を取得するには、それらのアプリケーション、およびそれらのアプリケーションがインストールされているデバイスのメータリングを有効にする必要があります。

メータリングするデバイスおよびアプリケーションの選択

デバイス上でメータリングを有効化しても、メータリング情報の取得が可能となるのみで、サーバーやネットワークの活動が大幅に増大することはありません。

したがってQuestでは、管理対象のすべてのWindowsおよびMacデバイスに対してメータリングを有効にすることをお勧めします。しかしながら、メータリングするアプリケーションの選択は慎重に行ってください。メータリング情報を取得するアプリケーションが多すぎると、ディスク容量が大幅に消費され、システムのパフォーマンスに影響が出ます。

デバイスのメータリングの有効化

管理対象デバイスでソフトウェアメータリングを有効にするには、メータリングが有効なラベルをデバイスに適用する必要があります。

メータリングが有効なラベルをデバイスに適用するには、次のいずれかを行います。

- デバイスに対して、「メータリングしたデバイス」という組み込みラベルを適用します。このラベルはメータリングオプションが有効になっています。詳細については、「アイテムのグループを管理するためのラベルのセットアップおよび使用」を参照してください。
- メータリングの手動ラベルを作成し、デバイスに適用します。詳細については、「手動ラベルによるデバイスのメータリングの有効化」を参照してください。
- メータリングのSmart Labelを作成します（自動的にデバイスに適用されます）。詳細については、「Smart Labelによるデバイスのメータリングの無効化」を参照してください。

ヒント: 管理対象デバイスでメータリングを有効にするには、手動ラベルまたはSmart Labelを使用できますが、ラベルを必ず使用する必要があります。メータリングはラベルレベルでのみ有効にできます。各デバイスの設定で有効にすることはできません。

手動ラベルによるデバイスのメータリングの有効化

デバイスのメータリングを有効化するには、手動ラベルに対するメータリングを有効化してから、そのラベルをデバイスに適用します。

1. Smart Label リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
    c. ラベル管理 パネルで、**ラベル** をクリックします。
2. **アクションの選択 > 新しい手動ラベル** を選択して、ラベル詳細 ページを表示します。

    ヒント: ラベル名にはバックスラッシュ（\）を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して（\\）エスケープします。
3. 次の情報を入力します。

オプション	説明
名前	ラベルの名前。
説明	任意の追加情報を入力します。
代替の場所	（オプション）管理対象インストール、ファイル同期、およびこのラベルに割り当てられたアイテムに対して実行される他の展開のために用意された代替のダウンロード場所。指定した場所が文字列KACE_ALT_LOCATIONと置き換わります。 **注意: このフィールドに値を指定するラベルが2つある場合、1つのデバイスに両方のラベルを適用することはできません。**
パス	代替のダウンロード場所を指定する場合は、その場所へのパスを指定します。
ログイン **パスワード**	代替のダウンロード場所を指定する場合は、その場所のためのユーザー名およびパスワードを指定します。
ラベル使用の制限対象	ラベルのタイプ。メータリングを有効にするラベルを作成するには、デバイスインベントリ チェックボックスをオンにします。必要に応じて、追加のラベルタイプを選択することができますが、メータリングは「デバイス」ラベルタイプが選択されている場合に限り有効にすることができます。
ソフトウェアの使用のメータリング	ラベルが割り当てられたデバイスのメータリングを有効にします。この操作でメータリングが有効になるのは、そのデバイスのみです。ソフトウェアをメータリングするには、個々のアプリケーションのメータリングも有効にする必要があります。
アプリケーション制御を許可	デバイスでアプリケーション制御を有効にします。「不許可」と指定されたソフトウェアは、ラベルが適用されたデバイス上では実行できません。 詳細については、「アプリケーション制御の使用」を参照してください。
ラベルグループ	（オプション）ラベルが割り当てられるラベルグループ。ラベルをラベルグループに割り当てるには、ラベルグループ フィールドの隣にある **編集** をクリックし、ラベルグループを選択します。これは、多数のラベルをサブラベルに整理する場合に便利です。例えば、ライセンスされたアプリケーションの複数のラベルを「ライセンス」という名前のラベルグループに含めることができます。また、ラベルが属するグループの制限は、ラベルに継承されます。

4. **保存** をクリックします。

ラベル ページが表示され、新しいラベルがリストに表示されます。メータリングアイコンが、ラベルの隣にあるメータリング列に表示されます。。

5. 管理対象デバイスに手動でラベルを適用するには：
    a. **インベントリ** をクリックします。

        デバイス ページが表示されます。

    b. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
    c. **アクションの選択 > ラベル > ラベルの適用** を選択します。

        デバイス リストのデバイス名の隣に、下記のメータリングアイコンのいずれかが表示されます。

アイコン	説明
	デバイスに対してメータリングが有効化されており、KACE エージェントはメータリングが有効となっているソフトウェアカタログのアプリケーションに関するメータリング情報をレポートするようスケジュールされています。詳細については、「デバイスとアプリケーションに対するメータリングの有効化および設定」を参照してください。 メータリングの間隔に応じて、アプライアンスが**管理者コンソール**内にメータリング情報を表示するまでに 24 時間かかる場合もあります。メータリング間隔を変更するには、ソフトウェアカタログのアプリケーションに対するメータリングの有効化を参照してください。
	メータリングの開始がスケジュールされています。デバイスにメータリングラベルが適用されていて、かつそのデバイスがメータリング情報をアプライアンスにまだレポートしていない場合に、このアイコンが表示されます。Linuxなどのサポートされていないオペレーティングシステムを実行しているデバイスにメータリングラベルが適用されている場合には、このメータリングアイコンは表示されません。

Smart Labelによるデバイスのメータリングの有効化

Smart Labelを使用したメータリングの有効化は、Smart Labelがデバイスラベルである場合に限り可能です。

Smart Labelは、アプライアンスがデバイスインベントリを処理するときに、管理対象デバイスに対して適用または削除されます。そのため、デバイスでメータリングを有効化するSmart Labelを作成しても、Smart Labelがデバイスに対して適用されるまでに時間がかかることがあります。また、デバイスがメータリング情報をレポートするまでにも時間がかかる場合があります。デバイスがインベントリ設定され、Smart Labelが適用された後にのみ、Smart Labelの基準に一致するデバイスでメータリングが有効化されます。

1. Smart Label リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。

c. ラベル管理 パネルで、**Smart Label** をクリックします。

2. **アクションの選択 > 新規作成 > デバイスSmart Label** を選択して、デバイスSmart Label パネルを表示します。
3. 使用可能なフィールドを使用して検索条件を指定します。
   - **行を追加するには、行の追加 をクリックします。**
   - **ルールのサブセットを追加するには、Smart Label基準の右側にある 演算子 ドロップダウンリストで および または または を選択してから、グループの追加 をクリックします。**

4. **テスト** をクリックして、指定した条件に一致するアイテムを表示します。
5. 目的の結果が得られるまで、必要に応じて条件を調整します。
6. Smart Label 基準の下部にある メータリングを有効化 チェックボックスをオンにします。
7. ラベルの選択 ドロップダウンリストで、次の操作のいずれかを行います。
   - **Smart Labelに関連付ける既存のラベルを選択します。**ラベルの選択 **フィールドに入力し、既存のラベルを検索します。**

     注: ラベルの代わりにラベルグループを選択すると、Smart Label をパッチ適用スケジュールに適用できなくなります。パッチ適用スケジュールでは、1 つのアイテムに基づいた Smart Label のみを使用できます。

   - ラベルの選択 **フィールドにSmart Labelの新しい名前を入力し、EnterまたはReturnキーを押します。**

注: 新しいSmart Label名を入力したら、**Enter**または**Return**キーを押し、テキストを検索フィールドからラベルフィールドに移動します。

8. **Create** をクリックします。

管理対象デバイスがインベントリに設定されると、指定した条件に一致するデバイスにSmart Labelが適用されます。ラベルがデバイスに適用されると、デバイス リストのデバイス名の隣に下記のいずれかのメータリングアイコンが表示されます。

アイコン	説明
	デバイスに対してメータリングが有効化されており、KACE エージェントはメータリングが有効となっているソフトウェアカタログのアプリケーションに関するメータリング情報をレポートするようスケジュールされています。詳細については、「デバイスとアプリケーションに対するメータリングの有効化および設定」を参照してください。 メータリングの間隔に応じて、アプライアンスが**管理者コンソール**内にメータリング情報を表示するまでに 24 時間かかる場合もあります。メータリング間隔を変更するには、ソフトウェアカタログのアプリケーションに対するメータリングの有効化を参照してください。
	メータリングの開始がスケジュールされています。デバイスにメータリングラベルが適用されているが、アプライアンスでメータリング情報がまだ使用できない場合に、このアイコンが表示されます。Linuxなどのサポートされていないオペレーティングシステムを実行しているデバイスにメータリン

アイコン	説明
	グラベルが適用されている場合には、このメータリングアイコンは表示されません。

ソフトウェアカタログのアプリケーションに対するメータリングの有効化

ソフトウェアカタログで「検出済み」および「未検出」とリストされているアプリケーション、およびローカルカタログに登録されているアプリケーションに対してメータリングを有効にすることができます。アプリケーションのメータリングを有効にすると、そのアプリケーションはメータリング対象として識別されます。

ただし、そのアプリケーションがインストールされているデバイスのメータリングも有効にする必要があります。つまり、メータリング情報を取得するには、デバイスとアプリケーションの両方に対してメータリングを有効にする必要があります。

アプリケーション、およびアプリケーションがインストールされているデバイスのメータリングを有効にすると、そのアプリケーションの Software Catalog Detail（ソフトウェアカタログの詳細）ページにメータリング情報が表示されます。メータリング情報は、アプリケーションがインストールされている管理対象デバイスの詳細ページにも表示されます。詳細については、「ソフトウェアカタログのメータリング情報の表示」を参照してください。

注意: メータリングは、オペレーティングシステムソフトウェア、サポートされていないオペレーティングシステム（Linuxなど）にインストールされているアプリケーション、およびソフトウェアカタログで「カタログ未登録」と表示されているアプリケーションに対して使用することはできません。しかしながら、ローカルバージョンのソフトウェアカタログに未登録アプリケーションを追加すれば、その未登録アプリケーションに対してメータリングを有効にすることができます。

1. ソフトウェアカタログ リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. 「検出済み」または「未検出」のアプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択 > メータリングを有効にする** を選択します。

選択したアプリケーションの隣にあるメータリング列に、次のメータリングアイコンが表示されます：。アプリケーションがインストールされているデバイスのメータリングが有効になっている場合に限り、メータリングのスケジュールに従ってメータリング情報がレポートされます。詳細については、以下を参照してください。

- デバイスのメータリングの有効化
- ソフトウェアカタログのアプリケーションに対するメータリングのオプション設定

ソフトウェアカタログのアプリケーションに対するメータリングのオプション設定

メータリング情報を収集する頻度や、メータリング情報をアプライアンスデータベースに保持する時間の長さなど、メータリングオプションを設定できます。

アプライアンス上で組織コンポーネントが有効化されている場合は、組織ごとに設定を個別に構成します。

1. 次のいずれかを実行します。
    - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから システム を選択します。続いて、組織 をクリックします。組織の情報を表示するには、組織の名前をクリックします。**

表示される 組織の詳細 ページで、通信とエージェントの設定 セクションを探します。

- **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインします。次に、設定 > プロビジョニング を選択し、プロビジョニング パネルで 通信設定 をクリックします。**

  通信設定 ページが表示されます。

2. エージェントおよび通信設定 セクションで、各設定を次のように指定します。

オプション	設定案	メモ
エージェントのログ記録	有効	管理対象デバイスにインストールされたエージェントから提供されるスクリプト結果を、アプライアンスが保存するかどうか。エージェントログは、データベース内のディスク領域を最大約1 GB消費します。ディスク領域に問題がない場合は、エージェントのログ記録 を有効にして、エージェント管理対象デバイスのログ情報をすべて保持します。これらのログは、トラブルシューティング時に役立ちます。ディスク領域を節約し、エージェント通信を高速化するには、エージェントのログ記録 を無効にします。
エージェントインベントリ	12時間	管理対象デバイスのエージェントがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
エージェント不要インベントリ	1日	エージェント不要デバイスがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
カタログインベントリ	24時間	管理対象デバイスが ソフトウェアカタログ ページにインベントリをレポートする頻度。
メータリング	4時間	管理対象デバイスがアプライアンスにメータリング情報をレポートする頻度。デバイスとアプリケーションに対してメータリングを有効にする必要があります。
スクリプト更新	4時間	管理対象デバイスのエージェントが、管理対象デバイスで有効にされているスクリプトの更新されたコピーを要求する頻度。この間隔はスクリプトの実行頻度に影響を与えません。

3. **保存** をクリックします。
4. メータリングのデータ保持設定を設定するには、管理者レベルの 一般設定 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**設定** をクリックして、**一般設定** をクリックします。

5. Data Retention（データの保持）セクションで、アプライアンスにデータを保持するためのオプションを選択します。

オプション	説明
メータリング情報の保持	メータリング情報がアプライアンスデータベースに保持される月数。選択した月数よりも古いメータリング情報は、毎月初日にデータベースから削除されます。詳細については、「メータリング情報について」を参照してください。

6. アプライアンスで組織コンポーネントが有効化されているかどうかに応じて、ページの下部にある **保存** または **保存してサービスを再起動** をクリックします。
7. 複数の組織がある場合、それぞれの組織について前の手順を繰り返します。

ソフトウェアカタログのメータリング情報の表示

メータリング情報は、ソフトウェアカタログの詳細 ページと デバイスの詳細 ページで表示できます。

注: メータリング情報は、デバイスやアプリケーションに対してメータリングが有効になっている場合にのみ使用可能です。この情報については、デバイスとアプリケーションに対するメータリングの有効化および設定を参照してください。

ソフトウェアカタログの詳細 ページでのメータリング情報の表示

ソフトウェアカタログのアプリケーションに関するメータリング情報は、Software Catalog Detail（ソフトウェアカタログの詳細）ページに表示できます。

Software Catalog Detail（ソフトウェアカタログの詳細）ページで使用可能なメータリング情報の量は、メータリング情報の保持設定によって決まります。詳細については、「メータリング情報について」を参照してください。

1. ソフトウェアカタログ リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. **オプション**：メータリング列のヘッダーをクリックし、メータリング対象のアプリケーションでリストを並び替えます：。
3. メータリング対象のアプリケーションの名前をクリックして、ソフトウェアカタログの詳細 ページを表示します。

   このページには次のような情報が表示されます。

列の名前	説明
インストール済みバージョンまたはインストール済みアプリケーション	
ファイル名	アプリケーションの場合、実行可能ファイルの名前。

列の名前	説明
製品名	スイートの場合、スイート名。
バージョン	アプリケーションに関連付けられたバージョン番号。
言語	アプリケーションの対象言語。例えば、英語などです。特定の言語向けに設計されていないアプリケーションは、「言語非依存」に指定されます。
インストール済み	アプリケーションをインストールしている管理対象デバイスの数。数字をクリックして、デバイスの情報を表示します。
メータリング	
過去1日	過去24時間にアプリケーションを起動した管理対象デバイスの数。
1〜7日前	過去7日間にアプリケーションを起動した管理対象デバイスの数。
8〜30日前	8日前から30日前の間にアプリケーションを起動した管理対象デバイスの数。

デバイスの詳細 ページでのメータリング情報の表示

ソフトウェアカタログのアプリケーションに関するメータリング情報は、デバイスの詳細 ページに表示できます。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. メータリングが有効化されている管理対象デバイスの名前をクリックして、デバイスの詳細 ページを表示します。
3. ソフトウェア セクションで、**メータリングしたソフトウェア** をクリックし、パネルを展開します。

    このセクションに、以下の情報が含まれています。

列の名前	説明
アプリケーション	メータリング対象アプリケーションの名前。アプリケーション名をクリックすると、そのアプリケーションの詳細ページが表示されます。
バージョン	インストールされているアプリケーションのバージョン。メジャーバージョンは、ソフトウェアカタログに個別にリスト表示され、個別にメータリングが行われます。例えば、アプリケーションのバージョン **4.1** とバージョン **4.2** は、個別のエントリとして表示されます。したがって、これらのソフ

列の名前	説明
	トウェアアプリケーションの管理と使用率のメータリングを個別に行うことができます。マイナーバージョン（**4.123**、**4.134**、**4.145**など）は、同じエントリ（**4.x**など）の下に表示されます。**4.x**というエントリの下にグループ化された各バージョンは、そのアプリケーションの詳細ページに表示されます。
使用時間	過去7日間でアプリケーションがデバイスで実行された時間数を小数で表したもの。例えば、実行時間が45分間だった場合は「0.75」と表示されます。
起動回数	過去7日間でデバイス上のアプリケーションが起動された回数。
前回の起動	過去7日間における最新の起動日時。

注: デバイスからインベントリが収集された時間と、メータリングレポートが生成された時間の間に新しいアプリケーションがインストールされた場合、このアプリケーションは、次にインベントリが収集されるまでレポートされません。

ソフトウェアカタログのアプリケーションおよび管理対象デバイスに対するメータリングの無効化

アプリケーションやデバイスに対するメータリングを無効化すると、それらのアプリケーションやデバイスのメータリング情報が保存されなくなります。ただし、既に保存されたメータリング情報は維持されます。

ソフトウェアカタログのアプリケーションに対するメータリングの無効化

ソフトウェアカタログのアプリケーションに対してメータリングが有効になっている場合は、必要に応じてメータリングを無効にすることができます。

1. ソフトウェアカタログ リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. アプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択 > メータリングを無効にする** を選択します。

メータリングが無効化され、メータリングアイコンが、選択したアプリケーションの隣にあるメータリング列から削除されます。ただし、既に保存されているメータリング情報は維持されます。

デバイスのメータリングの無効化

デバイスに対してメータリングが有効になっている場合は、必要に応じてメータリングを無効にすることができます。

手動ラベルによるデバイスのメータリングの無効化

手動ラベルによってデバイスに対するメータリングが有効になっている場合は、ラベルの詳細 でメータリングを無効にすることができます。

1. ラベル リストに移動します。

a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
c. ラベル管理 パネルで、**ラベル** をクリックします。

2. メータリングラベルの隣のチェックボックスをオンにします。
3. **アクションの選択 > メータリングを無効にする** を選択します。

ラベルが適用されているすべてのデバイスのメータリングが無効になります。ただし、既に保存されているメータリング情報は維持されます。

Smart Labelによるデバイスのメータリングの無効化

Smart Labelによってデバイスに対するメータリングが有効になっている場合は、Smart Labelの詳細 でメータリングを無効にすることができます。

1. Smart Labelの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーの、**ホーム** セクションで、**ラベル管理** をクリックします。
   c. ラベル管理 パネルで、**Smart Label** をクリックします。
   d. Smart Label の名前をクリックします。
2. メータリングを有効にする チェックボックスをオフにします。

ラベルが適用されているすべてのデバイスのメータリングが無効になります。ただし、既に保存されているメータリング情報は維持されます。

メータリングの管理とインベントリコレクションのスケジュール

メータリングは「ソフトウェアカタログ」のアプリケーションでのみ使用できます。メータリングは ソフトウェア ページに表示されるアプリケーションでは使用できません。

メータリングの有効化の詳細については、メータリング情報についてを参照してください。

メータリングおよびインベントリコレクションの間隔のスケジュール

メータリングおよびインベントリコレクションの間隔により、メータリングおよびインベントリ情報が管理対象デバイスから収集される頻度が決まります。アプライアンスで組織コンポーネントが有効化されている場合は、各組織のメータリングおよびインベントリコレクション間隔を個別にスケジュールできます。

1. 次のいずれかを実行します。
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから システム を選択します。続いて、組織 をクリックします。組織の情報を表示するには、組織の名前をクリックします。**

     表示される 組織の詳細 ページで、通信とエージェントの設定 セクションを探します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。次に、設定 > プロビジョニング を選択し、プロビジョニング パネルで 通信設定 をクリックします。**

     通信設定 ページが表示されます。
2. エージェントおよび通信設定 セクションで、各設定を次のように指定します。

オプション	設定案	メモ
エージェントのログ記録	有効	管理対象デバイスにインストールされたエージェントから提供されるスクリプト結果を、アプライアンスが保存するかどうか。エージェントログは、データベース内のディスク領域を最大約1 GB消費します。ディスク領域に問題がない場合は、エージェントのログ記録 を有効にして、エージェント管理対象デバイスの ログ情報をすべて保持します。これらのログは、トラブルシューティング時に役立ちます。ディスク領域を節約し、エージェント通信を高速化するには、エージェントのログ記録 を無効にします。
エージェントインベントリ	12時間	管理対象デバイスのエージェントがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
エージェント不要インベントリ	1日	エージェント不要デバイスがインベントリをレポートする頻度。この情報は、インベントリ セクションに表示されます。
カタログインベントリ	24時間	管理対象デバイスが ソフトウェア カタログ ページにインベントリをレポートする頻度。
メータリング	4時間	管理対象デバイスがアプライアンスにメータリング情報をレポートする頻度。デバイスとアプリケーションに対してメータリングを有効にする必要があります。
スクリプト更新	4時間	管理対象デバイスのエージェントが、管理対象デバイスで有効にされているスクリプトの更新されたコピーを要求する頻度。この間隔はスクリプトの実行頻度に影響を与えません。

3. **保存** をクリックします。

アプリケーション制御の使用

アプリケーション制御を使用すると、アプリケーションを「不許可」としてマーク付けして、エージェント管理対象の Windows デバイスおよび Mac デバイスでの実行をブロックしたり、禁止したりできます。これは、環境内で特定のアプリケーションの実行を制限する場合に役立ちます。

アプリケーション制御により、以下が可能になります。

- エージェント管理対象のWindowsおよびMacデバイスで特定のアプリケーションの実行を防止する。この機能はLinuxまたはエージェント不要デバイスでは使用できません。詳細については、「アプリケーションをブロックする要件」を参照してください。
- 「不許可」としてマーク付けされたアプリケーションのレポートを作成する。詳細については、「「不許可」としてマーク付けされたアプリケーションを表示するレポートの作成」を参照してください。
- 「高度な検索」を使用して、「不許可」としてマーク付けされたアプリケーションを検索する。詳細については、「情報の検索およびリストのフィルタリング」を参照してください。

「不許可」としてマーク付けされたアプリケーションは組織固有のものです。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のアプリケーションを個別に「不許可」としてマーク付けします。

アプリケーションをブロックする要件

アプリケーションをブロックするには、アプリケーション制御要件が満たされている必要があります。

アプリケーションをブロックし、管理対象デバイスでの起動を防ぐには、以下を実行する必要があります。

- **デバイスへの KACE エージェントバージョン 6.0 以降のインストール。**バージョン6.0より前のエージェントでは、アプリケーション制御は使用できません。また、Linuxデバイスやエージェント不要デバイスでも使用できません。詳細については、「管理対象デバイスでの KACE エージェントの更新」を参照してください。
- **「アプリケーション制御」が有効になったラベルのデバイスへの適用。**これにより、さまざまなアプリケーション（「不許可」としてマーク付けされたアプリケーションも含む）の起動をエージェントで監視できるようになります。詳細については、「アプリケーション制御ラベルのデバイスへの適用」を参照してください。
- **アプリケーションへの「不許可」のマーク付け。**WindowsおよびMacアプリケーションは、ソフトウェアカタログで検出済み、未検出、またはローカルカタログ登録済みのアプリケーションとして分類されている場合にのみ、「不許可」としてマーク付けすることができます。カタログ未登録のアプリケーションは、ソフトウェアカタログに追加されない限り、「不許可」としてマーク付けすることはできません。詳細については、「ソフトウェアカタログへのアプリケーションの追加」を参照してください。Linuxアプリケーションは「不許可」としてマーク付けすることはできません。
- **ブロックするアプリケーションのバージョンの指定。**例えば、Adobe Acrobat®のすべてのバージョンをブロックする場合、アプリケーションのすべてのバージョンを「不許可」としてマーク付けする必要があります。例：Acrobat 8.x、Acrobat 9.xなど。スイートを「不許可」としてマーク付けすると、そのスイート内のすべてのアプリケーションも「不許可」としてマーク付けされます。WindowsとMacデバイス両方で実行するアプリケーションを「不許可」としてマーク付けすると、そのアプリケーションはWindowsとMacデバイス両方でブロックされます。

アプリケーションをブロックする方法

「不許可」としてマーク付けされたアプリケーションを、「アプリケーション制御」が有効になったラベルが適用された管理対象デバイスで起動すると、エージェントはそのアプリケーションを終了してデバイスにメッセージを表示します。

メッセージには、そのアプリケーション名が表示され、アプリケーションが「不許可」リストに載っているため終了されたことが示されます。終了させられたアプリケーションは、ソフトウェアの使用率を記録するローカルデータベースで識別されます。

実行ファイルを共有するアプリケーションエディションに対するアクセスの拒否について

ProおよびStandardなど、異なるエディションが同じ実行ファイルを共有するアプリケーションがあります。このようなアプリケーションがブロックされると、その実行ファイルを共有するすべてのエディションもブロックされます。

ブロックできないアプリケーション

他のアプリケーションのプラグインなど、一部のアプリケーションはブロックできません。

次のアプリケーションは「不許可」としてマーク付けできますが、管理対象デバイスでの実行をブロックしたり、禁止したりすることはできません。

- ブラウザのプラグインまたは外部 DLL
- InfragisticsなどのMicrosoft Visual Studio®のプラグイン
- Java®アプリケーション

アプリケーション制御ラベルのデバイスへの適用

アプリケーション制御をデバイスで有効化するには、ApplicationControlDevices ラベルまたはアプリケーション制御が有効化された任意のラベルをデバイスに適用する必要があります。

ラベルがデバイスに適用されると、「不許可」としてマーク付けされたアプリケーションは、そのデバイスでの実行がブロックされるか、禁止されます。

1. デバイス リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. 1つまたは複数のデバイスの横にあるチェックボックスを選択します。
3. **アクションの選択 > ラベルの適用** を選択します。
4. **ApplicationControlDevices** ラベルを選択します。

デバイス ページのデバイス名の隣にラベルが表示されます。

アプリケーションおよびスイートへの「不許可」のマーク付け

個別のアプリケーションおよびアプリケーションスイートを「不許可」としてマーク付けして、それらがエージェント管理対象デバイスで実行されないようにすることができます。

スイートを「不許可」としてマーク付けすると、そのスイート内のアプリケーションも「不許可」としてマーク付けされます。スイートの一部のアプリケーションのみを「不許可」としてマーク付けする場合は、スイートから「不許可」の指定を削除してから、個々のアプリケーションを「不許可」としてマーク付けします。

1. ソフトウェアカタログ リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。

2. 1つまたは複数のアプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択 > 不許可に指定する** を選択します。

アプリケーションが「不許可」としてマーク付けされ、次の「不許可」アイコンがアプリケーション名の隣に表示されます：  。

「不許可」としてマーク付けされたアプリケーションの表示

「不許可」としてマーク付けされたアプリケーションおよびスイートは、ソフトウェアカタログ ページに表示されます。

1. ソフトウェアカタログ リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。
2. 次のいずれかを実行します。
   - **左側のリストの上部にある 検出済み タブまたは 未検出 タブをクリックし、ソフトウェアカタログ ページの 不許可 ボタンをクリックして、「不許可」としてマーク付けされたアプリケーションを基準にして結果を並べ替えます。ボタン：**  。
   - **右側のリストの上にある 高度な検索 タブをクリックして、以下のように、「不許可」としてマーク付けされたアプリケーションを表示するために必要な条件を指定します。**

     ソフトウェアカタログ: 不許可 | is | True
3. **検索** をクリックします。

「不許可」としてマーク付けされたアプリケーションを表示するレポートの作成

「不許可」としてマーク付けされたアプリケーションとそのアプリケーションがインストールされたデバイスを表示するレポートを作成できます。

1. 次のいずれかの操作を行って、Reports（レポート）リストに移動します。
   - **アプライアンスの組織コンポーネントが有効で、システムレベルのレポートにアクセスする必要がある場合：**

     アプライアンスシステム管理コンソール（https://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。次に、**レポート作成** をクリックします。
     システムレベルのレポートには、すべての組織からの情報を集約した総合レポートと、各種のアプライアンスコンポーネントの標準レポートが含まれます。
   - **アプライアンスで組織コンポーネントが有効化されていない場合、または組織レベルレポートにアクセスする場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。次に、レポート作成 をクリックします。**

     組織レベルのレポートには、各種のアプライアンスコンポーネントの標準レポートが含まれます。アプライアンスで組織コンポーネントが有効になっている場合、これらのレポートは選択された組織に固有の情報を提供します。

レポート リストが表示されます。

2. **アクションの選択 > 新規作成 (ウィザード)** を選択して、レポートタイトル ページを表示します。
3. 次の設定を指定します。

オプション	説明
タイトル	「不許可」のソフトウェア。
カテゴリ	ソフトウェア。
説明	「不許可」としてマーク付けされたソフトウェア。
行番号の表示	(オプション) 行番号がある列をレポートに追加する場合は、このチェックボックスをオンにします。
トピック	ソフトウェアカタログ - 検出されたソフトウェア
サブトピック	デバイス

4. **次へ** をクリックして、表示するフィールド ページを表示します。
5. 次のようなレポートフィールドを選択します。
   - **名前 : アプリケーションの名前。**
   - **インストール数: アプリケーションをインストールしているデバイスの数。**
   - **カテゴリ: アプリケーションのカテゴリ。**
   - **デバイス: アプリケーションをインストールしているデバイスに関する情報。**
6. **次へ** をクリックして、列の順番 ページを表示します。
7. 列をドラッグして、レポートで列を表示する順序を設定し、**次へ** をクリックして、並べ替えとブレーク ページを表示します。
8. 並べ替えとブレークのオプションを選択して、**次へ** をクリックして、フィルタ ページを表示します。
9. **レコードをフィルタリングするルールの指定** をクリックし、以下のように、「不許可」としてマーク付けされたアプリケーションを検出するために必要な条件を指定します。

   検出されたソフトウェアの情報: 不許可 | = | 1
10. その行で **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

    新しいレポートがリストされた レポート リストが表示されます。右側の表の上部に表示される 特定基準で表示 リストが、自動的に新しいレポートのカテゴリに設定されます。
11. レポートを実行するには、レポートの生成 列の形式をクリックします。

レポートが生成されます。HTML 形式のレポートでは、最初のデータ列が**管理者コンソール**のアイテムの詳細ページに自動的にリンクされます。レポートの詳細については、レポートの作成を参照してください。

アプリケーションからの「不許可」指定の削除

アプリケーションを「不許可」としてマーク付けした場合、必要に応じて「不許可」の指定を削除することができます。

「不許可」の指定は組織固有のものです。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のアプリケーションに対し、「不許可」の指定を個別に適用および削除することができます。

ヒント: デフォルトでは、アプリケーションは、「不許可」としてマーク付けされていない限り、「許可」されています。

1. ソフトウェアカタログ リストに移動します。

a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェアカタログ** をクリックします。

2. 1つまたは複数のアプリケーションの隣のチェックボックスをオンにします。
3. **アクションの選択 > 許可に指定する** を選択します。

   アプリケーションが「許可」としてマーク付けされ、「不許可」の記号が削除されます。

ソフトウェアカタログの更新および再インストール

ソフトウェアカタログは継続的に、新しいアプリケーションが使用可能になった場合と、カタログ登録要求を受け取った場合に更新されます。これらの更新は定期的に自動でダウンロードされ、KACE SMA にインストールされます。ソフトウェアカタログの更新を手動で確認したり、カタログを再インストールしたりすることができます。

インターネットに接続していないオフラインのアプライアンスを使用している場合に、ソフトウェアカタログの更新を取得するには、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。

注: カタログの更新がダウンロードされると、アプライアンスにより、ローカルカタログ登録済みのアプリケーションがパブリックのソフトウェアカタログに追加されたかどうかが確認されます。アプリケーションが追加されていると、ローカルのカタログ登録は削除されます。アプリケーションが追加されていない場合、ローカルのカタログ登録は保持されます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。
3. 次のいずれかを実行します。
   - ソフトウェアカタログ **セクションで 更新の確認 をクリックします。**

     ソフトウェアカタログが最新の状態である場合、ログ ページが表示されて、バージョン情報が示されます。更新が使用できる場合は、インストール情報が表示されます。次のいずれかに該当する場合は、完全版のカタログがインストールされることがあります。アプライアンスにベースラインのカタログがない場合、完全版のカタログを更新する手段がない場合、または使用できる更新が5つより多い場合。
   - ソフトウェアカタログ **セクションで 再インストール をクリックします。**

     アプライアンスに格納されているソフトウェアカタログのバージョンが、Quest KACE から入手可能な最新のソフトウェアカタログに置き換えられます。完全版のソフトウェアカタログには、最新の完全版のカタログに加えて、最新版がリリースされてから追加されたすべての更新（つまり、差異）が含まれています。
   - **アプライアンスがオフラインで、インターネットにアクセスしていない場合は、Questサポート（https://support.quest.com/contact-support）までお問い合わせください。**

プロセス、スタートアッププログラム、およびサービスインベントリの管理

アプライアンスインベントリ内のプロセス、スタートアッププログラム、およびサービスを管理できます。

プロセスインベントリの管理

管理対象デバイスでプロセスが検出されると、これらはレポートされ、インベントリ セクションで管理できるようになります。

プロセスインベントリを管理するには、次の手順を実行します。

- 過去1/2/3/6/12ヶ月のプロセスの使用情報を表示する
- プロセスにラベルを適用する/プロセスからラベルを削除する
- カテゴリと脅威レベルをプロセスに割り当てる
- プロセスを削除する

プロセスインベントリはメータリングできず、プロセスをブロックすることはできません。ただし、アプリケーションをブロックすることはできます。詳細については、「アプリケーションおよびスイートへの「不許可」のマーク付け」を参照してください。

プロセス詳細の表示および編集

インベントリ内のプロセスの詳細を表示および編集することができます。

1. プロセス詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**プロセス** をクリックします。
    c. プロセスの名前をクリックします。
2. 次の情報を入力します。

オプション	説明
ラベルへの割り当て	（ オプション ）アイテムに関連付けられるラベル。
メモ	任意の追加情報を入力します。
カテゴリ	アイテムのカテゴリ。ビジネス、ドライバ、セキュリティなど。
脅威レベル	アイテムの脅威レベル。 脅威レベルは次の通りです。 a. 安全 b. まずまず安全 c. 不明

オプション	説明
	d. 有害の危険性あり e. 有害

3. **保存** をクリックします。

プロセスへのラベルの追加

ラベルを手動で追加して、インベントリ内のプロセスをグループとして管理します。

1. プロセス リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**プロセス** をクリックします。
2. **アクションの選択 > ラベルの追加** を選択します。
3. ラベルの追加 ウィンドウで、ラベルの名前を入力します。

    ヒント: ラベル名にはバックスラッシュ（\）を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して（\\）エスケープします。

4. **保存** をクリックします。

プロセスへのラベルの適用またはラベルの削除

ラベルは、必要に応じてインベントリのプロセスに対して適用または削除されます。

1. プロセス リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**プロセス** をクリックします。
2. 1つまたは複数のプロセスの隣のチェックボックスをオンにします。
3. 次のいずれかを実行します。
    - **アクションの選択 > ラベルの適用 を選択して、適用するラベルを選択します。**
    - **アクションの選択 > ラベルの削除 を選択して、削除するラベルを選択します。**

プロセスの分類

インベントリ内のプロセスを整理して管理するには、これらをカテゴリに手動で割り当てます。

1. プロセス リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**プロセス** をクリックします。
2. 1つまたは複数のプロセスの隣のチェックボックスをオンにします。
3. **アクションの選択 > カテゴリの設定** を選択して、カテゴリを選択します。

プロセスへの脅威レベルの割り当て

デバイスおよびシステムの脅威となる可能性のあるプロセスを管理するには、脅威レベルをこれらのプロセスに手動で割り当てます。

脅威レベルを使用して、アイテムの相対的な安全性、およびそのアイテムがインストールされているデバイスの数を示すことができます。この情報は、追跡のみを目的としています。アプライアンスが、脅威レベルに基づきポリシーを強制することはありません。

1. プロセス リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**プロセス** をクリックします。
2. 1つまたは複数のプロセスの隣のチェックボックスをオンにします。
3. **アクションの選択 > レベルの設定** を選択して、脅威レベルを選択します。

プロセスを削除する

必要に応じてインベントリからプロセスを手動で削除できます。

ただし、削除したプロセスが管理対象デバイスで見つかった場合、デバイスがインベントリ情報を更新したときに、それらのプロセスのレコードが新しいIDで再作成されます。

1. プロセス リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**プロセス** をクリックします。
2. 次のいずれかを実行します。
    - **1つまたは複数のプロセスの横にあるチェックボックスをオンにして、アクションの選択 > 削除 を選択します。**
    - **プロセス名をクリックし、**Process Detail **（プロセスの詳細）ページで 削除 を選択します。**
3. **はい** をクリックして確定します。

スタートアッププログラムインベントリの管理

管理対象デバイスでスタートアッププログラムが検出されると、これらはレポートされ、インベントリ セクションで管理できるようになります。

インベントリのスタートアップページでは、管理対象デバイスで検出されたスタートアッププログラムに関する情報を表示および編集することができます。

スタートアップインベントリの詳細には、スタートアッププログラムを実行しているデバイスの名前、システムの説明、および最新のユーザーが含まれます。

スタートアッププログラムはメータリングできません。

スタートアッププログラムの詳細の表示および編集

インベントリ内のスタートアッププログラムの詳細を表示および編集することができます。

1. スタートアッププログラムの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**スタートアッププログラム** をクリックします。
    c. スタートアッププログラムの名前をクリックします。

    プログラムを実行中のデバイスがページ下部に表示されます。
2. 次の情報を入力します。

オプション	説明
ラベルへの割り当て	（オプション）アイテムに関連付けられるラベル。
メモ	任意の追加情報を入力します。
カテゴリ	アイテムのカテゴリ。ビジネス、ドライバ、セキュリティなど。
脅威レベル	アイテムの脅威レベル。 脅威レベルは次の通りです。 a. 安全 b. まずまず安全 c. 不明 d. 有害の危険性あり e. 有害

3. **保存** をクリックします。

スタートアッププログラムへのラベルの追加

ラベルを手動で追加して、インベントリ内のスタートアッププログラムをグループとして管理します。

1. スタートアッププログラム リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**スタートアッププログラム** をクリックします。
2. **アクションの選択 > ラベルの追加** を選択します。
3. ラベルの追加 ウィンドウで、ラベルの名前を入力します。

    ヒント: ラベル名にはバックスラッシュ（\）を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して（\\）エスケープします。
4. **保存** をクリックします。

スタートアッププログラムへのラベルの適用またはラベルの削除

ラベルは、必要に応じてインベントリのスタートアッププログラムに対して適用または削除されます。

1. スタートアッププログラム リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**スタートアッププログラム** をクリックします。
2. 1つまたは複数のプログラムの隣のチェックボックスをオンにします。
3. 次のいずれかを実行します。
    - **アクションの選択 > ラベルの適用 を選択して、適用するラベルを選択します。**
    - **アクションの選択 > ラベルの削除 を選択して、削除するラベルを選択します。**

スタートアッププログラムの分類

インベントリ内のスタートアッププログラムを整理して管理するには、これらをカテゴリに手動で割り当てます。

1. スタートアッププログラム リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**スタートアッププログラム** をクリックします。
2. 1つまたは複数のプログラムの隣のチェックボックスをオンにします。
3. **アクションの選択 > カテゴリの設定** を選択して、カテゴリを選択します。

スタートアッププログラムへの脅威レベルの割り当て

デバイスおよびシステムの脅威となる可能性のあるスタートアッププログラムを管理するには、脅威レベルをこれらのプログラムに手動で割り当てます。

脅威レベルを使用して、アイテムの相対的な安全性、およびそのアイテムがインストールされているデバイスの数を示すことができます。この情報は、追跡のみを目的としています。アプライアンスが、脅威レベルに基づきポリシーを強制することはありません。

1. スタートアッププログラム リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**スタートアッププログラム** をクリックします。
2. 1つまたは複数のプログラムの隣のチェックボックスをオンにします。
3. **アクションの選択 > 脅威レベルの設定** を選択して、脅威レベルを選択します。

スタートアッププログラムの削除

必要に応じてインベントリからスタートアッププログラムを手動で削除できます。

ただし、削除したスタートアッププログラムが管理対象デバイスで見つかった場合、デバイスがインベントリ情報を更新したときに、それらのプログラムのレコードが新しいIDで再作成されます。

1. スタートアッププログラム リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**スタートアッププログラム** をクリックします。
2. 次のいずれかを実行します。
    - **1つまたは複数のプログラムの横にあるチェックボックスをオンにして、アクションの選択 > 削除 を選択します。**
    - **プログラム名をクリックし**、Startup Program Detail **（スタートアッププログラムの詳細）ページで削除 を選択します。**
3. **はい** をクリックして確定します。

サービスインベントリの管理

管理対象デバイスでサービスが検出されると、これらはレポートされ、インベントリ セクションで管理できるようになります。

サービスインベントリのページでは、管理対象のデバイスで実行しているサービスを追跡できます。

サービスの詳細 ページにはサービスに関する情報が表示されます。例えば、サービスを実行しているデバイスの名前、システムの説明、最新のユーザーなどです。

サービスインベントリはメータリングできません。

サービスの詳細の表示および編集

インベントリ内のサービスの詳細を表示および編集することができます。

1. サービスの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**サービス** をクリックします。
    c. サービスの名前をクリックします。

    サービスを実行中のデバイスがページ下部に表示されます。
2. 次の情報を入力します。

オプション	説明
ラベルへの割り当て	（オプション）アイテムに関連付けられるラベル。
メモ	任意の追加情報を入力します。

オプション	説明
カテゴリ	アイテムのカテゴリ。ビジネス、ドライバ、セキュリティなど。
脅威レベル	アイテムの脅威レベル。 脅威レベルは次の通りです。 a. 安全 b. まずまず安全 c. 不明 d. 有害の危険性あり e. 有害

3. **保存** をクリックします。

サービスへのラベルの追加

ラベルを手動で追加して、インベントリ内のサービスをグループとして管理します。

1. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **インベントリ > サービス** の順に選択して、サービス ページを表示します。
3. **アクションの選択 > ラベルの追加** を選択します。
4. ラベルの追加 ウィンドウで、ラベルの名前を入力します。

   ヒント: ラベル名にはバックスラッシュ（\）を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して（\\）エスケープします。

5. **保存** をクリックします。

サービスへのラベルの適用またはラベルの削除

ラベルは、必要に応じてインベントリのサービスに対して適用または削除されます。

1. サービス リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**サービス** をクリックします。
2. 1つまたは複数のサービスの隣のチェックボックスをオンにします。
3. 次のいずれかを実行します。
   - **アクションの選択 > ラベルの適用 を選択して、適用するラベルを選択します。**
   - **アクションの選択 > ラベルの削除 を選択して、削除するラベルを選択します。**

サービスの分類

インベントリ内のサービスを整理して管理するには、これらをカテゴリに手動で割り当てます。

1. サービス リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**サービス** をクリックします。

2. 1つまたは複数のサービスの隣のチェックボックスをオンにします。
3. **アクションの選択 > カテゴリの設定** を選択して、カテゴリを選択します。

サービスへの脅威レベルの割り当て

デバイスおよびシステムの脅威となる可能性のあるサービスを管理するには、脅威レベルをこれらのサービスに手動で割り当てます。

脅威レベルを使用して、アイテムの相対的な安全性、およびそのアイテムがインストールされているデバイスの数を示すことができます。この情報は、追跡のみを目的としています。アプライアンスが、脅威レベルに基づきポリシーを強制することはありません。

1. サービス リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**サービス** をクリックします。
2. 1つまたは複数のサービスの隣のチェックボックスをオンにします。
3. **アクションの選択 > 脅威レベルの設定** を選択して、脅威レベルを選択します。

サービスの削除

必要に応じてインベントリからサービスを手動で削除できます。

ただし、削除したサービスが管理対象デバイスで見つかった場合、デバイスがインベントリ情報を更新したときに、それらのサービスのレコードが新しいIDで再作成されます。

1. サービス リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**サービス** をクリックします。
2. 1つまたは複数のサービスの隣のチェックボックスをオンにします。
3. 次のいずれかを実行します。
   - **1つまたは複数のプログラムの横にあるチェックボックスをオンにして、アクションの選択 > 削除 を選択します。**
   - **プログラム名をクリックし、**Startup Program Detail **（スタートアッププログラムの詳細）ページで削除 を選択します。**
4. **はい** を選択して確定します。

カスタムインベントリルールの記述

カスタムインベントリルールを記述して、インベントリ内のアイテムの詳細情報を収集できます。

インベントリコンポーネントの使用に関する詳細については、ソフトウェア ページでのアプリケーション管理を参照してください。

カスタムインベントリルールについて

カスタムインベントリルールにより、カスタマイズされた情報をインベントリコレクションプロセス中に取得できます。

カスタムインベントリルールは、以下の処理に効果的です。

- Windowsの プログラムの追加と削除 セクションにリストされていないソフトウェアの管理。
- Windows の プログラムの追加と削除 セクションの同じエントリにリストされている複数のソフトウェアのバージョンで、特に バージョンの表示 情報が間違っているか不完全であるものの管理。
- カスタマイズされた詳細をレポートで使用するために取得。
- KACE エージェントによってレポートされない既存のアプリケーションまたは値に基づく、展開ルール、スクリプト、およびレポートの作成。

カスタムインベントリルールのタイプ

カスタムインベントリルールでは、レジストリキーとエントリの値、プログラム、ファイル、スクリプト、環境変数、システムプロパティ、およびコマンドの出力をテストおよび取得します。

カスタムインベントリルールには次の2つのタイプがあります。

- **条件付きルール**: これらのルールは、条件がデバイスに存在するかどうかをテストします。ルールによって true が返されると、KACE エージェントは インストールされているプログラム としてアイテムをレポートします。ルールによってfalseが返されると、アイテムは「インストールされているプログラム」として表示されません。
- **値戻しルール**: これらのルールは、デバイスからデータを取得します。値が存在する場合、KACE エージェントは インストールされているプログラム としてアイテムをレポートし、対応する カスタムインベントリフィールド を設定します。

カスタムインベントリルールの作成

カスタムアプリケーション、およびそれらのアプリケーションのカスタムインベントリルールを作成し、アプリケーションに関する情報が管理対象デバイスから収集されるようにすることができます。

1. ソフトウェアの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ソフトウェア** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. 次の一般情報を入力します。「名前」、「バージョン」、および「発行元」。

    ダウンストリームへのレポート処理が適切に実行されるように、この情報がソフトウェアインベントリ全体で整合するようにします。
3. 次の情報を入力します。

オプション	説明
ラベルへの割り当て	（ オプション ）アイテムに関連付けられるラベル。

オプション	説明
メモ	任意の追加情報を入力します。
サポートされているオペレーティングシステム	アプリケーションが実行されるオペレーティングシステム。アプリケーションは、選択したオペレーティングシステムがインストールされているデバイスにのみ導入されます。
カスタムインベントリルール	（オプション）アプリケーションに適用されるカスタムインベントリルール。カスタムインベントリルールを使用すると、デバイス上のアプリケーションおよび他のアイテムを検出したり、レポート目的で詳細を取得したりできます。 例えば、アプライアンスでは、デバイス上にアプリケーションが存在するかどうかを確認してから、アプリケーションが展開されます。にもかかわらず、インストールされているプログラムが プログラムの追加と削除 またはレジストリの標準領域に登録されていない場合があります。そのような場合、アプライアンスは、管理者からの追加の情報なしでは、アプリケーションの存在を検出できないことがあります。そのため、デバイスが接続されるたび、アプライアンスでインストールが繰り返される場合があります。カスタムインベントリルールを使用すると、この繰り返しを回避できます。 次のルールを使用して、デバイスにインストールされているNetwork Associates VirusScanのバージョンが展開前の所定のバージョンよりも新しいことを確認します。 RegistryValueGreaterThan(HKEY_LOCAL_MACHINE\Software\Network Associates\TVD\ Network Associates\TVD\Shared Components\VirusScanEngine\4.0.xx,szDatVersion,4.0.44)

4. ファイルのアップロードと関連付け の隣にある **ファイルの選択** をクリックしてファイルを参照し、 **開く** または **選択** をクリックします。

   管理対象インストールまたはファイル同期によってアプリケーションを配布するには、そのアプリケーションに実際のアプリケーションファイルを関連付ける必要があります。

5. ファイルがレプリケーション共有にコピーされないようにするには、**関連付けられたファイルを複製しない** を選択します。この設定は、ソフトウェアスイートなど、ユーザーにレプリケーション共有にインストールしてほしくない大きいファイルに役立ちます。
6. **オプション**：ソフトウェアの カテゴリ と 脅威レベル を設定します。
7. **保存** をクリックします。

関連トピック

ラベルについて

デバイス（カスタムインベントリフィールド）からの値の取得

ソフトウェア脅威レベルとカテゴリの使用

カスタムインベントリルールの実装方法

KACE エージェントは、新規カスタムインベントリルールの作成後の最初のデバイスインベントリ中に、そのルールを受け取ります。その最初のインベントリ中、エージェントは新しいルールを実行し、検出内容をアプライアンスにレポートします。

エージェントは、すべてのルールを実行すると同時に、そのセッションについてスケジュールされた他のあらゆるプロセスも実行します。したがって、デバイスがインベントリ設定されてからエージェントが結果をレポートするまでに、すべてのルールとその他のプロセスの実行に数分かかる場合があります。

エージェントが結果をレポートした後、デバイスの詳細ページでは、ソフトウェア の下の Installed Program（インストールされているプログラム）と Custom Inventory Fields（カスタムインベントリフィールド）にその結果が表示されます。

注: カスタムインベントリフィールド を設定する値戻しルールが適用されたアプリケーションは、「インストールされているプログラム」としても表示されます。

期待通りの結果が得られない場合は、デバイスが最近インベントリ設定されたことを確認します。インベントリ時間は、デバイスの詳細 ページの 前回のインベントリ フィールドに表示されます。

カスタムインベントリルールの構文

カスタムインベントリルールの関数の名前と引数に正しい構文を使用します。

条件付きルールと値戻しルールでは次の構文を使用します。

functionName(argument,argument,...)

関数とそれらの引数の詳細については、次の情報を参照してください。

- 条件の確認（条件付きルール）
- デバイス（カスタムインベントリフィールド）からの値の取得
- 正規表現を使用したファイル名のマッチ

関数の構文

開始かっこの前に「**functionName**」を入力し、その開始かっこと終了かっこで引数を囲みます。関数の名前と開始かっことの間にスペースは許可されません。

引数の構文

コマンドとregex（正規表現）を除くすべてのルールについて、**引数**を次のような構文で入力します。

- 引数をコンマで区切る。
- コンマは、ルールでの値としてのコンマとかっこで説明している場合を除き、文字列内のその他のどこにも許可されない。
- 一重引用符や二重引用符を含めない。
- 各引数の前後のスペースは無視される。

例えば、次の構文は同じです。

RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox, CurrentVersion, 78.0.2)
RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox,CurrentVersion,78.0.2)

ルールでの値としてのコンマとかっこ

コンマ、開始かっこ、または終了かっこをルール内の値として使用する場合、{{comma}}、{{op}}、および{{cp}}のようにそれぞれエスケープする必要があります。

- パラメータ値の一部としてコンマが必要な引数では、関数内の最後の引数の場合を除き、{{comma}}としてエスケープする必要があります。

  例えば、ユーザーが、値の名前が「**test,value**」であるレジストリ値に対してテストを実行する場合、レジストリ値の名前がカスタムインベントリ（CI）関数の最後の引数ではないため、この場合はコンマをエスケープする必要があります。

  RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\TestSoft, **test{{comma}}value**, HelloWorld)

  ユーザーが、値自体にコンマが含まれるレジストリ値に対してテストを実行する場合、値がカスタムインベントリ関数の最後の引数であるため、エスケープする必要はありません。次のカスタムインベントリでは、レジストリ値HKLM\SOFTWARE\TestSoft\test1をテストし、値が「**2,4**」と等しいかどうかを確認します。

  RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\TestSoft,test1,**2,4**)

  カスタムインベントリ関数に1つのパラメータのみが含まれる場合、かっこで囲まれたすべてを引数の値としてとります。この場合のコンマはエスケープする必要はなく、カスタムインベントリ関数の引数の一部となります。

  ShellCommandTextReturn(**wmic MEMORYCHIP get BankLabel,Capacity,description,manufacturer**)

- リテラルの開始かっこにはペアとなる終了かっこがないため、**{{op}}**としてエスケープする必要があります。パーサーは、関数の引数をトークン化する場合、開始かっこと終了かっこの数をカウントして、関数と引数の末尾を識別します。このため、ペアとなっていないリテラルの開始かっこは、カウントを誤らせ、引数値が正常に解析されない原因となります。リテラルの開始かっこが引数値の一部として必要な場合は、**{{op}}**で表す必要があります。

  例えば、ユーザーが文字列「**Hello (World**」を工コーする必要がある場合、CIは次のようになります。

  ShellCommandTextReturn(echo **Hello {{op}} World**)

- リテラルの終了かっこにはペアとなる開始かっこがないため、**{{cp}}**としてエスケープする必要があります。

  パーサーは、関数の引数をトークン化する場合、開始かっこと終了かっこの数をカウントして、ペアとなっている最後の終了かっこがある場合に関数の末尾であることを識別します。ただし、引数値自体に（ペアとなる開始かっこがない）終了かっこが含まれる場合、パーサーはそのかっこが関数の末尾であると錯覚し、その引数値は完全に切り捨てられます。

  リテラルの終了かっこが引数値の一部として必要な場合は、**{{cp}}**で表す必要があります。

  例えば、ユーザーが文字列「**Hello) World**」を工コーする必要がある場合、CIは次のようになります。

  ShellCommandTextReturn(echo **Hello {{cp}} World**)

条件の確認（条件付きルール）

アプリケーションがインストールされているかどうか（true/false）を識別するカスタムインベントリルールを記述できます。

条件付きルールを使用すると、ルールによって true が返される場合、カスタムアプリケーションの表示名（タイトル）が インベントリセクションにある デバイスの詳細 ページの Software:Installed Programs（ソフトウェア:インストールされているプログラム） セクションに表示されます。

次のセクションでは、条件をテストするルールについて説明します。

- 条件付きルールのリファレンス
- 条件が存在するかどうかの確認（Existsルール）
- デバイス設定の評価（Equalsルール）
- デバイス値の比較（Greater ThanルールとLess Thanルール）
- 複数の条件のテスト

ルールによってfalseが返されると、アプリケーションはデバイスのインベントリ詳細の インストールされているプログラム セクションに表示されません。

ヒント: アイテムがインストールされているデバイスのリストは、インベントリ > ソフトウェア > Custom_item: 詳細 ページに表示されます。

条件付きルールのリファレンス

次の表に、比較で使用できるデータ型を示します。

比較関数でサポートされるデータ型

条件付きルール	比較関数でサポートされるデータ型 「Equals」、「GreaterThan」、「LessThan」
EnvironmentVariable	DATE、NUMBER、TEXT
FileInfo	DATE、NUMBER、TEXT
FilenamesMatchingRegex	番号
FileVersion	テキスト
PlistValue	NUMBER、TEXT
ProductVersion	テキスト
RegistryValue	テキスト

次の表は、比較が行われる方法を示します。

比較が行われる方法

データ型	考慮事項
日付	• 評価の前に、PHP DateTimeクラスと同じルールを使用してターゲット値が日付として解析され、次の書式を使用するように標準化されます： MM/DD/YYYY HH:MM:SS • アプライアンスデータベースにリストされるタイムスタンプは、24 時間表記（0 ー 24 時）を使用します。 • アプライアンスデータベースにリストされるタイムスタンプは UTC（協定世界時）時刻を

データ型	考慮事項
	反映するので、タイムゾーンに関係なく、すべてのデバイスに対して標準化されます。 • ターゲット値に日付のみが含まれている場合、UTCの深夜零時に基づくタイムスタンプが追加されます。
番号	• 整数のみが評価されます。 • ターゲット値に他の文字（アルファベット、句読点など）が含まれている場合、最初の非数値までの数値が評価されます。 例えば、ターゲット値が52a1の場合、52のみが評価されます。 • 32ビットで表される正の最大整数値（2,147,483,647）までの数がサポートされます。
テキスト	• 値は文字通りに評価され、DATEおよびNUMBERのデータ型で発生するような書式変換は何も行われません。 • テキスト文字列は、辞書式順序で評価されます。 • コンマを評価対象の文字列に含めることができます。エスケープ処理は必要ありません。

使用可能な条件付きルール、および引数の指定方法の詳細へのリンクを、次の表で説明します。

条件付きルールのリファレンス

構文	Win	RHEL	OS X	説明
DirectoryExists (path)	X	X	X	デバイス上の指定したパスにあるディレクトリを確認します。
FileExists (path)	X	X	X	デバイス上の指定したパスにあるファイルを確認します。パスにはファイルの名前と拡張子を含めます。
FileVersionEquals (path, version)	X			パスにある指定したファイルの **バージョン** > **ファイルのバージョン** プロパティが、入力した TEXT 値に一致することを確認します。

構文	Win	RHEL	OS X	説明
FileVersionLessThan (path, version)	X			パスにある指定したファイルの **バージョン > ファイルのバージョン** プロパティが、入力した TEXT 値より小さいことを確認します。
FileVersionGreaterThan (path, version)	X			指定したファイルの **バージョン > ファイルのバージョン** プロパティが、入力した TEXT 値より大きいことを確認します。
ProductVersionEquals (path, version)	X			指定した実行可能ファイルまたはインストールファイルの **バージョン > 製品のバージョン** プロパティが、入力した TEXT 値に一致することを確認します。
ProductVersionLessThan (path, version)	X			指定した実行可能ファイルまたはインストールファイルの **バージョン > 製品のバージョン** プロパティが、入力した TEXT 値より小さいことを確認します。
ProductVersionGreaterThan (path, version)	X			指定した実行可能ファイルまたはインストールファイルの **バージョン > 製品のバージョン** プロパティが、入力した TEXT 値より大きいことを確認します。
FileInfoGreaterThan (fullpath, attribute, type, value)	X	X	X	指定した実行可能ファイルまたはインストールファイルの「**ファイル情報**」プロパティが、入力した値よりも大きいことを確認します。

構文	Win	RHEL	OS X	説明
FileInfoLessThan (fullpath, attribute, type, value)	X	X	X	指定した実行可能ファイルまたはインストールファイルの「**ファイル情報**」プロパティが、入力した値よりも小さいことを確認します。
FileInfoEquals (fullpath, attribute, type, value)	X	X	X	指定した実行可能ファイルまたはインストールファイルの属性が、入力した値に一致することを確認します。
RegistryKeyExists (registryPath)	X			レジストリキーが存在することを確認します。
RegistryValueEquals (registryPath, valueName, value)	X			レジストリエントリが、指定した値に完全に一致することを確認します。値はTEXTとして比較されます。
RegistryValueLessThan (registryPath, valueName, value)	X			レジストリエントリが、指定した値より小さいことを確認します。値はTEXTです。
RegistryValueGreaterThan (registryPath, valueName, value)	X			レジストリエントリが、指定した値より大きいことを確認します。値はTEXTです。
EnvironmentalVariableExists (var)	X	X	X	指定した名前の環境変数が存在することを確認します。
EnvironmentalVariableGreaterThan (var, type, value)	X	X	X	環境変数定義が、指定した値より大きいことを確認します。 TEXT、DATE（完全な形式はmm/dd/yyyy hh:mm:ss）、およびNUMBERの

構文	Win	RHEL	OS X	説明
				3つすべてが有効な型です。
EnvironmentalVariableLessThan (var, type, value)	X	X	X	環境変数定義が、指定した値より小さいことを確認します。 TEXT、DATE（完全な形式はmm/dd/yyyy hh:mm:ss）、およびNUMBERの3つすべてが有効な型です。
EnvironmentalVariableEquals (var, type, value)	X	X	X	環境変数定義が、指定した値に完全に一致することを確認します。 TEXT、DATE（完全な形式はmm/dd/yyyy hh:mm:ss）、およびNUMBERの3つすべてが有効な型です。
PlistValueExists (fullpath, entry)			X	名前付きの値がPLISTファイルに存在することを確認します。
PlistValueGreaterThan (fullpath, entry, type, value)			X	名前付きの値が、指定した値より大きいNUMBERまたはTEXTであることを確認します。
PlistValueLessThan (fullpath, entry, type, value)			X	名前付きの値が、指定した値より小さいNUMBERまたはTEXTであることを確認します。
PlistValueEquals (fullpath, entry, type, value)			X	名前付きの値が、指定した値に完全に一致するNUMBERまたはTEXTであることを確認します。

FilenamesMatchingRegex の Equals、GreaterThan、およびLessThan については、正規表現ルールのリファレンスを参照してください。

条件が存在するかどうかの確認（Existsルール）

名前が「**Exists**」で終わるルールは、ファイル、ディレクトリ、レジストリキー、またはその他のアイテムの存在を確認するために使用されます。KACE エージェントがデバイス上でアイテムを見つけた場合、そのルール

によって true が返され、アイテムのインベントリ詳細は インストールされているプログラム として表示されます。

次のいずれかのExistsルールを使用します。

- DirectoryExists (path)
- FileExists (path)
- RegistryKeyExists (registryPath)
- EnvironmentalVariableExists (var)
- PlistValueExists (fullpath, entry)
- FilenameMatchingRegexExist (fullpath, regex)

例：ディレクトリ（フォルダ）を確認する

次の例では、Windowsディレクトリがデバイス上に存在するかどうかを確認するテストを行います。

DirectoryExists(C:\WINDOWS\)

例：ファイルを確認する

注: 次の例では、メモ帳実行可能ファイルがデバイス上に存在することを確認します。

FileExists(C:\WINDOWS\notepad.exe)

デバイス設定の評価（Equalsルール）

名前が**Equals**で終わるルールは、デバイス上で設定した値を、ルールで指定した値に比較するために使用します。値が正確に一致する場合は、ルールによってtrueが返されます。

データ型を設定した引数を使用するルールでは、同じ型の値のみを比較できます。

次のいずれかのEqualsルールを使用します。

- FileVersionEquals (path, version)
- ProductVersionEquals (path, version)
- FileInfoEquals (fullpath, attribute, type, value)
- RegistryValueEquals (registryPath, valueName, value)
- EnvironmentalVariableEquals (var, type, value)
- PlistValueEquals (fullpath, entry, type, value)
- FilenameMatchingRegexEqual (fullpath, regex, value)

例：JAVA_HOME設定をテストする

JAVA_HOME 設定が C:\Program Files\Java\jdk1.6.0_02 であることを確認するには：

EnvironmentVariableEquals(JAVA_HOME, TEXT, C:\Program Files\Java\jdk1.6.0_02)

例：McAfee®レジストリエントリ設定をテストする

設定で使用されている形式がエントリ内の日付の形式と同じであることを確認します。

RegistryValueEquals(HKEY_LOCAL_MACHINE\Software\McAfee\AVEngine, AVDatDate, 2014/03/01)

例：Windows 7 Service Pack 1 を検出する

Windows 7 Service Pack 1 は、もともとは Windows 7 がインストールされていて SP1 にアップグレードされたデバイスでのみ、プログラムの追加と削除 に表示されます。このアイテムのデフォルトアプリケーションインベントリには、SP1上で既に動作しているデバイスは反映されません。それらのデバイスは、もともとSP1のレベルでイメージを作成されているためです。

Windows 7 Service Pack 1 の展開にアプライアンスを使用するときは、カスタムアプリケーションについて次のカスタムインベントリルールを作成します。

RegistryValueEquals(HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\
CurrentVersion,CSDVersion,Service Pack 2)

このアイテムがインストールされているデバイスを除外して、SP2 レベルに既にあるデバイス (つまり、アップグレードされた Windows 7 デバイスと、SP1 レベルでもともとイメージを作成されたデバイス) にアプライアンスが SP2 を展開しないようにします。

デバイス値の比較 (Greater ThanルールとLess Thanルール)

名前が **GreaterThan** と **LessThan** で終わる関数は、Table 24でリストされている値を比較します。

次のいずれかのGreater ThanルールとLess Thanルールを使用します。

- FileVersionGreaterThan (path, version)とFileVersionLessThan (path, version)
- ProductVersionGreaterThan (path, version)とProductVersionLessThan (path, version)
- FileInfoGreaterThan (fullpath, attribute, type, value)とFileInfoLessThan (fullpath, attribute, type, value)
- RegistryValueGreaterThan (registryPath, valueName, value)とRegistryValueLessThan (registryPath, valueName, value)
- EnvironmentalVariableGreaterThan (var, type, value)とEnvironmentalVariableLessThan (var, type, value)
- PlistValueGreaterThan (fullpath, entry, type, value)とPlistValueLessThan (fullpath, entry, type, value)
- FilenameMatchingRegexGreaterThan (fullpath, regex, value)とFilenameMatchingRegexLessThan (fullpath, regex, value)

例：製品のバージョンが次以降であるかをテストする

製品バージョンが特定の番号以降であることを確認します。

ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe, 78)

製品バージョンが特定の番号以降であることを確認するには、次のように入力します。

ProductVersionEquals(C:\Program Files\Mozilla Firefox\firefox.exe, 78)
または ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe,
78)

例：製品バージョンの範囲をテストする

製品バージョンが範囲内であるかをテストするには、less thanルールとgreater thanルールを組み合わせます。

ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe, 77)
および ProductVersionLessThan(C:\Program Files\Mozilla Firefox\firefox.exe, 79)

重要: ルールを個別の行に入力しないでください。ルールの区切りにはスペースのみを使用します。ルールを個別の行に配置すると、複合ルールが無効になります。

複数の条件のテスト

「および」演算子や「または」演算子を使用してルールを連結して複数の条件をテストできます。

注: 同じカスタムインベントリルールでの「および」と「または」の両方の演算子の使用はサポートされていません。個別のアプリケーションをセットアップします。

条件付きルールの連結により次の結果が得られます。

- 「および」演算子：すべてのルールによってtrueが返されると、結果としてtrueが返されて、インストールされているプログラムとしてアプリケーションがレポートされます。
- 「または」演算子：1つのルールのみによってtrueが返されると、インストールされているプログラムとしてアプリケーションがレポートされます。

重要: ルールを個別の行に入力しないでください。ルールの区切りにはスペースのみを使用します。ルールを個別の行に配置すると、複合ルールが無効になります。

複数のtrue条件の確認（「および」）

すべてのルールがtrueである場合のみ、インストールされているプログラムとしてアイテムがレポートされるようにするには、「カスタムインベントリフィールド」で「および」演算子を使用して条件付きルールを連結します。

カスタムインベントリフィールド で、次の構文を使用してルールを連結します。

Function
(**arguments...**
) AND **Function**
(**arguments**
) AND ...

条件文と演算子の区切りにはスペースを使用します。

例：レジストリキーを確認して値を比較する

Windowsデバイス上のレジストリキーとレジストリエントリ値を確認するには、次に示しているように、「および」を使用してルールを連結します。

RegistryKeyExists(registryPath) AND RegistryValueEquals(registryPath, valueName, value)

1つのtrue条件の確認（「または」）

または演算子を使用してルールを連結すると、Custom Inventory Field（カスタムインベントリフィールド）でのいずれかのルールが true である場合、アプリケーションがデバイスの Installed Program（インストールされているプログラム）リストに表示されます。

カスタムインベントリフィールド で、次の構文を使用してルールを連結します。

Function
(**arguments**
) OR **Function**
(**arguments**
) OR ...

関数ステートメントと演算子の区切りにはスペースを使用します。

例：レジストリ値を確認する

レジストリエントリがある値か別の値であることを確認します。

RegistryValueEquals(registryPath, valueName, value) OR RegistryValueEquals(registryPath, valueName, value)

ヒント: 範囲を指定するには、RegistryValueGreaterThanルールとRegistryValueLessThanルールを「および」演算子で連結して使用します。

デバイス（カスタムインベントリフィールド）からの値の取得

ValueReturn で終わるルールを使用すると、デバイスから情報を収集できます。これらのルールを使用して、KACE エージェントでは通常収集されない情報を収集できます。

返された値は、カスタムアプリケーション表示名（タイトル）に設定されます。これは、デバイスの詳細 ページの Installed Programs（インストールされているプログラム） と Custom Inventory Fields（カスタムインベントリフィールド）にある ソフトウェア に表示されます。

カスタムインベントリフィールド の値は、インストールの管理およびソフトウェアの配布に使用します。さらに、各種レポート、特定基準で表示 のフィルタ、Smart Labelの検索条件に加えて、自動的に検出された設定を使用して実行できるその他のプロセスにも使用できます。

このセクションでは、次のトピックを取り上げます。

- 値戻しルールのリファレンス
- レジストリキー値の取得
- コマンド出力の取得
- PLIST値の取得
- 複数の値の取得

値戻しルールのリファレンス

次の表には、カスタムインベントリフィールド の設定に使用できるすべての値戻しルールを示しています。

構文	Win	RHEL	OS X	説明
RegistryValueReturn (registryPath, valueName, type)	X			レジストリエントリの値を返し、データ型を指定した型に設定します。
EnvironmentalVariableReturn (var, type)環境またはユーザー変数の指定	X	X	X	環境変数の値を返し、データ型を指定した型に設定します。
FileInfoReturn (path, attribute, type)	X	X	X	ファイル属性の値を返します。有効な型については、ルールでの引数の定義を参照してください。
ShellCommandTextReturn (command)	X	X	X	コマンドの出力を返し、データ型をTEXTに設定します。
ShellCommandDateReturn (command)	X	X	X	コマンドの出力を返し、データ型をDATEに設定します。
ShellCommandNumberReturn (command)	X	X	X	コマンドの出力を返し、データ型をNUMBERに設定します。
PlistValueReturn (fullpath, entry, type)			X	PLISTキーの値を返し、データ型をTEXT、NUMBER、またはDATEに設定します。

ファイル情報値の取得

FileInfoReturnルールを使用して、カスタムインベントリフィールド に任意のWindowsファイル情報属性を設定できます。

例：Mozilla Firefox のバージョンを取得

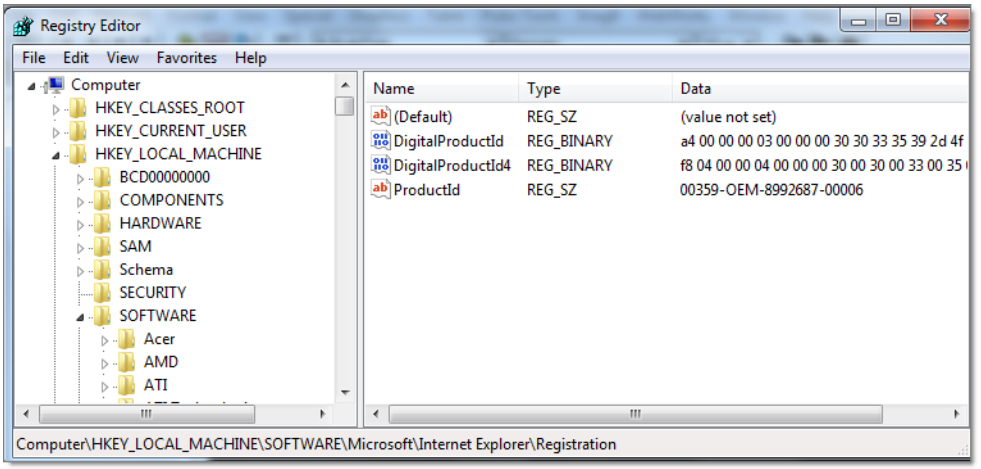
次の例では、Mozilla Firefox の製品バージョンを取得するために、カスタムインベントリフィールド を NUMBER として設定します。

カスタムインベントリフィールド で、次のように入力します。

FileInfoReturn(C:\Program Files\Mozilla Firefox\firefox.exe,CurrentVersion,TEXT)

レジストリキー値の取得

RegistryValueReturn ルールを使用して、Custom Inventory Field（カスタムインベントリフィールド）にレジストリキーを設定できます。ここで、registryPath（左側）はエントリへのパスです。valueName（右側上）は返されるキーです。



例：Mozilla Firefox CurrentVersion キーを取得

カスタムインベントリフィールド を CurrentVersion レジストリキーとして設定するには：

RegistryValueReturn (HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion, TEXT

コマンド出力の取得

コマンドルールを使用すると、カスタムインベントリフィールド にコマンドの出力を設定できます。コマンドは、デバイス上のコマンドインタプリタと実行可能パスによって異なります。

例えば、Windowsデバイスでは、MS-DOSコマンドを記述できます。しかし、Cygwinがインストールされておらず、一部のユーザーしかデフォルトパスを使用できない場合、CygwinスタイルのUNIXコマンドは記述できません。

次のいずれかのルールを使用して、カスタムインベントリフィールド にコマンドの出力を設定します。

- ShellCommandTextReturn (command)
- ShellCommandDateReturn (command)
- ShellCommandNumberReturn (command)

例：Mac OS Xで稼働時間を取得する

カスタムインベントリフィールド を稼働時間として設定します。

ShellCommandTextReturn(/usr/bin/uptime | sed -e 's/.*load averages://'| awk '{print $1}')

PLIST値の取得

PlistValueReturnルールを使用すると、カスタムインベントリフィールド をプロパティリスト（ PList ）キーとして設定できます。

例：システムロケールを取得する

システム指定言語に基づいた管理対象インストールを使用してアプリケーションを配布するには、まず、次のルールを入力してデバイスロケールを取得してから、対応する Smart Label を作成します。この Smart Label は、KACE エージェントによって カスタムインベントリフィールド にレポートされた言語コードに基づいてデバイスに適用されます。

PlistValueReturn(~/Library/Preferences/GlobalPreferences.plist, AppleLocale, TEXT)

複数の値の取得

「および」または「または」のいずれかの演算子を使用して、ValueReturnルールを連結します。いずれの値も空でない場合は、ルールにより、インストールされているプログラムとしてアプリケーションが表示されます。

連結された値はすべて、演算子によって区切られた同じ カスタムインベントリフィールド に設定されます。したがって、検索条件、フィルタ、レポート、およびその他のアプライアンスのプロセスに使用される場合、手法的にはTEXTと見なされます。

演算子を使用した ValueReturn ルールの連結：

- 「および」演算子：すべての値は カスタムインベントリフィールド にレポートされます。
- 「または」演算子：すべての値は カスタムインベントリフィールド にレポートされます。

カスタムインベントリフィールドで、次の構文を使用してルールを連結します。

Function (**arguments...**)「および」 **Function** (**arguments**) 「および」 ...

条件文と演算子の区切りにはスペースを使用します。同じルールで「および」演算子と「または」演算子を連結しないでください。

正規表現を使用したファイル名のマッチ

正規表現を使用して、指定したディレクトリ内のファイルに対して、指定した文字または文字列とファイル名とのマッチを行います。

このセクションでは、条件付きルールと値戻しルールで正規表現を使用してファイル名のマッチを行う正規表現について説明します。

注: KACE エージェントには、正規表現を使用してファイル名を比較する関数のみが用意されています。

正規表現の理解

正規表現構文を使用して、ファイル名のマッチを実行できます。

ヒント: 正規表現の記述の詳細については、http://msdn.microsoft.com/en-us/library/az24scfc.aspxを参照してください。

次の表に、ファイル名のマッチに使用できる正規表現構文の概要を示します。

文字	説明	式の例	ターゲットファイル	マッチするファイル
（任意の文字列）	特殊文字以外の文字を入力すると、その文字列が含まれるすべてのファ	abc	abcFile.xls Example.jpg File.doc	abcFile.xls Myabc.txt MyFile.abc

文字	説明	式の例	ターゲットファイル	マッチするファイル
	イル名とマッチします。		Myabc.txt MyFile.abc	
.	ドットは任意の1文字とマッチします。単独で入力すると、すべてのファイルとマッチします。	.	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc
\	バックスラッシュが特殊文字をエスケープ処理し、前方参照を作成するために使用されます。 詳細については、http://rexegg.com/regex-capture.htmlを参照してください。	.*\.txt$	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc	Myabc.txt
^	キャレットは、指定した文字をファイル名の先頭でマッチさせます。	^k	install.exe kinstaller.exe runkbot.bat	kinstaller.exe
|	パイプは、マッチさせる一連のオプションを区切ります。	run|install	install.exe kinstaller.exe runkbot.bat	install.exe kinstaller.exe runkbot.bat
$	ドルは、指定した文字をファイル名の末尾でマッチさせます。	bat$	install.exe kinstaller.exe runkbot.bat	runkbot.bat
?	疑問符は、直前の文字と0回または1回マッチします。	\.log10?$	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 mylog.log10
*	アスタリスクは、直前の文字と0回以上マッチします。	\.log1*$	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 app.log appconf.log11

文字	説明	式の例	ターゲットファイル	マッチするファイル
+	正符号は、直前の文字と1回以上マッチします。	ap+.*\.log	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log appconf.log11
[ ]	角かっこは、文字クラスを囲み、角かっこ内の任意の1文字とマッチします。 文字クラスの特殊文字のルールが通常の正規表現と異なります。	[123]	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 afile.txt3 appconf.log11 mylog.log10
()	文字を丸かっこで囲むと、後方参照が作成され、前の文字または囲んだ文字、あるいはその両方とマッチします。 詳細については、http://rexegg.com/regex-capture.htmlを参照してください。	(p)\1	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log appconf.log11
{n}	中かっこは、指定した回数だけ直前の文字を繰り返します。ここで、**n**は1以上です。	{p}\.log$	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log

正規表現ルールのリファレンス

正規表現ルールの構文は、他のファイルルールとはわずかに異なります。fullpath引数はファイルの場所への絶対パスにマッチする文字列ですが、ファイル名を含みません。ファイル名は、正規表現を使用して個別の引数として指定します。

次の表に、正規表現を使用できる一連のルールを示します。

構文	Win	RHEL	OS X	説明
FilenamesMatchingRegex (fullpath,regex)	X	X	X	指定したディレクトリ内のいずれかのファイルが正規表現を使用して入力したファイル名にマッチする場合

構文	Win	RHEL	OS X	説明
				は、trueが返されます。
FilenamesMatchingRegexGreaterThan (fullpath,regex,value)	X	X		マッチするファイルの数が指定した値より大きい場合は、trueが返されます。
FilenamesMatchingRegexLessThan (fullpath,regex,value)	X	X		マッチするファイルの数が指定した値より小さい場合は、trueが返されます。
FilenamesMatchingRegexEqual (fullpath,regex,value)	X	X		マッチするファイルの数が指定した値と同じ場合は、trueが返されます。
FilenamesMatchingRegexReturn (fullpath,regex,type)	X	X		カスタムインベントリフィールドにマッチしたファイル名（パスを含む）を設定します。

ルールでの引数の定義

カスタムインベントリルールで引数を定義して、パス、ファイル、レジストリキー、レジストリエントリ、バージョン情報、環境変数、およびその他の属性を検索できます。

ルールの構文については、条件の確認（条件付きルール）、デバイス（カスタムインベントリフィールド）からの値の取得、および正規表現を使用したファイル名のマッチの表を参照してください。

パスまたはファイルの検索

pathとfullpathは、デバイス上のディレクトリまたはファイルへの絶対パスを指定する文字列です。例：

C:\Program Files\Mozilla Firefox\firefox.exe

KACE エージェントはディレクトリまたはファイルを見つけて、特定のテストを行います。

レジストリキーとエントリの検索

registryPathは、レジストリ内のレジストリキーへの絶対パスを指定する文字列です。例：

HKEY_LOCAL_MACHINE/application/kace

バージョンの指定

version は、KACE エージェントがデバイスでテストするアイテムのバージョンと比較する整数（型は TEXT）です。

例えば、FileVersionGreaterThanテストでは、指定した値がファイルまたはフォルダのバージョン番号より大きい場合は「true」が返され、それ以外の場合は「false」が返されます。

範囲をテストするには、Less ThanとGreater Thanのルールを次のように連結します。

FileVersionGreaterThan(C:\Program Files\Adobe\Acrobat\7.0\Acrobat\Acrobat.exe, 6.99)
「および」FileVersionLessThan(C:\Program Files\Adobe\Acrobat\7.0\
Acrobat\Acrobat.exe, 8.00)

環境またはユーザー変数の指定

varは、デバイス上の環境変数の実際の名前にマッチする文字列です。

例えば、Program Filesディレクトリ変数が正しく設定されていることをテストするには、次のように入力します。

EnvironmentVariableEquals(ProgramFiles, TEXT,
C:\Program Files)

ファイル属性の指定

attribute は、システムプロパティ、ファイル / フォルダのプロパティ、またはデバイス上で KACE エージェントに割り当てられたプロパティです。アプライアンスには、オペレーティングシステムに依存した引数の型が用意されています。

Windowsファイル属性の使用

FileInfoGreaterThan、FileInfoLessThan、FileInfoEquals の各関数を使用して、Windows 上のファイルプロパティを次の構文でテストできます。

FunctionName (fullpath, attribute, type, value)

次の表に、Windowsでサポートされる属性を示します。

属性	タイプ	説明
AccessedDate	日付	ファイルがアクセスされた前回の日時。
Comments	テキスト	診断目的に提供する追加の情報。
CompanyName	テキスト	ファイルを生成した会社の名前。
CreatedDate	日付	ファイルが作成された日付。
FileBuildPart	番号	ファイルのバージョンの3番目の数字。例：バージョン1.2.3の場合、3=ビルド。
FileDescription	テキスト	Windowsファイルプロパティの詳細 ページのファイルの説明。
FileMajorPart	番号	ファイルのバージョンの1番目の数字。例：バージョン1.2.3の場合、1=メジャー。
FileMinorPart	番号	ファイルのバージョンの2番目の数字。例：バージョン1.2.3の場合、2=マイナー。
FileName	テキスト	ファイルの現在の名前。FileExistsも参照してください。

属性	タイプ	説明
FilePrivatePart	番号	ファイルのバージョンの4番目の数字。例：バージョン1.2.3.4の場合、4=プライベート。
FileVersion	テキスト	ファイルプロパティの 詳細 ページに表示された完全なファイルのバージョン。 FileVersionEquals、FileVersionGreaterThan、およびFileVersionLessThanも参照してください。
InternalName	テキスト	コンポーネント名などの、ファイルの内部名（存在する場合）。 ファイルに内部名がない場合、拡張子を省いた元のファイル名と同じです。
言語	テキスト	言語コード。ファイルプロパティの 詳細 ページに表示されている対応する名前です。
LegalCopyright	テキスト	ファイルに適用される著作権情報。
LegalTrademarks	テキスト	ファイルに適用される商標と登録商標。
ModifiedDate	日付	ファイルが修正された前回の日時。
OriginalFilename	テキスト	デバイスに配置またはインストールされたときのファイルのフルネームを指定します。
PrivateBuild	テキスト	ファイルのバージョンに関する情報。
ProductBuildPart	番号	製品のバージョンの3番目の数字。例：バージョン1.2.3の場合、3=ビルド。
ProductMajorPart	番号	製品のバージョンの1番目の数字。例：バージョン1.2.3の場合、1=メジャー。
ProductMinorPart	番号	製品のバージョンの2番目の数字。例：バージョン1.2.3の場合、2=マイナー。
ProductName	テキスト	Windowsのプロパティの製品名にマッチする文字列。

属性	タイプ	説明
ProductPrivatePart	番号	製品のバージョンの4番目の数字。例：バージョン1.2.3.4の場合、4=プライベート。
ProductVersion	テキスト	製品版。 ProductVersionEquals、ProductVersionGreaterThan、およびProductVersionLessThanも参照してください。
SpecialBuild	テキスト	ビルドに関する追加の情報。

LinuxとMacのファイル属性のテスト

LinuxデバイスとMacデバイス上で、次の引数を使用してファイル属性をテストできます。

属性	タイプ	説明
access_time	日付	ユーザーまたはシステムがファイルに前回アクセスした時刻
block_size	番号	ファイルのブロックサイズ
blocks	番号	ファイルによって使用されているブロックの数
creation_time	日付	ファイルが作成された時刻
device_number	番号	ファイルが格納されているデバイス（ディスク）の識別番号
group	テキスト	ファイル所有者のグループ名
inode	番号	ファイルのinode番号
modification_time	日付	変更が前回加えられたか保存された時刻
number_links	番号	ファイルへのハードリンクの数
owner	テキスト	ファイルを所有するユーザーの名前
size	番号	ファイルのサイズ

データ型の指定

typeは、テストされるか返されるデータの型を識別します。

KACE エージェントは次の型をサポートしています。

- TEXT - 文字列です。Equalsのような条件付きルールで完全に一致する場合にのみ有効です。ValueReturnルールでは、「カスタムインベントリフィールド」のタイプが文字列に設定されるため、検索条件とフィルタはマッチ演算子に制限されます。
- NUMBER - 整数です。すべての条件付きルールで有効なため、比較対象として整数を指定できます。
- DATE - 必ず MM/dd/yyyy HH:mm:ss の形式にしてください。例：09/28/2006 05:03:51。時刻は必須です。例えばgreater thanのような比較で、少なくとも00:00:00として時刻を指定する必要があります。

テストする値の指定

バージョンルールでのようにデータ型が既知であるルールを除いて、valueは通常、typeに従います。指定する値は、型と一致している必要があります。詳細については、「データ型の指定」を参照してください。

レジストリエントリの名前の指定（Windowsのみ）

valueNameは、テストするレジストリエントリの名前にマッチする文字列です。Windowsデバイスのレジストリテストでのみ使用します。

PLISTキーの指定（Macのみ）

entryはNUMBER、TEXT、またはDATEのいずれかであり、Mac OS Xデバイス上のPLISTファイル内のキーにマッチします。必要なキーがPLISTファイル内のアレイ/辞書に含まれている場合、アレイ/辞書の名前/整数、区切りコロン、キーの名前/整数（**dictionary**:**key**）をentry引数に指定して参照できます。

引数の例：

- **PackageGroups**というアレイ内のキー**Item 0**は、引数にPackageGroups:0を使用して参照されます。
- **Item 102**という辞書内のキー**contentType**は、引数に102:contentTypeを使用して参照されます。

正規表現の使用

regexは、条件付きルールまたは値戻しルールでファイル名にマッチさせる正規表現です。詳細については、正規表現を使用したファイル名のマッチを参照してください。

コマンドの定義

シェルコマンド関数を使用すると、デバイスで実行するコマンドを指定できます。ルールの引数を記述するためのガイドラインはコマンドに適用されません。ただし、開始かっこの直後と終了かっこの直前のスペースはコマンドから削除されます。

カスタムインベントリルールのテスト

カスタムインベントリルールをテストするために、KACE エージェント管理対象デバイスでカスタムインベントリコマンドを実行することができます。この機能により、インベントリプロセス全体を実行せずにカスタムインベントリルールをデバッグできます。

1. KACE エージェントがインストールされているデバイスで、コマンドプロンプトを開きます。
2. 次のコマンドを入力します。kdeploy -custominventory

   エージェントがアプライアンスに接続し、カスタムインベントリを実行します。クエリと戻り値が表示されます。

管理対象デバイスへのパッケージの展開

管理対象デバイスにパッケージを展開し、アプライアンスを使用してソフトウェアをリモートでインストールできます。

ソフトウェアの配布とWake On LANの使用

アプライアンスからアプリケーション、アップデート、およびファイルを管理対象デバイスに配布できます。また、Wake On LANを使用して、デバイスの電源をリモートでオンにすることができます。

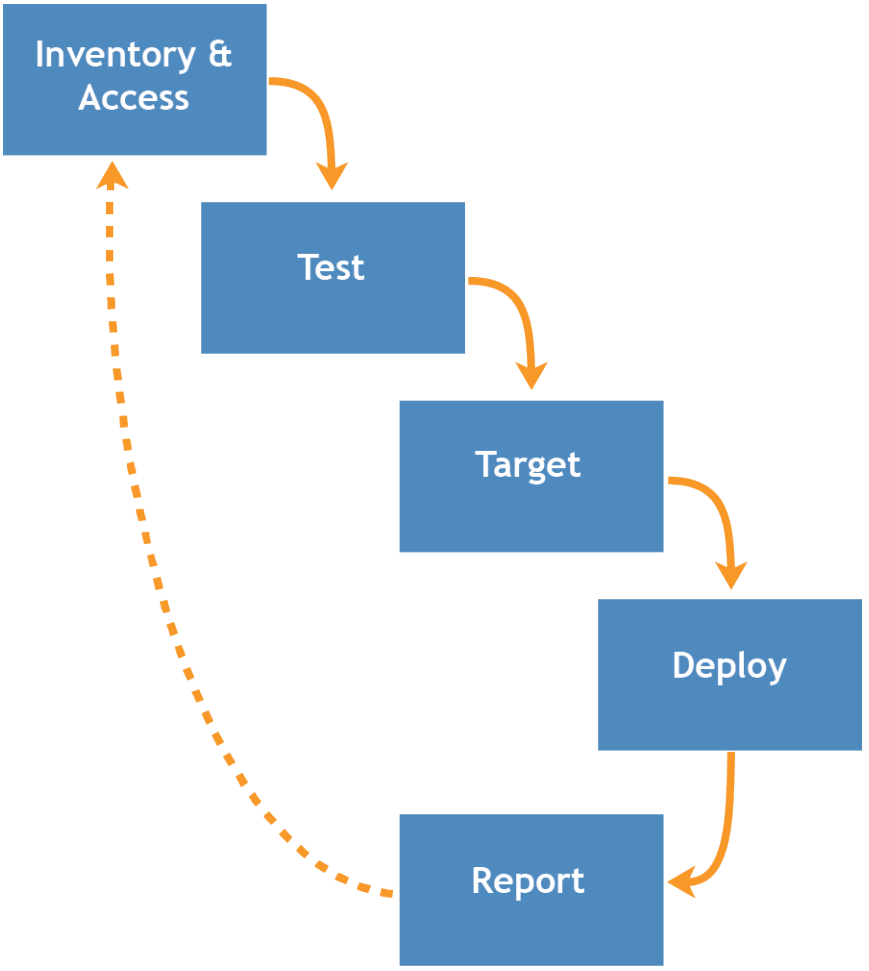
ソフトウェアの配布について

ソフトウェアは、アプライアンスからエージェント管理対象の Windows、Mac、および Linux デバイスに配布できます。

ヒント: ソフトウェアの配布は、ソフトウェア ページのアイテムおよびエージェントによって管理されるデバイスのみに実行できます。ソフトウェアカタログ ページのアイテム、Microsoft Application Virtualization（App-V）ソフトウェア、またはエージェント不要デバイスでは実行できません。

次の図に、ソフトウェア配布プロセスの例を概要レベルで示します。必要に応じてこのプロセスを変更できます。

ソフトウェア配布手順



ソフトウェアの配布のテストについて

数多くの管理対象デバイスにソフトウェアを配布する前に、代表的なデバイスの小さなグループで展開をテストして、パッケージにターゲットとなるオペレーティングシステムおよびその他のアプリケーションとの互換性があることを確認します。

アプライアンスは、ソフトウェアを管理対象デバイスに配布するときに、特定のデバイスまたはオペレーティングシステムに対してパッケージが指定されているかどうかを確認します。しかし、デバイス上の他のソフトウェアとのソフトウェアの互換性に関して、アプライアンスは評価できません。そのため、すべての展開をテストするプロセスを開発する必要があります。

例えば、デバイスにラベルを適用してテストグループを作成することができます。そのラベルを使用して、必要なアプリケーションをテストグループに展開し、それからデバイスのより大きなグループへの展開を実行します。このようにすることで、アプリケーションと、テストグループ内のオペレーティングシステムおよびその他のアプリケーションとの互換性を簡単に確認できます。デバイスのラベル付けの詳細については、手動ラベルの追加または編集を参照してください。

このセクションでは、このプロセスのテスト、ターゲット、および展開部分を主に取り上げます。インベントリの管理の詳細については、ソフトウェア ページでのアプリケーション管理を参照してください。

配布設定に対する変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

配布パッケージのタイプ

パッケージは、管理対象インストール、ファイル同期、ユーザーコンソールパッケージ、およびMSIインストーラとして管理対象デバイスに配布できます。

- **管理対象インストール**: サイレントモードまたはユーザーとの対話モードで設定が実行されるインストールパッケージ。管理対象インストールには、インストール用、アンインストール用、コマンドラインのパラメータが含まれています。詳細については、「管理対象インストールの使用」を参照してください。
- **ファイル同期**: 管理対象デバイスにファイルを配布する手段。ただし、管理対象インストールとは異なり、ファイル同期ではファイルがインストールされません。ファイルが単に配布されるだけです。詳細については、「ファイル同期の作成および使用」を参照してください。
- **ユーザーコンソールパッケージ**: プリンタドライバおよび他のアプリケーションが含まれ、ユーザーコンソールを通じて配布されるインストールパッケージ。詳細については、「サービスデスクについて」を参照してください。
- **MSI Installer template（MSIインストーラーテンプレート）**: Windows MSIベースのインストーラーを実行するためのポリシーを作成したり、基本的なコマンドライン引数を設定したりするユーティリティです。詳細については、「「MSIインストーラー」スクリプトの追加」を参照してください。

アプリケーションへのデジタル資産の添付とサポートされているオペレーティングシステムの選択

管理対象インストールまたは**ユーザーコンソール**ダウンロードを使用して管理対象デバイスにアプリケーションを配布するには、適切なデジタル資産をアプリケーションに添付する必要があります。デジタル資産は、展開に必要なファイルです（インストーラなど）。また、アプリケーションに対してサポートされているオペレーティングシステムを選択する必要があります。これらのタスクは、ソフトウェア 詳細ページで実行します。

このルールは、以下の場合にも適用されます。

- デバイスに、インストールファイルやデジタルファイルではなく、コマンドを送信する。
- EXE や MSI ファイルなどのデジタル資産を代替のダウンロード場所から取得するため、管理対象デバイスにインストールされている KACE エージェントをリダイレクトしようとしている。

詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。

アプライアンスからのパッケージの配布

アプライアンスから配布されるパッケージは、インベントリアイテムがデバイスのオペレーティングシステム上で実行されるように指定されている場合にのみ、管理対象デバイスに展開されます。

例えば、インベントリアイテムがWindows 7専用として指定されている場合、そのインベントリアイテムはWindows 8が実行されているデバイスには展開されません。

同様に、パッケージの展開もラベル要件を満たすデバイスに限定されます。例えば、パッケージが オフィス A というラベルに展開されるように設定されている場合、そのパッケージは オフィス A 以外のラベルのデバイス

には展開されません。アプライアンスでアプリケーションイベントアイテムが作成されると、そのアイテムがインストールされたオペレーティングシステムのみがインベントリ詳細レコードに記録されます。

管理対象インストールを展開するには、実行アクションと展開期間を選択する必要があります。詳細については、「管理対象インストールの使用」を参照してください。

代替のダウンロード場所およびレプリケーション共有からのパッケージの配布

パッケージは、代替のダウンロード場所およびレプリケーション共有から配布できます。

この配布方法は次の場合に役立ちます。

- リモートサイトの帯域幅が制限されており、アプライアンスへのアクセスで問題が発生する可能性がある。
- サイズの大きい配布パッケージがアプライアンスに保存されないようにする必要がある。

代替のダウンロード場所について

代替のダウンロード場所は、アプライアンスから他の管理対象デバイスへのソフトウェアの配布に必要なファイルをホストできる管理対象デバイスです。

代替のダウンロード場所には、特定のアプリケーションをインストールするために必要なすべてのファイルが格納されている任意のネットワーク上の場所を指定できます。UNCアドレスやDFSソースなどの代替のダウンロード場所からパッケージを配布できます。CIFSとSMBのプロトコル、SAMBAサーバー、およびファイルサーバーアプライアンスがサポートされています。代替のダウンロード場所は、管理対象インストールを作成する際に指定します。

詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。

レプリケーション共有について

レプリケーション共有は、配布用ファイルのコピーを保持するデバイスです。レプリケーション共有は、管理対象デバイスが地理上の複数の場所にわたって展開している場合に特に効果的です。

例えば、レプリケーション共有を使用すると、ロサンゼルスにあるアプライアンスからニューヨークにあるデバイスにファイルをダウンロードしなくても、ニューヨークの同じオフィスにある別のデバイスからファイルをダウンロードできます。レプリケーション共有は、すべてのデジタル資産の完全なレプリケーションであり、アプライアンスによって自動的に管理されます。ラベルでレプリケーション共有を指定していると、そのラベルに含まれるデバイスは、常にレプリケーション共有にアクセスしてファイルを取得します。

デバイスに適用されるラベルにレプリケーション共有が指定されていない場合、KACE エージェントは常にアプライアンスの配布ファイルを検索します。アプライアンスが複数のレプリケーション共有を使用している場合、エージェントはランダムに選択します。

詳細については、「レプリケーション共有の使用」を参照してください。

Mac OS Xデバイスへのアプリケーションの配布

アプライアンスでは、アプリケーション、更新、およびファイルをMac OS Xデバイスに配布するさまざまな方法が用意されています。

インストーラーおよびプレーンなパッケージについて

Mac OS Xには、通常のPKGファイル拡張子の付いたユニバーサルインストーラーがあります。PKGファイルを直接アップロードすることはできません。これらのファイルは下位ディレクトリで構成されており、アップロードするディレクトリ全体をWebブラウザが処理できないためです。

プレーンな（APP）パッケージは、Mac上のApplicationsフォルダにドラッグしてインストールできるので、インストーラーは必要ありません。ただし、APPパッケージもインストーラーパッケージと同様に下位ディレクトリで構成されるため、アーカイブする必要があります。

プレーンなアプリケーションと一緒にインストーラーをアーカイブできます。アプライアンスは、まずインストーラーを実行し、次にApplicationsフォルダにアプリケーションをコピーします。

Mac OS Xでサポートされているパッケージ展開

サポートされているパッケージ展開は、PKG、APP、DMG、ZIP、TGZ、およびTAR.GZです。

ディスクイメージとしてファイルをパッケージした場合、アプライアンスはそれをQuietモードでマウントおよびアンマウントします。このセクションでは、各タイプの展開の例を示します。これらの各例で、管理対象インストールパッケージを作成する前にアプライアンスにファイルをアップロードしておく必要があります。Questでは、アプリケーションをテストデバイスにインストールすることをお勧めします。KACE エージェントがアプライアンスに接続すると、アプライアンスはアプリケーション用にインベントリアイテムと管理対象インストールパッケージを作成します。

管理対象インストールの使用

管理対象インストール（MI）は、管理対象デバイスにアプリケーションを展開する、または管理対象デバイスからアプリケーションを削除するためのプライマリメカニズムです。各管理対象インストールでは、インストールまたは削除される特定のアプリケーションのタイトルおよびバージョンの情報（インストールコマンド、インストールファイル、ターゲットデバイス（ラベルによって識別）など）が記述されます。

管理対象インストールは、管理対象デバイスがアプライアンスにインベントリデータをアップロードするのと同時に常に実行されます。このように、アプライアンスは、インストールが実際に必要かどうかを、インストールを実行する前に確認します。インストールパッケージは、サイレントモードまたはユーザーとの対話モードで実行されるよう設定できます。管理対象インストールには、インストール用、アンインストール用、コマンドライン用のパラメータを含めることができます。

管理対象インストールでは、アプライアンスへのアクティブなネットワーク接続が必要です。インストール中に接続が中断された場合、エージェントが再接続したときにプロセスが続行されます。

Windowsでの最も一般的な管理対象インストールのパッケージ展開は、MSI、EXE、およびZIPファイルです。

Linuxデバイスでサポートされているパッケージ展開には、RPM、ZIP、BIN、TGZ、およびTAR.GZファイルなどがあります。

インベントリへのアプリケーションの追加

管理対象インストールを作成する前に、展開するファイルが ソフトウェア ページのアプリケーションと関連付けられている必要があります。アプリケーションが ソフトウェア ページにない場合は、必要に応じて追加できます。

ソフトウェア ページにないアプリケーションを追加するには、次のようにします。

- 管理対象デバイスにアプリケーションをインストールして、デバイスにインベントリの更新を要求する。詳細については、「インベントリ更新の強制実行」を参照してください。
- 手動でインベントリにアプリケーションを追加する。詳細については、「ソフトウェア ページインベントリへのアプリケーションの手動による追加」を参照してください。

注意: **アプリケーションインベントリアイテムの表示名が** Add/Remove **(プログラムの追加と削除)に登録されているアプリケーションの名前と完全に一致していない場合、パッケージの展開が(既に展開が完了している場合であっても)繰り返し試行されることがあります。この問題を解決するには、アプリケーションを** ソフトウェア **インベントリリストに追加し、登録したアプリケーション名を管理対象インストールで使用します。**

管理対象インストールの作成について

ソフトウェア ページに表示されるアイテムの管理対象インストールを作成できます。

詳細については、以下を参照してください。

- Windowsデバイス用の管理対象インストールの作成
- Mac OS Xデバイス用の管理対象インストールの作成
- RPMファイル用の管理対象インストールの作成
- TAR.GZファイル用の管理対象インストールの作成
- ZIPファイル用の管理対象インストールの作成

パラメータ、ラベル、展開定義などの特別な設定を使用してパッケージを作成する場合、1つのインベントリアイテムに対して複数の配布パッケージを作成できます。ただし、管理対象インストールでは、インベントリアイテムが1つのみであることが検証されるため、インベントリアイテムが複数あると検証エラーになります。

これらの各例で、管理対象インストールパッケージを作成する前にアプライアンスにファイルをアップロードしておく必要があります。アプリケーションをテストデバイスにインストールし、KACE エージェントがアプライアンスに接続され、アプリケーションのインベントリアイテムが作成された後、そのアプリケーションから管理対象インストールパッケージを作成することを、Quest ではお勧めします。

注: エージェントの展開については、KACE エージェントのプロビジョニングで説明しています。エージェントの既存のバージョンの更新の詳細については、エージェントのアップデートの手動アップロードを参照してください。

インストールパラメータについて

インストールパラメータは、管理対象デバイスでのアプリケーションの配布およびインストールに使用されるパッケージ定義に追加できます。

パッケージ定義には、MSI、EXE、ZIPの他、アプリケーションの導入に必要なその他のファイルタイプを含めることができます。管理者がローカルデバイスにファイルをインストールしている場合、1つのファイル、BATファイル、またはVBScriptを実行することにより、アプライアンスがパッケージをリモートでインストールすることができます。

配布とインストールのプロセスを効率化するために、ローカルデバイス上での実行時にインストーラに渡されるパラメータをパッケージ定義に含めることもできます。例えば、パラメータをカスタムインストール設定として使用すると、自動再起動を回避できます。

インストーラーファイルでサポートされているパラメータの確認

インストーラファイルでサポートされているパラメータは、 Windowsのコマンドラインで表示できます。

1. コマンドプロンプトを開きます。
2. ターゲットインストーラーが格納されているディレクトリに移動します。

   例：c:\...\adobe.exe
3. 「**filename** /?」と入力します。

例：adobe.exe /?

そのパッケージがサポートしているパラメータが表示されます。例：/quiet、/norestart

4. 確認されたパラメータを使用してパッケージ定義を更新します。

詳細については、アプリケーションベンダーのドキュメントを参照してください。

Windowsデバイス用の管理対象インストールの作成

エージェント管理対象のWindowsデバイスにソフトウェアを展開するための管理対象インストールを作成できます。

Windowsプラットフォーム用の管理対象インストールを作成する際、インストールの前後にユーザーにメッセージを表示するかどうかを指定できます。ユーザーのログイン時にパッケージを展開するかどうかを示したり、特定のラベルに展開を制限したりすることもできます。

MSI、EXE、または ZIP ファイル用の管理対象インストールの作成の詳細については、Windowsでの一般的な展開の例を参照してください。

管理対象デバイスにアプリケーションを配布するには、インストールに必要なファイルであるデジタル資産をアプリケーションに添付する必要があります。また、アプリケーションに対してサポートされているオペレーティングシステムを選択する必要があります。詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。

1. 管理対象インストールの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**配布** をクリックして、**管理対象インストール** をクリックします。
   c. **アクションの選択 > 新規作成** を選択します。
2. 設定 セクションで、次の情報を入力します。

オプション	説明
名前	管理対象インストールを識別するための名前。この名前は、管理対象インストール ページに表示されます。
実行	パッケージの展開設定。オプションは次の通りです。 • **無効**: パッケージを展開しません。 • **いつでも**: 次の機会にパッケージを展開します。次の機会とは、KACE エージェントがインベントリ情報を次回アプライアンスに送信するときなどです。 • **起動時**: デバイスが次回起動するときにパッケージを展開します。

オプション	説明
	注: Active Directoryまたはグループポリシーオブジェクトの設定により、ログイン前にユーザーの承認を必要とするメッセージがデバイスに表示される場合、メッセージが承認されるまでパッケージは展開されず、スクリプトも実行されません。 • **ログイン後**: ユーザーのログオン後、デスクトップが読み込まれる前にパッケージを展開します。 • **ユーザーのログオン中に実行**: ユーザーのログオン中にパッケージを展開します。 • **ユーザーのログオフ中に実行**: デバイスが実行中で、ユーザーがログオフしているときにのみパッケージを展開します。
インベントリ	このオプションの1つを選択して **カタログソフトウェア** または **ソフトウェア** からソフトウェアタイトルを展開するかどうかを示します。 • 特定のタイトルを検索するには、ソフトウェア フィールドまたは カタログソフトウェア フィールドに入力を始めます。 **注:** **未使用のソフトウェアライセンスのみを再利用します。**アンインストールするソフトウェアの名前が、デフォルトでこのフィールドに表示されます。詳細については、「未使用のソフトウェアライセンスの再利用」を参照してください。 • 1つまたは複数の関連ファイルがあるソフトウェアのみを表示するには、**関連付けられたファイルのあるソフトウェアのみを表示** を選択します。
関連付けられたファイル	ソフトウェアおよびカタログソフトウェアのタイトルには、必要に応じて1つまたは複数のファイルを添付できます。選択したソフトウェアのタイトルに関連する特定のファイルを選択するかどうかを指定します。 • **関連付けされたファイルを選択**：ファイルを関連付ける場合は、このオプションを選択します。ファイルは一覧から選択できます。ファイル名がわかっている場合は、ボックスに入力し始めます。リストに表示される使用可能なエントリからファイル名を選択します。 • **ファイルを関連付けない**：ファイルを関連付けない場合は、このオプションを選択します。
代替の場所	特定の管理対象インストール用ファイルのダウンロード元の場所を指定します。

オプション	説明
	パス: KACE エージェントがデジタルインストールファイルを取得できる場所を入力します。 **チェックサム**: リモートファイル共有のMD5チェックサムと一致する代替のチェックサム（MD5）を入力します。チェックサムを入力しない場合は、ファイル共有上のデジタル資産がアプライアンス上の展開パッケージに関連付けられたデジタル資産と一致する必要があります。また、ターゲットパスには完全なファイル名を含める必要があります（例: \\fileserver_one\software\adobe.exe）。チェックサムは、KACE エージェントと共にインストールされている KDeploy.exe など、任意のツールを使用して作成できます。 **KDeploy.exeを使用してチェックサムを作成するには:** a. KACE エージェントがインストールされているデバイス上で、コマンドプロンプトまたはターミナルウィンドウを開きます。 b. Quest KACEのインストールディレクトリに移動します。例： Windows 32ビットデバイス: C:\Program Files \Quest\KACE Windows 64ビットデバイス: C:\Program Files (x86)\Quest\KACE Mac OS Xデバイス: /Library/Application Support/Quest/KACE/bin c. 次のコマンドを入力します: KDeploy -hash=**filename** この場合の **filename** は、ファイルへの UNC パスです。パスにスペースが含まれる場合は、二重引用符でパス全体を囲みます。 d. **Ctrl + Cキー**または**Command + Cキー**を押して、MD5チェックサムをコピーします。コピーしたチェックサムをメモ帳などの他のファイルに貼り付けます。 **資格情報**：デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。 **注:** ターゲットデバイスがレプリケーションラベルの一部である場合、アプリケーションは代替のダウンロード場所から取得されません。既存のラベルを編集するか、新しいラベルを作成して、代替の場所をグローバルに指定します。そのラベルは任意の管理対象インストールに固有のラベルではないため、リモートファイル共有のチェックサムと一致する代替のチェックサムを指定できません。

オプション	説明
	代替のダウンロード場所およびレプリケーション共有からのパッケージの配布および手動ラベルの追加または編集を参照してください。
デフォルトのインストール	インストール時にデフォルトのコメントを使用します。 **その他のパラメータ**: 次のようにインストール動作を指定します。 • 最大フィールド長は256文字です。パスがこの制限を超える場合は、コマンドラインを使用して、パスとコマンドが含まれるBATファイルを指定します。 • ファイルパスにスペースが含まれる場合は、二重引用符でパス全体を囲みます。例："\\kace_share\demo files\share these files\setup.bat"
デフォルトのインストールのオーバーライド	完全なコマンドラインパラメータを指定します。使用可能な実行時オプションについては、MSIコマンドラインのドキュメントを参照してください。 • **アンインストール**: コマンドラインからアプリケーションをアンインストールします。 • **コマンドのみで実行（ファイルをダウンロードしない）**: コマンドラインのみを実行します。 • **msiexec.exeを先頭に追加しない**: ファイルの先頭に msiexec.exe が追加されないようにします。
ダウンロードされたファイルを削除する	展開の完了後、ファイルを削除します。
ITNinja	ITNinjaからの展開に関するヒント。このヒントは、使用率データを共有している場合のみ使用可能です。詳細については、「データ共有の基本設定の構成」を参照してください。

3. 次の展開設定を指定します。

オプション	説明
全デバイス	すべてのデバイスに展開します。展開を特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
ラベル	指定したラベルに属するデバイスだけに展開を制限します。ラベルを選択するには、**編集** をクリックしてラベルを 展開の制限対象 ウィンドウにドラッグし、**保存** をクリックします。 レプリケーション共有または代替のダウンロード場所が指定されているラベルを選択した場合、デジタル資産は、アプライアンスから直接ダウンロードされるのではなく、指定されたレプリケーション共有

オプション	説明
	または代替のダウンロード場所からコピーされます。 **注:** アプライアンスがKACE代替の場所を使用する前にレプリケーション共有を使用することが明らかになりました。
デバイス	展開対象を特定のデバイスのみに限定します。ドロップダウンリストから、アプリケーションの展開先のデバイスを選択します。リストをフィルタリングするには、デバイス フィールドに数文字入力します。フィールドの横の数字は、使用可能なデバイスの数を示しています。 **注:** **未使用のソフトウェアライセンスのみを再利用します。**該当するソフトウェアを削除するすべてのデバイスが表示されます。必要に応じて、デバイスのリストを編集できます。すべてのデバイスからソフトウェアを削除するには、上記の説明に従って、単にを選択するだけです。詳細については、「未使用のソフトウェアライセンスの再利用」を参照してください。

4. ユーザー通知設定を指定します。

オプション	説明
実行前にユーザーに警告	インストールの前に管理対象デバイスにメッセージを表示します。このオプションを選択すると、次のフィールドが表示されます。 • **メッセージ**: インストールの開始前に管理対象デバイスに表示されるメッセージ。まず、ユーザーが後で管理対象インストールを実行できるようにする、再通知オプションを使用します。 • **タイムアウト**: メッセージが表示される期間（分単位）。 • **アクション**: **初期メッセージタイムアウト** で指定した期間の終了時に実行されるアクション。オプションとして、**後でインストール** または **今すぐインストール** があります。**今すぐインストール** を選択すると、アプリケーションが即座にインストールされます。**後でインストール** を選択すると、ユーザーの応答があるまでインストールが先送りされます。後でインストール は、インストールまたは再起動を実行前にユーザーに通知する場合に便利です。

オプション	説明
初期メッセージ	インストールの前に管理対象デバイスにメッセージを表示します。このオプションを選択すると、次のフィールドが表示されます。 • **メッセージ**: インストールの開始前に管理対象デバイスに表示されるメッセージ。 • **タイムアウト**: メッセージが表示される期間（分単位）。 • **アクション**: **初期メッセージタイムアウト** で指定した期間の終了時に実行されるアクション。オプションとして、**後でインストール** または **今すぐインストール** があります。**今すぐインストール** を選択すると、アプリケーションが即座にインストールされます。**後でインストール** を選択すると、ユーザーの応答があるまでインストールが先送りされます。後でインストール は、インストールまたは再起動を実行前にユーザーに通知する場合に便利です。
完了メッセージ	インストールの完了後、管理対象デバイスにメッセージを表示します。このオプションを選択すると、次のフィールドが表示されます。 • **メッセージ**: インストールの完了後に管理対象デバイスに表示されるメッセージ。 • **タイムアウト**: メッセージが表示される期間（分単位）。

5. スケジュールオプションを選択します。

オプション	説明
展開ウィンドウ 開始 終了	パッケージの展開を開始および終了する時刻（24時間制）。Deployment Window（展開期間）の時刻は、すべての Action（アクション）オプションに反映されます。また、アプライアンスの 設定 で定義した実行間隔は、特定のパッケージの展開期間より優先されるか、組み合わせて使用されます。
優先順位	アプリケーションをインストールまたはアンインストールする順序。最小値を指定したアプリケーションが最初に展開されます。同じ順序の値を持つインストールアクションとアンインストールアクションがある場合、アンインストールアクションが最初に実行されます。 **注:** 管理対象インストールは、指定したソフトウェアパッケージがソフトウェアカタログに含まれているかソフトウェアリストに含まれているかにかかわらず、常に順番に展開されます。展開順序の数値が小さい管理対象インストールがある場合、それらが正常にインストールされるか、指定された再試行時間を超えるまで、他の管理対象インストールは常に実行されません。

オプション	説明
最大試行回数	最大試行回数。パッケージのインストールが試行される回数を0〜99の間で指定します。「0」を指定すると、パッケージのインストールが無制限に試行されます。

6. 保存 をクリックします。

Windowsでの一般的な展開の例

最も一般的な管理対象インストールのパッケージ展開は、MSI、EXE、およびZIPファイルです。

標準MSIの例

MSIファイルの使用は、Windowsデバイスにソフトウェアを展開するための簡単で自己完結的な方法です。MSIファイルに対して特殊な変換やカスタマイズを必要としない場合は、簡単に展開できます。

インストールで他のスイッチを使用する場合は、/i スイッチが必要です。

アプライアンスのパラメータ行にファイル名やmsiexec構文は必要ありません。/*の入力のみが必要です。

/qn /I（正）

msiexec /I /qn（誤）

注: MSIファイルでパラメータを使用するには、すべてのターゲットデバイスに同じバージョンのWindowsインストーラ（Microsoftから入手可能）が存在している必要があります。一部のスイッチは、より古いバージョンではアクティブではない場合があります。Windowsインストーラの最新のバージョンはアプライアンスを使用してデバイスに配布できます。

ヒント: Windowsインストーラー3.0以上を使用している場合、サポートされているパラメータを確認するには、スタート メニューから **プログラムの実行** を選択します。ポップアップウィンドウに「msiexec」と入力します。サポートされているパラメータのリストが示されたウィンドウが表示されます。

標準EXEの例

EXEファイルは、1つの例外を除き、MSIファイルに似ています。

EXEファイルとMSIファイルの相違点は、次のとおりです。EXEファイルを使用する場合は、実行パラメータ 行で「/I」を指定する必要はありません。

実行可能ファイルを使用するときは、多くの場合、Quietまたはサイレントインストールのスイッチパラメータを指定することが役立ちます。パラメータを切り替えるには、実行パラメータ フィールドで「/?」を指定します。

ZIPファイル用の管理対象インストールの作成

ZIPファイルを使用したソフトウェアの展開は、タイトルの展開で複数のファイルが必要な場合にソフトウェアをパッケージ化する便利な方法です。

例えば、ソフトウェアタイトルにはsetup.exeファイル、設定ファイル、データファイルが必要な場合があります。特定のアプリケーションをインストールするために必要なファイルのグループが格納されているCD-ROMがある場合、それらのファイルを1つのZIPファイルにパッケージ化し、展開対象としてアプライアンスにアップロードできます。

注: KACE エージェントでは、拡張子が MSI および EXE の展開パッケージは自動的に実行されます。

注: さらに、複数のファイルを含むZIPアーカイブを作成し、アーカイブの解凍時に特定のファイルが実行されるように指定することもできます。展開パッケージ内のコマンド（実行可能）フィールドで、実行するファイルの名前を指定します（例：runthis.exe）。

管理対象デバイスにアプリケーションを配布するには、インストールに必要なファイルであるデジタル資産をアプリケーションに添付する必要があります。また、アプリケーションに対してサポートされているオペレーティングシステムを選択する必要があります。詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。

1. 必要なインストールファイルが格納されている場所を参照してすべてのファイルを選択し、WinZIP®などのユーティリティを使用してZIPファイルを作成します。
2. アプライアンス管理者コンソールにログインします。
3. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
4. ターゲット展開用のインベントリアイテムを作成します。

   インベントリ > ソフトウェア ページから、または定期的にアプライアンスに接続するデバイスへのパッケージのインストールにより、この作成を手動で行うことができます。詳細については、「ソフトウェアページについて」を参照してください。
5. ZIPファイルとインベントリアイテムを関連付けて、アプライアンスにアップロードします。
   a. 左側のナビゲーションバーで、**配布** をクリックして、**管理対象インストール** をクリックします。
   b. **アクションの選択 > 新規作成** を選択します。
   c. ソフトウェア ドロップダウンリストから、ZIPファイルが関連付けられているアプリケーションタイトルを選択します。すべてのアプリケーションタイトルを表示するには、**関連ファイルがあるレコードのみを表示する** チェックボックスをオフにします。
6. 実行パラメータ フィールドで、引数を付けて完全なコマンドを指定します。

   例：setup.exe /qn
7. 必要に応じて、追加の設定を指定します。

   詳細については、「Windowsデバイス用の管理対象インストールの作成」を参照してください。
8. **保存** をクリックします。

RPMファイル用の管理対象インストールの作成

Linuxベースデバイスに、RPMファイルを使用してソフトウェアを展開するための管理対象インストールを作成できます。

管理対象デバイスにアプリケーションを配布するには、インストールに必要なファイルであるデジタル資産をアプリケーションに添付する必要があります。また、アプリケーションに対してサポートされているオペレーティングシステムを選択する必要があります。詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。

1. 管理対象インストールの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**配布** をクリックして、**管理対象インストール** をクリックします。
   c. **アクションの選択 > 新規作成** を選択します。
2. ソフトウェア ドロップダウンリストから、ソフトウェアタイトルを選択します。タイトルを検索するには、ソフトウェア フィールドに入力し始めます。

   KACE エージェントで RPM ファイルのインストールが試行される際、デフォルトでは以下のコマンドが使用されます。一般的に、新しいパッケージをインストールするか、既存のパッケージを新しいバージョンに更新するためには、このコマンドで十分です。

   rpm -U **packagename.rpm**

ZIP、TGZ、またはTAR.GZファイルを選択している場合は、コンテンツが解凍され、ルートディレクトリですべてのRPMファイルが検索されます。インストールコマンドは検出された各RPMファイルに対して実行されます。アプライアンスでは、すべてのRPMファイルがアーカイブのトップレベルで自動的に検索されます。そのため、一度に複数のパッケージをインストールできます。また、シェルスクリプトを格納したアーカイブを作成し、完全なコマンドとしてそのスクリプト名を指定することもできます。アーカイブが見つかった場合はアプライアンスでそのコマンドが実行され、見つからなかった場合はアプライアンスのログにエラーが記録されます。

Run Parameters（実行パラメータ）フィールドでパラメータを指定しない限り、デフォルトのパラメータが使用されます。

使用するファイル名内にワイルドカードを指定できます。ファイル名にスペースが含まれる場合は、一重または二重引用符でファイル名を囲みます。ファイルは「/tmp」ディレクトリに抽出され、そのディレクトリがコマンドの現在の作業ディレクトリになります。

注: Red Hat Linux上では、必要とされているのがスクリプトの実行のみの場合、アーカイブに他のファイルを格納する必要がありません。

root アカウントの path 環境変数に現在の作業ディレクトリが含まれていない場合、アーカイブに格納したシェルスクリプトまたはその他の実行可能ファイルを実行するときは、Full Command Line（完全なコマンドライン）フィールドで実行可能ファイルへの相対パスを指定します。コマンドは、抽出されたファイルのあるディレクトリ内で実行されます。

例えば、installThis.shというシェルスクリプトを実行するには、RPMファイルのあるディレクトリ内でそのスクリプトをパッケージしてから、インストールコマンド フィールドに「./installThis.sh」というコマンドを入力します。別のディレクトリにスクリプトをアーカイブする場合は、インストールコマンド フィールドに次のように入力します。

./dir/filename.sh

これらの例は両方とも、アプライアンスの他の一部の機能と同様、sh がルートのパスに含まれていることを前提としています。別のスクリプト言語を使用している場合は、実行するコマンドプロセッサへの完全なパスをインストールコマンドで指定しなければならないことがあります。例えば、次のようなパスを指定します。

/bin/sh ./**filename**.sh

無人バッチスクリプトの該当する引数を含めます。

MI の詳細でアンインストールのチェックボックスをオンにした場合、KACE エージェントでは、スタンドアロン RPM ファイルまたはアーカイブ内で見つかった各 RPM ファイルに対して次のコマンドが実行され、パッケージが自動的に削除されます。

//usr/sbin/rpm -e **packagename**.rpm

パッケージが削除されるのは、アーカイブまたはパッケージがデバイスにダウンロードされている場合のみです。「完全なコマンドライン」を使用したアンインストール チェックボックスをオンにした場合は、インストールコマンド フィールドで完全なコマンドラインを指定して、正しい削除コマンドが適切パッケージに対して確実に実行されるようにします。この場合はパッケージがダウンロードされないため、パッケージの受取確認が保存されるインストールデータベースでパスを指定します。

3. パッケージで追加のオプションが必要な場合は、以下の情報を入力します。

オプション	説明
名前	管理対象インストールを識別するための名前。この名前は、管理対象インストール ページに表示されます。
実行	このパッケージを展開する最適なタイミングを選択できます。Linux プラットフォームの場合、オプションは **Anytime (next available)**（いつでも実行（次回に有効））と **無効** です。

オプション	説明
インベントリ	このオプションの1つを選択して **カタログソフトウェア** または **ソフトウェア** からソフトウェアタイトルを展開するかどうかを示します。 • 特定のタイトルを検索するには、ソフトウェア フィールドまたは カタログソフトウェア フィールドに入力を始めます。 **注: 未使用のソフトウェアライセンスのみを再利用します。**アンインストールするソフトウェアの名前が、デフォルトでこのフィールドに表示されます。詳細については、「未使用のソフトウェアライセンスの再利用」を参照してください。 • 1つまたは複数の関連ファイルがあるソフトウェアのみを表示するには、**関連付けられたファイルのあるソフトウェアのみを表示** を選択します。
関連付けられたファイル	ソフトウェアおよびカタログソフトウェアのタイトルには、必要に応じて1つまたは複数のファイルを添付できます。選択したソフトウェアのタイトルに関連する特定のファイルを選択するかどうかを指定します。 • **関連付けされたファイルを選択**：ファイルを関連付ける場合は、このオプションを選択します。ファイルは一覧から選択できます。ファイル名がわかっている場合は、ボックスに入力し始めます。リストに表示される使用可能なエントリからファイル名を選択します。 • **ファイルを関連付けない**：ファイルを関連付けない場合は、このオプションを選択します。
代替の場所	特定の管理対象インストール用ファイルのダウンロード元の場所を指定します。 **パス**: KACE エージェントがデジタルインストールファイルを取得できる場所を入力します。 **チェックサム**: リモートファイル共有のMD5チェックサムと一致する代替のチェックサム（MD5）を入力します。チェックサムを入力しない場合は、ファイル共有上のデジタル資産がアプライアンス上の展開パッケージに関連付けられたデジタル資産と一致する必要があります。また、ターゲットパスには完全なファイル名を含める必要があります（例：\\fileserver_one\software\adobe.exe）。チェックサムは、KACE エージェントと共にインストールされている KDeploy.exe など、任意のツールを使用して作成できます。 **KDeploy.exeを使用してチェックサムを作成するには:**

オプション	説明
	a. KACE エージェントがインストールされているデバイス上で、コマンドプロンプトまたはターミナルウィンドウを開きます。 b. Quest KACEのインストールディレクトリに移動します。例： Windows 32ビットデバイス: C:\Program Files \Quest\KACE Windows 64ビットデバイス: C:\Program Files (x86)\Quest\KACE Mac OS Xデバイス: /Library/Application Support/Quest/KACE/bin c. 次のコマンドを入力します: KDeploy -hash=**filename** この場合の **filename** は、ファイルへの UNC パスです。パスにスペースが含まれる場合は、二重引用符でパス全体を囲みます。 d. **Ctrl + Cキー**または**Command + Cキー**を押して、MD5チェックサムをコピーします。コピーしたチェックサムをメモ帳などの他のファイルに貼り付けます。 **資格情報**：デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。 **注:** ターゲットデバイスがレプリケーションラベルの一部である場合、アプリケーションは代替のダウンロード場所から取得されません。既存のラベルを編集するか、新しいラベルを作成して、代替の場所をグローバルに指定します。そのラベルは任意の管理対象インストールに固有のラベルではないため、リモートファイル共有のチェックサムと一致する代替のチェックサムを指定できません。 代替のダウンロード場所およびレプリケーション共有からのパッケージの配布および手動ラベルの追加または編集を参照してください。
インストールコマンド	インストールコマンドのオプション。
デフォルトのインストール	RPMファイルを使用しており、かつアプライアンスでデフォルトのインストールコマンドが実行されるようにする場合は、このオプションを選択します。Linuxデバイスで使用されるコマンド: rpm [-U | Run Parameters] "**packagename**.tgz" **実行パラメータ**:（オプション）**デフォルトの使用**を選択した場合は、使用するパラメータを指定します。RPMファイルを使用している場合、実行パラメータは不要です。 優先させる値を入力します（デフォルトは「-U」）。

オプション	説明
	例えば、次のように **Run Parameters** を設定したとします。-ivh --replacepkgs。この場合、デバイス上で実行されるコマンドは次のようになります。 rpm -ivh –replacepkgs package.rpm
デフォルトのインストールのオーバーライド	完全なコマンドラインを指定する場合は、このオプションを選択します。アーカイブファイルを使用している場合は、検出されたすべてのRPMファイルに対してこのコマンドが実行されます。
アンインストール	コマンドラインを使用して、デバイスからパッケージを削除します。完全なコマンドライン フィールドでコマンドを指定した場合は、そのコマンドが実行されます。それ以外の場合、KACE エージェントでは、パッケージを削除する際に一般的に使用されるコマンドの実行が試行されます。
コマンドのみで実行 (ファイルをダウンロードしない)	コマンドのみを実行します。実際のデジタル資産はダウンロードしません。
ダウンロードされたファイルを削除する	展開の完了後、ファイルを削除します。
ITNinja	ITNinjaからの展開に関するヒント。このヒントは、使用率データを共有している場合のみ使用可能です。詳細については、「データ共有の基本設定の構成」を参照してください。

4. 次の展開設定を指定します。

オプション	説明
全デバイス	すべてのデバイスに展開します。展開を特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
ラベル	指定したラベルに属するデバイスだけに展開を制限します。ラベルを選択するには、**編集** をクリックしてラベルを 展開の制限対象 ウィンドウにドラッグし、**保存** をクリックします。 レプリケーション共有または代替のダウンロード場所が指定されているラベルを選択した場合、デジタル資産は、アプライアンスから直接ダウンロードされるのではなく、指定されたレプリケーション共有または代替のダウンロード場所からコピーされます。 **注:** アプライアンスがKACE代替の場所を使用する前にレプリケーション共有を使用することが明らかになりました。
デバイス	展開対象を特定のデバイスのみに限定します。ドロップダウンリストから、アプリケーションの展開先のデバイスを選択します。リストをフィルタリングするには、デバイス フィールドに数文字入力しま

オプション	説明
	す。フィールドの横の数字は、使用可能なデバイスの数を示しています。 **注: 未使用のソフトウェアライセンスのみを再利用します。**該当するソフトウェアを削除するすべてのデバイスが表示されます。必要に応じて、デバイスのリストを編集できます。すべてのデバイスからソフトウェアを削除するには、上記の説明に従って、単にを選択するだけです。詳細については、「未使用のソフトウェアライセンスの再利用」を参照してください。

5. ユーザー通知設定を指定します。

オプション	説明
実行前にユーザーに警告	インストールの前に管理対象デバイスにメッセージを表示します。このオプションを選択すると、次のフィールドが表示されます。 • **メッセージ**: インストールの開始前に管理対象デバイスに表示されるメッセージ。まず、ユーザーが後で管理対象インストールを実行できるようにする、再通知オプションを使用します。 • **タイムアウト**: メッセージが表示される期間（分単位）。 • **アクション**: **初期メッセージタイムアウト** で指定した期間の終了時に実行されるアクション。オプションとして、**後でインストール** または **今すぐインストール** があります。**今すぐインストール** を選択すると、アプリケーションが即座にインストールされます。**後でインストール** を選択すると、ユーザーの応答があるまでインストールが先送りされます。後でインストール は、インストールまたは再起動を実行前にユーザーに通知する場合に便利です。
初期メッセージ	インストールの前に管理対象デバイスにメッセージを表示します。このオプションを選択すると、次のフィールドが表示されます。 • **メッセージ**: インストールの開始前に管理対象デバイスに表示されるメッセージ。 • **タイムアウト**: メッセージが表示される期間（分単位）。 • **アクション**: **初期メッセージタイムアウト** で指定した期間の終了時に実行されるアクション。オプションとして、**後でインストール** または **今すぐインストール** があります。**今すぐインストール** を選択すると、アプリケーションが即座にインストールされます。**後でインストール** を選択すると、ユーザーの応答があるまでインストールが先送りされます。後でインストール は、インストールまたは再起動

オプション	説明
	を実行前にユーザーに通知する場合に便利です。
完了メッセージ	インストールの完了後、管理対象デバイスにメッセージを表示します。このオプションを選択すると、次のフィールドが表示されます。 • **メッセージ**: インストールの完了後に管理対象デバイスに表示されるメッセージ。 • **タイムアウト**: メッセージが表示される期間（分単位）。

6. スケジュールオプションを選択します。

オプション	説明
展開ウィンドウ 開始 終了	パッケージの展開を開始および終了する時刻（24時間制）。Deployment Window（展開期間）の時刻は、すべての Action（アクション）オプションに反映されます。また、アプライアンスの 設定 で定義した実行間隔は、特定のパッケージの展開期間より優先されるか、組み合わせて使用されます。
優先順位	アプリケーションをインストールまたはアンインストールする順序。最小値を指定したアプリケーションが最初に展開されます。同じ順序の値を持つインストールアクションとアンインストールアクションがある場合、アンインストールアクションが最初に実行されます。 **注:** 管理対象インストールは、指定したソフトウェアパッケージがソフトウェアカタログに含まれているかソフトウェアリストに含まれているかにかかわらず、常に順番に展開されます。展開順序の数値が小さい管理対象インストールがある場合、それらが正常にインストールされるか、指定された再試行時間を超えるまで、他の管理対象インストールは常に実行されません。
最大試行回数	最大試行回数。パッケージのインストールが試行される回数を0〜99の間で指定します。「0」を指定すると、パッケージのインストールが無制限に試行されます。

7. **保存** をクリックします。

TAR.GZファイル用の管理対象インストールの作成

TAR.GZファイルを使用したソフトウェアの展開は、特定のソフトウェアタイトルの展開で複数のファイルが必要な場合にソフトウェアをパッケージ化する便利な方法です。

例えば、一部のアプリケーションでは、展開のためにRPMなどの複数のファイル、設定、およびデータファイルが必要です。これらのファイルをまとめてTAR.GZファイルにパッケージ化し、アプライアンスにアップロードして、TAR.GZファイルを使用する管理対象インストールを作成できます。

管理対象デバイスにアプリケーションを配布するには、インストールに必要なファイルであるデジタル資産をアプリケーションに添付する必要があります。また、アプリケーションに対してサポートされているオペレーティングシステムを選択する必要があります。詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。

1. 次の2つのコマンドを使用して、TAR.GZファイルを作成します。
    a. tar –cvf **filename**.tar **packagename**.rpm
    b. gzip **filename**.tar

    これにより、**filename**.tar.gz が作成されます。
2. アプライアンス管理者コンソールにログインします。
3. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
4. ターゲット展開用のインベントリアイテムを作成します。

    これを手動で行うには、インベントリ > ソフトウェア ページを選択するか、定期的にアプライアンスに接続される管理対象デバイスにパッケージをインストールします。詳細については、「ソフトウェア ページについて」を参照してください。
5. TAR.GZファイルとインベントリアイテムを関連付けて、アプライアンスにアップロードします。
    a. 左側のナビゲーションバーで、**配布** をクリックして、**管理対象インストール** をクリックします。
    b. **アクションの選択 > 新規作成** を選択します。
    c. ソフトウェア ドロップダウンリストから、TAR.GZファイルが関連付けられているアプリケーションタイトルを選択します。

        インストール時にこのファイルが解凍され、各RPMパッケージに対してインストールコマンドが実行されます。

    実行パラメータが指定されていない場合は、-Uが使用されます。

    完全なコマンドラインを指定する必要はありません。アプライアンスによってインストールコマンドは自動的に実行されます。Linuxデバイスは、次のコマンドを使用してインストールを試みます。

    rpm [-U | Run Parameters] "**packagename**.tgz"

    d. **オプション**：複数のファイルを使用している場合は、それらのファイルを含むZIPアーカイブを作成し、アーカイブの解凍時に特定のファイルが実行されるように指定できます。

    これを行うには、展開パッケージ内のコマンド（実行可能）フィールドで、実行するファイルの名前を指定します（例：runthis.exe）。追加のパッケージ詳細を提供します。詳細については、「管理対象インストールの使用」を参照してください。

    e. **保存** をクリックします。

KACE エージェントでは、拡張子が RPM の展開パッケージは自動的に実行されます。

Mac OS Xデバイス用の管理対象インストールの作成

必要に応じて、Mac OS Xデバイス用の管理対象インストールを作成できます。

管理対象デバイスにアプリケーションを配布するには、インストールに必要なファイルであるデジタル資産をアプリケーションに添付する必要があります。また、アプリケーションに対してサポートされているオペレーティングシステムを選択する必要があります。詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。

1. 管理対象インストールの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**配布** をクリックして、**管理対象インストール** をクリックします。
c. **アクションの選択 > 新規作成** を選択します。

2. ソフトウェア ドロップダウンリストでアプリケーションを選択します。

   KACE エージェントで PKG ファイルのインストールが試行される際、デフォルトでは以下のコマンドが使用されます。

   installer -pkg packagename.pkg -target / [Run Parameters]

   DMG、ZIP、または TGZ を選択している場合、その内容が解凍され、ルートディレクトリですべての PKG ファイルが検索されます。インストールコマンドは各 PKG ファイルに対して実行され、各ファイルをアルファベット順に処理します。

   次に、アプライアンスは、アーカイブのトップレベルですべてのプレーンなアプリケーション（APP）を検索し、次のコマンドを使用して Applications フォルダに各アプリケーションをコピーします。

   ditto -rscs Application.app /Applications/Application.app

   スクリプトを実行するか、これらのコマンドラインのいずれかを変更するために、**完全なコマンドライン**として該当するスクリプト呼び出しを指定できます。使用するファイル名内にワイルドカードを指定できます。ファイル名にスペースが含まれる場合は、一重または二重引用符でファイル名を囲みます。ファイルは「/tmp」ディレクトリに抽出され、そのディレクトリがコマンドの現在の作業ディレクトリになります。

   ヒント: Mac OS X上では、必要な作業がスクリプトの実行だけの場合、アーカイブにその他のファイルを格納する必要はありません。

3. パッケージに追加のオプションが必要な場合は、次の詳細を指定します。

オプション	説明
名前	管理対象インストールを識別するための名前。この名前は、管理対象インストール ページに表示されます。
実行	パッケージの展開設定。オプションは次の通りです。 • **無効**: パッケージを展開しません。 • **いつでも**: 次の機会にパッケージを展開します。次の機会とは、KACE エージェントがインベントリ情報を次回アプライアンスに送信するときなどです。 • **起動時**: デバイスが次回起動するときにパッケージを展開します。

オプション	説明
	注: Active Directoryまたはグループポリシーオブジェクトの設定により、ログイン前にユーザーの承認を必要とするメッセージがデバイスに表示される場合、メッセージが承認されるまでパッケージは展開されず、スクリプトも実行されません。 • **ログイン後**: ユーザーのログオン後、デスクトップが読み込まれる前にパッケージを展開します。 • **ユーザーのログオン中に実行**: ユーザーのログオン中にパッケージを展開します。 • **ユーザーのログオフ中に実行**: デバイスが実行中で、ユーザーがログオフしているときにのみパッケージを展開します。
インベントリ	このオプションの1つを選択して **カタログソフトウェア** または **ソフトウェア** からソフトウェアタイトルを展開するかどうかを示します。 • 特定のタイトルを検索するには、ソフトウェア フィールドまたは カタログソフトウェア フィールドに入力を始めます。 **注:** **未使用のソフトウェアライセンスのみを再利用します。**アンインストールするソフトウェアの名前が、デフォルトでこのフィールドに表示されます。詳細については、「未使用のソフトウェアライセンスの再利用」を参照してください。 • 1つまたは複数の関連ファイルがあるソフトウェアのみを表示するには、**関連付けられたファイルのあるソフトウェアのみを表示** を選択します。
関連付けられたファイル	ソフトウェアおよびカタログソフトウェアのタイトルには、必要に応じて1つまたは複数のファイルを添付できます。選択したソフトウェアのタイトルに関連する特定のファイルを選択するかどうかを指定します。 • **関連付けされたファイルを選択**：ファイルを関連付ける場合は、このオプションを選択します。ファイルは一覧から選択できます。ファイル名がわかっている場合は、ボックスに入力し始めます。リストに表示される使用可能なエントリからファイル名を選択します。 • **ファイルを関連付けない**：ファイルを関連付けない場合は、このオプションを選択します。
代替の場所	特定の管理対象インストール用ファイルのダウンロード元の場所を指定します。

オプション	説明
	パス: KACE エージェントがデジタルインストールファイルを取得できる場所を入力します。 **チェックサム**: リモートファイル共有のMD5チェックサムと一致する代替のチェックサム（MD5）を入力します。チェックサムを入力しない場合は、ファイル共有上のデジタル資産がアプライアンス上の展開パッケージに関連付けられたデジタル資産と一致する必要があります。また、ターゲットパスには完全なファイル名を含める必要があります（例: \\fileserver_one\software\adobe.exe）。チェックサムは、KACE エージェントと共にインストールされている KDeploy.exe など、任意のツールを使用して作成できます。 **KDeploy.exeを使用してチェックサムを作成するには:** a. KACE エージェントがインストールされているデバイス上で、コマンドプロンプトまたはターミナルウィンドウを開きます。 b. Quest KACEのインストールディレクトリに移動します。例： Windows 32ビットデバイス: C:\Program Files \Quest\KACE Windows 64ビットデバイス: C:\Program Files (x86)\Quest\KACE Mac OS Xデバイス: /Library/Application Support/Quest/KACE/bin c. 次のコマンドを入力します: KDeploy -hash=**filename** この場合の **filename** は、ファイルへの UNC パスです。パスにスペースが含まれる場合は、二重引用符でパス全体を囲みます。 d. **Ctrl + Cキー**または**Command + Cキー**を押して、MD5チェックサムをコピーします。コピーしたチェックサムをメモ帳などの他のファイルに貼り付けます。 **資格情報**：デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。 **注:** ターゲットデバイスがレプリケーションラベルの一部である場合、アプリケーションは代替のダウンロード場所から取得されません。既存のラベルを編集するか、新しいラベルを作成して、代替の場所をグローバルに指定します。そのラベルは任意の管理対象インストールに固有のラベルではないため、リモートファイル共有のチェックサムと一致する代替のチェックサムを指定できません。

オプション	説明
	代替のダウンロード場所およびレプリケーション共有からのパッケージの配布および手動ラベルの追加または編集を参照してください。
デフォルトのインストール	インストールコマンドを指定する必要はありません。サーバーによってインストールコマンドは自動的に実行されます。Mac OS Xデバイスは、次のコマンドを使用してパッケージのインストールを試みます。 installer -pkg packagename.pkg -target / [Run Parameters] または ditto -rsrc packagename.app /Applications/theapp アーカイブファイルを指定している場合、このコマンドは見つかったPKGファイルまたはAPPファイルのすべてに対して実行されます。
デフォルトのインストールのオーバーライド	完全なコマンドラインパラメータを指定します。使用可能な実行時オプションについては、MSIコマンドラインのドキュメントを参照してください。 **注:** DMG パッケージを使用する場合は、マウントされた DMG ファイルのファイルパスはコマンドラインに相対的にする必要があります。 • **アンインストール**: コマンドラインからアプリケーションをアンインストールします。 • **コマンドのみで実行 (ファイルをダウンロードしない)**: コマンドラインのみを実行します。 • **msiexec.exeを先頭に追加しない**: ファイルの先頭に msiexec.exe が追加されないようにします。
ダウンロードされたファイルを削除する	展開の完了後、ファイルを削除します。
ITNinja	ITNinjaからの展開に関するヒント。このヒントは、使用率データを共有している場合のみ使用可能です。詳細については、「データ共有の基本設定の構成」を参照してください。

注: ユーザー通知メッセージは、Mac OS Xデバイスでは使用できません。

4. 次の展開設定を指定します。

オプション	説明
全デバイス	すべてのデバイスに展開します。展開を特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
ラベル	指定したラベルに属するデバイスだけに展開を制限します。ラベルを選択するには、**編集** をクリックし

オプション	説明
	てラベルを 展開の制限対象 ウィンドウにドラッグし、**保存** をクリックします。 レプリケーション共有または代替のダウンロード場所が指定されているラベルを選択した場合、デジタル資産は、アプライアンスから直接ダウンロードされるのではなく、指定されたレプリケーション共有または代替のダウンロード場所からコピーされます。 **注:** アプライアンスがKACE代替の場所を使用する前にレプリケーション共有を使用することが明らかになりました。
デバイス	展開対象を特定のデバイスのみに限定します。ドロップダウンリストから、アプリケーションの展開先のデバイスを選択します。リストをフィルタリングするには、デバイス フィールドに数文字入力します。フィールドの横の数字は、使用可能なデバイスの数を示しています。 **注:** **未使用のソフトウェアライセンスのみを再利用します。**該当するソフトウェアを削除するすべてのデバイスが表示されます。必要に応じて、デバイスのリストを編集できます。すべてのデバイスからソフトウェアを削除するには、上記の説明に従って、単にを選択するだけです。詳細については、「未使用のソフトウェアライセンスの再利用」を参照してください。

5. スケジュールオプションを選択します。

オプション	説明
展開ウィンドウ 開始 終了	パッケージの展開を開始および終了する時刻（24時間制）。Deployment Window（展開期間）の時刻は、すべての Action（アクション）オプションに反映されます。また、アプライアンスの 設定 で定義した実行間隔は、特定のパッケージの展開期間より優先されるか、組み合わせて使用されます。
優先順位	アプリケーションをインストールまたはアンインストールする順序。最小値を指定したアプリケーションが最初に展開されます。同じ順序の値を持つインストールアクションとアンインストールアクションがある場合、アンインストールアクションが最初に実行されます。 **注:** 管理対象インストールは、指定したソフトウェアパッケージがソフトウェアカタログに含まれているかソフトウェアリストに含まれているかにかかわらず、常に順番に展開されます。展開順序の数値が小さい管理対象インストールがある場合、それらが正常にインストールされるか、指定された再試行時間を超えるまで、他の管理対象インストールは常に実行されません。

オプション	説明
最大試行回数	最大試行回数。パッケージのインストールが試行される回数を0〜99の間で指定します。「0」を指定すると、パッケージのインストールが無制限に試行されます。

6. **保存** をクリックします。

詳細については、次を参照してください。

- ソフトウェアの配布とWake On LANの使用
- 管理対象インストールの使用

ファイル同期の作成および使用

ファイル同期を使用すると、エージェント管理対象デバイスにあらゆるタイプのファイルをプッシュアウトできます。

ファイル同期を使用すると、ファイルを管理対象デバイスに配布できます。ただし、管理対象インストールとは異なり、ファイル同期ではファイルがインストールされません。ファイルが単に配布されるだけです。ファイル同期は、管理対象デバイスに任意のタイプのファイルをコピーする場合に使用してください。

代替の場所 フィールドの文字列KACE_ALT_Locationは、対応するラベルによって割り当てられた値に置き換えられます。1つ以上のラベル内のデバイスに代替の場所を指定しないでください。

1. ファイル同期 リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**配布** をクリックして、**ファイル同期** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。

    このオプションを使用できない場合は、インベントリ内に関連ファイルがあるアプリケーションが存在しません。詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。
2. 設定 セクションで、次の情報を入力します。

オプション	説明
有効	ファイル同期を有効にします。選択したデバイス上の KACE エージェントがアプライアンスにチェックインすると、ファイルが配布されます。
名前	ファイル同期を識別する名前。この名前は、ファイル同期 ページに表示されます。
パス	ファイルを保存するターゲットデバイス上のディレクトリの場所。
パスの作成	パス フィールドで指定した場所がまだ存在しない場合は、その場所を作成します。
資格情報	デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格

オプション	説明
	情報を追加します。詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。
ファイル	ターゲットデバイスに配布されるファイル。リストにアプリケーションを表示するには、アプリケーションがインベントリ内のファイルに関連付けられている必要があります。詳細については、「アプリケーションへのデジタル資産の添付およびサポートされるオペレーティングシステムの選択」を参照してください。
配布を解凍しない	アプライアンスでファイルが解凍されないようにします。
維持	ファイルの配布を試行する前に、そのファイルがまだターゲットデバイスに存在しないことを確認します。
ショートカットの作成	ファイルの場所へのデスクトップショートカットをデバイス上に作成します。
名前	デスクトップショートカットの表示名。
一時ファイルの削除	展開の完了後、ファイルを削除します。
ITNinja	ITNinjaからの展開に関するヒント。このヒントは、使用率データを共有している場合のみ使用可能です。詳細については、「データ共有の基本設定の構成」を参照してください。

3. 次の展開設定を指定します。

オプション	説明
全デバイス	すべてのデバイスに展開します。展開を特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
ラベル	指定したラベルに属するデバイスだけに展開を制限します。ラベルを選択するには、**編集** をクリックしてラベルを 展開の制限対象 ウィンドウにドラッグし、**保存** をクリックします。 レプリケーション共有または代替のダウンロード場所が指定されているラベルを選択した場合、デジタル資産は、アプライアンスから直接ダウンロードされるのではなく、指定されたレプリケーション共有または代替のダウンロード場所からコピーされます。 **注:** アプライアンスがKACE代替の場所を使用する前にレプリケーション共有を使用することが明らかになりました。

オプション	説明
デバイス	展開対象を特定のデバイスのみに限定します。ドロップダウンリストから、アプリケーションの展開先のデバイスを選択します。リストをフィルタリングするには、デバイス フィールドに数文字入力します。フィールドの横の数字は、使用可能なデバイスの数を示しています。
初期メッセージ	インストールの前にデバイスにメッセージを表示します。
完了メッセージ	インストールの完了後、デバイスにメッセージを表示します。
ブラックアウトウィンドウ	管理対象デバイスのエージェントがファイル同期を実行できない期間。
代替の場所	特定の管理対象インストール用ファイルのダウンロード元の場所を指定します。 **パス**: KACE エージェントがデジタルインストールファイルを取得できる場所を入力します。 **チェックサム**: リモートファイル共有のMD5チェックサムと一致する代替のチェックサム（MD5）を入力します。チェックサムを入力しない場合は、ファイル共有上のデジタル資産がアプライアンス上の展開パッケージに関連付けられたデジタル資産と一致する必要があります。また、ターゲットパスには完全なファイル名を含める必要があります（例: \\fileserver_one\software\adobe.exe）。チェックサムは、KACE エージェントと共にインストールされている KDeploy.exe など、任意のツールを使用して作成できます。 **KDeploy.exeを使用してチェックサムを作成するには:** a. KACE エージェントがインストールされているデバイス上で、コマンドプロンプトまたはターミナルウィンドウを開きます。 b. Quest KACEのインストールディレクトリに移動します。例： Windows 32ビットデバイス: C:\Program Files\Quest\KACE Windows 64ビットデバイス: C:\Program Files (x86)\Quest\KACE Mac OS Xデバイス: /Library/Application Support/Quest/KACE/bin c. 次のコマンドを入力します: KDeploy -hash=**filename** この場合の **filename** は、ファイルへの UNC パスです。パスにスペースが含まれる場合は、二重引用符でパス全体を囲みます。 d. **Ctrl + Cキー**または**Command + Cキー**を押して、MD5チェックサムをコピーします。コピーしたチェックサムをメモ帳などの他のファイルに貼り付けます。

オプション	説明
	資格情報：デバイスに接続してコマンドを実行するために必要なサービスアカウントの詳細。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。 **注:** ターゲットデバイスがレプリケーションラベルの一部である場合、アプリケーションは代替のダウンロード場所から取得されません。既存のラベルを編集するか、新しいラベルを作成して、代替の場所をグローバルに指定します。そのラベルは任意の管理対象インストールに固有のラベルではないため、リモートファイル共有のチェックサムと一致する代替のチェックサムを指定できません。 代替のダウンロード場所およびレプリケーション共有からのパッケージの配布および手動ラベルの追加または編集を参照してください。

4. **保存** をクリックします。

ヒント: 展開期間の経過後、以前に展開されたファイルを配布するには、ファイル同期 の File Synchronization Detail（ファイル同期の詳細）ページにアクセスして、ページ下部の **ファイル保存して再送信する** をクリックします。

Wake On LANの使用

Wake On LAN を使用すると、KACE エージェントのインストールの有無にかかわらず、アプライアンスからリモートでデバイスの電源を投入できます。

注: Wake On LANを使用するには、デバイスにWake On LAN対応のネットワークインターフェイスカード（NIC）とBIOSが装備されている必要があります。

Wake On LAN の場合、アプライアンスではポート 7 を使用してネットワーク上に UDP トラフィックがブロードキャストされます。ターゲットデバイスへの「マジックパケット」を取得するために必要なブロードキャストアドレスを推測する必要があるため、アプライアンスでは Wake On LAN 要求あたり 16 個のパケットが送信されます。このトラフィックは、電源がリモートでオンにされていないデバイスでは無視されるため、このトラフィックによるネットワークへの重大な影響はありません。

アプライアンスと同じサブネットまたは別のサブネットに属するデバイスの電源をオンにできます。別のサブネットに関連付けられているデバイスの電源をオンにするには、KACE エージェントを Wake On LAN リレーとして指定する必要があります。

Wake On LAN要求の発行

複数のデバイスを一度にスリープ解除するには、それらのデバイスが属するラベルを指定します。または、デバイスを個別にスリープ解除できます。

スリープ解除するデバイスがアプライアンスでインベントリ登録されていなくても、MAC（ハードウェア）アドレスとデバイスの最新かつ既知のIPアドレスが分かっていれば、これらの情報を手動で入力してデバイスをスリープ解除できます。

1. Wake On LANスケジュール リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**配布** をクリックして、**Wake On LAN** をクリックします。

2. **アクションの選択 > 新規作成 > シンプル** を選択します。
3. 使用するデバイスのタイプを選択します。
   - **ラベルに属するデバイスをスリープ解除するには**、ラベル ドロップダウンリストからレベルを選択します。
   - **個々のデバイスをスリープ解除するには**、管理対象デバイス フィールドでデバイスを選択します。リストを検索するには、フィールドに入力し始めます。
   - **検出されたデバイスをスリープ解除するには**、検出されたデバイス フィールドでデバイスを選択します。リストを検索するには、フィールドに入力し始めます。
4. デバイス情報を手動で入力するには、次のいずれかを実行します。
   - IPアドレス フィールドで、**デバイスの IP アドレスを指定します。**
   - Manual Entry（**手動エントリ**）**セクションで、デバイスの MAC アドレスを指定します。**
5. **今すぐ実行** をクリックします。

ページ上部に結果が表示され、要求を受け取ったデバイスの数とそれらのデバイスが属するラベル（存在する場合）が示されます。

Wake On LAN要求のスケジュール

Wake On LAN要求のスケジュール設定は、デバイスを定期的にスリープ解除する場合に便利です。これは毎月のメンテナンスを実行するなどの繰り返しタスクに役立ちます。

別のサブネットに属しているデバイスのスリープを解除する場合は、そのデバイスのサブネットに属し、KACE エージェントインスタンスを実行しているマシンを見つけ、ラベルを割り当てることによりそのマシンをリレーとして指定する必要があります。ラベルの詳細については、アイテムのグループを管理するためのラベルのセットアップおよび使用を参照してください。

1. Wake-on-LAN Schedules（Wake On LANスケジュール）リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

   b. 左側のナビゲーションバーで、**配布** をクリックして、**Wake On LAN** をクリックします。
2. **アクションの選択 > 新規作成 > 高度** を選択します。
3. 使用するデバイスのタイプを選択します。
   - **ラベルに属するデバイスを選択するには**、設定 **セクションの** ラベル **の下で 関連づけられたラベルの管理 をクリックします。表示される** ラベルを選択 **ダイアログボックスで、選択するデバイスに関連付けられている 1 つまたは複数のラベルを選択します。ダイアログボックスを閉じます。**
   - **オペレーティングシステムでデバイスを選択するには オペレーティングシステムの管理 をクリックします。表示される オペレーティングシステム ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。**

     ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**すべて > Windows > Windows 10** の順に選択し、**x64** を選択します。
4. 別のサブネットに属しているデバイスをスリープ解除するには、リレーマシンを選択します。
   a. 設定 セクションの リレーラベル で、**関連ラベルの管理** をクリックします。

b. 表示される ラベルを選択 ダイアログボックスで、リレーデバイスに関連付けられているラベルを選択します。
c. ダイアログボックスを閉じます。

5. Wake On LAN 設定 ページの スケジュール セクションで、次のスケジュール設定を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（,）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（-）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（/）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（*）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。

オプション	説明
	例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

6. **保存** をクリックします。

Wake On LAN ページが表示され、スケジュール済みの要求が示されます。

Wake On LANのトラブルシューティング

特定の状況においてWake On LANが失敗する場合があります。

Wake On LANが失敗する可能性がある条件は、次のとおりです。

- デバイスにWake On LAN対応のネットワークカードが装備されていないか、適切に設定されていない。
- デバイスが接続されているサブネットに関して、間違った情報がアプライアンスに登録されている。
- UDPトラフィックがサブネット間でルーティングされないか、ネットワークデバイスによってフィルタリングされている。
- ブロードキャストトラフィックがサブネット間でルーティングされないか、ネットワークデバイスによってフィルタリングされている。
- ポート7上のトラフィックがネットワークデバイスによってフィルタリングされている。

詳細については、http://www.intel.com/content/www/us/en/support/network-and-i-o/ethernet-products/000005793.htmlを参照してください。

管理対象インストールのエクスポート

複数の組織またはアプライアンスがある場合は、必要に応じて、管理対象インストールをエクスポートし、組織間またはアプライアンス間で転送できます。

詳細については、「リソースのインポートとエクスポートについて」を参照してください。

管理対象デバイスへの警告のブロードキャスト

ポップアップメッセージとして表示される警告を、エージェント管理対象デバイス上にブロードキャストすることによって、ユーザーにメッセージを送信できます。

警告は、緊急情報を送信する必要がある場合、またはデバイス上でアクションやスクリプトを実行する際に前もってユーザーに通知する必要がある場合に便利です。

また、一定条件が満たされた場合に自動で送信されるEメール通知を作成することもできます。詳細については、「通知のスケジュール」を参照してください。

注: 管理対象デバイスにメッセージを表示するには、エージェントとアプライアンスが接続されている必要があります。エージェント接続の詳細については、エージェント設定の構成を参照してください。

注: このタイプの警告はアプライアンスで生成され、エージェント管理対象デバイスにブロードキャストされます。その他のタイプの警告として警告の監視があり、サーバデバイスでの監視を有効化して、基本的なパフォーマンス監視を実行している場合にサーバデバイスからアプライアンスに送信されます。詳細については、「サーバーの監視」を参照してください。

ブロードキャストされる警告の作成

必要に応じて、警告を作成し、エージェント管理対象デバイスにブロードキャストされるようにスケジュールできます。

1. 警告の詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**配布** をクリックして、**警告** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. 次の情報を入力します。

オプション	説明
メッセージ	表示する警告の内容を入力します。メッセージは500文字まで入力できます。
全デバイス	KACE エージェントがアプライアンスに接続されているすべてのデバイスに、メッセージを表示します。
緊急	メッセージが画面の中央に表示されます。ユーザーはこのメッセージを移動したり、バックグラウンドで表示したりすることはできません。作業を続行する前に、警告に対処する必要があります。
デバイス	選択したデバイスにメッセージを表示します。複数のデバイスを選択するには、**Ctrl**キーを押しながらクリックするか、**Command**キーを押しながらクリックします。

オプション	説明
ラベル	選択されたラベルに割り当てられたデバイスにのみメッセージを表示します。**関連ラベルの管理** をクリックして、デバイスラベルを選択します。複数のラベルを選択するには、**Ctrl**キーを押しながらクリックするか、**Command**キーを押しながらクリックします。
有効期限	メッセージが有効である時間の長さを指定します。ターゲットデバイスがアプライアンスに接続している場合は、ユーザーが **OK** をクリックしてメッセージを承認するまで、このメッセージはブロードキャストされ表示されます。 **注:** デバイスがアプライアンスに接続されていない場合、警告メッセージはエージェントコマンドキューに送信され、デバイスがアプライアンスに接続されるまでキューにとどまります。ターゲットデバイスが接続されると、有効期限が経過したかどうかにかかわらず、メッセージが表示されます。

3. スケジュール セクションで、次のスケジュール設定を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
ごとに	設定された時間ごとに実行します。
毎日 HH:MM から実行	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。

オプション	説明
	例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

4. **保存** をクリックします。

管理対象デバイスでのスクリプトの実行

タスクおよび設定を自動化するためのスクリプトを作成し、管理対象デバイスで実行することができます。

スクリプトについて

スクリプトはポイントアンドクリックインターフェイスを備えており、通常は手動のプロセスや高度なプログラミングが必要なタスクをポイントアンドクリック操作で実行できます。スクリプトを作成および実行して、ネットワークを経由してターゲットデバイス上でタスクを実行できます。

スクリプトにより、次のようなタスクが自動化されます。

- 電源管理の設定
- ソフトウェアのインストール
- ウイルス対策ステータスの確認
- レジストリ設定の変更
- ソフトウェア展開のスケジュール設定

作成できるスクリプトのタイプは次の通りです。

オプション	説明
オフラインKScript	ターゲットデバイスのクロックに基づいて、スケジュールされた時間に実行されるスクリプト。オフライン KScript は、デバイスの起動時やユーザーのログイン時など、ターゲットデバイスがアプライアンスに接続されていないときでも実行できます。スクリプトは、スクリプト作成テンプレートを使用して作成できます。
オンラインKScript	ターゲットデバイスがアプライアンスに接続されている場合にのみ実行されるスクリプト。オンライン KScriptは、アプライアンスのクロックに基づいて、スケジュールされた時間に実行されます。これらのスクリプトは、スクリプト作成テンプレートを使用して作成できます。
オンラインシェルスクリプト	ターゲットデバイスがアプライアンスに接続されている場合にのみ、アプライアンスのクロックに基づいて、スケジュールされた時間に実行されるスクリプト。オンラインシェルスクリプトは、ターゲットデバイスのオペレーティングシステムによってサポートされている簡単なテキストベースのスクリプト（Bash、Perl、バッチなど）を使用して作成します。バッチファイルはWindowsでサポートされていますが、同様にさまざまなシェルスクリプト形式がターゲットデバイスの各オペレーティングシステムによってサポートされています。

各スクリプトの構成要素は次の通りです。

- メタデータ。
- ZIPファイルやBATファイルなど、スクリプトの実行に必要なすべての実行可能サポートファイルを含む依存関係。
- オフラインKScriptやオンラインKScriptなどの、従うルール。
- オフラインKScriptやオンラインKScriptなどの、完了するタスク。各スクリプトには任意数のタスクを含めることができます。また、次のタスクが実行される前に各タスクが正常に完了する必要があるかどうかを設定できます。
- 展開の設定。
- スケジュールの設定。

スクリプト依存関係の取得

スクリプト依存関係には、スクリプトで使用されるファイルおよびその他のアイテムが含まれます。スクリプトに依存関係があり、その依存関係がターゲットデバイスに存在する場合、その依存関係は使用されています。スクリプトに依存関係がない場合、スクリプトは、指定された順序でリポジトリの依存関係を検索します。

スクリプトは、ターゲットデバイスおよびリポジトリから次の順番で依存関係を取得します。

1. ターゲットデバイス
2. 代替のダウンロード場所（KACE_ALT_LOCATION）
3. レプリケーション共有
4. アプライアンス

注: 代替のダウンロード場所とレプリケーション共有の詳細については、代替のダウンロード場所およびレプリケーション共有からのパッケージの配布を参照してください。

スクリプト設定の変更追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

デフォルトスクリプトについて

デフォルトスクリプトは、デバイスでインベントリの報告、デバイスでのデバッグの有効化と無効化、デバイスのシャットダウン、およびデバイスでのその他のタスクのリモートでの実行を強制的に実行するために使用できる、事前設定済みのスクリプトです。

デフォルトスクリプト

スクリプト名	説明
C:ドライブを最適化する	デバイスのドライブCを最適化します。
強制的にチェックイン	KACE エージェントがインストールされた Windows デバイスを強制的にインベントリしてアプライアンスと同期させます。 **重要: 選択したデバイスの数が50を超える場合は「強制的にチェックイン」機能を実行しないでください。アプライアンスに要求が集中する可能性があります。**
強制的なチェックイン（Mac/Linux）	KACE エージェントがインストールされた Mac および Linux デバイスを強制的にインベントリしてアプライアンスと同期させます。 **重要: 選択したデバイスの数が50を超える場合は「強制的にチェックイン」機能を実行しないでください。アプライアンスに要求が集中する可能性があります。**

スクリプト名	説明
インベントリスタートアッププログラムの修正	一部のデバイス上では、レジストリエントリが欠損していると、system32ディレクトリのすべてのコンテンツが、スタートアッププログラムとしてレポートされます。このスクリプトは、欠損がある場合にレジストリエントリを修正します。
DOSコマンドの発行例	Windows デバイス上で DOS-DIR コマンドを発行します。DOSコマンドの実行例として使用されます。
Macコマンドの発行例	AppDir.txt コマンドを発行して、Mac OS X の Applications ディレクトリの内容を表示します。Mac OS X上でのコマンドの実行例として使用されます。
K1000 は詳細な DDPE インベントリ（ Windows ）を有効化	Dell Data Protection | Encryption エージェントによってポリシーデータがファイルシステムに書き込まれるようにするレジストリキーを設定します。これにより、KACE エージェントはより詳細なインベントリコレクションを実行できます。Windows PowerShell 2.0 以降が必要です。
K1000リモートコントロールを無効にする	ターミナルサービスを適切に設定することにより、Windows XP Professionalでアプライアンスのリモートコントロール機能を無効にします。
K1000リモートコントロールを有効にする	ターミナルサービスを適切に設定することにより、Windows XP Professionalでアプライアンスのリモートコントロール機能を有効にします。
リムーバブルドライブを読み取り専用にする	リムーバブルドライブを、読み取り専用としてのみマウントできるようにします。このアクションにより、データへの未承認のアクセスを制御します。
リムーバブルドライブを読み取り/書き込みにする	リムーバブルドライブのプロパティを、読み取り/書き込み可能としてマウントできるように設定します。
メッセージウィンドウのスクリプト例	メッセージウィンドウの使用例を示します。スクリプトが適切に機能するためには、メッセージウィンドウの作成/破棄コマンドを適切に組み合わせておく必要があります。次のいずれかのイベントが発生するまで、メッセージウィンドウが表示されたままになります。 • ユーザーがメッセージを閉じる。 • スクリプトが実行されて完了する。 • タイムアウトの期間が終了する。
Macをスリープ状態にする	Mac OS Xデバイスをスリープモードにします。 **注:** このスクリプトはMac OS X 10.5以上で機能します。それ以前のバージョンのMac OS Xでは機能しません。

スクリプト名	説明
KUIDをリセットする	Windowsデバイスを識別するレジストリキーを削除して、新しいキーを生成できるようにします。ResetKUIDRunOnce レジストリフラグを使用して、デバイスごとに 1 回実行します。
Macをシャットダウンする	Mac OS Xデバイスの電源をオフにします。
Macの再通知付きシャットダウン	**実行前にユーザーに警告**機能を使用して、管理者がシャットダウンを再通知できるようにするオンライン KScript の例です。
Windowsシステムをシャットダウンする	ユーザーにメッセージが表示されている間の遅延を秒単位で指定します。サイレントモードですぐにデバイスをシャットダウンするには、-t パラメータを省略します。
Windowsシステムの再通知付きシャットダウン	**実行前にユーザーに警告**機能を使用して、管理者がシャットダウンを再通知できるようにするオンライン KScript の例です。
USBドライブを無効にする	USBドライブの使用を無効にします。
USBドライブを有効にする	USBドライブの使用を有効にします。

スクリプトの追加と編集

管理者コンソールを使用してスクリプトを追加または編集できます。

スクリプトを追加および編集するには、次のいずれかを実行します。

- XML形式の既存のスクリプトをインポートします。詳細については、「インポート可能スクリプトの構造」を参照してください。
- 既存のスクリプトを複製します。詳細については、「スクリプトの複製」を参照してください。
- スクリプトを作成します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。

ヒント: スクリプトの作成は繰り返し作業になります。スクリプトの作成後、それを限定数のデバイスに展開し、そのスクリプトが正常に動作することを確認してから、すべての管理対象デバイスにそのスクリプトを展開する必要があります。この検証を行うためのテストラベルを作成できます。必ずスクリプトをテストしてから、そのスクリプトを有効にします。

トークン置換変数

トークン置換値を使用して、スクリプトに変数を追加します。次のリストに、スクリプトのXMLで使用できるトークン置換値を示します。実行時に、これらの変数はデバイス上で該当する値に置き換えられます。

トークン置換値

アイテム	説明
$(KACE_DEPENDENCY_DIR)	このスクリプトのどのスクリプト依存関係もクライアントにダウンロードされて、このフォルダに配置されます。 **5.2以上**: $(KACE_DATA_DIR)\kbots_cache\packages\kbots\xxx **5.1** : $(KACE_INSTALL)\packages\kbots\xxx
$(KACE_SYS_DIR) **$(KBOX_SYS_DIR)**	エージェントデバイスのシステムディレクトリ。 両方とも同意語です。優先: **$(KACE_SYS_DIR)** **Windows**: C:\Windows\System32 **Mac OS X** : / **Linux**: /
$(KACE_MAC_ADDRESS) **$(MAC_ADDRESS)** **$(KBOX_MAC_ADDRESS)**	エージェントデバイスのプライマリイーサネットMACアドレス。 すべて同意語です。優先: **$(KACE_MAC_ADDRESS)**
$(KACE_IP_ADDRESS) **$(KBOX_IP_ADDRESS)**	エージェントのローカルIPアドレス（KACE_MAC_ADDRESSのネットワークエントリに対応）（http://kace.kbox.com:80）。 両方とも同意語です。優先: **$(KACE_IP_ADDRESS)**
$(KACE_SERVER_URL)	サーバー、ポート、およびurlプレフィックスの組み合わせ（http://kace.kbox.com:80）。
$(KACE_SERVER)	アプライアンスサーバのホスト名（kbox）。
$(KACE_SERVER_PORT)	アプライアンスサーバへの接続時に使用するポート（80/433）。
$(KACE_SERVER_URLPREFIX)	アプライアンスサーバへの接続時に使用する Web プロトコル（http/https）。
$(KACE_COMPANY_NAME)	サーバーの設定ページからのエージェントの設定のコピー。
$(KACE_KUID) **$(KBOX_MACHINE_ID)**	このエージェントに割り当てられた固有のQuest KACE ID。 両方とも同意語です。優先: **$(KACE_KUID)**
$(KACE_APP_DIR)	Quest KACEエージェントとプラグインが配置されているインストールディレクトリ。 より古いエージェントの場合、これは**$(KACE_INSTALL)**にマップされます。 **Windows**: C:\Program Files\Quest\KACE\ または C:\Program Files (x86)\Quest\KACE\

アイテム	説明
	Mac OS: /Library/Application Support/Quest/KACE/bin **Linux**: /opt/quest/kace/bin
$(KACE_DATA_DIR)	実行可能ファイル、スクリプト、パッケージなど用のインストールディレクトリ。 より古いエージェントの場合、これは**$(KACE_INSTALL)**にマップされます。 **Windows Vista以降**: C:\ProgramData\Quest\KACE\ **Mac OS**: /Library/Application Support/Quest/KACE/data **Linux**: /var/quest/kace
$(KACE_AGENT_VERSION)	インストールされたエージェントのバージョン番号を置き換えます。"5.2.12345"。 **5.2以上のみ。**
$(KACE_AGENT_ARCH)	インストールされたエージェントのアーキテクチャを置き換えます（x86/x64）。 **5.2以上のWindowsのみ。**
$(KACE_HARDWARE_ARCH)	物理ハードウェアのアーキテクチャを置き換えます（x86/x64）。 **5.2以上のWindowsのみ。**
$(KACE_OS_FAMILY)	エージェント管理対象デバイスのオペレーティングシステムに応じて、Windows、Mac、またはLinuxを置き換えます。 **5.2以上のみ。**
$(KACE_OS_ARCH)	Microsoft Windowsのインストールされたバージョンに応じて、x86またはx64を置き換えます。 **5.2以上のWindowsのみ。**

オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加

KScriptの追加、スクリプトを実行するデバイスの指定、および実行するスクリプトのスケジュールを必要に応じて行うことができます。

オフラインKScriptとオンラインKScriptには1つ以上のタスクが含まれます。各 タスク セクション内には、さらにスクリプトの動作を定義できる 検証 と 修復 のセクションがあります。セクションを空白にした場合、そのセクションはデフォルトで「正常終了」になります。

1. スクリプトの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
c. **アクションの選択 > 新規作成** を選択します。

2. 設定セクションで、スクリプトの設定項目を次のように指定します。

オプション	説明
名前	スクリプト リストの他のスクリプトと区別するための、対象スクリプトを表す意味のある名前。 ヒント: スクリプト ページでは、1 つまたは複数のスクリプトを有効または無効にできます。これを行うには、テーブルで選択し、をクリックして、必要に応じて **有効** または **無効** をクリックします。
有効	スクリプトを有効にし、ターゲットデバイス上で実行するかどうか。スクリプトの編集とテストが完了して、実行準備ができるまで、スクリプトを有効にしないでください。スクリプトはテストラベルに対して有効にしてから、すべてのデバイスに対して有効にします。
カテゴリ	スクリプトのカテゴリ。ドロップダウンリストから既存のカテゴリを選択するか、**新しいカテゴリ** をクリックしてカテゴリを追加します。このスクリプトにカテゴリを割り当てない場合は、このフィールドが **なし** に設定されていることを確認します。 ヒント: スクリプト ページでは、1 つまたは複数のスクリプトに 1 つのカテゴリを割り当てることができます。これを行うには、テーブルでそれらを選択し、**アクションの選択 > カテゴリ** をクリックして、リストからカテゴリを選択します。
タイプ	スクリプトのタイプ。スクリプトのタイプは次の通りです。 • **オンラインKScript**: ターゲットデバイスがアプライアンスに接続されている場合にのみ実行されるスクリプト。オンラインKScriptは、アプライアンスのクロックに基づいて、スケジュールされた時間に実行されます。これらのスクリプトは、スクリプト作成テンプレートを使用して作成できます。 • **オフラインKScript**: ターゲットデバイスのクロックに基づいて、スケジュールされた時間に実行されるスクリプト。これらのスクリプトは、デバイスの起動時やユーザーのログイン時など、ターゲットデバイスがアプライアンスに接続されていないときでも実行できます。スクリプトは、スクリプト作成テンプレートを使用して作成できます。 • **オンラインシェルスクリプト**: ターゲットデバイスがアプライアンスに接続されている場合にのみ、アプライアンスのクロックに基づいて、スケジュールされた時間に実行され

オプション	説明
	るスクリプト。オンラインシェルスクリプトは、ターゲットデバイスのオペレーティングシステムによってサポートされている簡単なテキストベースのスクリプト（Bash、Perl、バッチなど）を使用して作成します。バッチファイルはWindowsでサポートされていますが、同様にさまざまなシェルスクリプト形式がターゲットデバイスの各オペレーティングシステムによってサポートされています。PowerShell スクリプトは、Windows ベースのターゲットデバイスでもサポートされています。 **重要: スクリプトをターゲット OS で実行できるようにするには、スクリプトに適切なファイル拡張子が関連付けられていることを確認する必要があります。たとえば、Mac および Linux デバイスでは .sh スクリプト、Windows デバイスでは .ps1 PowerShell スクリプトを実行できます。**
ステータス	スクリプトの状態。開発中（**ドラフト**）であるのか、ネットワークにロールアウト済み（**本番**）であるのか。今後のスクリプトのひな型として使用するスクリプトを作成する場合は、「**テンプレート**」ステータスを使用します。
説明	（オプション）スクリプトによって実行されるアクションの簡単な説明。このフィールドは、スクリプト リストでスクリプトを区別するのに役立ちます。
メモ	任意の追加情報を入力します。

3. 展開 セクションで、次の展開オプションを指定します。

オプション	説明
全デバイス	すべてのデバイスに展開します。展開を特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
ラベル	指定したラベルに属するデバイスだけに展開を制限します。ラベルを選択するには、**編集** をクリックしてラベルを 展開の制限対象 ウィンドウにドラッグし、**保存** をクリックします。 レプリケーション共有または代替のダウンロード場所が指定されているラベルを選択した場合、デジタル資産は、アプライアンスから直接ダウンロードされるのではなく、指定されたレプリケーション共有または代替のダウンロード場所からコピーされます。 **注:** アプライアンスがKACE代替の場所を使用する前にレプリケーション共有を使用することが明らかになりました。

オプション	説明
デバイス	1つまたは複数のデバイスに、展開を制限します。デバイスを検索するには、フィールドに入力し始めます。
オペレーティングシステム	アプリケーションが実行されるオペレーティングシステム。アプリケーションは、選択したオペレーティングシステムがインストールされているデバイスにのみ導入されます。 a. **オペレーティングシステムの管理** をクリックします。 b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**すべて > Windows > Windows 10** の順に選択し、**x64** を選択します。

4. 「Windowsを別のユーザーとして実行」設定を指定します（Windowsデバイスでのみ実行されるオンラインシェルスクリプトとKScriptの場合）。

オプション	説明
ローカルシステム	ローカルデバイス上で管理者権限を使用してスクリプトを実行します。テンプレートを使用して作成されたすべてのスクリプトに、この設定を使用します。
ログインしているユーザー	ローカルデバイスにログインしているユーザーとしてスクリプトを実行します。これは、そのユーザーのプロファイルに影響を与えます。
すべてのログインしているユーザー	デバイスにログインしているすべてのユーザーとして一度スクリプトを実行します。これは、すべてのユーザーのプロファイルに影響を与えます。
資格情報	ここで指定した資格情報のコンテキストでオンラインシェルスクリプトと KScript を実行します。ドロップダウンリストから既存の資格情報を選択するか、**新しい資格情報の追加** を選択して、まだリストされていない資格情報を追加します。 詳細については、「ユーザーとパスワード資格情報の追加および編集」を参照してください。

オプション	説明
	注: オンライン Kscript を Windows デバイスで実行する場合、スクリプトを特定の資格情報を持つユーザーとして実行するオプションを選択すると、メッセージウィンドウはターゲットデバイスに表示されません。メッセージウィンドウを表示するには、スクリプトをローカルシステム、ログインユーザー、またはすべてのログインしているユーザーとして実行します。

5. ユーザー通知 セクションで、ユーザー警告設定を指定します。警告は、KACE エージェントバージョン 5.1 以上を実行する Windows デバイスおよび Mac デバイス上のオンライン KScript およびオンラインシェルスクリプトに対してのみ使用できます。

オプション	説明
実行前にユーザーに警告	ユーザーによるアクションの実行、キャンセル、または遅延を許可します。再起動が必要な場合、この設定は特に重要です。ログインしているユーザーがいない場合、スクリプトはすぐに実行されます。
オプション	次のオプションが、警告 ダイアログでユーザーに表示されます（**実行前にユーザーに警告** を選択した場合に使用可能）。 • **OK**: すぐに実行されます。 • **キャンセル**: 次のスケジュールされた実行までキャンセルされます。 • **再通知**: 再通知間隔 の経過後に再度プロンプトが表示されます。 ユーザーが応答することなく、タイムアウト で指定した時間が経過した場合、スクリプトはその時点で実行されます。 別のユーザーとして実行する場合の対話： • コンソールユーザーのみが、別のユーザーとして実行 の設定にかかわらず警告ダイアログを表示でき、したがって再通知かキャンセルを選択できます。 • スクリプトがすべてのユーザーまたは別のユーザーとして実行されるように設定されている場合でも、警告を有効にするとコンソールユーザーにプロンプトが表示されます。
タイムアウト	アクションの実行前にダイアログが表示される期間（分単位）。この期間が経過するまでの間にユーザーがボタンを押さないと、Timeout（タイムアウト）ドロップダウンリストで指定されたアクションをアプライアンスが実行します。
タイムアウトアクション	ユーザーがオプションを選択することなく **Timeout**（タイムアウト）で指定した期間が経過した場合に実行されるアクション。

オプション	説明
再通知間隔	ユーザーが **再通知** をクリックした後の期間（分単位）。この期間が経過すると、ダイアログが再度表示されます。
初期メッセージ	アクションが実行される前に、ユーザーに表示されるメッセージ。 ダイアログに表示されるロゴをカスタマイズするには、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。

6. スケジュール セクションで、次の実行オプションを指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（,）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（-）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィール

オプション	説明
	ドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（/）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（*）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

7. スケジュールオプション セクションで、適用可能なオプションを選択します。

オプション	説明
次のデバイスチェックインでも1回実行（オフラインKScriptの場合のみ）	新しいスクリプトがアプライアンスからダウンロードされたときに、オフラインKScriptを1回のみ実行します。
ログイン前にも実行（オフラインKScriptの場合のみ）	デバイス起動時にオフラインKScriptを実行します。これにより、デバイスの起動に通常より時間がかかる場合があります。 **注:** Active Directoryまたはグループポリシーオブジェクトの設定により、ログイン前にユーザーの承認を必要とするメッセージがデバイスに表示される場合、メッセージが承認されるまでスクリプトは実行されません。
ログイン後（デスクトップ読み込み前）にも実行（オフラインKScriptの場合のみ）	ユーザーがWindowsログイン資格情報を入力した後に、オフラインKScriptを実行します。
切断されている間の実行を許可（オフラインKScriptの場合のみ）	ターゲットデバイスがアプライアンスに接続して結果をレポートできない場合でも、オフラインKScriptを実行できるようにします。接続されていない場合、結果はデバイスに保存され、次回の接続中にアプライアンスにアップロードされます。
ログインしているユーザーがいなくても実行を許可	ユーザーがログインしていない場合でもスクリプトを実行できるようにします。ユーザーがデバイスに

オプション	説明
	ログインしている場合のみ、スクリプトが実行されるようにするには、このオプションをオフにします。
オフラインの場合は次の接続時に実行	オンラインKscriptまたはシェルスクリプトについて、このオプションを有効にすると、オフラインのマシン上で再びオンラインになったときにこのスクリプトが実行されます。 スクリプトが実行されると、マシンのラベルまたはそのオペレーティングシステムに基づいて、あるいは選択するマシンを手動で識別することで、実行をサポートするマシンの数が算出されます。一連のマシンが指定されると、スクリプトでは次に現在オンラインになっているマシンを特定し、Konductor内の現在オンラインのマシンに対するタスクをキューに登録します。 このオプションを選択すると、スクリプトではオンラインのマシンを識別するステップがスキップされ、スクリプトがオンラインのマシン上で実行されます。オフラインのマシンの場合、タスクはKonductorのキューに追加されます。このタスクは、これらのマシンがオンラインになったときに実行されます。 それ以降に同じスクリプトを実行するすべてのタスク（例えば、Konductorのキューにすでに存在しているオフラインのマシン用のタスク）は、既存のタスクを上書きします。このため、同じマシンに対するKonductorのキュー内のタスクが複数になることはありません。 Konductor内のタスク数が多いとアプライアンスのパフォーマンスに影響する場合があります。このため、ベストプラクティスは、通常はオフラインのマシンにはオフラインのスクリプトを使用し、ターゲットマシンがオンラインと思われるときにのみオンラインスクリプトでこのオプションを使用して、Konductorのキュー内のタスクが多くなりすぎないようにすることです。 デフォルトでは、このオプションは無効にされています。

8. スクリプトに必要なファイルをアップロードするには
   a. 依存関係 セクションで、**新しい依存関係の追加** をクリックします。
   b. **参照** または **ファイルの選択** をクリックします。
   c. ファイルを選択し、**開く** または **選択** をクリックします。

      レプリケーション共有を指定して有効にしている場合、依存関係は指定したレプリケーション共有からダウンロードされます。

   注: レプリケーション共有にアクセスできない場合、依存関係はアプライアンスからダウンロードされます。この設定を有効にするには、レプリケーションスケジュールの詳細 ページで アプライアンスへのフェールオーバー チェックボックスをオンにします。詳細については、「レプリケーション共有の作成」を参照してください。

   この手順を繰り返し、必要に応じて依存関係を追加します。
9. **オンラインまたはオフラインの KScripts のみ**。タスク セクションで、**新しいタスク** をクリックしてタスクを追加します。

タスクのプロセスフローは次のようなスクリプトです。

```
IF Verify THEN
        Success
ELSE IF Remediation THEN
        Remediation Success
ELSE
        Remediation Failure
```

a. ポリシー または ジョブルール セクションで、タスク 1 の次のオプションを指定します。

オプション	説明
試行回数	アプライアンスがスクリプトの実行を試みる回数を入力します。 スクリプトは失敗するが、修復が成功する場合は、もう一度タスクを実行して修復手順を確認することもできます。これを行うには、試行回数を 2 回以上に設定します。検証 セクションが失敗した場合、このフィールドで指定した回数だけスクリプトが実行されます。
失敗時	• **中止** を選択すると、失敗時に実行が停止されます。 • **続行** を選択すると、失敗時に修復手順が実行されます。

b. 検証 セクションで **追加** をクリックして 1 つの手順を追加し、その後、実行する 1 つ以上の手順を選択します。

詳細については、「スクリプトのタスクセクションへの手順の追加」を参照してください。

c. 成功時 セクションと 修復 セクションで、実行する 1 つ以上の手順を選択します。

詳細については、「スクリプトのタスクセクションへの手順の追加」を参照してください。

d. 修復の成功時 セクションと 修復の失敗時 セクションで、実行する 1 つ以上の手順を選択します。

詳細については、「スクリプトのタスクセクションへの手順の追加」を参照してください。

ヒント: 依存関係を削除するには、アイテムの隣にある **削除** ボタン をクリックします。このボタンは、アイテムの上にカーソルを置くと表示されます。

ヒント: ポリシーまたはジョブのルール の隣にある **編集** ボタンをクリックすると、スクリプト内の任意の場所で使用できるトークン置換変数が表示されます。。これらの変数は、実行時に、適切な値に置き換えられます。

ヒント: 詳細については、「トークン置換変数」を参照してください。

10. **オンラインシェルスクリプトのみ**。スクリプト セクションで、各設定を次のように指定します。

オプション	説明
スクリプトテキスト	スクリプトの内容を入力します。
スクリプトファイル名	指定したスクリプトを含むファイルの名前と拡張子を入力します。

オプション	説明
	重要: スクリプトをターゲット OS で実行できるようにするには、スクリプトに適切なファイル拡張子が関連付けられていることを確認する必要があります。たとえば、Mac および Linux デバイスでは .sh スクリプト、Windows デバイスでは .ps1 PowerShell スクリプトを実行できます。
タイムアウト (分)	ターゲットデバイスでスクリプトを実行できる最大時間 (分) を指定します
ファイルのアップロード	スクリプトによってファイルが作成され、そのファイルをアプライアンスにアップロードする場合は、このオプションを選択し、次の情報を指定します。 • **アップロードファイル名**：ファイルの名前を入力します。 • **アップロードファイルディレクトリパス**：ファイルを保存するディレクトリを指定します。デフォルトのスクリプトディレクトリ (<appliance_installation_directory>/scripts) を使用する場合は、このフィールドをブランクのままにします。
ダウンロードされたファイルを削除する	スクリプトでインストーラーなどの他のファイルを実行する必要があり、スクリプトの実行後にそれらを削除する場合は、このオプションを選択します。

11. 次のいずれかを実行します。
    - **今すぐ実行 をクリックすると、すべてのデバイスにスクリプトがすぐにプッシュされます。**

      このオプションの使用には注意が必要です。詳細については、「実行 および 今すぐ実行 コマンドの使用」を参照してください。
    - **保存 をクリックします。**

スクリプトの編集

オフライン KScript、オンライン KScript、およびオンラインシェルスクリプトという 3 つのタイプのスクリプトを編集できます。オフラインKScriptとオンラインKScriptはXML工ディタを使用しても編集できます。

スコープユーザーは、すべてのスクリプトの詳細を表示できますが、保存できるのは、自身のスコープに関連付けられているデバイスまたはラベルに影響するスクリプトの詳細に対する変更だけです。スコープユーザーの詳細については、ユーザーの役割の追加または編集を参照してください。

1. スクリプトの詳細 ページに移動します。
    a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。

c. スクリプトの詳細 ページを表示するには、次のいずれかを実行します。

- スクリプトの名前をクリックします。
- **アクションの選択** > **新規作成** を選択します。

2. 必要に応じてスクリプトを修正します。
3. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
4. スクリプトの生XMLを編集するには、スケジュール セクションまでスクロールして、**XMLの編集** をクリックします。
5. **保存** をクリックします。

スクリプト ページからのスクリプトの削除

スクリプトは、スクリプト ページから削除できます。

1. スクリプト リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
2. 1つまたは複数のスクリプトの隣のチェックボックスをオンにします。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

スクリプトの詳細 ページからのスクリプトの削除

スクリプトは、Script Detail（ スクリプトの詳細 ）ページから削除できます。

1. スクリプトの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
   c. スクリプトの名前をクリックします。
2. **削除** をクリックし、**はい** をクリックして確認します。

インポート可能スクリプトの構造

外部のXMLエディタでスクリプトを作成し、それをアプライアンスにインポートできます。

インポートするスクリプトは次の構造に一致する必要があります。

- ルート要素<kbots></kbots>内にKACE DTDの以下のURLが含まれている："kbots xmlns="http://kace.com/Kbots.xsd">...<kbots>
- 1つ以上の<kbot>要素。
- 各<kbot>要素内に正確に1つの<config>要素。
- 各<config>要素内に正確に1つの<execute>要素。
- 各<kbot>要素内に1つ以上の<compliance>要素。

アプライアンススクリプトのXML構造の例を次に示します。

```
<?xml version="1.0" encoding="utf-8" ?>
<kbots xmlns="http://kace.com/Kbots.xsd">
<kbot>
<config name="name="" type="policy" id="0" version="version="" description=
  "description="">
                    <execute disconnected="false" logged_off="false">
                    </execute>
</config>
<compliance>
</compliance>
</kbot>
</kbots>
```

上記の例では、</config> 要素は、スクリプトの詳細 ページの 設定 セクションに対応します。この要素内では、ポリシーまたはジョブの名前（オプション）、およびスクリプトタイプ（ポリシーまたはジョブ）を指定します。また、この要素ではターゲットデバイスがアプライアンスから切断または ログオフしているときに、スクリプトを実行可能かどうかを指定することもできます。

<compliance>要素内では、スクリプトを有効にするかどうかを指定し、スクリプトが実行する特定のタスクを記述できます。

ヒント: 既存のスクリプトと同じタスクをいくつか実行するスクリプトを作成するには、既存のスクリプトを複製し、XML工ディタでそのスクリプトを開きます。スクリプトの<compliance>要素を見ると、どのようにスクリプトが機能し、そのスクリプトをどのように変更できるかがわかります。詳細については、「スクリプトの複製」を参照してください。

スクリプトのインポート

必要に応じて、スクリプトをアプライアンスにインポートできます。

1. スクリプト リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
2. **アクションの選択 > インポート** を選択します。
3. 表示された領域に既存のスクリプトを貼り付け、**保存** をクリックします。

スクリプトの複製

作成しようとしているスクリプトに類似したスクリプトがある場合は、そのスクリプトを複製し、必要に応じて編集できます。複製を使用すると、最初から新しいスクリプトを作成するよりも迅速な処理ができます。

1. スクリプトの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
    c. スクリプトの名前をクリックします。
2. ページの一番下で **複製** をクリックして、スクリプト ページを表示します。

    複製されたスクリプトがリストに表示されます。
3. 複製されたスクリプトのリンク名をクリックすると、そのスクリプトが編集用に開きます。

詳細については、「スクリプトの編集」を参照してください。

実行 および 今すぐ実行 コマンドの使用

実行 および **今すぐ実行** コマンドを使用すると、スケジュールを設定せずに、ターゲットデバイス上でスクリプトをすぐに実行できるようになります。

スケジュールを設定せずにスクリプトを実行することは、次の場合に役立ちます。

- ネットワーク上のデバイスにウイルスの感染や脆弱性への攻撃があると疑われる場合や、すぐに解決しなければネットワーク全体が危険にさらされる可能性がある場合。
- 開発中に特定のデバイスまたは一連のデバイスでスクリプトをテストおよびデバッグする場合。

オンライン KScript を実行するには、ターゲットデバイスにアプライアンスへのエージェント接続が必要です。

ヒント: 意図しないデバイスにスクリプトを展開するリスクを最小限に抑えるには、「**今すぐ実行**」コマンドを実行するデバイスを表すラベルを作成します。

今すぐ実行 コマンドは、次の**管理者コンソール**ページで使用できます。

- 今すぐ実行 および Script Detail（スクリプトの詳細）ページ：スクリプト、今すぐ実行 ページからスクリプトを実行することにより、選択したスクリプトをターゲットデバイスで実行できます。
- スクリプト ページ：アクションの選択 メニューで **今すぐ実行** オプションを使用して、スクリプト ページからスクリプトを実行することにより、複数のスクリプトを同時に実行できます。
- Mac Profile Detail（Mac プロファイルの詳細）：Mac プロファイルの詳細 ページで **今すぐ実行** コマンドを使用すると、アプライアンスへのエージェント接続があるターゲットデバイスに対して、選択した Mac プロファイルをインストールまたは除去するスクリプトが実行されます。
- Mac Profiles：Mac プロファイル ページで **アクションの選択**、**実行** の順に選択すると、ターゲットデバイスにアプライアンスへのエージェント接続がある場合は、複数の Mac プロファイルを同時にインストールまたは除去するスクリプトが実行されます。

注: スクリプトの実行中にエラーが発生した場合は、問題の診断に役立つ可能性のあるエラーコードのリストについて、パッチとスクリプトによるエラーコードを参照してください。

今すぐ実行 ページからのスクリプトの実行

今すぐ実行 ページから、ターゲットデバイスでスクリプトを実行できます。

注意: **今すぐ実行 をクリックすると、スクリプトはすぐに展開されます。**

- 「今すぐ実行」は慎重に使用してください。
- ターゲットデバイスでスクリプトを実行することが確定していない場合は、**今すぐ実行** はクリックしないでください。

1. 今すぐ実行 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**今すぐ実行** をクリックします。
2. スクリプト ドロップダウンリストから、スクリプトを選択します。スクリプトを検索するには、フィールドに入力し始めます。
3. 展開 セクションで、次の展開オプションを指定します。

オプション	オプションと説明
ラベル	指定したラベルに属するデバイスだけに展開を制限します。ラベルを選択するには、**編集** をクリックしてラベルを 展開の制限対象 ウィンドウにドラッグし、**保存** をクリックします。 レプリケーション共有または代替のダウンロード場所が指定されているラベルを選択した場合、デジタル資産は、アプライアンスから直接ダウンロードされるのではなく、指定されたレプリケーション共有または代替のダウンロード場所からコピーされます。 **注:** アプライアンスがKACE代替の場所を使用する前にレプリケーション共有を使用することが明らかになりました。
デバイス	1つまたは複数のデバイスに、展開を制限します。デバイスを検索するには、フィールドに入力し始めます。スコープユーザーは、役割にラベルが割り当てられている場合に、自身の役割に関連付けられているデバイスだけを表示できます。ユーザーの役割へのデバイスのスコープ設定の詳細については、「ユーザーの役割の追加または編集」を参照してください。

4. **今すぐ実行** をクリックします。

   今すぐ実行のステータス ページが表示されます。

スクリプトの詳細 ページからのスクリプトの実行

スクリプトの詳細 ページから、ターゲットデバイスでスクリプトを実行できます。

1. スクリプトの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
   c. スクリプトの名前をクリックします。
2. ページの下部までスクロールし、**今すぐ実行** をクリックします。

   今すぐ実行のステータス ページが表示されます。

スクリプト ページからのスクリプトの実行

スクリプトを スクリプト ページから実行できます。

1. スクリプト リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。

2. 1つまたは複数のスクリプトの隣のチェックボックスをオンにします。
3. **アクションの選択 > 今すぐ実行** を選択します。

   今すぐ実行のステータス ページが表示されます。

「今すぐ実行のステータス」の監視とスクリプト詳細の表示

「**今すぐ実行**」コマンドを使用して開始したスクリプトのステータスを表示し、スクリプトの詳細にアクセスできます。

ファイアウォール設定によって、KACE エージェントのポート 443 でのリッスンがブロックされていないことを確認します。

今すぐ実行 コマンドの通信にはポート 443 が使用されます。ファイアウォールの設定で、KACE エージェントによるそのポートのリッスンがブロックされていると、スクリプトを展開できないことがあります。ポート要件の詳細については、ポート設定、NTPサービス、およびWebサイトアクセスの検証を参照してください。

1. 今すぐ実行のステータス リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**今すぐ実行のステータス** をクリックします。
2. 今すぐ実行のステータス リストの情報を確認します。

   このページには次のような情報が表示されます。

   - **開始**：「**今すぐ実行**」コマンドが発行された時間。
   - **名前**：スクリプトの名前。このスクリプト名をクリックすると、今すぐ実行の詳細 ページが表示されます。
   - **対象**：スクリプトの実行がスケジュールされているデバイスの数。
   - **プッシュ済み、実行中、保留中**：スクリプトの実行を試みているデバイスの数。
   - **成功、失敗、完了**：スクリプトが実行されたデバイスの数。
   - **成功率**：ターゲットデバイスで正常に実行されたスクリプトのパーセンテージ。

   プッシュ済み、実行中、保留中、成功、失敗、および 完了 列内の数字は、スクリプトがターゲットデバイスに展開されるにつれて増えます。選択したデバイスにスクリプトをプッシュしたときにエラーが発生した場合は、スクリプトログを検索して原因を特定できます。詳細については、「スクリプトログの検索」を参照してください。
3. スクリプトの 開始 列のリンクをクリックして、今すぐ実行のステータスの詳細 ページを表示します。

このページには次のような情報が表示されます。

- **今すぐ実行の統計**：プッシュされたスクリプトの結果、プッシュの失敗、プッシュの正常終了、完了したデバイス、実行中のデバイス、および成功と失敗の数と割合。
- **展開は失敗しました**：アプライアンスが接続できなかったため、ポリシーを受け取れなかったデバイス。スクリプトがプッシュされると、デバイスがポリシーを完了するまで一定の時間がかかる場合があります。
- **実行中**：ポリシーは受け取っているが結果が報告されていないデバイス。ポリシーが実行された後、成否が報告されます。結果は、適切なセクションの下で並べ替えられます。各デバイスのページにも、そのデバイス上で実行された「今すぐ実行」イベントの結果が表示されます。
- **実行は失敗しました**：スクリプトが失敗したデバイス。
- **実行は成功しました**：スクリプトが正常に実行されたデバイス。

設定ポリシーテンプレートについて

設定ポリシーテンプレートを使用すると、ポリシー関連のスクリプトを作成できます。これらのスクリプトを展開して、管理対象デバイスでポリシーを設定できます。

このセクションでは、作成可能な各スクリプトの設定について説明します。

Windowsテンプレートは次の通りです。

- Dell Command | Monitor スクリプトの追加
- 「デスクトップの壁紙」スクリプトの追加
- 「デスクトップショートカット」スクリプトの追加
- 「イベントログリポーター」スクリプトの追加
- 「MSIインストーラー」スクリプトの追加
- 「電源管理」スクリプトの追加
- 「レジストリ」スクリプトの追加「レジストリ」スクリプトの追加
- 「リモートデスクトップコントロールトラブルシューター」スクリプトの追加
- UltraVNCスクリプトの追加
- 「アンインストーラ」スクリプトの追加

Mac OS Xテンプレートは次の通りです。

- 「Active Directory」スクリプトの追加
- 「電源管理」スクリプトの追加
- 「VNC」スクリプトの追加

Windows設定ポリシーの使用

設定ポリシーテンプレートを使用して、Windowsデバイスで実行する設定ポリシーまたはスクリプトを作成できます。

注: テンプレートベースのポリシーを編集する場合は、Run As（別のユーザーとして実行）設定でローカルシステムとして実行するように設定します。

Windowsデバイス上のWindows自動更新の起動について

Windows管理対象デバイス上でWindows自動更新を起動するには、複数の方法があります。

Windows自動更新を起動するには、次のいずれかを実行します。

- アプライアンスのWindows自動更新設定ポリシーを有効にする。詳細については、「」を参照してください。
- デバイス上でWindows自動更新のローカルポリシーを有効にする。
- デバイス上でWindows自動更新のレジストリキーを修正する。
- デバイス上でWindows自動更新のドメイングループポリシーをセットアップする。

デバイス上で Windows の更新を自動展開するためにアプライアンスのパッチ適用機能を使用している場合は、異なる展開プロセス間の競合を避けるために、他のプロセスによる Windows 自動更新を無効にする必要があります。

Dell Command | Monitor について

Dell Command | Monitor は、Dell Command Suite の監視ツールです。これにより、アプライアンスなどのリモート管理アプリケーションで管理および監視アクティビティを実行できます。

Dell Command | Monitor の使用により、特定の Dell デバイスに対して次の機能がアプライアンスに提供されます。

- 管理情報へのアクセスを取得します。
- デバイスステータスを監視します。
- エンタープライズクライアントシステムの状態を変更します。

Dell Command | Monitor の以前のバージョンは、Dell OpenManage™ Client Instrumentation（OMCI）という名前でした。アプライアンスでは Dell Command | Monitor 9.0 以降のみがサポートされます。

サポート対象物理ハードウェア

Dell Command | Monitor は、次のデルのハードウェアで使用できます。

- Dell Venue 11 Pro
- Dell OptiPlex™
- Dell Precision Workstation™
- Dell Latitude™

サポート対象 Microsoft オペレーティングシステム

Dell Command | Monitor では、次のオペレーティングシステムがサポートされます。

- Microsoft Windows 8.1（32 ビットおよび 64 ビット）、Microsoft Windows 8.1 Professional（32 ビットおよび 64 ビット）、および Enterprise（32 ビットおよび 64 ビット）
- Microsoft Windows 8（32 ビットおよび 64 ビット）、Microsoft Windows 8 Professional（32 ビットおよび 64 ビット）、および Enterprise（32 ビットおよび 64 ビット）
- Microsoft Windows 7、Windows 7 Service Pack 1（SP1）、Professional、Enterprise、および Ultimate x86（32 ビット）および x64（64 ビット）エディション
- Microsoft Windows Vista Business SP1 x86（32 ビット）および x64（64 ビット）エディション
- Microsoft Windows Vista Ultimate SP1、SP2 x86（32 ビット）および x64（64 ビット）エディション
- Microsoft Windows Vista Enterprise SP1、SP2 x86（32 ビット）および x64（64 ビット）エディション

詳細についてクエリの対象となるクラスおよびプロパティ

Dell Command | Monitor を使用すると、次の DCIM Windows Management Instrumentation（WMI）クラスおよびプロパティがアプライアンスによるクエリの対象となります。

クエリから返された情報は、インベントリ内のデルのハードウェアデバイスについて デバイスの詳細 ページの Dell Command | Monitor グループに表示されます。

レポートウィザードを使用して、プロパティの任意の組み合わせを収集するカスタムレポートを作成できます。詳細については、「レポートウィザードを使用したレポートの作成」を参照してください。

クラス	プロパティ	レポートウィザードの Fields to Display（表示するフィールド）グループ	レポートウィザードの Fields to Display（表示するフィールド）アイテム名
DCIM_FlatPanel	なし	Dell Command | Monitor - Flat Panel Display（フラットパネルディスプレイ）	Aspect Ratio（縦横比）
	DisplayType		Display Type（ディスプレイタイプ）
	HorizontalResolution		Horizontal Resolution（水平解像度）
	PrimaryStatus		Primary Status（プライマリステータス）
	VerticalResolution		Vertical Resolution（垂直解像度）
DCIM_DesktopMonitor	なし	Dell Command | Monitor - Monitor（監視）	Aspect Ratio（縦横比）
	CurrentResolutionH		Current Horizontal Resolution（現在の水平解像度）
	CurrentResolutionV		Current Vertical Resolution（現在の垂直解像度）
	説明		説明
	InputDisplayPort		Supports DisplayPort（DisplayPort をサポート）
	InputDVI		Supports DVI（HDMI をサポート）
	InputHDMI		Supports HDMI（HDMI をサポート）
	ManufactureDate		Manufacture Date（製造日）

クラス	プロパティ	レポートウィザードの Fields to Display（表示するフィールド）グループ	レポートウィザードの Fields to Display（表示するフィールド）アイテム名
	なし		Physical Diagonal Size (cm)（物理対角線サイズ（cm））
	なし		Physical Diagonal Size (in)（物理対角線サイズ（インチ））
	PhysicalSizeH		Physical Horizontal Size (cm)（物理水平サイズ（cm））
	PhysicalSizeV		Physical Vertical Size (cm)（物理垂直サイズ（cm））
	PrimaryStatus		PrimaryStatus
	SerialNumber		シリアルナンバー
	StandbyModeSupported		Supports Standby Mode（スタンバイモードをサポート）
	SuspendModeSupported		Supports Suspend Mode（サスペンドモードをサポート）
	VeryLowPowerSupported		Supports Very Low Power Mode（低電力モードをサポート）
DCIM_VProSettings	VProCharacteristics	Dell Command | Monitor - vPro Settings（vPro 設定）	vPro Characteristics（vPro 特性）
DCIM_AMTSettings	AMTSupported	Dell Command | Monitor - AMT Settings（AMT 設定）	AMT対応
	IDEREnabled		IDE-R Enabled（IDE-R 有効）
	SOLEnabled		SOLを有効にする
DCIM_PhysicalMemory	BankLabel	Dell Command | Monitor - Physical Memory（物理メモリ）	Bank Label（バンクラベル）
	容量		Capacity (bytes)（容量（バイト））

クラス	プロパティ	レポートウィザードの Fields to Display (表示するフィールド) グループ	レポートウィザードの Fields to Display (表示するフィールド) アイテム名
	ElementName		名前
	ManufactureDate		Manufacture Date (製造日)
	製造元		製造元
	MemoryType		Memory Type (メモリのタイプ)
	モデル		モデル
	PartNumber		パーツナンバー
	PrimaryStatus		Primary Status (プライマリステータス)
	SerialNumber		シリアルナンバー
	Speed		Speed (MHz) (スピード (MHz))
DCIM_Processor	Caption	Dell Command | Monitor - Processor (プロセッサ)	Caption
	CurrentClockSpeed		Current Clock Speed (MHz) (現在のクロックスピード (MHz))
	ElementName		名前
	MaxClockSpeed		Max Clock Speed (MHz) (最大クロックスピード (MHz))
	NumberOfEnabledCores		Number of Cores Enabled (有効なコア数)
	PrimaryStatus		Primary Status (プライマリステータス)
	Stepping		Stepping
DCIM_ProcessorCapabilities	NumberOfHardwareThreads		Hardware Threads (ハードウェアスレッド)
	NumberOfProcessorCores		Number of Cores (コア数)

クラス	プロパティ	レポートウィザードの Fields to Display（表示するフィールド）グループ	レポートウィザードの Fields to Display（表示するフィールド）アイテム名
DCIM_Battery	なし	Dell Command | Monitor - Battery（バッテリ）	Charge Health (%)（充電正常性（%））
	Chemistry		Chemistry
	DesignCapacity		Design Capacity (mWh)（設計容量（mWh））
	DesignVoltage		Design Voltage (mV)（設計電圧（mV））
	ExpectedLife		Expected Life (minutes)（想定寿命（分））
	FullChargeCapacity		Full Charge Capacity (mWh)（フル充電容量（mWh））
	HealthState		Health State（正常性状態）
	名前		名前
	PrimaryStatus		Primary Status（プライマリステータス）
	RechargeCount		Recharge Count（再充電カウント）
DCIM_LogEntry	CreationTimeStamp	なし	なし
	RecordData		
	RecordFormat		

Dell Command | Monitor からレポートで使用可能なハードウェアアラート

次の設定によって、レポートウィザードで作成されたレポートに含まれるアラート情報の量が決まります。

レポートウィザードの Fields to Display（表示するフィールド）グループ	レポートウィザードの Fields to Display（表示するフィールド）アイテム名
Dell Command | Monitor - Hardware Alerts（ハードウェアアラート）	カテゴリ
	説明
	重要度

レポートウィザードの Fields to Display（表示するフィールド）グループ	レポートウィザードの Fields to Display（表示するフィールド）アイテム名
	タイムスタンプ

Dell Command | Monitor スクリプトの追加

Dell Command | Monitor は、Dell Command Suite の監視ツールです。これにより、アプライアンスなどのリモート管理アプリケーションで管理および監視アクティビティを実行できます。Dell Command | Monitor ページを使用して、Dell Command | Monitor を展開するため、または Dell Command | Monitor をサポートするアプライアンス管理対象デバイスからこのツールを除去するために使用する、管理対象インストールに名前を付けて保存できます。

サポート対象のデルのハードウェアおよび Microsoft オペレーティングシステムを備えたデバイスが必要です。詳細については、「Dell Command | Monitor について」を参照してください。

Dell Command | Monitor を Dell TechCenter（http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7531.dell-command-monitor）からダウンロードしておきます。

注: このトピックではインストールについて説明しますが、Dell Command | Monitor - Monitor ページを使用して Dell Command | Monitor をデバイスから除去することもできます。

1. Windows Dell Command | Monitor ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。
    c. 設定ポリシー パネルの Windows セクションで、**Dell Command | Monitor** をクリックします。
2. **オプション**：デフォルトよりも明確な名前が必要な場合は、名前を変更します。
3. Action（アクション）を設定します。デフォルトの **インストール** のままにするか、**アンインストール** に変更します。
4. **保存** をクリックして、選択したアクションの設定情報が入力された 管理対象インストールの詳細 ページを表示します。

    アプライアンスによって 名前、ソフトウェア、関連付けられたソフトウェア、および 完全なコマンドライン フィールドに自動的に入力されます。

管理対象インストールの詳細 ページで必要な情報の入力を完了します。詳細については、「Windowsデバイス用の管理対象インストールの作成」を参照してください。

「デスクトップの壁紙」スクリプトの追加

このテンプレートを使用して、Windowsデバイスのデスクトップの壁紙の設定を制御するスクリプトを構築します。

壁紙ファイルに推奨される形式はビットマップ（BMP）です。スクリプトを実行すると、指定した壁紙のファイルがデバイスに配布されます。

1. デスクトップの壁紙 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。

c. 設定ポリシー パネルの Windows セクションで、**デスクトップの壁紙** をクリックします。

2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
壁紙の使用	ターゲットデバイスのデスクトップに壁紙ファイルが表示されます。
壁紙ビットマップファイル	**参照** または **ファイルの選択** をクリックし、壁紙に使用するファイルを選択してアップロードします。このファイルはBMP形式またはJPG形式である必要があります。
位置	位置 ドロップダウンリストからオプションを選択します。 • **拡大**: イメージが拡大されて画面全体に表示されます。 • **中央**: イメージが画面の中央に表示されます。 • **並べて表示**: イメージが画面全体で繰り返して表示されます。

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
5. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
6. **保存** をクリックします。

「デスクトップショートカット」スクリプトの追加

このテンプレートを使用して、Windowsデバイスのデスクトップまたは スタート メニューにインターネットショートカットを追加するスクリプトを作成します。

例えば、このスクリプトを使用して、企業のWebサイトやその他のURLへのショートカットを追加できます。

1. Windowsデスクトップショートカット ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。
   c. 設定ポリシー パネルの Windows セクションで、**デスクトップのショートカット** をクリックします。
2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。

3. **ショートカットの追加** をクリックします。
4. ショートカットの設定を指定します。

オプション	説明
名前	ショートカットの下または隣に表示されるテキストラベル。
ターゲット	ショートカットが選択されたときに起動するアプリケーション、ファイル、またはURLへのフルパス。例： explorer.exeのショートカットを作成するには、次の形式を使用します：C:\Windows\explorer.exe explorer.exeのUNC共有からショートカットを作成するには、次の形式を使用します： \\192.168.1.1\WINDOWS\explorer.exe または \\HostName\WINDOWS\explorer.exe
パラメータ	ショートカットに必要なコマンドラインパラメータ。例： /S /IP=123.4
作業ディレクトリ	現在の作業ディレクトリへの変更。例：C:\Windows\Temp
場所	ショートカットを表示する場所。オプションは次の通りです。「**デスクトップ**」と「**スタート メニュー**」。

5. **変更の保存** をクリックして、ショートカットを保存します。
6. **ショートカットの追加** をクリックして、さらにショートカットを追加します。ショートカットを編集または削除するには、マウスをショートカットの上に置き、次の **編集** ボタンまたは **削除** ボタンをクリックします。 または 。
7. **保存** をクリックして、スクリプトの詳細 ページを表示します。
8. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
9. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
10. **保存** をクリックします。

「イベントログリポーター」スクリプトの追加

このテンプレートを使用して、Windowsイベントログにクエリを送信し、その結果をアプライアンスにアップロードするスクリプトを作成します。

1. Windowsイベントログリポーター ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。

c. 設定ポリシー パネルの Windows セクションで、**イベントログリポーター** をクリックします。

2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
出力ファイル名	スクリプトによって作成されるログファイルの名前。
ログファイル	クエリを実行するログのタイプ：「ソフトウェア」、「システム」、または「セキュリティ」。
イベントタイプ	クエリを実行するイベントのタイプ：「情報」、「注意喚起」、または「エラー」。
ソース名	（オプション）クエリが制限されるソース名。

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
5. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
6. **保存** をクリックします。
7. デバイスのイベントログを表示するには、**インベントリ** をクリックし、次にデバイス名をクリックします。
8. スクリプトログ の 現在展開されているジョブとポリシー の下で、**イベントログ** の隣の ログの表示 リンクをクリックします。

「MSIインストーラー」スクリプトの追加

このテンプレートを使用して、Windowsデバイス上でMSIベースのインストーラーを実行するための基本的なコマンドライン引数を設定するためのスクリプトを作成します。

コマンドラインオプションについては、次の Microsoft の MSI コマンドラインに関するドキュメントを参照してください。http://msdn.microsoft.com/en-us/library/windows/desktop/aa367988%28v=vs.85%29.aspx.

1. Windows MSIインストーラ ページに移動します。

a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。

c. 設定ポリシー パネルの Windows セクションで、**MSIインストーラー** をクリックします。

2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
アクション	実行を待機中のタスク。タスクには、「**インストール**」、「**アンインストール**」、「**見つからないファイルの修復**」、および「**すべてのファイルの再インストール**」があります。
ソフトウェア	スクリプトに使用するアプリケーション。アプリケーションを検索するには、フィールドに入力し始めます。
MSIファイル名	MSIファイル名（ファイルがZIPアーカイブの場合に必要）。
ユーザーの操作	ユーザーにインストールを表示する方法。オプションは次の通りです。「**デフォルト**」、「**サイレント**」、「**基本UI**」、「**簡易UI**」、「**完全UI**」。
インストールディレクトリ	アプリケーションがインストールされるターゲットデバイスのディレクトリ。
その他のスイッチ	追加のインストーラースイッチ。その他のスイッチは msiexe.exe 引数と /i foo.msi 引数の間に挿入されます。
その他のプロパティ	追加のプロパティ。これらのプロパティはコマンドラインの終わりに挿入されます。例： msiexec.exe /s1 /switch2 /i patch123.msi TARGETDIR=C:\patcher PROP=A PROP2=B
機能の一覧	インストールする機能。コンマを使用して、複数の機能を区切ります。
デバイス単位の設定の保存	各デバイスの設定情報を保存するかどうか。
インストール後	インストール後に実行するアクション。
再起動オプション	デバイスの再起動後に実行するアクション。
ログ記録	インストールログに記録する情報。複数の項目を選択するには、**Ctrl**キーを押しながらクリックするか、**Command**キーを押しながらクリックします。
ログファイル名	ログファイルの名前。

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
5. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
6. **保存** をクリックします。

電源管理と消費電力について

デバイスの電力消費量の概要を得るために、設定した期間（1ヶ月など）に対する電源管理レポートを実行できます。

レポートの 電源管理 カテゴリの詳細については、レポートの作成を参照してください。

デバイス稼働時間に関する情報の保持期間を設定することもできます。詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。このオプションは、最新の設定オプションの1つです。

デスクトップデバイスの電力消費量についての情報を収集するには：

- シャーシタイプのインベントリのSmart Labelを作成する。
- シャーシタイプ別にデバイスをグループ化するレポートを作成する。
- 該当する期間が含まれる「**前回の再起動からの稼働時間**」について、インベントリのSmart Labelを作成する。

Windowsデバイス用の「電源管理」スクリプトの追加

このテンプレートを使用して、Windowsデバイス用の電源管理プロファイルを作成します。電力消費設定は、CPU使用率と電力消費との間の交換条件になります。

Windows デバイスの場合、電源管理は組み込みの **powercfg** コマンドを使用して設定します。

1. Windows電源管理 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。
    c. 設定ポリシー パネルの Windows セクションで、**電源管理** をクリックします。
2. 設定ポリシー：Windows電源管理 ページで、ターゲットオペレーティングシステムを選択します。
3. プロファイルとして、**調整されました**、**ハイパフォーマンス**、**省電力**、または **カスタム** を選択します。

    注: カスタム プロファイルを選択し、ハードディスク で ハードディスクを無効にするまでの秒数を「0」（ゼロ）に設定すると、ハードディスクの電源はオフになりません。

4. **保存** をクリックして、スクリプト：編集の詳細 ページを表示します。
5. 設定、展開、およびスケジュールオプションを選択し、**保存** をクリックします。詳細については、「スクリプトの追加と編集」を参照してください。

「レジストリ」スクリプトの追加

このテンプレートを使用して、Windowsデバイス上でレジストリ設定を適用するスクリプトを作成します。

1. regedit.exeを使用して、目的のレジストリから値を見つけて エクスポートします。
2. notepad.exeで、必要なレジストリ値が含まれる.regファイルを開き、テキストをコピーします。
3. Windowsレジストリ ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。

c. 設定ポリシー パネルの Windows セクションで、**レジストリ** をクリックします。

4. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
レジストリファイル	スクリプトの実行時に適用するレジストリ値。

5. **保存** をクリックして、スクリプトの詳細 ページを表示します。
6. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
7. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
8. **保存** をクリックします。

新しいスクリプトが作成されます。このスクリプトは、レジストリファイル内の値がターゲットデバイスで見つかった値に一致するかを確認します。見つからないか間違った値があれば置き換えます。

「リモートデスクトップコントロールトラブルシューター」スクリプトの追加

このテンプレートを使用して、Windowsデバイス上のリモートデスクトップコントロール機能のトラブルシューティングスクリプトを作成します。

このスクリプトは、次のものをテストします。

- **ターミナルサービス**: リモートデスクトップを使用して Windows デバイスにアクセスするには、ターミナルサービスが実行されている必要があります。このスクリプトは、ターミナルサービスが実行されていることを確認します。
- **ファイアウォール構成**: Windows ファイアウォールがデバイス上で実行されている場合、このスクリプトはリモートデスクトップコントロールの要求をブロックする構成がないかをテストします。

1. リモートデスクトップコントロールトラブルシューター ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。
   c. 設定ポリシー パネルの Windows セクションで、**リモートデスクトップコントロールトラブルシューター** をクリックします。
2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。

オプション	説明
ファイアウォール構成	スクリプトの実行時に適用する設定を指定します。

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
5. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
6. **保存** をクリックします。

UltraVNCスクリプトの追加

このテンプレートを使用して、UltraVNCをWindowsデバイスに配布するスクリプトを作成します。UltraVNCは、管理者によるデバイスへのリモートログインを可能にする、無料のアプリケーションです。

UltraVNC の詳細については、http://www.uvnc.comを参照してください。

1. Windows UltraVNC ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。
    c. 設定ポリシー パネルの Windows セクションで、**UltraVNC** をクリックします。
2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
ミラードライバのインストール	オプションのUltraVNC Mirror Video Driverをインストールします。 Mirror Video Driverは、より高速で正確なアップデートを可能にするドライバです。また、ビデオドライバのフレームバッファメモリとUltraWinVNCサーバーとの間の直接リンクも行います。 これにより、フレームバッファが使用されるため、集中的な画面のビットブロック転送にCPUが使用されなくなり、CPUの処理速度は向上し、負荷は軽減されます。
ビューアのインストール	オプションのUltraVNCビューアをインストールします。ビューアは、複数のVNCサーバーを接続してリモートでデスクトップを表示するために使用するツールです。ビューアは、管理対象デバイスからリモートセッションを開始する必要がある場合にのみ、インストールします。
トレイアイコンを無効にする	UltraVNCトレイアイコンが、デバイス上で表示されないようにします。

オプション	説明
トレイアイコンメニューのクライアントオプションを無効にする	クライアントオプションが、デバイスのトレイアイコンメニューに表示されないようにします。このオプションは、「**トレイアイコンを無効にする**」が有効になっている場合のみ、使用可能です。
プロパティパネルを無効にする	デバイスでUltraVNCのプロパティパネルを無効にします。
エンドユーザーによるUltraVNCの終了をブロック	デバイスユーザーがWinVNCを終了できないようにします。
Password（パスワード）および **Read Only Password**（読み取り専用パスワード）	認証用のパスワードを指定します。
Windows ログオンが必要	Windowsログオン認証を使用し、VNC®インストールからACLをエクスポートします。MSLogonACL.exe /e acl.txtを使用します。このテキストファイルの内容をコピーして ACL フィールドに貼り付けます。
暗号化キー	キーベースの暗号化を使用します。キーベースの暗号化を使用するには、次の手順でキーを作成してアップロードします。 a. UltraVNCビューアで、DSPLugin リストから「MSRC4Plugin」を選択します。 b. **Config** をクリックして、キーファイルを配置するフルパスを入力します。 c. **Gen Key** をクリックし、キーファイルをアップロードします。

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. このテンプレートによって生成されるスクリプトを参照して、出力を確認します。
5. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
6. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
7. **保存** をクリックします。

「アンインストーラ」スクリプトの追加

このテンプレートを使用して、Windowsデバイス上のアプリケーションとプロセスを管理するスクリプトを作成します。スクリプトを使用して、アンインストールコマンドを実行し、プロセスを強制終了して、ディレクトリを削除できます。

1. Windowsアンインストーラー ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。

c. 設定ポリシー パネルの Windows セクションで、**アンインストーラ** をクリックします。

2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
ソフトウェア	スクリプトに使用するアプリケーション。アプリケーションを検索するには、フィールドに入力し始めます。
ファイル	コマンド情報。アプリケーションを選択すると、テンプレートはアンインストールコマンドディレクトリ、ファイル、およびパラメータの入力を試みます。値が正しいことを確認します。
パラメータ	
ディレクトリ	
ディレクトリの削除	アンインストールコマンドを実行した後に、削除するディレクトリのフルネーム。例：C:\Program Files**Example_App**\
プロセスの強制終了	アンインストールコマンドの実行前に強制終了させるプロセスのフルネーム。例：notepad.exe

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
5. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
6. **保存** をクリックします。

Mac OS X設定ポリシーの使用

設定ポリシーテンプレートを使用して、Mac OS Xデバイスでのポリシーを設定するスクリプトを作成できます。

「Active Directory」スクリプトの追加

このテンプレートを使用して、Mac OS Xデバイスで、デバイスをドメインに追加するスクリプトや、ドメインから削除するスクリプトを作成します。また、このスクリプトを使用して、Mac OS XデバイスがActive Directoryデータベースに確実にチェックインするようにもできます。

スクリプトを作成するときに指定するユーザー名とパスワードは、特定のドメインに対するデバイスの追加や削除を行える管理権限を持つ、ネットワークアカウントのものである必要があります。

1. Mac Active Directory ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。

c. 設定ポリシー パネルの Mac セクションで、**Active Directory** をクリックします。

2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
アクション	現在のドメインからデバイスを追加または削除するかどうかを指定します。
ネットワーク資格情報	管理者のユーザー名とパスワードを入力します。 **注:** 生成されるスクリプトでは、rootアクセスがあることを前提とし、復号化された（クリアテキスト）パスワードが使用されます。したがって、このスクリプトのユーザーがすべて信頼されていることを確認してください。
設定するドメイン	LDAPドメイン名、ユーザー認証情報、およびその他の情報を指定します。

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
5. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
6. **保存** をクリックします。

「電源管理」スクリプトの追加

このテンプレートを使用して、Mac OS Xデバイス用の電源管理プロファイルを作成します。電力消費設定は、CPU使用率と電力消費との間の交換条件になります。

各電源に独自の設定を適用するには、複数の設定スクリプトを作成します。一部のデバイスでは、サポートされない機能もあります。

1. Mac電源管理 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。
   c. 設定ポリシー パネルの Mac セクションで、**電源管理** をクリックします。
2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
プロファイル名	使用するプロファイルオプションを指定します。 • 「**電力節約優先**」: エネルギーを節約する設定を適用します。その結果、パフォーマンスが

オプション	説明
	低下することがあります。この設定を選択すると、プロファイルオプション セクションのオプションは編集できません。 • 「**標準**」: デフォルト設定を使用します。この設定を選択すると、プロファイルオプション セクションのオプションは編集できません。 • 「**パフォーマンス優先**」: パフォーマンスを最適化する設定を適用します。その結果、エネルギー消費量が多くなることがあります。この設定を選択すると、プロファイルオプション セクションのオプションは編集できません。 • **カスタム**: カスタムプロファイルオプションを使用します。この設定を選択すると、プロファイルオプション セクションのオプションが編集可能になります。
電源	電源を選択します。 • 「**すべて**」 : デバイスの電源に関係なく、常にポリシーが適用されます。 • 「**バッテリ**」: デバイスで内蔵バッテリが使用されている場合のみ、ポリシーが適用されます。 • 「**充電器 (壁面コンセント)**」: デバイスがコンセントに接続されている場合のみ、ポリシーが適用されます。 • 「**UPS**」: デバイスがUPS (無停電電源装置) に接続されている場合のみ、ポリシーが適用されます。
オペレーティングシステム	プロファイル ドロップダウンリストで **カスタム** を選択した場合は、このポリシーを適用するオペレーティングシステムを指定します。プロファイルオプション が更新され、選択したバージョンで使用できるオプションのみが表示されます。

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
5. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
6. **保存** をクリックします。

「VNC」スクリプトの追加

このテンプレートを使用して、Mac OS®デバイス上で組み込みのVNC (仮想ネットワークコンピューティング) の設定を行うスクリプトを作成します。VNC設定によって、ビューアでデバイス画面を制御できるかどうかが決定されます。

このスクリプトにより、画面共有の有効/無効も設定できます。Mac OS Xを実行する別のMacから接続するには、Macのアカウントのユーザー名とパスワードが必要です。このスクリプトの使用には注意が必要です。資格情報は暗号化されますが、VNCセッションは暗号化されない場合があります。

1. Mac VNC ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**設定ポリシー** をクリックします。
    c. 設定ポリシー パネルの Mac セクションで、**VNC** をクリックします。
2. 次の情報を入力します。

オプション	説明
名前	スクリプトを識別するための名前。この名前は、スクリプト ページに表示されます。
有効	ポリシーを有効にします。
パスワード	VNCのパスワードを指定します。

3. **保存** をクリックして、スクリプトの詳細 ページを表示します。
4. 設定、展開、およびスケジューリング用のオプションを選択します。詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。
5. スクリプトで使用される生XMLを編集するには、スケジュール セクションの下の **XMLの編集** をクリックします。
6. **保存** をクリックします。

ポリシーとスクリプトの編集

必要に応じてポリシーとスクリプトを編集できます。

1. スクリプトの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
    c. スクリプトの詳細 ページを表示するには、次のいずれかを実行します。
    - スクリプトの名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. 設定、展開、およびスケジュールオプションを変更します。

詳細については、「オフライン KScript、オンライン KScript、またはオンラインシェルスクリプトの追加」を参照してください。

3. ページの一番下で、次のオプションの隣にある **ここをクリックします** をクリックします。
   - 「元の工ディタを使用してポリシーを再編集するには」：**テンプレートで使用可能な元の設定を表示して編集します。**
   - 「この工ディタを使用してポリシーを編集するには」：**すべての設定を表示して編集します。**
4. ポリシーを編集して、**保存** をクリックします。

スクリプトログの検索

スクリプトログで文字列を検索することができます。アプライアンス上で組織コンポーネントが有効化されている場合は、組織ごとにスクリプトログを個別に検索します。

スクリプトが管理対象デバイスで実行されると、ログが作成されてアプライアンスにアップロードされます。スクリプトログで文字列を検索し、検索文字列に一致したログがあるデバイスにラベルを適用できます。必要に応じて、そのラベルの付いたデバイスでアクションが実行することができます。

1. スクリプトログの検索 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプトログの検索** をクリックします。
2. 検索対象 フィールドに、検索条件または検索する文字列を入力します。文字列の長さは4文字以上である必要があります。これより短い文字列で検索すると、一致する結果がゼロになります。

   検索条件を入力するときは、次の演算子を使用します。

演算子	関数
+	プラス記号を先頭に付けると、そのテキストを含むエントリを検索します。
-	マイナス記号を先頭に付けると、そのテキストを含まないエントリを検索します。
*****	末尾にアスタリスクが付いていると、その特定の文字で始まる単語を含むログを検索します。
"	テキストを二重引用符で囲むと、そのフレーズとまったく同じフレーズを検索します。

3. 検索条件を選択します。

オプション	説明
全アップロードログ	すべての利用可能なスクリプトログを検索します。アプライアンスで組織コンポーネントが有効になっている場合、選択した組織のすべてのログが検索されます。

オプション	説明
	注: スクリプトログはアプライアンスのアップグレード時に削除されます。アプライアンスがアップグレードされると、アップグレード前にアップロードされたログは利用できなくなります。
最新アップロードログ	最新のスクリプトログを検索します。アプライアンスで組織コンポーネントが有効になっている場合、選択した組織のすべてのログが検索されます。
スクリプト	すべてのスクリプトに関連するログ、または指定したスクリプトのみを検索します。
ログ	すべてのログ、または指定したログのみを検索します。
ラベル	すべてのデバイスからアップロードされたログ、または指定したラベルに関連付けられたデバイスからからアップロードされたログを検索します。

4. **検索** をクリックします。

   検索結果には、ログが表示されると共に、ログをアップロードしたデバイスも表示されます。
5. 表示されたデバイスにラベルを適用するには、検索結果の下にあるドロップダウンリストからラベルを選択します。

スクリプトのエクスポート

複数の組織またはアプライアンスがある場合は、必要に応じて、スクリプトをエクスポートし、組織間またはアプライアンス間で転送できます。

詳細については、「リソースのインポートとエクスポートについて」を参照してください。

Mac プロファイルの管理

アプライアンスを使用して、エージェント管理対象デバイスに Mac プロファイルを配布できます。Mac プロファイルには、ユーザーレベルおよびシステムレベルのポリシーのペイロード（設定）が含まれています。

アプライアンスを使用した Mac プロファイルの配布は、管理対象の Mac デバイスの設定を行う効率的な方法であり、OS X サーバを使用したプロファイルの設定および配布に替わる方法です。

ユーザーレベルおよびシステムレベルの Mac プロファイルペイロード（設定）をアプライアンス**管理者コンソール**で設定できます。また、Apple プロファイルマネージャを使用したカスタムペイロードの作成、それらのペイロードを格納する MOBILECONFIG ファイルのダウンロード、および配布のためのファイルのアプライアンスへのアップロードを行うことができます。

Mac プロファイルの詳細については、http://help.apple.com/profilemanager/mac/4.0を参照してください。

KACE エージェントによるプロファイルの配布方法

新しい Mac プロファイルを追加またはアップロードすると、アプライアンスによって、デバイスでのプロファイルのインストールまたは削除に必要なオンライン KScript が作成されます。他のオンライン KScript と同様に、Mac プロファイルを含むスクリプトは、スケジュールおよびプロファイルで指定された展開オプションに従って KACE エージェントがターゲットデバイスに接続されたときに実行されます。

Mac プロファイル設定に対する変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。

詳細については、「履歴設定について」を参照してください。

Mac プロファイルの追加、編集、およびアップロード

Mac ユーザープロファイルおよびシステムプロファイルをアプライアンスに追加でき、必要に応じて Mac プロファイルを編集できます。また、設定情報が含まれた MOBILECONFIG ファイルをアプライアンスにアップロードできます。

Mac ユーザープロファイルの追加または編集

管理者コンソールを使用して、Mac ユーザープロファイルをアプライアンスに追加できます。ユーザープロファイルには、ユーザーに適用される設定（E メール設定など）が含まれています。アプライアンスに追加されたユーザープロファイルは、エージェント管理対象 Mac OS X デバイスに展開できます。サポートされている Mac OS X バージョンのリストについては、製品マニュアルページの技術仕様を参照してください。https://support.quest.com/kace-systems-management-appliance/technical-documents.

プロファイルを追加または編集する場合、Exchange、LDAP、またはメールのペイロードを設定するために必要なアカウント情報、サーバー情報、およびポート情報があることを確認します。

注: **管理者コンソール**で設定したプロファイルのペイロードを編集できます。ただし、**管理者コンソール**にアップロードされたプロファイルのペイロードは表示または編集できません。

1. Mac Profile Detail（Mac プロファイルの詳細）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
    c. 次のいずれかを実行します。
    - プロファイルの名前をクリックします。
    - **アクションの選択 > 新しいユーザープロファイル** をクリックします。
2. 一般的なオプション セクションで、次の情報を入力します。

オプション	説明
プロファイル名	Mac Profiles リストに表示される名前。この名前は一意である必要はありませんが、リストでプロファイルを識別できるようにする必要があります。 **注:** プロファイル名はいつでも変更できます。ただし、プロファイルがデバイスにインストールされた後で名前を変更した場合、デバイス上のプロファイル名は更新されません。プロファイルはインストール時の名前で識別され続けます。

オプション	説明
説明	プロファイルに関する追加情報。設定や意図された用途などです。
User ability to remove profile（プロファイル除去のユーザー機能）	ユーザーがデバイスからプロファイルを除去できるかどうか。オプションは次の通りです。 • **無効**：ユーザーはプロファイルを除去できません。 • **Always**（常に）：ユーザーはパスワードを入力せずにいつでもプロファイルを除去できます。 • **With Password**（パスワードを使用）：ユーザーはプロファイルに関連付けられたパスワードを入力すればプロファイルを除去できます。
Automatically remove profile（プロファイルの自動除去）	指定した時間の後でプロファイルが自動的に除去されるかどうか。このアクションは、学期の終了後など、特定の日付の後でプロファイルを変更する必要があるデバイスを設定する場合に便利です。オプションは次の通りです。 • **無効**：プロファイルは自動的に除去されるようにスケジュールされません。 • **On Date**（日付指定）：プロファイルは指定した日付で自動的に除去されるようにスケジュールされます。日付は **mm/dd/yyyy** 形式で指定する必要があります。 • **After**（経過後）：プロファイルは指定した時間の経過後に除去されるようにスケジュールされます。時間は日数または時間で指定できます。

3. **オプション**：Payloads（ペイロード）セクションで、Exchange、LDAP、またはメールの設定を追加または編集します。
   - Exchange 設定情報を追加または編集します。

     注: ユーザー名、E メールアドレス、パスワードなどのユーザー自身の情報の入力を求めるプロンプトをユーザーに表示するには、フィールドを空のままにします。ただし、Account Name（アカウント名）などのフィールドは空のままにすることはできません。

オプション	説明
Account Name（アカウント名）	アカウントを識別するために使用される名前。
ユーザー	ユーザーの名前。
Eメールアドレス	E メールアカウントに使用するアドレス。
パスワード	E メールアカウントのパスワード。
Internal Exchange Host and Port（内部 Exchange ホストおよびポート）	内部 Exchange サーバーのホスト名および E メール通信に使用されるポート。

オプション	説明
External Exchange Host and Port（外部 Exchange ホストおよびポート）	外部 Exchange サーバーのホスト名および E メール通信に使用されるポート。
Internal Server Path（内部サーバーパス）	内部ネットワーク上のサーバーへのパス。
External Server Path（外部サーバーパス）	外部ネットワーク上のサーバーへのパス。
Use SSL for Internal Exchange Host（内部 Exchange ホストに SSL を使用）	ドメイン内で送信される E メールに対して Secure Sockets Layer を使用するかどうか。
Use SSL for External Exchange Host（外部 Exchange ホストに SSL を使用）	ドメイン外で送信される E メールに対して Secure Sockets Layer を使用するかどうか。

- LDAP 設定情報を追加または編集します。

注: ユーザー名やパスワードなどのユーザー自身の情報の入力を求めるプロンプトをユーザーに表示するには、フィールドを空のままにします。ただし、Account Hostname（アカウントホスト名）などのフィールドは空のままにすることはできません。

オプション	説明
Account Description（アカウント説明）	LDAP アカウントの名前（Example Corporation LDAP Account など）。
Account Username（アカウントユーザー名）	LDAP サーバーへのログインに使用されるアカウントのユーザー名。
Account Password（アカウントパスワード）	LDAP サーバーへのログインに使用されるアカウントのパスワード。
Account Hostname（アカウントホスト名）	LDAP サーバーのホスト名または IP アドレス。
SSLを使用	LDAP サーバーへの接続に Secure Sockets Layer を使用するかどうか。

オプション	説明
Search Settings（検索設定）	LDAP サーバー上の情報を検索するために使用される設定。
• **説明**	リスト内の検索情報を識別する情報。
• **Scope（スコープ）**	検索の深さ。検索が次のものに対して実施されるかどうかを示します。 • **Base**（ベース）：ベースつまりゼロレベルのオブジェクトのみが含まれます。 • **1レベル**：ベースに直接従属しているオブジェクトが含まれます（ベースは含まれません）。 • **Subtree**（サブツリー）：ベースおよびサブツリー内のオブジェクトが含まれます。
• **Search Base（検索ベース）**	**Search Base**（検索ベース）：検索を開始するディレクトリ内の場所。検索ベースによって、LDAP または Active Directory 構造における場所またはコンテナを指定します。この基準には、認証するすべてのユーザーが含まれる必要があります。基準を満たす OU、DC、または CN のベース DN の最も明確な組み合わせを入力します（一番左は最も限定的、一番右は最も一般的です）。例えば、このパスが、認証対象となるユーザーが属するコンテナを指している場合は、次の通りです。 「OU=end_users,DC=company,DC=com」。

◦ メール設定情報を追加または編集します。

注: 表示名や E メールアドレスなどのユーザー自身の情報の入力を求めるプロンプトをユーザーに表示するには、フィールドを空のままにします。ただし、Incoming Mail Server（受信メールサーバー）などのフィールドは空のままにすることはできません。

オプション	説明
Account Description（アカウント説明）	アカウントの名前（Example Corporation Mail Account など）。
Account Type（アカウントタイプ）	アカウントへのアクセスに使用されるプロトコル（POP または IMAP）。
User Display Name（ユーザー表示名）	E メールメッセージの From（送信者）フィールドに表示されるユーザー名。
Eメールアドレス	ユーザーの E メールアドレス。
Incoming Mail Server and Port（受信メールサーバーおよびポート）	受信メールに対して使用されるホスト名または IP アドレスとポート番号。

オプション	説明
Outgoing Mail Server and Port（送信メールサーバーおよびポート）	送信メールに対して使用されるホスト名または IP アドレスとポート番号。次の標準のポート割り当てを使用します。 • SMTP：25（SSL では 465） • POP3：110（SSL では 995） • IMAP：143（SSL では 993）
Incoming Mail User Name（受信メールユーザー名）	受信メールサーバーに対して使用するユーザー名。
Outgoing Mail User Name（送信メールユーザー名）	送信メールサーバーに対して使用するユーザー名。
Incoming Mail Authentication Type（受信メール認証タイプ）	受信メールのユーザーを認証する方法。認証タイプには、パスワード、MD5 チャレンジ / レスポンス、NTLM、HTTP MD5 Digest があります。
Outgoing Mail Authentication Type（送信メール認証タイプ）	送信メールのユーザーを認証する方法。認証タイプには、パスワード、MD5 チャレンジ / レスポンス、NTLM、HTTP MD5 Digest があります。
Incoming mail use SSL（受信メールで SSL を使用）	ユーザーアカウントに送信されるメールに対して Secure Socket Layer を使用するかどうか。
Outgoing mail use SSL（送信メールで SSL を使用）	ユーザーアカウントから送信されるメールに対して Secure Socket Layer を使用するかどうか。

4. （オプション）展開 セクションで、プロファイルのターゲットデバイスを選択します。

ヒント: ターゲットデバイスを選択しないでプロファイルを作成できます。ただし、ターゲットデバイスを選択するまでプロファイルを展開できません。

オプション	説明
全デバイス	Mac OS X のサポート対象バージョン（バージョン 10.8、10.9、または 10.10）を実行しているすべての KACE エージェント管理対象デバイスにプロファイルを配布します。アプライアンスで組織コンポーネントが有効になっている場合、選択した組織のすべてのサポート対象 Mac デバイスがこの配布に含まれます。
ラベル	選択したラベル内のデバイスにのみプロファイルを配布します。ラベル、特に Smart Label に配布を制限すると、プロファイルを適切に適用するのに役立ちます。 このオプションを使用するには、予めラベルまたは Smart Labelを作成しておく必要があります。詳細については、「デバイスに対するSmart Labelの追加」を参照してください。
デバイス	選択したサポート対象 Mac OS X デバイス（バージョン 10.8、10.9、または 10.10）にプロファイル

オプション	説明
	を配布します。デバイスを検索するには、フィールドに入力し始めます。
オペレーティングシステム	アプリケーションが実行されるオペレーティングシステム。アプリケーションは、選択したオペレーティングシステムがインストールされているデバイスにのみ導入されます。 a. **オペレーティングシステムの管理** をクリックします。 b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Mac 10.11 El Capitan x86 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**Mac > 10.11 El Capitan** の順に選択し、**x86** を選択します。
すべて削除	選択されているすべてのデバイスをこのセクションの デバイス リストから除去します。

5. スケジュール セクションで、プロファイルをターゲットデバイスに配布するためのオプションを選択します。

オプション	説明
なし	プロファイルをスケジュールに基づいて配布しません。スケジュールが **なし** に設定されたプロファイルは、Mac Profiles リストでステータスは **無効** です。ただし、スケジュールが **なし** に設定されたプロファイルも、ページの一番下で **今すぐ実行** を選択した場合は展開できます。
n 分 / 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。

オプション	説明
	* * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

6. Deployment Options（展開オプション）セクションで、プロファイルのインストールに関するプロンプトをユーザーに表示するためのオプションを選択します。

オプション	説明
Runtime prompt for logged-in users（ログインユーザーの実行時プロンプト）	エージェントによってプロファイルのインストールが開始されると、ターゲットデバイスにログインしているユーザーにプロンプトが表示されます。

オプション	説明
Login prompt for all users（全ユーザーのログインプロンプト）	ユーザーがターゲットデバイスにログインすると、まだ実行していない場合はプロファイルのインストールを求めるプロンプトが表示されます。
Both runtime and login prompts（実行時とログイン両方のプロンプト）	エージェントによってプロファイルのインストールが開始されると、ターゲットデバイスにログインしているユーザーに、まだ実行していない場合はプロファイルのインストールを求めるプロンプトが表示されます。スクリプトの実行後にログインするユーザーにも、プロファイルのインストールを求めるプロンプトが表示されます。

7. ページの一番下で、次のいずれかのアクションを選択します。

オプション	説明
保存	プロファイルを保存して Mac Profiles リストに戻ります。
今すぐ実行	アプライアンスへのアクティブなエージェント接続があるターゲットデバイスで、選択した展開オプションに従ってプロファイルをすぐにインストールします。詳細については、「実行 および 今すぐ実行 コマンドの使用」を参照してください。
複製	プロファイル名の前に Copy of を付加してプロファイルのコピーを作成します。このオプションは、まだ保存されていない新しいプロファイルに対しては使用できません。詳細については、「既存のプロファイルをテンプレートとして使用した Mac プロファイルの追加」を参照してください。
削除	ターゲットデバイスからプロファイルを除去するために使用できるプロファイルを作成します。このオプションは、まだ保存されていない新しいプロファイルに対しては使用できません。詳細については、「管理対象デバイスからの Mac プロファイルの除去」を参照してください。
削除	アプライアンスからプロファイルを除去します。プロファイルがインストールされているデバイスからはプロファイルは除去されません。このオプションは、まだ保存されていない新しいプロファイルに対しては使用できません。詳細については、「アプライアンスからの Mac プロファイルの削除」を参照してください。
キャンセル	変更を破棄して Mac Profiles リストに戻ります。

Mac システムプロファイルの追加または編集

管理者コンソールを使用して、Mac システムプロファイルをアプライアンスに追加できます。システムプロファイルには、デバイスに適用される設定（パスコード要件など）が含まれています。アプライアンスに追加されたシステムプロファイルは、エージェント管理対象 Mac OS X デバイスに展開できます。サポートされてい

る Mac OS X バージョンのリストについては、製品マニュアルページの技術仕様を参照してください。https://support.quest.com/kace-systems-management-appliance/technical-documents.

アプリへのアクセスとパスコードの設定のポリシーを確立しておきます。

注: **管理者コンソール**で設定したシステムプロファイルのペイロードを編集できます。ただし、**管理者コンソール**にアップロードされたプロファイルのペイロードは表示または編集できません。

1. Mac Profile Detail（Mac プロファイルの詳細）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
   c. 次のいずれかを実行します。
   - プロファイルの名前をクリックします。
   - **アクションの選択 > 新しいシステムプロファイル** をクリックします。
2. 一般的なオプション セクションで、次の情報を入力します。

オプション	説明
プロファイル名	Mac Profiles リストに表示される名前。この名前は一意である必要はありませんが、リストでプロファイルを識別できるようにする必要があります。 **注:** プロファイル名はいつでも変更できます。ただし、プロファイルがデバイスにインストールされた後で名前を変更した場合、デバイス上のプロファイル名は更新されません。プロファイルはインストール時の名前で識別され続けます。
説明	プロファイルに関する追加情報。設定や意図された用途などです。
User ability to remove profile（プロファイル除去のユーザー機能）	ユーザーがデバイスからプロファイルを除去できるかどうか。オプションは次の通りです。 • **無効**：ユーザーはプロファイルを除去できません。 • **Always**（常に）：ユーザーはパスワードを入力せずにいつでもプロファイルを除去できます。 • **With Password**（パスワードを使用）：ユーザーはプロファイルに関連付けられたパスワードを入力すればプロファイルを除去できます。
Automatically remove profile（プロファイルの自動除去）	指定した時間の後でプロファイルが自動的に除去されるかどうか。これは、学期の終了後など、特定の日付の後でプロファイルを変更する必要があるデバ

オプション	説明
	イスを設定する場合に便利です。オプションは次の通りです。 • **無効**：プロファイルは自動的に除去されるようにスケジュールされません。 • **On Date**（日付指定）：プロファイルは指定した日付で自動的に除去されるようにスケジュールされます。日付は **mm/dd/yyyy** 形式で指定する必要があります。 • **After**（経過後）：プロファイルは指定した時間の経過後に除去されるようにスケジュールされます。時間は日数または時間で指定できます。

3. Payloads（ペイロード）セクションで、Gatekeeper（ゲートキーパー）設定情報を追加または編集します。

オプション	説明
Allow Apps Downloaded From（アプリのダウンロード元）	ユーザーが次の場所からアプリをダウンロードできるかどうか。 • **Mac App Store**：ユーザーは Mac App Store からのみアプリをダウンロードできます。 • **Mac App Store and Identified Developers**（Mac App Store および識別された開発者）：ユーザーは Mac App Store から、および Apple の一意の開発者 ID を使用してアプリにデジタル署名した開発者からアプリをダウンロードできます。 • **Anywhere**（任意の場所）：ユーザーは任意の場所から制限なしにアプリをダウンロードできます。
Don't allow user to override Gatekeeper setting（ユーザーにゲートキーパー設定を上書きさせない）	ユーザーがアプリのダウンロード設定を変更できるかどうか。

4. Passcode（パスコード）設定情報を追加または編集します。

注: このセクションでは、**パスコード**という用語は**パスワード**という用語と同じ意味です。

オプション	説明
Allow simple value（単純な値を許可）	ユーザーは繰り返し、昇順、降順の文字シーケンスのパスコードを選択できます。
Require alphanumeric value（英数字の値が必要）	ユーザーは最低 1 つの文字と 1 つの数字を含むパスコードを選択する必要があります。
Minimum passcode length（パスコードの最小の長さ）	パスコードで許可される最小文字数。

オプション	説明
Minimum number of complex characters（特殊文字の最小数）	パスコードで許可される英数字以外の文字（* や！など）の最小数。
Maximum number of failed attempts（最大失敗試行回数）	アカウントがロックアウトされるまでに、ユーザーがデバイスをアンロックするために間違ったパスコードを入力できる回数。
Maximum grace period for device lock（デバイスロックの最大猶予時間）	システム設定で一定時間何もしないとデバイスがロックされるように指定されている場合、この設定によってユーザーがパスコードを入力しなくてもデバイスをアンロックできる時間が設定されます。猶予時間が過ぎると、ユーザーはパスコードを入力してデバイスをアンロックする必要があります。
Maximum passcode age in days（最大パスコード有効期限（日数））	パスコードの変更が必要になるまでの日数。
Passcode history（パスコード履歴）	パスコードの再利用が可能になるまでに一意である必要があるパスコードの数。
Delay after failed login attempts in minutes（失敗ログイン試行後の遅延（分））	最大失敗ログイン試行回数に達した後、ユーザーがログインを試行できるようになるまでに経過する必要がある分数。

5. 展開 セクションで、プロファイルのターゲットデバイスを選択します。

オプション	説明
全デバイス	Mac OS X のサポート対象バージョン（バージョン 10.8、10.9、または 10.10）を実行しているすべての KACE エージェント管理対象デバイスにプロファイルを配布します。アプライアンスで組織コンポーネントが有効になっている場合、選択した組織のすべてのサポート対象 Mac デバイスが含まれます。
ラベル	選択したラベル内のデバイスにのみプロファイルを配布します。ラベル、特に Smart Label に配布を制限すると、プロファイルを適切に適用するのに役立ちます。 このオプションを使用するには、予めラベルまたは Smart Labelを作成しておく必要があります。詳細については、「デバイスに対するSmart Labelの追加」を参照してください。
デバイス	選択したサポート対象 Mac OS X デバイス（バージョン 10.8、10.9、または 10.10）にプロファイルを配布します。デバイスを検索するには、フィールドに入力し始めます。
オペレーティングシステム	アプリケーションが実行されるオペレーティングシステム。アプリケーションは、選択したオペレーティングシステムがインストールされているデバイスにのみ導入されます。

オプション	説明
	a. **オペレーティングシステムの管理** をクリックします。 b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Mac 10.11 El Capitan x86 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**Mac > 10.11 El Capitan** の順に選択し、**x86** を選択します。
すべて削除	すべてのデバイスをこのセクションの デバイス リストから除去します。

6. スケジュール セクションで、プロファイルをターゲットデバイスに配布するためのオプションを選択します。

オプション	説明
なし	プロファイルをスケジュールに基づいて配布しません。スケジュールが **なし** に設定されたプロファイルは、Mac Profiles リストでステータスは **無効** です。ただし、スケジュールが **なし** に設定されたプロファイルも、ページの一番下で **今すぐ実行** を選択した場合は展開できます。
n 分 / 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59)

オプション	説明
	値の指定は次の要領で行います。 • **スペース ( )**：各フィールドはスペースで区切ります。 • **アスタリスク (*)**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。

7. ページの一番下で、次のいずれかのアクションを選択します。

オプション	説明
保存	プロファイルを保存して Mac Profiles リストに戻ります。
今すぐ実行	アプライアンスへのアクティブなエージェント接続があるターゲットデバイスで、選択した展開オプションに従ってプロファイルをすぐにインストールします。詳細については、「実行 および 今すぐ実行 コマンドの使用」を参照してください。
複製	プロファイル名の前に Copy of を付加してプロファイルのコピーを作成します。このオプションは、まだ保存されていない新しいプロファイルに対しては使用できません。詳細については、「既存のプロファイルをテンプレートとして使用した Mac プロファイルの追加」を参照してください。
削除	ターゲットデバイスからプロファイルを除去するために使用できるプロファイルを作成します。このオ

オプション	説明
	プションは、まだ保存されていない新しいプロファイルに対しては使用できません。詳細については、「管理対象デバイスからの Mac プロファイルの除去」を参照してください。
削除	アプライアンスからプロファイルを除去します。プロファイルがインストールされているデバイスからはプロファイルは除去されません。このオプションは、まだ保存されていない新しいプロファイルに対しては使用できません。詳細については、「アプライアンスからの Mac プロファイルの削除」を参照してください。
キャンセル	変更を破棄して Mac Profiles リストに戻ります。

既存のプロファイルをテンプレートとして使用した Mac プロファイルの追加

既存のプロファイルを複製して Mac プロファイルを追加できます。これは、既存のプロファイルをさまざまなデバイスにインストールしたり、プロファイルのインストールをさまざまな時点で行うようにスケジュールしたりする場合に便利です。プロファイルを複製し、必要に応じてターゲットデバイスまたはスケジュールを変更できます。

ユーザープロファイルまたはシステムプロファイルをアプライアンスに追加しておきます。

インポートされたプロファイルを複製することはできません。

1. Mac Profiles ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
2. プロファイルの名前をクリックして、Mac Profile Detail（ Mac プロファイルの詳細 ）ページを表示します。
3. ページの一番下で**複製** をクリックします。

    プロファイルが複製され、Mac Profile（ Mac プロファイル ）リストに表示されます。プロファイル名の前に Copy of が付加されます。複製されたプロファイルのプロパティと ID 番号は元のプロファイルと同じですが、複製されたアクションが同じデバイスで実行されないように、スケジュールは自動的に **なし** に設定されます。

アプライアンスへの Mac プロファイルのアップロード

アプライアンスでは、Mac プロファイルの作成に必要な設定を含む MOBILECONFIG ファイルをアップロードできます。

プロファイルに必要な設定（ ペイロード ）を含むファイルを取得しておきます。そのファイルでは、ファイル拡張子 MOBILECONFIG が使用されています。例えば、mail.mobileconfig です。Mac プロファイルの作成とそれらの Mac OS X サーバーからのダウンロードの詳細については、http://help.apple.com/profilemanager/mac/4.0を参照してください。

注: **管理者コンソール**にアップロードされたプロファイルのペイロードは、表示または編集できません。ただし、MOBILECONFIG ファイル内のペイロードを**管理者コンソール**の外部で変更し、編集済みのファイルを新しいプロファイルとしてアップロードできます。

1. Mac プロファイル リストページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
2. **アクションの選択 > プロファイルのアップロード** をクリックします。
3. **参照** または **ファイルの選択** をクリックし、MOBILECONFIG ファイルを見つけます。
4. **アップロード** をクリックします。

    プロファイルが Mac Profiles リストに表示されます。ソース 列は Imported（ インポート ）です。

プロファイルの展開およびスケジュールのオプションを選択します。詳細については、以下を参照してください。

- Mac ユーザープロファイルの追加または編集
- Mac システムプロファイルの追加または編集

Mac プロファイルのインストールおよび管理

Mac プロファイルのインストール、Mac プロファイルがインストールされているデバイスの表示、およびアプライアンスに追加されているプロファイルのリストのエクスポートを行うことができます。

スケジュールに基づく Mac プロファイルの配布

スケジュールに従ってエージェント管理対象 Mac OS X デバイスに Mac プロファイルを定期的に配布するように、アプライアンスを設定できます。この設定は、実行 オプションを選択したときにオフラインでインストールできない可能性があるデバイスがある場合や、インベントリに追加された新しいデバイスにプロファイルを定期的にインストールする場合に便利です。

Mac プロファイルを追加またはアップロードしておきます。エージェント管理対象 Mac OS X デバイスがインベントリ内にあります。

1. Mac Profile Detail（ Mac プロファイルの詳細 ）ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
    c. プロファイルの名前をクリックします。
2. スケジュール セクションで、プロファイルをターゲットデバイスに配布するためのオプションを選択します。

オプション	説明
なし	プロファイルをスケジュールに基づいて配布しません。スケジュールが **なし** に設定されたプロファイルは、Mac Profiles リストでステータスは **無効** です。ただし、スケジュールが **なし** に設定されたプロファイルも、ページの一番下で **今すぐ実行** を選択した場合は展開できます。

オプション	説明
n 分 / 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。

3. **保存** をクリックします。

   Mac Profiles ページが表示されます。Targeted（ターゲット）列に、プロファイルのインストールがスケジュールされたデバイスの数が表示されます。Succeeded（成功）列に、プロファイルがインストールさ

れたデバイスの数が表示されます。ターゲットデバイスのエージェントは、指定されたスケジュールと展開オプションに従って次の接続時にプロファイルをインストールする手順を受信します。

実行オプションを使用したデバイスへの Mac プロファイルのインストール

Mac プロファイルをアプライアンスに追加またはアップロードした後で、実行 オプションを使用して、それらのプロファイルをバージョン 10.8、10.9、または 10.10 を実行しているエージェント管理対象 Mac OS X デバイスにインストールできます。

Mac プロファイルを追加しておきます。エージェント管理対象 Mac OS X デバイスがインベントリ内にあります。

ヒント: 実行 オプションを使用して Mac プロファイルをデバイスにインストールする場合、プロファイルがインストールされるのは、スクリプトの実行時にアプライアンスへのエージェント接続がデバイスにある場合のみです。オフラインのデバイスにプロファイルがインストールされるようにするには、プロファイルを展開するスケジュールを設定することを検討してください。詳細については、「スケジュールに基づく Mac プロファイルの配布」を参照してください。

1. Mac Profile Detail（Mac プロファイルの詳細）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
    c. プロファイルの名前をクリックします。
2. プロファイルをさまざまなデバイスにインストールするには、ページの一番下にある **複製** をクリックしてプロファイルのコピーを作成し、複製されたプロファイルの名前をクリックして Mac Profile Detail（Mac プロファイルの詳細）ページに戻ります。
3. Mac Profile Detail（Mac プロファイルの詳細）ページで、ターゲットデバイスと展開オプションを選択します。詳細については、以下を参照してください。
    - Mac ユーザープロファイルの追加または編集
    - Mac システムプロファイルの追加または編集
4. ページの一番下で **今すぐ実行** をクリックします。

    Mac Profiles ページが表示されます。Targeted（ターゲット）列に、プロファイルのインストールがスケジュールされたデバイスの数が表示されます。Succeeded（成功）列に、プロファイルがインストールされたデバイスの数が表示されます。アプライアンスへのアクティブなエージェント接続があるターゲットデバイスで、選択した展開オプションに従ってプロファイルがインストールされます。
5. 複数のプロファイルを一度に実行するには、Mac Profiles ページでプロファイルの隣のチェックボックスをオンにして、**アクションの選択 > 実行** をクリックします。
6. プロファイルのインストールの詳細を表示するには、左側のナビゲーションバーで **今すぐ実行のステータス** をクリックします。

Mac プロファイルがインストールされているデバイスの識別

デバイスの詳細ページにはデバイスにインストールされている Mac プロファイルが表示され、Mac プロファイルの詳細ページには Mac プロファイルがインストールされているデバイスが表示されます。

1. Mac Profile Detail（Mac プロファイルの詳細）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。

c. プロファイルの名前をクリックします。

2. ページの一番下の Results（結果）セクションまでスクロールします。

   この表には、プロファイルがインストールされているデバイスが表示されます。Installed（インストール）列は、プロファイルがデバイスにインストールされた日付を示します。前回更新日 列は、プロファイルがデバイスにインストールされたことを KACE エージェントが検出した最新の日付を示します。

3. デバイスの詳細 ページに移動します。
   a. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
   b. デバイスの名前をクリックします。

4. Mac Profiles セクションまでスクロールします。

   この表には、デバイスにインストールされているすべてのプロファイルが表示されます。Installed（インストール）列は、プロファイルがデバイスにインストールされた日付を示します。前回更新日 列は、プロファイルがデバイスにインストールされたことを KACE エージェントが検出した最新の日付を示します。

Mac プロファイルの表示

特定基準で表示 リストを使用して、Mac プロファイルをソース、アクション、およびスコープで並べ替えることができます

Mac プロファイルをアプライアンスに追加またはアップロードしておきます。

1. Mac Profiles リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。

2. 右側の表の上部に表示される 特定基準で表示 ドロップダウンリストで、次のいずれかを選択します。

オプション	説明
すべてのアイテム	プロファイルの完全なリストを表示します。
ソース	選択したソースと一致するプロファイルのみを表示します。 • **インポート済み**：アプライアンスにアップロードされているプロファイル。 • **Configured**（設定済み）：**管理者コンソール**を使用してペイロードが設定されたプロファイル。
アクション	選択したアクションと一致するプロファイルのみを表示します。 • **追加**：設定をターゲットデバイスにインストールするように設定されているプロファイル。 • **削除**：設定をターゲットデバイスから除去するように設定されているプロファイル。

オプション	説明
Scope (スコープ)	選択したスコープと一致するプロファイルのみを表示します。 • **システム**：システム設定 (パスコード設定など) を設定するプロファイル。 • **ユーザー**: ユーザー設定 (E メールアカウント設定など) を設定するプロファイル。
ステータス	選択したステータスと一致するプロファイルのみを表示します。 • **アクティブ**：スケジュールに従って実行するように設定されているプロファイル。 • **無効**: スケジュールが **なし** に設定されているプロファイル。

Mac プロファイルリストのエクスポート

Mac Profiles リストに表示されるプロファイルのリストを、CSV (コンマで区切られた値)、Excel、または TSV (タブで区切られた値) 形式にエクスポートできます。

Mac プロファイルを作成またはアップロードしておきます。

1. Mac Profiles リストに移動します。
    a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
2. **オプション**：選択したプロファイルをエクスポートするには、エクスポートするプロファイルの隣のチェックボックスをオンにします。
3. 次のいずれかを実行します。
    - **リストのすべてのプロファイルをエクスポートするには、アクションの選択 > エクスポート > フォーマット名にすべてエクスポート をクリックします。**
    - **選択したプロファイルのみをエクスポートするには、アクションの選択 > フォーマット名に選択したものをエクスポート をクリックします。**

Mac プロファイルの除去および削除

アプライアンスを使用して Mac プロファイルを管理対象デバイスから除去でき、Mac プロファイルをアプライアンスから削除できます。

管理対象デバイスからの Mac プロファイルの除去

ユーザープロファイルおよびシステムプロファイルを管理対象 Mac OS X デバイスから除去するように Mac プロファイルを設定できます。この設定は、プロファイルを多数のデバイスにインストールしており、そのプロファイルをそれらのデバイスすべて、またはそれらのデバイスのサブセットから除去する必要がある場合に便利です。

アプライアンスを使用してプロファイルを管理対象デバイスにインストールしてあり、元の Mac プロファイルはアプライアンスから削除されていません。

重要: **プロファイルをアプライアンスから削除した場合、アプライアンスを使用してそのプロファイルを管理対象デバイスから除去できなくなります。**

1. Mac Profile Detail（Mac プロファイルの詳細）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
   c. プロファイルの名前をクリックします。
2. ページの一番下で **削除** をクリックします。

   除去プロセスを説明するダイアログボックスが表示されます。
3. **デバイスから削除** をクリックします。

   新しいプロファイルの Mac Profile Detail（Mac プロファイルの詳細）ページが表示され、Action（アクション）は 削除 に設定されています。新しいプロファイルは、元のプロファイルと同じ Profile Name（プロファイル名）および Profile Identifier（プロファイル識別子）を持ちます。Action（アクション）が 追加 に設定された元のプロファイルは、その スケジュール が なし に設定されてリストに残ります。これにより、同じプロファイルが同じデバイスに対してインストールまたは除去されないようになり、必要に応じて後で元のプロファイルを再アクティブ化できます。
4. Mac Profile Detail（Mac プロファイルの詳細）ページの 展開 セクションで、プロファイルを除去するデバイスを選択します。

オプション	説明
全デバイス	Mac OS X のサポート対象バージョン（バージョン 10.8、10.9、または 10.10）を実行しているすべての KACE エージェント管理対象デバイスからプロファイルを除去します。アプライアンスで組織コンポーネントが有効になっている場合、選択した組織のすべてのサポート対象 Mac デバイスがこのアクションに含まれます。
ラベル	選択したラベル内のデバイスからプロファイルを除去します。ラベル、特に Smart Label に除去を制限すると、プロファイルを適切に除去するのに役立ちます。 このオプションを使用するには、予めラベルまたは Smart Labelを作成しておく必要があります。詳細については、「デバイスに対するSmart Labelの追加」を参照してください。
デバイス	選択したサポート対象 Mac OS X デバイス（バージョン 10.8、10.9、または 10.10）からプロファイルを除去します。デバイスを検索するには、フィールドに入力し始めます。
オペレーティングシステム	プロファイルを除去するデバイスのオペレーティングシステムを選択します。サポート対象オペレーティングシステム（Mac OS X バージョン 10.8、10.9、または 10.10）のみが表示されます。すべてのサポート対象 Mac オペレーティングシステムからプロファイルを除去するには、オペレーティングシステムをすべて選択しないでおきます。

オプション	説明
すべて削除	選択されているすべてのデバイスをこのセクションの デバイス リストから除去します。

5. スケジュール セクションで、プロファイルをターゲットデバイスから除去するためのオプションを選択します。

オプション	説明
なし	プロファイルをスケジュールに基づいて除去しません。スケジュールが **なし** に設定されたプロファイルは、Mac Profiles リストでステータスは **無効** です。ただし、スケジュールが なし に設定されたプロファイルも、ページの一番下で **今すぐ実行** を選択した場合は除去できます。
n 分 / 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。

オプション	説明
	例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。

6. ページの一番下で、次のいずれかのアクションを選択します。

オプション	説明
保存	プロファイルを保存して Mac Profiles リストに戻ります。
今すぐ実行	アプライアンスへのアクティブなエージェント接続があるターゲットデバイスで、選択した展開オプションに従ってプロファイルをすぐに除去します。詳細については、「実行 および 今すぐ実行 コマンドの使用」を参照してください。
複製	プロファイル名の前に Copy of を付加してプロファイルのコピーを作成します。
削除	アプライアンスからプロファイルを除去します。このアクションによって、プロファイルがインストールされているデバイスからプロファイルは除去されません。詳細については、「アプライアンスからの Mac プロファイルの削除」を参照してください。
キャンセル	変更を破棄して Mac Profiles リストに戻ります。

Mac Profiles ページが表示されます。Targeted (ターゲット) 列に、プロファイルの除去がスケジュールされたデバイスの数が表示されます。Succeeded (成功) 列に、プロファイルが除去されたデバイスの数が表示されます。アプライアンスへのアクティブなエージェント接続があるターゲットデバイスで、選択したオプションに従ってプロファイルが除去されます。

例：指定したデバイスに展開されているプロファイルの除去

プロファイルをターゲットデバイスに誤ってインストールした場合、削除 プロファイルを作成することで、それらを除去できます。

1. 次のスケジュールおよび展開オプションで Mac システムプロファイルを作成しました。
   - 毎日午前 8 時にインストールされるようにスケジュール。
   - 100 台のターゲットデバイスにインストール (インストールされるようにスケジュール) 。
2. プロファイルの作成後に、100 台のうち 10 台のターゲットデバイスにはプロファイルをインストールする必要がないことがわかります。10 台のデバイスからプロファイルを除去し、残りの 90 台のデバイスでは引き続きプロファイルを使用可能にしておく必要があります。

注: この例では Mac システムプロファイルを使用しますが、必要に応じて Mac システムプロファイルと Mac ユーザープロファイルの両方を除去できます。

1. Mac Profile Detail（Mac プロファイルの詳細）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
    c. プロファイルの名前をクリックします。この例では、このプロファイルを **Profile A** と呼びます。
2. **Profile A** の Mac Profile Detail（Mac プロファイルの詳細）ページで、**削除** をクリックします。

    除去プロセスを説明するダイアログボックスが表示されます。
3. **デバイスから削除** をクリックします。

    新しいプロファイルの Mac Profile Detail（Mac プロファイルの詳細）ページが表示され、Action（アクション）は 削除 に設定されています。新しいプロファイルは、元のプロファイルと同じ Profile Name（プロファイル名）および Profile Identifier（プロファイル識別子）を持ちます。この例では、これは **Profile A Remove** です。Action（アクション）が 追加 に設定された元のプロファイルは、その スケジュール が なし に設定されてリストに残ります。これにより、同じプロファイルが同じデバイスに対してインストールまたは除去されないようになり、必要に応じて後で **Profile A** を再アクティブ化できます。
4. **Profile A Remove** の Mac Profile Detail（Mac プロファイルの詳細）ページの 展開 セクションで、プロファイルを除去するデバイスを選択します。
5. 次のいずれかを実行します。
    - スケジュールに従って実行するようにプロファイルを設定した場合は、ページの一番下で **保存** をクリックします。
    - 現在アプライアンスに接続されているデバイスでプロファイルを実行するには、**今すぐ実行** をクリックします。

    Mac Profiles ページでは、ターゲットデバイスの数が Targeted（ターゲット）列に、プロファイルが除去されたデバイスの数が **Profile A Remove** の Succeeded（成功）列に表示されます。
6. プロファイルがすべてのターゲットデバイスから除去されたことが Succeeded（成功）列で示されている場合、**Profile A Remove** は必要なくなったため、アプライアンスから削除できます。詳細については、「アプライアンスからの Mac プロファイルの削除」を参照してください。
7. **Profile A** で、正しいデバイスが対象になっていることを確認し、プロファイルを有効にします。
    a. **Profile A** の Mac Profile Detail（Mac プロファイルの詳細）ページに移動します。
    b. ターゲットデバイスのリストを、正しい 90 台のデバイスのみが含まれるように変更します。
    c. プロファイルを有効にします。詳細については、以下を参照してください。
    - Mac ユーザープロファイルの追加または編集
    - Mac システムプロファイルの追加または編集

アプライアンスからの Mac プロファイルの削除

必要に応じて、アプライアンスから Mac プロファイルを削除できます。

プロファイルを削除しても、プロファイルがインストールされているデバイスからは除去されません。プロファイルをデバイスからは除去するには、**削除** オプションを使用します。詳細については、「管理対象デバイスからの Mac プロファイルの除去」を参照してください。

注: プロファイルをアプライアンスから削除した場合、アプライアンスを使用してそのプロファイルを管理対象デバイスから除去できなくなります。

1. Mac Profile Detail（Mac プロファイルの詳細）ページに移動します。

a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左側のナビゲーションバーで、**スクリプト** をクリックして、**Mac Profiles** をクリックします。
c. プロファイルの名前をクリックします。

2. ページの一番下で **削除** をクリックします。

   ダイアログが表示されます。

3. プロファイルをアプライアンスから削除することを確認したら、**Delete Profile** をクリックします。

   プロファイルはアプライアンスから除去され、Mac Profiles リストに表示されなくなります。ただし、プロファイル識別子はプロファイルがインストールされているデバイスの デバイスの詳細 ページに引き続き表示されます。

タスクチェーンの使用

タスクチェーンを使用すると、特定の順序で実行する一連のタスクを作成できます。

1 つまたは複数のパッチスケジュール、スクリプト、ファイル同期アイテム、および Wake On LAN 要求をタスクチェーンに追加できます。例えば、管理対象インストールを展開してから、ターゲットデバイス上でスクリプトを実行する必要がある場合に、タスクチェーンを使用します。タスクチェーンでのタスクの順序は、必要に応じて簡単に変更できます。

注: タスクチェーンに個別の管理対象インストールを追加することはできません。

各タスクチェーンは、タスクチェーンで定義されているように、設定されたデバイスセットに対して実行されます。

タスクチェーン内のターゲットデバイスがオフラインになっている場合は、そのデバイスが接続状態になると実行するようにタスクチェーンを設定することができます。ターゲットデバイスが複数のタスクチェーンで参照される場合、一度に 1 つのタスクチェーンのみがデバイスに対して実行されます。

次の概念が、タスクチェーンでのデバイスの選択に適用されます。

- タスクチェーンで選択されたデバイスは、タスクチェーンの一部として実行されるときに、パッチスケジュールとスクリプト用の設定を上書きします。
- タスクチェーンで選択されているデバイスは、そのデバイスに関連付けられている管理対象インストール（ MI ）またはファイル同期（ FS ）アイテムには影響しません。すべてのインベントリ、MI、および FS タスクは、タスクチェーンの各デバイスのキューに入れられ、各マシンで実行するように設定されている MI および FS は展開されます。
- Wake On LAN（ WoL ）スケジュールは、タスクチェーンの最初のデバイスが WoL タスクを検出したときに、タスクチェーンごとに 1 回実行されます。WoL タスクは、タスクチェーンで選択したデバイスに対して実行されます。

  注: WoL タスクは、常にタスクチェーンの最初のタスクとしてスケジュールされている必要があります。これにより、WoL パケットが一度にすべてのデバイスにプッシュされ、デバイスは、このタスクが最初のタスクであるため、これを待機します。WoL タスクがタスクチェーンの最初のタスクではない場合、WoL パケットは、タスクチェーンで実行しているタスクの現在の状態に関係なく、一度にすべてのデバイスにプッシュされます。

タスクチェーンの追加と編集

タスクチェーンは、特定の順序で実行できる一連のタスクです。タスクチェーンの詳細 ページを使用して、タスクチェーンを追加および編集します。

1. タスクチェーン リストページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**配布** をクリックして、**タスクチェーン** をクリックします。
2. 次のいずれかを実行します。
    - **アクションの選択 > 新規作成** を選択します。
    - タスクチェーンの名前をクリックします。
3. 設定 セクションで、次のオプションを指定します。

オプション	説明
名前	タスクチェーンの名前。
有効	このチェックボックスをオンにすると、このタスクチェーンを実行できます。
説明	タスクチェーンの簡単な説明。

4. そのまま　設定　セクションで、タスクチェーンを実行するデバイスを指定します。
    - **ラベルに属するデバイスを選択するには、設定 セクションの ラベル の下で 関連づけられたラベルの管理 をクリックします。表示される ラベルを選択 ダイアログボックスで、選択するデバイスに関連付けられている 1 つまたは複数のラベルを選択します。ダイアログボックスを閉じます。**
    - **オペレーティングシステムでデバイスを選択するには オペレーティングシステムの管理 をクリックします。表示される オペレーティングシステム ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。**

      ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**すべて > Windows > Windows 10** の順に選択し、**x64** を選択します。
5. スケジュール セクションで、次のスケジュール設定を指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。

オプション	説明
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（,）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（-）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（/）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（*）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

6. タスク セクションで、1 つまたは複数のタスクを追加します。

a. **新しいタスク** をクリックしてタスクを追加します。
b. 表示される 新しいタスク 領域で、**タスクタイプ** をクリックし、必要に応じて、使用可能なタイプから選択します。

タスクのタイプの一部：

- **失敗時に中止** オプションがあります。このオプションを選択すると、タスクチェーンが指定のマシンで失敗した場合に、そのマシンでの実行を停止します。
- Wake On LAN、スクリプト、パッチスケジュールなど、特定のユーザー定義タスクを選択できます。
- 管理対象インストール（MI）タスクやファイル同期（FS）タスクなど、マシン上で適用可能なすべてのタスクを実行します。

また、特定のタスクタイプでは、特定のユーザー定義タスクを選択できます。管理対象インストール（MI）タスクやファイル同期（FS）タスクなどのその他のタスクタイプは、適用可能なすべての MI および FS タスクをマシン上で実行します。

選択したタスクが タスク セクションに表示されます。

7. タスクチェーン内のタスクの順序を変更するには、タスク領域の右上隅で ☰ をクリックし、シーケンス内の目的の場所にタスクをドラッグアンドドロップします。
8. タスクチェーンからタスクを削除するには、タスク領域の右下隅で 🗑 をクリックします。
9. **保存** をクリックします。

タスクチェーンを実行するには、タスクチェーン リストページでタスクチェーンを選択し、**アクションの選択 > 実行** の順にクリックします。

デバイスのパッチ適用とセキュリティの維持

アプライアンスでは管理対象デバイスにパッチを適用して、ソフトウェアの機能を向上させ、デバイスとネットワークの脆弱性を保護することができます。

セキュリティダッシュボードの使用

セキュリティダッシュボードには、選択した組織（該当する場合）またはアプライアンスのパッチ適用プロセスの概要が表示されます。

アプライアンスで組織コンポーネントが有効化されており、管理者コンソール（http://**appliance_hostname**/admin）に口グインしている場合は、セキュリティダッシュボードに選択した組織の情報が表示されます。

ユーザーアカウントに関連付けられた 1 つまたは複数の役割によってこのダッシュボードへのアクセス権が与えられている場合は、セキュリティダッシュボードにアクセスできます。非表示にする場合は、必要に応じて、ユーザーの役割を編集します。詳細については、「ユーザーの役割の追加または編集」を参照してください。

ヒント: アプライアンスは、概要ウィジェットを定期的に更新します。任意の時間にほとんどのウィジェットを更新するには、ページの右上にある **更新** ボタンをクリックします：。ほとんどのウィジェットを個々に更新するには、ウィジェットの上にマウスを置き、ウィジェットの上の **更新** ボタンをクリックします。一部のウィジェットでは、追加の手順が必要になる場合があります。

セキュリティダッシュボードウィジェットについて

セキュリティダッシュボード ウィジェットには、管理対象デバイスのパッチコンプライアンス全体に関する情報が含まれています。

このセクションでは、セキュリティダッシュボードで使用可能なウィジェットについて説明します。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには管理者レベルで選択した組織の情報が表示されます。

このダッシュボードには、環境内のパッチコンプライアンスの概要と、パッチプロセスに関する情報が表示されます。管理対象デバイスにインストールされたシステムパッチのレベルをすばやく確認し、システムセキュリティを改善するためのインジケータを探すために使用します。たとえば、デバイスのパッチコンプライアンスに重点を置き、パッチスケジュールを確認して、管理対象デバイスに最新のシステムアップデートがインストールされ、実行されていることを確認できます。

ウィジェット	説明
緊急のパッチのコンプライアンス	このウィジェットには、「緊急」とマーク付けされたパッチの適用状況が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。

ウィジェット	説明
Dellアップデート	このウィジェットは、管理対象デバイスに適用可能なDellアプリケーション、BIOS、およびファームウェアのアップデートを表示します。これらのアップデートは、その緊急度に応じて、中、重要、重大として分類されます。Dellアップデートスケジュールを作成すると、データがウィジェットに表示されます。詳細については、「Dell アップデートスケジュールの設定」を参照してください。 アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
マシン別のコンプライアンス	このウィジェットにはドーナツグラフが表示され、グラフのそれぞれの部分は各管理対象デバイスのパッチのコンプライアンスの割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択したデバイスのパッチのコンプライアンスの割合が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
パッチ別のコンプライアンス	このウィジェットにはドーナツグラフが表示され、グラフのそれぞれの部分は該当する各パッチのコンプライアンスの割合を表します。グラフのそれぞれの部分にカーソルを置くと、選択したパッチのコンプライアンスの割合が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
パッチインストールの進行状況	このウィジェットには、管理対象デバイスで現在実行中のパッチタスクの進行状況が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
パッチが展開されました	このウィジェットには、現在展開されているパッチの数が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィ

ウィジェット	説明
	ジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
パッチが失敗しました	このウィジェットには、展開に失敗したパッチの数が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
パッチリリース済み	このウィジェットには、リリースされ、展開可能なパッチの数が表示されます。 パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択して、ウィジェットに表示される情報を変更できます。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。インスタンスごとに異なるパラメータセットを使用して、このウィジェットの複数のインスタンスをセキュリティダッシュボードにインストールすることもできます。
完了したパッチ適用タスク	このウィジェットには、管理対象デバイスでのパッチ適用タスク（タスクの検出、展開、およびロールバックなど）の進行状況が表示されます。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
レポート	このウィジェットには、一般的なパッチ適用レポートへのリンクがあります。これらを使用して、緊急および最新の通知リスト、パッチ未対応のデバイスなどの特定のレポートをすばやく生成します。
SCAPの概要	このウィジェットは、デバイスで実行されたSCAPスキャンに関する情報を提供します。アプライアンスで組織コンポーネントが有効になっている場合、ウィジェットには選択した組織の情報が表示されます。
ビュー	このウィジェットには、作成したすべてのカスタムビューを含む、一般的なパッチ適用のページとウィザードへのリンクが含まれています。パッチカタログ などの特定のページにすばやく移動するために使用します。カスタムビューがある場合は、それらはアルファベット順にソートされます。カスタムビューを特定の順序で表示する場合は、必要に応じて名前の前に数字を付けることができます。
Windows 10 リリース	このウィジェットには棒グラフが表示され、チャート内の各項目は特定の Windows 10 リリースとそのバージョンを実行している管理対象デバイスの数を

ウィジェット	説明
	表します。これにより、公開されている Windows 10 更新プログラムの対象となるデバイスの数を把握できます。

セキュリティダッシュボードのカスタマイズ

インベントリダッシュボードをカスタマイズして、必要に応じて、ウィジェットを表示または非表示にできます。

1. インベントリダッシュボードに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**ダッシュボード** をクリックします。
2. ウィジェットの上にマウスを置き、次のボタンのいずれかを使用します。
    - : ウィジェットの情報を更新します。
    - : ウィジェットに関する情報を表示します。
    - : ウィジェットを非表示にします。
    - : ウィジェットのサイズを変更します。
    - : ウィジェットをページ上の別の場所にドラッグできます。
3. 一部のウィジェットは編集可能で、表示する情報をフィルタリングできます。編集可能なウィジェットを編集するには、 をクリックし、表示されるダイアログボックスで、パッチ発行者、オペレーティングシステム、ラベル、分類、重大度、KB 番号と利用可能日を選択します。必要に応じて、棒グラフとドーナツグラフの表示を切り替えることもできます。
4. ページの右上隅にある **カスタマイズ** ボタンをクリックすると、使用可能なウィジェットが表示されます。
5. 現在非表示のウィジェットを表示するには、**インストール** をクリックします。

パッチ管理について

パッチ管理は、デバイス上のソフトウェアのパッチを取得、テスト、およびインストールするプロセスです。アプライアンスではパッチ管理を自動化でき、これにより、ソフトウェアの機能を向上させ、デバイスとネットワークの脆弱性を保護することができます。

パッチ管理を使用すると、最新のセキュリティパッチおよびソフトウェアの更新を検出し、アプライアンスを使用する Windows および Mac デバイスに展開できます。

注: パッチ管理コンポーネントは、WindowsおよびMacデバイスでのみサポートされます。パッチ管理はLinuxデバイスに使用できません。

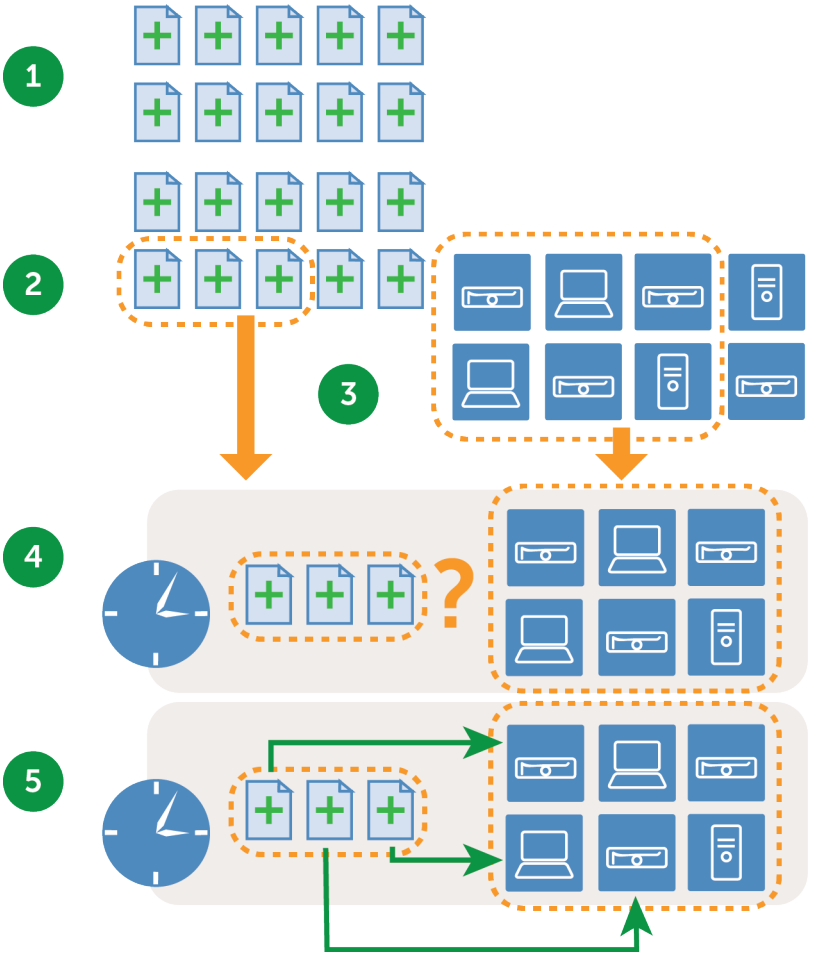
パッチ適用ワークフロー

パッチ適用ワークフローには、パッチのサブスクライブ、パッチダウンロード設定の選択、ラベルを使用したパッチおよびパッチの適用先デバイスの識別、およびパッチ適用ジョブのスケジュール設定があります。

パッチ適用ワークフローは次のタスクで構成されます。

- ダウンロードするパッチをサブスクライブします。アプライアンス上に組織コンポーネントがインストールされている場合は、各組織のサブスクリプション設定を個別に設定します。追加のワークフローの詳細が、初回パッチサブスクリプションのために用意されています。詳細については、「パッチのサブスクライブとダウンロード設定項目の設定」を参照してください。
- パッチのサブスクリプション設定 ページで、パッチダウンロード設定を選択します。詳細については、「パッチおよび機能更新プログラムのダウンロード設定の選択」を参照してください。
- Smart Labelを作成し、パッチを適用するデバイスおよび展開するパッチをグループ化します。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
- パッチスケジュールを作成し、検出して展開するパッケージを選択します。アプライアンス上に組織コンポーネントがインストールされている場合は、各組織のパッチスケジュールを個別に設定します。詳細については、「パッチスケジュールの設定」を参照してください。

パッチ適用ワークフロー



凡例の番号	アクション
1	サブスクライブしているパッチの署名ファイルがQuest からアプライアンスにダウンロードされます。パッチパッケージは Quest およびソフトウェアベンダーからダウンロードされます。
2	Smart Labelにより、ダウンロードされたパッチがグループ化されます。
3	Smart Labelにより、パッチを適用するデバイスが選択されます。
4	スケジュールに従って、デバイスに必要なパッチが検出されます。
5	スケジュールに従って、デバイスにパッチが展開されます。

パッチ署名ファイルについて

パッチ署名ファイルには、セキュリティ通知およびパッチを定義する他のファイルが含まれています。パッチ署名ファイルには、パッチのインストールに使用するパッチパッケージは含まれていません。

パッチ署名ファイルは、選択したサブスクリプションオプションおよびダウンロードオプションに従って Quest からダウンロードされます。パッチ署名ファイルのダウンロードの詳細については、パッチおよび機能更新プログラムのダウンロード設定の選択を参照してください。

パッチパッケージについて

パッチパッケージは、パッチのインストールに必要なファイルです。

パッチパッケージは、選択したサブスクリプションオプションおよびダウンロードオプションに従って Quest からダウンロードされます。また、パッチパッケージは、MicrosoftおよびAdobeなどのベンダーから直接ダウンロードされる場合もあります。

パッチパッケージをダウンロードするオプションには、次の2つがあります。

- **必要なパッチのみダウンロード**: 管理対象デバイスに必要であると検出されたパッケージのみダウンロードするよう選択できます。この方法でダウンロードすると、ダウンロード時間とディスク領域が削減されます。さらに、検出結果でパッチが不要であると示された場合に、指定した時間を経過したらパッチを自動的に削除するよう選択できます。
- **パッチの完全キャッシュを保持**: 管理対象デバイスでパッケージが必要かどうかに関係なく、パッケージの完全キャッシュを保持するよう選択できます。この方法では、迅速に展開できるようパッケージを使用可能な状態に保持しますが、必要なパッケージのみをダウンロードする場合と比べてより多くのダウンロード時間とディスク領域を必要とします。

パッケージのダウンロードオプションの詳細については、パッチおよび機能更新プログラムのダウンロード設定の選択を参照してください。

パッチテストおよびセキュリティについて

Quest では、Windows および Mac オペレーティングシステム、および多くの一般的なアプリケーションに対して、安全でタイムリーかつ高品質なパッチ署名を提供しています。

パッチ署名がアプライアンスに対して使用可能となる前に、Quest では次のセキュリティチェックを実施します。

- 各コンテンツ開発チームによって作成されたパッチメタデータの確認
- パッチのインストールおよびアンインストールプロセスの検証
- 対象とするオペレーティングシステムおよびアプリケーションの動作がパッチ適用後に不安定にならないことについての確認

パッチテスト環境について

Quest では、VMware?? ESX??、VMware?? vCenter???、Microsoft?? Azure??、およびカスタムハードウェアベンチテストを使用します。

テスト方法には、パッチ命名規則が Quest ポリシーに準拠していることについての検証が含まれます。

評価テストについて

評価テストでは、パッチ管理コンポーネントが正しく機能していることを確認します。

テストでは次の点が確認されます。

- 適用可能でパッチ未適用のデバイスが、適用可能およびパッチ未適用と表示される。
- パッチ適用済みのデバイスが、インストール済みおよび適用対象外として表示される。
- デジタル指紋の検出で偽陽性がない。
- パッチコンテンツが必須のベースラインに準拠している。
- 脆弱性がUpdate Serverで正しく表示される。
- すべてのSmart Label、並べ替え、およびその他の視覚的な機能がすべて正しく機能する。

展開テストについて

展開テストでは、パッチが適切に展開されていることを確認します。

テストでは次の点が確認されます。

- パッケージが展開可能である。
- 再起動禁止機能が機能する。
- アンインストール機能が機能する。
- オンデマンドパッケージキャッシュが機能する。
- 自動展開スケジュールが機能する。
- エージェントパッケージダウンロードが機能する。
- SHA1 チェックサムによりパッケージの完全性が確保される。
- エージェントによってパッチ導入後に自動的に評価が実行される。
- 再起動後にエージェントが自動的に再起動する。

パッチ品質保証プロセスについて

Quest は、コンテンツ開発および品質保証プロセスを通じて、パッチ管理カスタマにさらに多くの価値を提供します。品質保証チームは、パッチのインストールおよびアンインストールプロセスに加えて、コンテンツ開発チームが生み出したパッチメタデータも検証します。カスタマに高品質なコンテンツを提供することが高優先です。コンテンツ配信の成功を確保するために、Quest は以下のテストコンポーネントを対象にテストを実施します。

テスト環境

Quest は、テストインフラストラクチャに巨額の投資を行っています。コンテンツ開発および品質保証チームは、さまざまな設定のノードを想定して作成された、仮想エンタープライズ環境にアクセスできます。Quest では、テストインフラストラクチャが最先端であるように、カスタム物理ベンチテストに加え、仮想デスクトップおよびサーバーを組み合わせて使用しています。

アプリケーションテスト

パッチの要件が確実に満たされるように、Quest では、必要に応じてさまざまなアプリケーションに対してテストします。

テスト方法

Quest は以下のタイプのテストを使用します。

- **一般的なテスト** では、以下を検証します。
  - パッチ命名規則は、Quest ポリシーに準拠している。
- **評価テスト** では、以下を検証します。
  - 適用可能でパッチ未適用のシステムが、適用可能およびパッチ未適用と表示される。
  - パッチ適用済みのデバイスが、インストール済みおよび適用対象外として表示される。
  - デジタル指紋の検出での偽陽性。
  - コンテンツが必須のベースラインに準拠している。
  - パッチが、すべてのフィルタリング、並べ替えおよびその他の視覚的機能を含め、パッチサーバーで正しく表示される。
- **展開テスト** では、以下を検証します。
  - パッケージが正常に展開される。
  - 再起動禁止機能が正しく機能する。
  - アンインストール機能が正しく機能する。
  - オンデマンドパッケージキャッシュが正しく機能する。
  - 自動展開スケジュールが正しく機能する。
  - エージェントパッケージがダウンロードできる。
  - パッケージハッシュによりパッケージの完全性が確保される。
  - エージェントによって各パッチ展開後に自動的に評価が実行される。
  - 再起動後にエージェントが自動的に再起動する。

信頼済みの配信および柔軟性

Quest プロセスは、安全なコンテンツ配布ネットワークによるグローバルな可用性を最大化するように設計および実装されます。Quest によるすべての通信は、セキュリティコンテンツの整合性を確保するために、暗号化された、安全なチャネルで実行されます。

ベストプラクティスのアプローチを使用して、重要なセキュリティパッチは、サブスクリプションオプションに基づいて、自動的にカスタマの場所にダウンロードされます。追加のセキュリティパッチを必要に応じてダウンロードして、カスタマ独自の安全なエンタープライズ環境内にカスタマイザされたバージョンのKACEパッチコンテンツリポジトリを作成できます。

パッチ適用に関するベストプラクティス

デバイスへのパッチ適用に関するベストプラクティスには、パッチ適用のテスト、ラベルを使用したデバイスおよびパッチの整理、システムに対するパッチ適用時のユーザーへの通知などがあります。

- **展開前のパッチのテスト**

  パッチをすべてのデバイスに展開する前に、選択したデバイスでそれらのパッチをテストします。このテストにより、パッチが広く展開される前に、パッチによって壊されるものがないことを確認できます。

  テストデバイスを選択するときには、次の特性を備えたデバイスを選択します。

  - 高い技術知識を持ち、問題について効果的に報告できるユーザーが所有するデバイス
  - 作業環境を反映したシステムおよびソフトウェアにアクセス可能なデバイス

  綿密なテストを実施するために、デバイスはパッチ適用後、最低1週間は正常に動作する必要があります。1週間後、問題が報告されなければ、ネットワーク上の残りのデバイスにパッチを展開できます。

- **ラベルを使用したデバイスおよびパッチの整理**

  Smart Labelを使用して、ノートPC、デスクトップ、およびサーバーなどの種類別にデバイスを自動的にグループ化できます。さらに、Smart Labelでは、緊急のオペレーティングシステムパッチおよび他のアプリケーション向けの優先度の低いパッチなど、重要度別にパッチを自動的にグループ化できます。その後、各種類のデバイスおよびパッチに合ったパッチスケジュールを作成できます。

  詳細については、以下を参照してください。

  - パッチ適用に対する Smart Label の使用
  - パッチスケジュールの作成および管理

- **Windows Update またはアプライアンスを使用した Windows デバイスへのパッチ適用**

  Windowsデバイスにパッチを適用するオプションには、次の2つがあります。

  - **Windows Updateを使用**: Windows Updateは、Microsoftが提供する機能で、Windowsオペレーティングシステムに対して更新をダウンロードしてインストールします。管理対象デバイスで Windows Update を有効にする場合は、アプライアンスのパッチ管理は、Windows オペレーティングシステムパッチの検出にのみ使用し、パッチの展開には使用しません。パッチは、Windows Updateによって展開されます。
  - **アプライアンスの使用** : パッチ管理を使用して、Windows オペレーティングシステムのパッチをダウンロードして展開できます。アプライアンスでパッチ管理を使用する場合は、アプライアンスによってパッチが適用されるため、管理対象デバイスで Windows Update を無効にします。

    ヒント: アプライアンスでは、管理対象デバイスで Windows Update を使用するかどうかを指定するポリシーを作成できます。詳細については、「Windows設定ポリシーの使用」を参照してください。

- **パッチ適用時のダウンタイムの最小化**

  ダウンタイムを最小化するよう、デバイスの使用率が低い時間帯にパッチの展開をスケジュールします。デバイスの使用率は、デバイスの種類によって異なることに注意してください。

  - **サーバー**: よく知られた方法で慎重にアップグレードする必要があります。サーバーにパッチを適用する場合は、数週間前までに計画の立案が必要な場合があります。
  - **デスクトップ**: 使用されていないときでも電源がオンのままになっていることが多いため、パッチ適用はより柔軟に行えます。
  - **ノートPC**: 使用中にのみパッチ適用が可能であるため、パッチ適用は最も困難です。

各種類のデバイスに対してパッチスケジュールを作成する方法の詳細については、次を参照してください。

- デスクトップおよびサーバー用の緊急のOSパッチのスケジュールについて
- ノートPCに対する緊急のパッチのスケジュールについて

- **デバイスに対するパッチ適用時のユーザーへの通知**

  ユーザーが使用しているデバイスに対してパッチを適用中であることを、必ずユーザーに通知します。このことは、パッチ適用プロセスでデバイスの再起動が必要な場合に特に重要です。いくつかの方法でパッチスケジュールをユーザーに通知できます。

  - **Eメールを送信または他のメッセージシステムを使用**: アプライアンスの**管理者コンソール**以外で E メールおよび他のメッセージングシステムを使用して、事前にユーザーに通知します。この通知は、パッチ適用により一定の時間、サーバーなどの重要なシステムにアクセスできない可能性がある場合に役立ちます。
  - **アプライアンスから警告メッセージを送信**: アプライアンスの**管理者コンソール**を使用してアラートを作成し、すべてのデバイスまたは選択したデバイスにアラートをブロードキャストします。これらのブロードキャストを使用すると、ユーザーにパッチ適用が開始間近であることを通知できます。

    アラート作成の詳細については、管理対象デバイスへの警告のブロードキャストを参照してください。
  - **パッチ適用時にアラートを送信**: パッチ適用をスケジュールする場合、パッチ適用前にユーザーに警告し、デバイスを再起動する前にユーザーにプロンプトを表示するようにします。また、必要があればユーザーに再通知したり、または再起動を延期させたりすることもできます。詳細については、「パッチスケジュールの設定」を参照してください。

  さまざまなデバイスに対するパッチ適用のスケジュールの詳細については、次を参照してください。

  - デスクトップおよびサーバー用の緊急のOSパッチのスケジュールについて
  - ノートPCに対する緊急のパッチのスケジュールについて

- **ユーザーへの影響を低減するためのパッチ適用ジョブに対する期限の設定**

  パッチ適用ジョブは、多大な帯域幅とリソースを必要とする場合があります。ユーザーへの影響を低減するために、パッチ適用ジョブに対して期限を設定できます。例えば、パッチ適用ジョブを 04:00 に開始して、07:00 に停止するように設定できます。07:00 の時点で進行中のパッチ適用ジョブがあれば、それらのジョブは中断されます。ジョブは、次回のスケジュールされたパッチ適用ジョブを開始するときに中断した時点から再開されます。詳細については、「パッチスケジュールの設定」を参照してください。

- **レプリケーション共有を使用したネットワークリソースの最適化**

  レプリケーション共有を使用して、ネットワークリソースの要件とダウンロード時間を最適化します。レプリケーション共有とは、配布用にファイルのコピーを保持するデバイスであり、複数の地理的な場所に管理対象デバイスが導入されている場合に役立つ場合があります。例えば、レプリケーション共有を使用すると、ロサンゼルスにあるアプライアンスからニューヨークにあるデバイスにパッチファイルをダウンロードしなくても、ニューヨークの同じオフィスにある別のデバイスからファイルをダウンロードできます。

  レプリケーション共有の設定および使用の詳細については、レプリケーション共有の使用を参照してください。

- **Questサポート技術情報での情報の検索**

  Questサポートでは、アプライアンスについての記事を掲載したサポート技術情報を https://support.quest.com/kace-systems-management-appliance/kb にご用意しています。サポート技術情報は、管理者が経験した実際のアプライアンスに関する問題への解決策で、継続的に更新されています。パッチ適用に関する記事を表示するには、サポート技術情報にアクセスし、「Security」を検索します。

- **ITNinja.comを使用した他のITプロフェッショナルとの情報共有**

  Quest KACEがスポンサーとなっているITNinja.com（以前のAppDeploy.com）は、ITに焦点を絞った製品不問のコミュニティウェブサイトです。このサイトは、ITプロフェッショナルが、システム管理に関連す

る情報を共有したり、質問したりする主要なインターネットサイトになっています。詳細については、「http://itninja.com」を参照してください。

パッチのサブスクライブとダウンロード

パッチ適用を有効にするには、パッチをサブスクライブし、アプライアンスへのパッチダウンロードをスケジュールする必要があります。

パッチのサブスクリプションおよびダウンロードについて

パッチサブスクリプションは、パッチを受け取るオペレーティングシステムとアプリケーションを選択するプロセスです。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のサブスクリプション設定を個別に選択します。

パッチをサブスクライブすると、設定したスケジュールに従って、アプライアンスによりパッチがダウンロードされます。パッチがダウンロードされたら、テストして展開できます。パッチが自動的に展開されるようにもできますが、そのような展開はリスクが低いか所要時間が重要なパッチにのみお勧めします。詳細については、以下を参照してください。

- パッチおよび機能更新プログラムのダウンロード設定の選択
- パッチ適用に対する Smart Label の使用

アプライアンスでパッチを適用できるアプリケーション

アプライアンスでパッチを適用できるアプリケーションのリストについては、https://support.quest.com/kb/112030 にアクセスして添付ファイルを開いてください。

NTPサービスの要件

HTTPS を使用してパッチをダウンロードするときに、アプライアンスで NTP（ネットワークタイムプロトコル）サービスが実行されている必要があります。証明書の有効性を確保するために、セキュアプロトコルによってアプライアンスのその時点の日付スタンプが使用されるため、NTPサービスが必要です。NTPサービスが実行されていないと、証明書が無効であると示されて、パッチのダウンロードが失敗する場合があります。

アプライアンスからアクセスできる必要がある Web サイト

パッチのダウンロード、製品情報へのアクセス、および **Questサポート**との対話のためには、ファイアウォール、DNS サーバ、およびプロキシサーバの設定で、アプライアンスからポート 80 とポート 443 で特定のドメインへのアクセスを許可する必要があります。

アプライアンスからアクセスできる必要があるドメイン

ドメイン	用途
https://support.quest.com/download-product-select	Questアップデート
http://servicecdn.kace.com	SCAP（Secure Content Automation Protocol）

ドメイン	用途
https://service.kace.com	Quest からのアプライアンスおよびエージェントの更新
https://support.quest.com	Questサポート
http://cdn01.catalog.kace.com/	Quest アップデート
https://cdn01.catalog.kace.com/	Quest アップデート
https://quest.com/kace	ローカライズされたコンテンツ、サードパーティソフトウェアのライセンス、および製品情報
http://www.itninja.com	ITNinjaコミュニティ機能
http://appdeploy.com	ITNinja.comへのリダイレクト
http://download.windowsupdate.com	Microsoftアップデート
http://download.microsoft.com	Microsoftアップデート
http://www.microsoft.com/en-us/default.aspx	Microsoftアップデート
https://api.dell.com	Dellアップデート
http://ftp.dell.com	Dellアップデート
http://ardownload.adobe.com/	Adobe アプリケーションの更新
http://armdl.adobe.com/	Adobe アプリケーションの更新
https://airdownload.adobe.com/	Adobe アプリケーションの更新
https://fpdownload.macromedia.com/	Adobe アプリケーションの更新
http://swcdn.apple.com/	Apple アップデート
https://swdist.apple.com	Apple アップデート
http://download.winzip.com/	WinZip を含む Corel アップデート
https://download.winzip.com/	WinZip を含む Corel アップデート
https://download.virtualbox.org/	Java を含む Oracle アップデート
http://download.autodesk.com/	Autodesk アップデート
http://knowledge.autodesk.com/	Autodesk アップデート
http://revit.downloads.autodesk.com/	Autodesk アップデート

ドメイン	用途
http://trial2.autodesk.com/	Autodesk アップデート
http://up.autodesk.com/	Autodesk アップデート
https://knowledge.autodesk.com/	Autodesk アップデート
https://up.autodesk.com/	Autodesk アップデート
https://cdn.sw.altova.com/	Altova アップデート
http://download.imgburn.com/	ImgBurn の更新
https://www.realvnc.com/	RealVNC アップデート
https://www.uvnc.eu/	UltraVNC アップデート
https://download-installer.cdn.mozilla.net/	Mozilla Firefox の更新
https://www.python.org/	Python アップデート
https://the.earth.li/	Putty アップデート
http://cdn1.evernote.com/	EverNote アップデート
https://cdn1.evernote.com/	EverNote アップデート
http://cdn01.foxitsoftware.com/	Foxit アップデート
https://download.ccleaner.com/	Piriform アップデート
https://media.inkscape.org/	InkScape アップデート
https://download.cdburnerxp.se/	Canneverbe アップデート
http://download.videolan.org/	VideoLAN アップデート
https://www.tightvnc.com/	TightVNC アップデート
http://downloadarchive.documentfoundation.org/	LibreOffice アップデート
https://download.filezilla-project.org/	FileZilla アップデート
https://e3.boxcdn.net/	Box Inc. アップデート
http://www.rarlab.com/	WinRAR GmbH アップデート
https://www.rarlab.com/	WinRAR GmbH アップデート

ドメイン	用途
http://ftp.uni-kl.de/	Wireshark アップデート
https://www.wireshark.org/	Wireshark アップデート
https://notepad-plus-plus.org/	Notepad++ アップデート

初回パッチサブスクリプションのワークフローの概要

デフォルトでは、パッチ検出署名とパッチパッケージは、アプライアンスにダウンロードされません。必要なパッチをサブスクライブし、ダウンロードする時刻をスケジュールする必要があります。

ネットワーク帯域幅とディスク領域を節約するために、Questでは最初にパッチ定義の署名をダウンロードすることをお勧めしています。これは、パッチ定義の署名がパッチパッケージよりも大幅にサイズが小さいためです。その後、必要なパッチを検出し、ネットワークに最も適したダウンロード設定を選択できます。

次に、初回パッチサブスクリプションのワークフローを示します。

1. **情報の収集**: サブスクライブする必要がある項目を把握するために、管理対象デバイスにインストールされているオペレーティングシステム、言語パッケージ、およびアプリケーションを特定します。この情報は、アプライアンスの ダッシュボード ページで、またはレポートを実行することでも入手できます。詳細については、「オペレーティングシステムとアプリケーションに関する詳細の表示」を参照してください。
2. **初回パッチサブスクリプションの設定の選択**: 管理対象デバイスに必要なオペレーティングシステムおよび言語をサブスクライブします。詳細については、「パッチのサブスクライブとダウンロード設定項目の設定」を参照してください。
3. **パッチ検出署名のダウンロード**: パッチ検出署名は、素早くダウンロードができる、大量のディスク領域を必要としない比較的小規模なファイルです。サブスクライブするパッチのパッチ検出署名をダウンロードします。これらの署名をダウンロードすることにより、使用可能なパッチを表示し、後でダウンロードが必要なパッチパッケージを特定できます。詳細については、「パッチおよび機能更新プログラムのダウンロード設定の選択」を参照してください。
4. **検出のみのパッチ適用ジョブの実行**: 検出のみのパッチ適用ジョブをスケジュールし、管理対象デバイスに必要なパッチを特定します。検出のみのパッチ適用ジョブは1回限りのアクションで、最初のパッチ適用ジョブがどれくらいの規模になるかが示されます。また、デバイスの稼働率に基づき、どのようにパッチのインストールと再起動にリソースを割り当てるべきかを判断する材料となります。検出のみのパッチ適用ジョブを実行するには、すべてのデバイスでパッチが検出されるよう、パッチスケジュールを作成します。詳細については、「パッチスケジュールの設定」を参照してください。
5. **パッチパッケージのダウンロード設定の選択**: 必要なパッチパッケージを特定した後、パッケージのダウンロードを実行する日時を設定します。詳細については、「パッチおよび機能更新プログラムのダウンロード設定の選択」を参照してください。

オペレーティングシステムとアプリケーションに関する詳細の表示

概要の詳細 ページでは、管理対象デバイスにインストールされているオペレーティングシステムとアプリケーションに関する情報を表示できます。

パッチをサブスクライブする前に、必要なサブスクリプションを把握するために、管理対象デバイスにインストールされているオペレーティングシステム、言語パッケージ、およびソフトウェアの情報を収集します。

1. 次のいずれかを実行します。
   - **アプライアンスで組織コンポーネントが有効になっており、アプライアンスの情報を表示する場合は、システム管理コンソール（http://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されていない場合、または組織レベル情報を表示する場合は、管理者コンソール（http://appliance_hostname/admin）にログインします。または、**管理ヘッダーに組織メニューを表示 **オプションが有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。**
2. **ホーム** をクリックして、ダッシュボード ページを表示します。
3. ページの右上隅で **詳細の表示** をクリックします。

   ダッシュボードの詳細 ページが表示されます。デバイス セクションに、アプライアンスまたは選択した組織の管理対象デバイスのオペレーティングシステムが表示されます。
4. ソフトウェア セクションで、**ソフトウェアタイトル** をクリックします。

管理対象デバイスにインストールされているソフトウェアを表示するレポートが実行されます。詳細については、「レポートについて」を参照してください。

パッチのサブスクライブとダウンロード設定項目の設定

パッチ適用ワークフローを作成するには、パッチをサブスクライブし、パッチダウンロード設定項目を設定します。

パッチのサブスクライブ

管理対象デバイスのオペレーティングシステムとアプリケーションのパッチをサブスクライブできます。

パッチをサブスクライブしてダウンロードする前に、管理対象デバイスにインストールされているオペレーティングシステムおよびアプリケーションを特定し、パッチ適用が必要かどうかを確認します。詳細については、「オペレーティングシステムとアプリケーションに関する詳細の表示」を参照してください。

1. パッチのサブスクリプション設定 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
   c. パッチ管理 パネルで **サブスクリプション** をクリックします。
2. パッチステータス セクションでは、最新のパッチダウンロードとアプライアンスのディスク領域に関する詳細が提供されます。ここでは、新しくダウンロードされたパッチをデフォルトでアクティブとマークするか、非アクティブとマークするかを決定することもできます。

オプション	説明
新しいパッチをアクティブ化する	新しいパッチを「アクティブ」とマークします。この設定により、ダウンロードするたびに、サブスクリプション設定に一致するパッチが有効になります。このオプションが選択されていない場合は、新しいパッチが「非アクティブ」とマークされます。

オプション	説明
	この場合、パッチを展開する前にテストを実施できます。

3. 「サブスクリプション」設定を指定します。ダウンロードされるパッチは、サブスクリプションで指定されたオペレーティングシステムとロケールによって制御されます。

オプション	説明
Windowsオペレーティングシステム	選択されたWindowsオペレーティングシステムのパッチをダウンロードします。編集 ボタンをクリックして、オペレーティングシステムのリストを管理します: をクリックします。管理対象デバイスに基づいて Windows オペレーティングシステムを選択するには、**インベントリのすべてのWindows** を選択します。Windowsオペレーティングシステムのパッチを無視するには、**無効** を選択します。または、1または複数のWindowsオペレーティングシステムの横にあるチェックボックスをオンにします。 選択したアイテムは、設定を保存した後に表示されます。
Macオペレーティングシステム	選択されたMacオペレーティングシステムのパッチをダウンロードします。編集 ボタンをクリックして、オペレーティングシステムのリストを管理します: をクリックします。管理対象デバイスに基づいて Mac オペレーティングシステムを選択するには、**インベントリ内のすべてのMac** を選択します。Macオペレーティングシステムのパッチを無視するには、**無効** を選択します。または、1つまたは複数のMacオペレーティングシステムの横にあるチェックボックスをオンにします。 選択したアイテムは、設定を保存した後に表示されます。
ロケール	選択された言語のパッチをダウンロードします。編集 ボタンをクリックして、ロケールのリストを管理します: をクリックします。ロケールに関係なくパッチをダウンロードするには、**すべてのロケール** を選択するか、1つまたは複数のロケールの横にあるチェックボックスをオンにします。 選択したアイテムは、設定を保存した後に表示されます。

注: パッチサブスクリプションに対して1つ以上のオペレーティングシステムと1つのロケールを選択する必要があります。

4. 「アプリケーションパッチ」設定を指定します。これらの設定は、パッチファイルがダウンロードされた場合にパッチステータスの決定に使用されます。これには、「アクティブ」、「非アクティブ」、または「無効」があります。

オプション	説明
発行元	ベンダーに基づいてアプリケーションパッチをサブスクライブします。編集 ボタンをクリックして、選択したタイプを管理します: をクリックしま

オプション	説明
	す。利用可能なすべての発行元のパッチを選択するには、**すべての発行元** を選択します。または、1つまたは複数の発行元の横にあるチェックボックスをオンにします。 選択したアイテムは、設定を保存した後に表示されます。

5. サブスクリプションの「詳細設定」を指定します。

オプション	説明
分類	このサブスクリプションのタイプをクリックして選択します。**すべての分類** を選択するか、**無効** にするか、または **分類の選択** をクリックして、既存の値の 1 つまたは複数を適宜選択できます。**重要な更新、定義の更新、機能パック、完全なソフトウェア、ホットフィックス、セキュリティの更新、サービスパック、ツール、更新ロールアップ、更新、および アップグレード。**
重要度	このサブスクリプションの重要度をクリックして選択します。**すべての重要度** を選択するか、**無効** にするか、または **重要度の選択** をクリックして、既存の値の 1 つまたは複数を適宜選択できます。**重大、重要、低、中、推奨。**
ラベル	選択したラベルと一致するパッチのみをダウンロードします。**関連ラベルの管理** をクリックして、ラベルを選択します。 この調整が重要になるのは、ディスク領域が限られている場合です。選択したパッチに必要なディスク領域の合計がアプライアンス上の使用可能なディスク領域を超えている場合は、パッチをダウンロードできません。 **注:** ページ上部のパッチステータス セクションに、アプライアンスのディスク領域情報が表示されます。
Windowsに埋め込まれたパッチを無効にする	埋め込まれたWindowsのパッチをすべて特定して無効にします。このオプションを選択すると、埋め込まれたパッチの署名がダウンロードされますが、サブスクリプションの条件に一致しない限り、パッチは展開できません。
置き換えられたパッチを非アクティブにする	ダウンロードするたびに、置き換えられたパッチが「非アクティブ」状態とマークされます。非アクティブな置き換えられたパッチは、パッチカタログページで「**非アクティブ**」として識別されます。
無効なパッチの検出	アプライアンスが検出ジョブを実行するときに、無効なパッチを特定するようにできます。このオプションを選択すると、無効なパッチに対する署名は、検出目的でのみダウンロードされます。サブス

オプション	説明
	クリプション条件に合わない場合、パッチは展開できません。

6. **保存** をクリックします。

次回のスケジュールされたダウンロード時間に、選択したパッチは自動的にダウンロードされます。ダウンロード後、サブスクリプション設定と一致しないパッチは、「**無効**」として表示されます。サブスクリプション設定が一致していても、置き換えられていたり、手動で非アクティブに設定されたりしているパッチは、状態が「**非アクティブ**」として表示されます。

パッチおよび機能更新プログラムのダウンロード設定の選択

サブスクライブしているパッチおよび Windows 機能更新プログラムは、選択する設定に従ってアプライアンスにダウンロードされます。

最初のパッチダウンロードでは、多くのネットワーク帯域幅が使用される可能性があることに注意してください。

1. パッチおよび機能更新プログラムのダウンロード設定 ページに移動します。
   - **組織コンポーネントがアプライアンスで有効になっていない場合、左側のナビゲーションバーで、セキュリティ をクリックします。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. パッチおよび機能更新プログラムのダウンロード設定 をクリックします。
3. ファイルダウンロードの設定 セクションで、次のオプションを選択します。

オプション	説明
パッチ適用	• **無効**: パッチパッケージのダウンロードを防ぎます。この予防措置の対象には、パッチをインストールするために必要なインストーラーも含まれます。 • **すべてのサブスクライブされたファイル**：アプライアンス上でサブスクライブしたパッケージの完全キャッシュを保持します。このオプションを選択すると、サブスクライブする展開パッケージがすべてダウンロードされます。展開パッケージが環境に必要かどうかを判断するためのチェックは行われません。環境によっては、完全キャッシュを保持することは重要です。例えば、**オフラインターゲット** または **オンラインソース** オプションを選択する場合、完全キャッシュが必要です。 • **不足しているファイルのみ**：アプライアンスが検出ジョブの結果に基づいてダウンロードするパッケージを決定できるようにします。管理対象デバイスのいずれかでパッチ検出署名が「未インストール」として検出された場合は、パッチパッケージがダウンロードされます。管理対象デバイスに「未インストール」として検出されたデバイスがない場合

オプション	説明
	は、このパッチのパッケージはダウンロードされません。
機能更新プログラム	• **無効**: Windows Feature Update がダウンロードされないようにします。この予防措置の対象には、パッチをインストールするために必要なインストーラーも含まれます。 • **不足しているファイルのみ**：アプライアンスが検出ジョブの結果に基づいてダウンロードするパッケージを決定できるようにします。管理対象デバイスのいずれかで機能更新プログラム署名が「パッチ未適用」として検出された場合は、Windows 機能更新プログラムパッケージがダウンロードされます。管理対象デバイスに「パッチ未適用」として検出されたデバイスがない場合は、この Windows 機能更新プログラムのパッケージはダウンロードされません。
__日経過後に、未使用のファイルを削除する	指定した日数内に展開されなかったパッチおよび Windows Feature Update を削除します。「非アクティブ」または「無効」とマークされたパッチおよび Windows 機能更新プログラムは、パッチのダウンロードプロセス中に自動的に削除されます。
オフライン更新	更新プロセスがスケジュールに従って開始されたときにアプライアンスがオフラインである場合に実行するアクション。アプライアンスがインターネットに接続されていて、パッチまたは Windows 機能更新プログラムを直接ダウンロードできる場合は、オフライン更新 オプションをオフにします。
オフラインターゲット	「オフラインターゲット」を使用するのは、アプライアンスがインターネットに接続されていないときに、ローカルディレクトリからパッチおよび Windows 機能更新プログラムのファイルをアップロードする場合です。インターネットに接続されているアプライアンスがある場合、そのアプライアンスをオフラインソースとして設定できます。設定後、Offline Source Patchesファイル共有から「オフラインターゲット」の次のディレクトリにパッチファイルを手動でコピーできます。**appliance_host**\patches **アップロード** をクリックすると、パッチのTARファイルが読み込まれます。
オンラインソース	別のアプライアンスのソースとしてアプライアンスを使用するかどうかを指定します。このオプションを選択すると、アプライアンスのパッチおよび Windows Feature Update のファイル共有にパッチファイルがダウンロードされます。

オプション	説明
更新 **説明** **アクション**	各タイプの更新虚グラム（署名、機能更新プログラムファイル、パッチファイル）について、説明と使用可能なアクションへのアクセスを提供します。 • **更新の確認**: クリックしてパッチ署名ファイルをダウンロードします。 • **削除**: クリックすると、アプライアンスからすべてのパッチまたは Windows 機能更新プログラムがただちに削除されます。このオプションは、今後パッチが不要となり、パッチのために使用したディスク領域をすぐに再利用する場合に便利です。 • **今すぐ実行**: クリックすると、サブスクリプションのスケジュールに関係なく、サブスクライブしたパッチまたは Windows 機能更新プログラムがすぐにダウンロードされます。

4. スケジュール セクションでパッチおよび Windows 機能更新プログラムの署名のスケジュールオプションを選択します。ファイル署名には、セキュリティ通知および Quest からダウンロードされるパッチおよび Windows Feature Update を定義するその他のファイルが含まれています。

オプション	説明
署名のダウンロード	パッチおよび Windows Feature Update 署名がダウンロードされないようにするには、**なし** を選択します。
__時間ごと	指定した間隔で署名をダウンロードします。このオプションを選択すると、帯域幅の要件が増える可能性があるため、間隔（4、8、または12時間）を指定する際には注意が必要です。
毎日、指定した時刻	**日** を選択して、パッチまたは Windows Feature Update 検出署名を毎日ダウンロードするか、または曜日を選択して週に 1 回ダウンロードします。 ダウンロードを開始する時間を選択します。時間は 24 時間形式で表示され、0 の場合は午前 0 時を、1 の場合は午前 1 時を、23 の場合は午後 11 時を表します。 **注:** パッチまたは Windows Feature Update のダウンロードを設定する場合、タイミングが重要です。アプライアンスのアクティビティログは午前 1 時 30 分に作成され、メンテナンスタスクは午前 1 時から 1 時 30 分の間に行われます。ログの作成とメンテナンスタスクが完了する午前 3 時頃よりも後に、ダウンロードをスケジュールすることをお勧めします。
毎月 / 特定月 n 日の HH:MM に実行	月の特定の日を選択して、1 か月ごとにパッチまたは Windows Feature Update 検出署名をダウンロードします。

5. 機能更新プログラムとパッチファイルのスケジュールオプションを設定します。

オプション	説明
署名のダウンロード後	署名がダウンロードされた後で、パッケージをダウンロードします。このオプションは、ファイルのダウンロード設定 セクションで **パッチ適用** が無効になっている場合は使用できません。
__分ごと	パッケージをダウンロードする頻度を指定します。ファイルのダウンロード設定 セクションの 不足しているパッチのみ が選択されている場合にのみ、このオプションは使用できます。
ダウンロードのブラックアウト: 開始: __、終了: __	ファイルがダウンロードできない時間帯を指定します。例えば、停止時間を早朝にして、通常の業務時間に多くのネットワーク帯域幅がプロセスによって使用されないようにします。 このオプションを選択すると、指定した時間にファイルダウンロードが停止します。次回の指定したファイルダウンロード時間になるまで、ダウンロードは開始されません。ダウンロードが再開されると、停止した時点からパッチダウンロードが開始されます。未完了のダウンロードは、パッチカタログ または Windows Feature Update カタログ ページに表示されない可能性があります。

6. **保存** をクリックします。

管理対象デバイスに対するパッチの検出および展開をスケジュールするには、パッチスケジュールの作成および管理を参照してください。管理対象の Windows 10 デバイスの Windows 機能更新プログラムの検出と展開をスケジュールするには、「Windows 機能更新プログラムのスケジュールの設定」を参照してください。

使用可能なパッチとダウンロードステータスの表示

使用可能なパッチを確認し、適切なパッチダウンロードフィルタを設定して必要なパッチのみダウンロードできます。

例えば、パッチパッケージのダウンロード後にフィルタを設定して、オペレーティングシステムのパッチだけを表示する、といったカテゴリに従ったパッチの表示が行えます。

使用可能なパッチの表示

パッチをサブスクライブし、パッチがダウンロードされた後に、使用可能なパッチを表示することができます。

パッチを表示するには、パッチ検出署名をサブスクライブし、パッチのダウンロード設定を選択する必要があります。詳細については、以下を参照してください。

- パッチのサブスクライブ
- パッチおよび機能更新プログラムのダウンロード設定の選択

1. パッチカタログ リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
c. パッチ管理 パネルで **カタログ** をクリックします。

2. アプリケーションパッチを検索します。
   a. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
   b. 検索条件を入力します。

      パッチリスト情報: カテゴリ | は | アプリケーション

   c. **検索** をクリックします。

パッチのダウンロードステータスの表示

パッチをサブスクライブした後、パッチのダウンロードステータスを表示できます。

パッチのダウンロードステータスを表示するには、パッチをサブスクライブする必要があります。詳細については、「パッチのサブスクライブ」を参照してください。

1. パッチカタログ リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
   c. パッチ管理 パネルで **カタログ** をクリックします。
2. 次のいずれかを実行します。
   - **右側のテーブルの上に表示される** 特定基準で表示 **ドロップダウンリストで、ダウンロードステータス > ダウンロード または ダウンロードステータス > ダウンロードされませんでした を選択します。**
   - **右側のテーブルの上に表示される 高度な検索 タブをクリックして、検索条件を選択します。例：**

     パッチリスト情報: ダウンロードステータス | は | ダウンロードされました

詳細については、「パッチ情報の表示」を参照してください。

パッチサブスクリプションの問題を解決するためのベストプラクティス

パッチサブスクリプションライセンスの有効期限が切れていることを示すエラーメッセージが表示されることがあります。

エラーメッセージ

パッチのサブスクリプションの有効期限が過ぎています。この場合の対応については、サポートにお問い合わせください。

KACE サポートに連絡する前に、いくつかの予備手順を実行して問題を解決できます。

このエラーは、次のいずれかの問題によって発生することがあります。

- ほとんどの場合、ライセンスキーの 3 年間の検証期間が経過したときに発生します。
- 新しいライセンスキーが提供されていても、アカウントがまだ KACE データベースと同期していないことがあります。

新しいキーが要求されたが、まだ通知されていない場合：

次の E メールメッセージがスパムフィルタによって停止されていないことを確認します。これは、KACE ライセンスチームが送信した新しいライセンスキー通知のメッセージ形式です。

送信者：license@quest.com

件名：**KACE システム管理アプライアンス**（ PO# <PO 番号>）order# <注文番号> のライセンス番号

新しいキーを適用したが、エラーが解決されない場合：

1. 製品ライセンスを検証します。
   a. アプライアンスの コントロールパネル に移動します。
      - アプライアンスで組織コンポーネントが有効化されていない場合は、**設定** をクリックします。
      - アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンス**システム管理コンソール**（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択して、**設定** をクリックします。

   b. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。
   c. ライセンス情報 の右側で をクリックします。
   d. ライセンスの検証 を選択し、**はい** をクリックして確定します。

      ヒント: このページの詳細については、「アプライアンスライセンスキーの更新」を参照してください。

2. 手動によるパッチ署名のダウンロードを実行します。
   a. パッチダウンロード設定 ページに移動します。
      - アプライアンスで組織コンポーネントが有効化されていない場合は、**設定** をクリックします。
      - アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンス（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択して、**設定** をクリックします。
      - **セキュリティ > パッチ管理 > パッチダウンロード設定** の順に移動します。

   b. **今すぐ実行** をクリックします。パッチダウンロードが完了すると、エラーメッセージは消えます。

      ヒント: このページの詳細については、「パッチおよび機能更新プログラムのダウンロード設定の選択」を参照してください。

上記の手順を完了しても、問題が解決されない場合：

1. https://support.quest.com/create-service-request に進み、新しいサービスリクエスト（ SR ）を作成します。
2. リクエストの次の質問に回答します。
   - 初めて問題が発生したのはいつですか。
   - 問題の前に何か変更しましたか。
   - パッチダウンロードのログで問題を検証し、確認します。SR で結果を文書として提出するか、SR にログファイルをアップロードします。
   - どのライセンスキーが現在使用されていますか。完全なライセンスキーが必要です。これが可能でない場合、最後の 5 文字が使用されます。
   - 使用可能な場合、古い（ 以前の ）ライセンスキーを教えてください。
   - アプライアンスの静的 IP アドレスを教えてください。
   - アプライアンスの MAC アドレスを教えてください。
3. アプライアンスログファイルを SR の添付ファイルとしてアップロードします。

a. アプライアンスの コントロールパネル に移動します。
   - アプライアンスで組織コンポーネントが有効化されていない場合は、**設定** をクリックします。
   - アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンス**システム管理コンソール**（http://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択して、**設定** をクリックします。

b. 左のナビゲーションバーで **サポート** をクリックします。
c. トラブルシューティングツール セクションで **アプライアンスのアクティビティログの取得** をクリックします。
d. **ファイルの保存** をクリックして、ログをダウンロードします。

注: パッチのダウンロード中は、エラー状況の発生後にブラウザのキャッシュをクリアしてください。このようにしないと、このエラーが発生した後で、アプライアンスがパッチをダウンロードできなくなる可能性があります。

パッチスケジュールの作成および管理

パッチスケジュールを管理して、サブスクライブしているパッチを検出、展開、およびロールバックできます。

パッチのサブスクライブ手順については、パッチのサブスクライブとダウンロードを参照してください。

デスクトップおよびサーバー用の緊急のOSパッチのスケジュールについて

スケジュールに従ってデスクトップおよびサーバーに緊急のOSパッチをインストールするようにアプライアンスを設定できます。

デスクトップはサーバーほど重要ではなく、ノートPCほど持ち運ばれることはありません。このため、デスクトップにパッチを適用する時間をスケジュールするのは、それほど難しくはありません。通常、日常的な更新をユーザーが出社する前の午前中の早い時間帯にスケジュールできます。

サーバーは、組織が必要とする重要なサービスを実行します。事前にサーバーへのパッチ適用をスケジュールし、パッチ適用に必要な一時的なサービス停止をユーザーに警告します。サーバーリソースを必要とするユーザーの数が最小になる午前中の早い時間帯などにサーバーパッチをプッシュします。

デスクトップおよびサーバー用の緊急のOSパッチのワークフロー

このワークフローは、デバイスの識別、パッチの識別、アクションのスケジュール、およびパッチの展開で構成されます。

- **デスクトップの識別**: すべてのデスクトップデバイスを識別するSmart Labelを作成する。このことによりサーバーとノートPCが除外されます。詳細については、「デスクトップに対するSmart Labelの追加」を参照してください。
- **サーバーの識別**: すべてのサーバーを識別するSmart Labelを作成する。詳細については、「サーバーに対するSmart Labelの追加」を参照してください。
- **緊急のOSパッチの識別**: すべての緊急のOSパッチを識別するSmart Labelを作成する。詳細については、「緊急のOSパッチに対するSmart Labelの追加」を参照してください。
- **検出および展開アクションのスケジュール**: Smart Labelが適用されているデバイスを更新する必要があるかどうかを識別する検出および展開ジョブをスケジュールし、緊急のパッチをそれらのデバイスに展開

し、必要があれば強制的に再起動する。詳細については、「パッチスケジュールの設定」を参照してください。

- **サーバー別のパッチ展開**: 必要に応じてサーバーにパッチを展開するジョブをスケジュールする。詳細については、「パッチスケジュールの設定」を参照してください。
- **ユーザーへの通知**: パッチ適用をスケジュールする場合は、ユーザーが使用しているデバイスに対してパッチを適用中であることが分かるように、必ずユーザーにスケジュールを通知する。このことは、パッチ適用プロセスでデバイスの再起動が必要となり、デバイスが使用できなくなる可能性がある場合に特に重要です。アプライアンスの管理者コンソール以外でEメールを送信したり、他のメッセージングサービスを使用したりして、ユーザーに通知できます。詳細については、「パッチ適用に関するベストプラクティス」を参照してください。

ノートPCに対する緊急のパッチのスケジュールについて

ノートPCは頻繁に電源がオフになったり、ネットワークから切断されたりするため、パッチ適用に適切な時間帯を見つけるのは難しくなる可能性があります。ノートPCへのパッチ適用のための最も一般的な選択肢は、業務開始時と昼食時の2つです。

Quest KACEのほとんどのお客様は、2つのスケジュール（検出用と展開用）を使用して、ノートPCにパッチを適用しています。

ノートPCに対する緊急のパッチのワークフロー

ノートPCに緊急のパッチを適用するワークフローは、デバイスの識別、パッチの識別、アクションのスケジュール、およびパッチの展開で構成されます。

自動検出と展開アクションのセットアップは、次のワークフローで構成されます。

- **緊急のパッチの識別**: ノートPC用の緊急のパッチを自動的に識別するパッチSmart Labelを作成する。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
- **検出アクションのスケジュール**: ノートPCに対して緊急のパッチを定期的に検出するスケジュールを作成して実行する。詳細については、「パッチスケジュールの設定」を参照してください。
- **展開アクションのスケジュール**: ノートPCに対して緊急のパッチを定期的に展開するスケジュールを作成して実行する。詳細については、「パッチスケジュールの設定」を参照してください。
- **パッチステータスの確認**: レポートとパッチを使用してパッチ適用ステータスを定期的に確認する。詳細については、「パッチスケジュール、ステータス、およびレポートの表示」を参照してください。
- **ユーザーへの通知**: ユーザーにパッチスケジュールを通知する。アプライアンスの**管理者コンソール**以外でE メールを送信したり、他のメッセージングサービスを使用したりして、ユーザーに通知できます。パッチ適用に関するベストプラクティスの「デバイスに対するパッチ適用時のユーザーへの通知」を参照してください。

緊急以外の更新プログラムのスケジュールについて

スケジュールに従って緊急以外のパッチをインストールするようにアプライアンスを設定できます。

緊急以外のパッチをスケジュールするには

- **パッチの検出**: パッチ適用ジョブの規模を確認するために、すべてのデバイス上のパッチを検出するパッチスケジュールを作成する。詳細については、「パッチスケジュールの設定」を参照してください。
- **パッチの非アクティブ化**: 展開しないパッチがある場合は、それらのパッチを**非アクティブ**とマークする。
- **パッチのテスト**: テストデバイスに対してパッチを検出して展開するスケジュールを作成する。詳細については、「パッチスケジュールの設定」を参照してください。
- **デスクトップおよびサーバーに対するパッチの識別**: サーバーに展開するパッチを自動的にキャプチャするパッチSmart Labelを作成する。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
- **デスクトップおよびサーバーパッチの検出と展開**（パッチスケジュールの設定を参照）:
  - デスクトップに対してパッチを定期的に検出して展開するスケジュールを作成する。
  - サーバーに対してパッチを定期的に検出して展開するスケジュールを作成する。
- **ラップトップパッチの検出と展開**（パッチスケジュールの設定を参照）:
  - ノートPCに対してパッチを定期的に検出するスケジュールを作成する。
  - ノートPCに対してパッチを定期的に展開するスケジュールを作成する。
- **パッチステータスの確認**: 定期的にパッチステータスを確認する。詳細については、「パッチスケジュール、ステータス、およびレポートの表示」を参照してください。

パッチスケジュールの設定

パッチスケジュールを作成および設定し、その実行時間をスケジュールすることができます。パッチスケジュールは、管理対象インストールやその他の配布には干渉しません。

パッチスケジュールの詳細 ページのフィールド

スケジュールの詳細 ウィザードと スケジュールの詳細 ページのフィールドでは、パッチアクションの設定とスケジュールを行うことができます。

一般的な情報

オプション	説明
名前	スケジュールを識別するための名前。この名前は、パッチスケジュール ページに表示されます。
説明	パッチスケジュールの簡単な説明。

アクション セクション

パッチスケジュールに関連付けられたアクション。

パッチアクションの動作は、再起動、検出、展開、ロールバックから選択した組み合わせによって異なります。パッチアクションによってパッチの検出とその他のアクションの両方が実行される場合は常に、展開または ロールバックするすべてのパッチが検出アクションによって検出されるまで、アクションが循環的に繰り返し実行されます。例えば、「検出と展開」および「検出と ロールバック」を実行する場合がこれに該当します。この動作により、スケジュール済みの実行が1つだけの場合でも、複数の再起動アクションが必要となることがあります。さらに、パッチを適用するデバイスの種類が、使用するパッチアクションの種類に影響します。

使用可能なアクションは以下の通りです。

- **検出**：管理対象デバイスにインストールされているパッチ、または管理対象デバイスから欠落しているパッチを検出します。パッチダウンロード設定 が、ダウンロード専用に設定されている場合は、検出のみ

のアクションが推奨されます。展開前に検出のみのアクションを実行すると、展開が始まる前に、ダウンロードするパッチファイルのリストが作成されます。

- **検出とステージング**：管理対象デバイスにインストールされているパッチまたは管理対象デバイスから欠落しているパッチを検出し、後で展開するためにパッチファイルをエージェントデバイスにダウンロードします。
- **検出と展開**：管理対象デバイスのパッチを検出して展開します。これらのタイプのアクションは、デスクトップとサーバを管理するときに使用されます。検出および展開のパッチ適用ジョブには、デバイスとアプライアンスの間に接続が必要です。これらのジョブはオフラインでは実行されません。メッセージプロトコル接続の詳細については、エージェント通信とログ設定の定義を参照してください。
- **検出、ステージ、およびオンデマンド展開**：管理対象デバイスにインストールされているパッチまたは管理対象デバイスから欠落しているパッチを検出し、パッチファイルをエージェントデバイスにダウンロードし、パッチの展開準備が整ったことをエージェントデバイスの Windows システムトレイでユーザーに警告します。その後、ユーザーは都合に合わせて展開プロセスを開始できます。
  - これらのスケジュールは、バージョン 11.0 以降のエージェントを持つ Windows デバイスでのみ使用できます。
  - エージェント通信設定で、デバイス上のエージェントステータスアイコン オプションが有効になっている必要があります。これらの設定は、組織の詳細 ページ、通信とエージェントの設定（1 つ以上の組織コンポーネントが有効になっている場合）の下、または 通信設定 ページ（組織コンポーネントがない場合）で確認できます。詳細については、「エージェント通信とログ設定の定義」を参照してください。
- **展開**：管理対象デバイスに適用可能なパッチを展開します。この方法は、管理対象デバイスに特定のパッチを適用する必要があることが分かっている場合に便利です。パッチが適用された後で、または再起動が必要な場合は、デバイスが再起動され、エージェントがアプライアンスと再接続した後で最終検出ジョブが実行されます。
- **検出とロールバック**：管理対象デバイスから不要なパッチを検出して削除します。ロールバックは、一部のパッチには使用できない場合があります。詳細については、「パッチがロールバック可能であるかどうかの確認」を参照してください。
- **ロールバック**：管理対象デバイスから不要なパッチを削除します。ロールバックは、一部のパッチには使用できない場合があります。詳細については、「パッチがロールバック可能であるかどうかの確認」を参照してください。

検出 セクション

オプション	説明
すべてのパッチ	使用可能なすべてのパッチを検出します。このプロセスの処理は長時間かかることがあります。また、管理対象デバイスにインストールされていないソフトウェアや、必要とされないソフトウェアのパッチが検出されることがあります。例えば、管理対象デバイスで使用しているウイルス対策アプリケーションのベンダーが1社だけの場合は、すべてのウイルス対策アプリケーションのベンダーに対してパッチを検出する必要がないこともあります。しかし、「すべてのパッチ」では、管理対象デバイスで必要であるかどうかにかかわらず、不足しているパッチがすべて検出されてしまいます。パッチ検出を絞り込むには、検出するパッチのラベルを設定し、パッチラベル オプションを使用します。
パッチラベル	選択したラベル内のパッチにアクションを制限します。これは、最も一般的に使用されるオプションです。 1. **関連ラベルの管理** をクリックします。

オプション	説明
	2. 表示された ラベルを選択 ダイアログボックスで、1 つ以上のラベル (該当する場合) を検出の制限対象 領域にドラッグし、**OK** をクリックします。 このオプションを使用するには、該当するパッチ用の Smart Label が既に存在している必要があります。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
推奨基準からの選択	事前定義された条件を使用してパッチを選択します。これにより、OS に基づいて特定の種類のパッチに集中できます。たとえば、過去 30 日間に発行された重要な Windows パッチを選択できます。 1. **推奨基準からの選択** をクリックします。 2. 表示される 推奨基準の選択 ダイアログボックスで、**推奨基準の選択** をクリックし、**保存** をクリックします。
検出のタイムアウト	パッチ適用アクションが完了するまでの時間 (時間単位) 。

展開 セクション

オプション	説明
すべてのパッチ	選択したデバイスにすべてのパッチを展開します。
パッチラベル	選択したラベル内のパッチにアクションを制限します。これは、最も一般的に使用されるオプションです。 1. **関連ラベルの管理** をクリックします。 2. 表示された ラベルを選択 ダイアログボックスで、1 つ以上のラベル (該当する場合) を展開の制限対象 領域にドラッグし、**OK** をクリックします。 このオプションを使用するには、該当するパッチ用の Smart Label が既に存在している必要があります。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
推奨基準からの選択	事前定義された条件を使用してパッチを選択します。これにより、OS に基づいて特定の種類のパッチに集中できます。たとえば、過去 30 日間に発行された重要な Windows パッチを選択できます。 1. **推奨基準からの選択** をクリックします。 2. 表示される 推奨基準の選択 ダイアログボックスで、**推奨基準の選択** をクリックし、**保存** をクリックします。
展開の最大試行回数	アプライアンスがパッチを展開またはロールバックする最大試行回数。「1」から「10」の数字を指定します。「0」を指定すると、展開または ロール

オプション	説明
	バックは実行されません。「10」を超える値を指定すると、エラーメッセージが表示されます。 パッチの展開やロールバックの最後の手順として、アプライアンスによってパッチが正常に展開またはロールバックされたかどうかが確認されます。展開やロールバックに失敗すると、アプライアンスは、次のいずれかの状態になるまで再度パッチの展開またはロールバックを試行します。 • 展開またはロールバックが成功する。 • 最大試行回数に達する。 • スケジュールされた展開またはロールバックの期間が終了し、パッチ適用が中断する。
展開のタイムアウト	パッチ適用アクションが完了するまでの時間（時間単位）。

ロールバック セクション

オプション	説明
すべてのパッチ	選択したデバイスのすべてのパッチをロールバックします。
パッチラベル	選択したラベル内のパッチにアクションを制限します。これは、最も一般的に使用されるオプションです。 1. **関連ラベルの管理** をクリックします。 2. 表示された ラベルを選択 ダイアログボックスで、1 つ以上のラベル（該当する場合）を ロールバックの制限対象 領域にドラッグし、**OK** をクリックします。 このオプションを使用するには、該当するパッチ用の Smart Label が既に存在している必要があります。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
推奨基準からの選択	事前定義された条件を使用してパッチを選択します。これにより、OS に基づいて特定の種類のパッチに集中できます。たとえば、過去 30 日間に発行された重要な Windows パッチを選択できます。 1. **推奨基準からの選択** をクリックします。 2. 表示される 推奨基準の選択 ダイアログボックスで、**推奨基準の選択** をクリックし、**保存** をクリックします。
ロールバックの最大試行回数	最大試行回数。アプライアンスによってパッチの展開またはロールバックが試行される回数を0〜99の間で指定します。「0」を指定すると、パッチの展開またはロールバックはアプライアンスによって無制限に試行されます。 パッチの展開やロールバックの最後の手順として、アプライアンスによってパッチが正常に展開または

オプション	説明
	ロールバックされたかどうかが確認されます。展開やロールバックに失敗すると、アプライアンスは、次のいずれかの状態になるまで再度パッチの展開またはロールバックを試行します。 • 展開またはロールバックが成功する。 • 最大試行回数に達する。 • スケジュールされた展開またはロールバックの期間が終了し、パッチ適用が中断する。
展開のタイムアウト	パッチ適用アクションが完了するまでの時間（時間単位）。

オンデマンド展開タイムアウトの設定 セクション

オプション	説明
指定の時間後に自動的に展開	エージェントデバイスがユーザーからの入力を受信しない場合に、展開が実行されるまでの時間。

デバイス セクション

オプション	説明
全デバイス	このスケジュールをすべての管理対象デバイスに適用するには、このオプションを選択します。パッチアクションを特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
デバイスラベル	選択したラベル内のパッチにアクションを制限します。これは、最も一般的に使用されるオプションです。 1. **関連ラベルの管理** をクリックします。 2. 表示された ラベルを選択 ダイアログボックスで、1 つ以上のラベルを 実行の制限対象 領域にドラッグし、**OK** をクリックします。 このオプションを使用するには、該当するパッチ用の Smart Label が既に存在している必要があります。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
デバイス	選択したデバイスでパッチアクションを実行します。 • デバイスを検索するには、フィールドに入力し始めます。 • 指定されたすべてのデバイスを削除してから再起動するには、**すべて削除** をクリックします。 • スコープユーザーは、役割にラベルが割り当てられている場合に、自身の役割に関連付けられているデバイスだけを表示できます。ユーザーの役割の詳細については、ユーザー

オプション	説明
	の役割の追加または編集を参照してください。
オペレーティングシステム	パッチを適用するデバイスのオペレーティングシステムを選択します。デフォルトは、すべてのオペレーティングシステムです。このオプションが設定されている場合、スケジュールは選択したオペレーティングシステムを搭載したデバイスにのみ適用されます。 1. **オペレーティングシステムの管理** をクリックします。 2. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**Windows > Windows 10** の順に選択し、**x64** を選択します。

通知 セクション

オプション	説明
オプション	パッチアクションの実行時にユーザーに表示されるアラート。ユーザーに通知することなくアクションを実行するには、オプション フィールドを空白のままにします。 • **OK**: すぐに実行されます。 • **キャンセル**: 次のスケジュールされた実行までキャンセルされます。 • **再通知**: 再通知間隔 の経過後に再度プロンプトが表示されます。
タイムアウト	アクションの実行前にダイアログが表示される期間（分単位）。この期間が経過するまでの間にユーザーがボタンを押さないと、Timeout（タイムアウト）ドロップダウンリストで指定されたアクションをアプライアンスが実行します。
タイムアウトアクション	ユーザーがオプションを選択することなく **Timeout**（タイムアウト）で指定した期間が経過した場合に実行されるアクション。

オプション	説明
再通知間隔	ユーザーが **再通知** をクリックした後の期間（分単位）。この期間が経過すると、ダイアログが再度表示されます。
限度まで再通知	ユーザーが指定回数だけパッチアクションを再通知できるようにするには、**限度まで再通知** チェックボックスをオンにします。**試行回数** を指定します。
初期メッセージ	アクションが実行される前に、ユーザーに表示されるメッセージ。ダイアログに表示される口ゴをカスタマイズするには、組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定を参照してください。
進行状況メッセージ	パッチアクションの実行中にユーザーに表示されるメッセージ。
完了メッセージ	パッチアクションの完了時にユーザーに表示されるメッセージ。

再起動 セクション

オプション	説明
オプション	管理対象デバイスの再起動のオプション： • **再起動しない**：パッチを有効にするために再起動が必要な可能性がある場合でも、デバイスを再起動しません。このオプションはお勧めしません。これは、再起動が必要な場合に、再起動しないでパッチを展開するため、システムが不安定な状態のままになることがあるからです。さらに、再起動が必要なパッチは、再起動後にのみ適用済みとして表示されます。 • **ユーザーにプロンプトを表示**：デバイスを再起動する前に、ユーザーが再起動に同意するまで待ちます。ユーザーが再通知を選択するか、または再起動をキャンセルすると、再起動されるまでパッチ適用は停止します。ターゲットデバイスに表示されるエージェントダイアログボックスで再通知間隔を選択すると、指定した再通知間隔の間、再起動プロンプトが一時停止します。 • **強制的に再起動**：再起動が必要なパッチが展開されるとすぐに再起動されます。強制的な再起動はキャンセルできません。強制的な再起動は、デスクトップとサーバーに対して効果的です。ノートPCの再起動を強制することはお勧めしません。通常サーバーには専属のユーザーがいないため、強制的な再起動はサーバーで効果的に機能します。ただし、サーバがパッチを適用し再起動しているときにサービスが使用できなくなることをユーザーに警告するのは重要です。詳細について

オプション	説明
	は、「パッチ適用に関するベストプラクティス」を参照してください。
誰もログインしていない場合、自動的に再起動	ユーザーがログインしていない場合、管理対象デバイスは自動的に再起動されます。
メッセージ	デバイスが再起動される前に、ユーザーに表示されるメッセージ。メッセージダイアログにカスタムロゴを追加する方法については、組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定を参照してください。
タイムアウト	アクションの実行前にダイアログが表示される期間（分単位）。この期間が経過するまでの間にユーザーがボタンを押さないと、Timeout（タイムアウト）ドロップダウンリストで指定されたアクションをアプライアンスが実行します。 強制的に再起動 を選択すると、タイムアウト動作でKUSerAlert およびグローバル KACE エージェントプロセスタイムアウトが考慮されます。エージェントおよび通信設定 セクションから設定されるグローバルタイムアウトは、KUserAlert タイムアウトを含め、エージェントが起動したプロセスの実行時間を常に決定します。例えば、KUserAlertタイムアウトが2時間に設定されていて、グローバルタイムアウトを1時間に設定した場合、実行時間が長すぎるため、エージェントがKUserAlertを停止します。そのため、グローバルタイムアウトは、KUserAlertタイムアウトより長い、目的のタイムアウトに設定する必要があります。この値はそれに合わせて設定する必要があります。 これらの設定の詳細については、「エージェント通信と口グ設定の定義」を参照してください。
タイムアウトアクション	ユーザーがオプションを選択することなく **Timeout**（タイムアウト）で指定した期間が経過した場合に実行されるアクション。
再起動の遅延（カウントダウン）	カウントダウンを使用して再起動を延期します。カウントダウンは分単位です。
今すぐ再起動	デバイスを直ちに再起動します。
後で再起動	デバイスを後で再起動します。
プロンプト数	デバイスが再起動される前に、ユーザーが受け取るプロンプトの数。例えば、値「5」を入力すると、5回目にユーザーが再起動のプロンプトを受け取ったときに、デバイスが自動的に再起動されます。つまり、**Number of prompts**（プロンプト数）の値として「5」を設定した場合、ユーザーは再起動を 4 回まで遅延させることができます。

オプション	説明
プロンプト再表示間隔	ユーザーに再起動を求めるプロンプトを再表示するまでの時間。

スケジュール セクション

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。このオプションは、サーバーに手動でパッチを適用するか、または定期的に実行しないパッチアクションを実行する場合に便利です。
毎 _ 時間	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
毎月 / 特定月の n 日、HH:MM に実行	毎月n日（例えば、毎月1日または2日）、または特定の月、特定の時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。

オプション	説明
	例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。
タイムゾーン	アクションをスケジュールするときに使用するタイムゾーン。**サーバー** を選択すると、アプライアンスのタイムゾーンを使用します。**エージェント** を選択すると、管理対象デバイスのタイムゾーンを使用します。
オフラインの場合は次の接続時に実行	管理対象デバイスが現在オフラインである場合、次回管理対象デバイスがアプライアンスに接続するときにアクションを実行します。このオプションは、定期的にオフラインになるノートPCおよびその他のデバイスに対して役立ちます。このオプションが選択されていない場合でデバイスがオフラインのときは、次回のスケジュールされた時間までアクションは再度実行されません。
再接続後の実行を遅延	指定した時間、スケジュールを遅延させます。遅延時間は、パッチアクションの実行がスケジュールされている時間から開始されます。
次の時間の経過後に終了:	パッチ適用アクションの期限。 例えば、04:00にパッチが実行されるようスケジュールする場合、07:00にパッチ適用アクションをすべて停止し、ユーザーが業務を開始するときに帯域幅の問題が発生しないようにすることができます。これを行うには、分 ボックスで「**180**」を指定します。 期限に到達すると、進行中のパッチ適用タスクはすべて中断され、これらのタスクに対するセキュリティログのステータスは「中断されました」になります。 これらのパッチ適用タスクは次回実行で再開されず、スケジュール済みの毎回のパッチ適用アクションで最初から開始されます。

パッチスケジュールの設定

パッチスケジュールを作成および設定し、その実行時間をスケジュールすることができます。パッチ適用スケジュールは、管理対象インストールやその他の配布には干渉しません。

1. スケジュールの詳細 ウィザードを開始します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **スケジュール** をクリックします。
    d. パッチスケジュール ページで、以下のいずれかの作業を行います。

    - 新しいパッチスケジュールを作成するには、**アクションの選択 > 新規作成（ウィザード）** の順にクリックします。
    - 既存のスケジュールを編集するには、リスト内のスケジュール名をクリックし、表示されるパッチスケジュールの概要 ページで **編集** をクリックします。

      選択した スケジュールの詳細 ウィザードが表示されます。スケジュールの詳細 ページでも同じオプションを使用できます。必要に応じて、右上隅にある **クラシックビュー** または **ウィザードビュー** をクリックして、ページとウィザードを切り替えることができます。
2. スケジュールの詳細 ウィザードの 一般情報 ページで、このスケジュールの一般的な詳細を指定します。

    オプションの説明については、一般的な情報を参照してください。
3. **次へ** をクリックします。
4. アクション ページで、スケジュールに関連付けるアクションを選択します。

    オプションの説明については、アクション セクションを参照してください。
5. **検出、検出とステージ、検出と展開、検出、ステージ、およびオンデマンド展開、検出とロールバックスケジュールのみ。**アクション ページの 検出 セクションで、スケジュールの検出オプションを指定します。

    オプションの説明については、検出 セクションを参照してください。
6. **検出と展開、検出、ステージ、およびオンデマンド展開、および展開スケジュールのみ。**展開 セクションで、スケジュールの検出オプションを指定します。

    オプションの説明については、展開 セクションを参照してください。
7. **検出とロールバックおよびロールバックスケジュールのみ。**ロールバック セクションで、スケジュールのロールバックオプションを指定します。

    オプションの説明については、ロールバック セクションを参照してください。
8. **検出、ステージ、およびオンデマンド展開スケジュールのみ。**オンデマンド展開タイムアウトの設定 セクションで、検出、ステージ、およびオンデマンド展開スケジュールの展開タイムアウトオプションを指定します。

    オプションの説明については、オンデマンド展開タイムアウトの設定 セクションを参照してください。
9. **次へ** をクリックします。
10. デバイス ページで、このスケジュールに関連付けるデバイスを指定します。

    オプションの説明については、デバイス セクションを参照してください。
11. **次へ** をクリックします。
12. **検出と展開、展開、検出とロールバック、およびロールバックスケジュールのみ。**通知 ページで、スケジュールの通知オプションを設定します。

オプションの説明については、通知 セクションを参照してください。

13. **次へ** をクリックします。
14. 再起動 セクションで、スケジュールの再起動オプションを指定します。

    オプションの説明については、再起動 セクションを参照してください。

15. **次へ** をクリックします。
16. スケジュール セクションで、スケジュールのオプションを指定します。

    オプションの説明については、スケジュール セクションを参照してください。

17. **保存** をクリックします。

    パッチスケジュールの概要 ページが表示され、新しく作成または更新されたスケジュールが表示されます。このページの詳細については、「パッチスケジュールの詳細を確認」を参照してください。Smart Label の基準に一致するデバイスを追加した場合、それらのデバイスはパッチスケジュールに自動的に含まれます。

パッチとスクリプトによるエラーコード

パッチ適用時（検出または展開フェーズのみ）またはスクリプト実行時に発生する可能性のある次の失敗エラーコード。

パッチ適用時またはスクリプト実行時に発生するエラーコード

エラーコード	説明
8001	プラグインに送信されたコマンドが KPluginsKacePatch に認識されていません
8002	プラグインに送信されたコマンドの解析に失敗しました
8003	マニフェストファイルのダウンロードに失敗しました
8004	ダウンロードしたマニフェストファイルの解凍に失敗しました
8005	PreDetect コマンドの処理中の一般的なエラー（無効な関数入力など）
8007	PreDetect 結果の生成に失敗しました
8008	Detect コマンドの処理中の一般的なエラー（無効な関数入力など）
8009	Detect マニフェストファイルの解析に失敗しました
8010	Detect 結果の生成に失敗しました
8011	再起動を保留しています
8012	結果ログのアップロードに失敗しました

エラーコード	説明
8013	Detect ファイルの処理中に一般的なエラーが発生しました（無効な関数入力など）
8014	パッチ Detect ファイルのダウンロードに失敗しました
8015	パッチ Detect ファイルと検出マニフェストレコードのチェックサムが一致しません
8016	パッチ Detect ファイルのチェックサムファイルの作成に失敗しました
8017	パッチ Detect ファイルのロードに失敗しました
8018	パッチ Detect ファイルの復号化に失敗しました
8019	パッチ Detect ファイルの解凍に失敗しました
8020	パッチ Detect ファイルの json を解析できませんでした
8021	パッチ Detect ファイルの検出タイプが有効な検出方法として認識されませんでした
8100	マニフェストファイルの解析に失敗しました
8101	Deploy コマンドの処理中に一般的なエラーが発生しました（無効な関数入力など）
8102	Rollback コマンドの処理中に一般的なエラーが発生しました（無効な関数入力など）
8103	無効なハンドラ固有データ（HSD）タイプ
8150	要求されたファイルとマニフェストレコードのチェックサムが一致しません
8151	要求されたファイルのダウンロードに失敗しました
8152	ダウンロードしたファイルのチェックサムファイルの作成に失敗しました
8200	無効なコマンドスカラ演算
8201	無効なコマンド文字列操作
8202	無効なコマンド
8250	結果ファイルへのパスが無効です

エラーコード	説明
8251	結果ファイルの作成に失敗しました

パッチスケジュール、ステータス、およびレポートの表示

パッチスケジュールおよびパッチのステータスを全体的またはデバイスごとに表示できます。また、パッチ内の個別のパッケージを検索でき、パッチ関連のレポートを表示できます。

パッチスケジュールのリストを表示する

アプライアンスで作成されたパッチスケジュールのサマリ情報を表示できます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のパッチスケジュールを個別に表示します。

1. Patch Schedule（パッチスケジュール）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **スケジュール** をクリックします。

Patch Schedules（パッチスケジュール）ページには、次の列があります。

オプション	説明
前回の更新	パッチスケジュールが更新された日付と時刻。
名前	パッチスケジュールの名前。クリックすると、パッチスケジュールの概要 ページの詳細が表示されます。詳細については、「パッチスケジュールの詳細を確認」を参照してください。
スケジュール	パッチスケジュールの実行が設定される頻度。無効は、パッチがスケジュールに従って実行されるように設定されていないことを示します。
アクション	実行されるパッチアクションのタイプ。
再起動オプション	パッチスケジュールにとってパッチの実行時に管理対象デバイスの再起動が必要かどうか。
全デバイス	パッチスケジュールがすべてのデバイス（はい）と選択されたデバイス（No（いいえ））のどちらを対象としているか。
保留中	パッチの実行がスケジュールされている管理対象デバイスの数。このステータスのパッチについて

オプション	説明
	は、デバイスの詳細 ページの セキュリティ セクションに次のいずれかが表示されます。 • 接続を待っています • スケジュール済み • スケジュールを待っています
ダウンロードしています	パッチをダウンロードしている管理対象デバイスの数。このステータスのパッチについては、デバイスの詳細 ページの セキュリティ セクションに次のように表示されます。ダウンロード
実行しています	パッチを実行している管理対象デバイスの数。このステータスのパッチについては、デバイスの詳細 ページの セキュリティ セクションに次のいずれかが表示されます。 • ハンドシェイク • 検出しています • rolling back（ロールバックしています ） • 展開しています • クリーンアップ • 確認しています • 警告しています • アップロード
再起動しています	パッチ適用プロセスの一部として再起動している管理対象デバイスの数。このステータスのパッチについては、デバイスの詳細 ページの セキュリティ セクションに次のいずれかが表示されます。 • 再起動しています • 再起動を保留しています • 接続しています
一時停止しています	パッチ適用プロセスが一時停止しているか再通知設定されている管理対象デバイスの数。このステータスのパッチについては、デバイスの詳細 ページの セキュリティ セクションに次のいずれかが表示されます。 • 再起動が再通知設定されました • 再通知設定されました
成功	パッチ適用プロセスが正常に終了した管理対象デバイスの数。このステータスのパッチについては、デバイスの詳細 ページの セキュリティ セクションに次のように表示されます。完了。

オプション	説明
失敗	パッチ適用プロセス中にエラーが報告された管理対象デバイスの数。このステータスのパッチについては、デバイスの詳細 ページの セキュリティ セクションに次のいずれかが表示されます。 • 中断されました • キャンセルされました
オフライン	パッチ適用プロセスの実行がスケジュールされたときに接続されていなかった管理対象デバイスの数。このステータスのパッチについては、デバイスの詳細 ページの セキュリティ セクションに次のように表示されます。スケジュールなし。
完了	パッチ適用プロセスがステータス 成功、失敗、または オフライン で完了した管理対象デバイスの数。

2. （ オプション ）列の表示を変更するには、右側の表の上部に表示される 表のオプション ドロップダウンリストから **列の表示・非表示** を選択します。

パッチスケジュールの詳細を確認

パッチ適用スケジュールを設定すると、このページにスケジュール設定とそのステータスに関する詳細が表示されます。

1. パッチスケジュールの概要 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **スケジュール** をクリックします。
    d. パッチスケジュールの名前をクリックします。
2. 構成 セクションの内容を確認します。

オプション	説明
作成済み	スケジュールが作成された日付と時刻。
修正日	スケジュールが最後に変更された日付と時刻。
前回の実行	スケジュールが最後に実行された日付と時刻。
名前	スケジュールの名前。
アクション	スケジュールに関連付けられたアクション： • **検出**：管理対象デバイスにインストールされているパッチ、または管理対象デバイスから欠落しているパッチを検出します。パッチダウンロード設定 が、ダウンロード専用に設定されている場合は、検出のみのアクションが推奨されます。展開前に検出のみのアクションを実行すると、展開が始まる前に、ダウン

オプション	説明
	ロードするパッチファイルのリストが作成されます。 • **検出とステージング**：管理対象デバイスにインストールされているパッチまたは管理対象デバイスから欠落しているパッチを検出し、後で展開するためにパッチファイルをエージェントデバイスにダウンロードします。 • **検出と展開**：管理対象デバイスのパッチを検出して展開します。これらのタイプのアクションは、デスクトップとサーバを管理するときに使用されます。検出および展開のパッチ適用ジョブには、デバイスとアプライアンスの間に接続が必要です。これらのジョブはオフラインでは実行されません。メッセージプロトコル接続の詳細については、エージェント通信とログ設定の定義を参照してください。 • **検出、ステージ、およびオンデマンド展開**：管理対象デバイスにインストールされているパッチまたは管理対象デバイスから欠落しているパッチを検出し、パッチファイルをエージェントデバイスにダウンロードし、パッチの展開準備が整ったことをエージェントデバイスの Windows システムトレイでユーザーに警告します。その後、ユーザーは都合に合わせて展開プロセスを開始できます。 ◦ これらのスケジュールは、バージョン 11.0 以降のエージェントを持つ Windows デバイスでのみ使用できます。 ◦ エージェント通信設定で、デバイス上のエージェントステータスアイコン オプションが有効になっている必要があります。これらの設定は、組織の詳細 ページ、通信とエージェントの設定（1 つ以上の組織コンポーネントが有効になっている場合）の下、または 通信設定 ページ（組織コンポーネントがない場合）で確認できます。詳細については、「エージェント通信とログ設定の定義」を参照してください。 • **展開**：管理対象デバイスに適用可能なパッチを展開します。この方法は、管理対象デバイスに特定のパッチを適用する必要があることが分かっている場合に便利です。パッチが適用された後で、または再起動が必要な場合は、デバイスが再起動され、エージェントがアプライアンスと再接続した後で最終検出ジョブが実行されます。 • **検出とロールバック**：管理対象デバイスから不要なパッチを検出して削除します。ロールバックは、一部のパッチには使用できない場合があります。詳細については、「パッチが

オプション	説明
	ロールバック可能であるかどうかの確認」を参照してください。 • **ロールバック**：管理対象デバイスから不要なパッチを削除します。ロールバックは、一部のパッチには使用できない場合があります。詳細については、「パッチがロールバック可能であるかどうかの確認」を参照してください。
説明	パッチスケジュールの簡単な説明。
デバイス	このフィールドは、すべてのデバイスに適用されるようにスケジュールが設定されている場合にのみ表示されます。
デバイスラベル	スケジュールが実行されるデバイスに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したデバイスに適用するようにスケジュールが設定されている場合にのみ表示されます。
デバイス名	スケジュールの実行対象である 1 つまたは複数の選択されたデバイス。このフィールドは、選択したデバイスに適用するようにスケジュールが設定されている場合にのみ表示されます。
検出するパッチ	**検出スケジュールのみ**。このフィールドは、すべてのパッチを検出するようにスケジュールが設定されている場合にのみ表示されます。
ラベルの検出	**検出スケジュールのみ**。スケジュールされたパッチに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したパッチを検出するようにスケジュールが設定されている場合にのみ表示されます。
展開するパッチ	**展開スケジュールのみ**。このフィールドは、すべてのパッチを展開するようにスケジュールが設定されている場合にのみ表示されます。
ラベルの展開	**展開スケジュールのみ**。スケジュールされたパッチに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したパッチを展開するようにスケジュールが設定されている場合にのみ表示されます。
ロールバックするパッチ	**ロールバックスケジュールのみ**。このフィールドは、すべてのパッチを削除するようにスケジュールが設定されている場合にのみ表示されます。

オプション	説明
ロールバックラベル	**ロールバックスケジュールのみ。**スケジュールされたパッチに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したパッチを削除するようにスケジュールが設定されている場合にのみ表示されます。
警告	**展開アクションなしのスケジュールのみ。**パッチアクションの実行時にユーザーに表示されるアラート： • **OK**: すぐに実行されます。 • **キャンセル**: 次のスケジュールされた実行までキャンセルされます。 • **再通知**: 再通知間隔 の経過後に再度プロンプトが表示されます。
再起動	**展開アクションなしのスケジュールのみ。**管理対象デバイスの再起動のオプション： • **再起動しない**：パッチを有効にするために再起動が必要な可能性がある場合でも、デバイスを再起動しません。このオプションはお勧めしません。これは、再起動が必要な場合に、再起動しないでパッチを展開するため、システムが不安定な状態のままになることがあるからです。さらに、再起動が必要なパッチは、再起動後にのみ適用済みとして表示されます。 • **ユーザーにプロンプトを表示**：デバイスを再起動する前に、ユーザーが再起動に同意するまで待ちます。ユーザーが再通知を選択するか、または再起動をキャンセルすると、再起動されるまでパッチ適用は停止します。ターゲットデバイスに表示されるエージェントダイアログボックスで再通知間隔を選択すると、指定した再通知間隔の間、再起動プロンプトが一時停止します。 • **強制的に再起動**：再起動が必要なパッチが展開されるとすぐに再起動されます。強制的な再起動はキャンセルできません。強制的な再起動は、デスクトップとサーバーに対して効果的です。ノートPCの再起動を強制することはお勧めしません。通常サーバーには専属のユーザーがいないため、強制的な再起動はサーバーで効果的に機能します。ただし、サーバがパッチを適用し再起動しているときにサービスが使用できなくなることをユーザーに警告するのは重要です。詳細については、「パッチ適用に関するベストプラクティス」を参照してください。

オプション	説明
スケジュール	選択したスケジュールの詳細。**タスクスケジュールの表示** をクリックして、詳細なタスクスケジューラを表示します。表示されるダイアログボックスで、タスクの詳細を確認するタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。
オフラインの場合は次の接続時に実行	管理対象デバイスが現在オフラインである場合、次回そのデバイスがアプライアンスに接続するときにスケジュールがアクションを実行するかどうかを示します。
再接続後の実行を遅延	設定されている場合、このオプションはスケジュールが遅延する時間を示します。遅延時間は、パッチアクションの実行がスケジュールされている時間から開始されます。
次の後に終了	設定されている場合、このオプションはスケジュールを実行できる最大時間を示します。この制限時間に達すると、進行中のパッチ適用タスクはすべて中断されます。

3. スケジュールステータス セクションで、パッチスケジュールの全体的なステータスを次のいずれかのタブで確認します。

タブ	コンテンツ
マシン別	パッチ適用対象として選択されたデバイス。各エントリには、デバイス名、IP アドレス、パッチ適用ステータス（「パッチ適用ステータスの定義」を参照）、パッチ結果、パッチ適用の完了日が表示されます。デバイスノードを展開して、適用可能なパッチを表示できます。各パッチエントリには、パッチ ID、関連するサポート技術情報記事番号、パッチ名、および現在のステータス（パッチ済み、パッチ未適用、ステージング済み、および検出、ステージ、または展開の失敗）が表示されます。
パッチ別	検出、ステージング、および展開用に選択されたパッチ。各エントリには、パッチ ID、関連するサポート技術情報記事番号、パッチ名、パッチが適用されたデバイス、パッチが適用されていないデバイス、および検出または展開に失敗したデバイスの数が表示されます。
パッチが適用されました	デバイスにパッチが正常にインストールされました。各エントリには、パッチ ID、関連するサポート技術情報記事番号、およびパッチ名が表示されます。パッチノードを展開して、パッチがインストールされたデバイスを表示できます。
パッチ未適用	デバイスにインストールされていないパッチ。各エントリには、パッチ ID、関連するサポート技術情報記事番号、およびパッチ名が表示されます。パッチ

タブ	コンテンツ
	ノードを展開して、パッチをインストールするデバイスを表示できます。
ステージング済み	インストール用にステージングされたパッチ。ステージングとは、後で導入するためにエージェントデバイスにコピーされるパッチファイルのことです。各エントリには、パッチ ID、関連するサポート技術情報記事番号、およびパッチ名が表示されます。パッチノードを展開して、パッチをインストールするデバイスを表示できます。
検出エラー	検出の失敗につながった未完了のパッチ。各エントリには、パッチ ID、関連するサポート技術情報、パッチ名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコード」を参照）。パッチノードを展開して、障害が発生したデバイスを表示できます。
ステージエラー	ステージングの失敗につながった未完了のパッチ。各エントリには、パッチ ID、関連するサポート技術情報記事番号、パッチ名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコード」を参照）。パッチノードを展開して、障害が発生したデバイスを表示できます。
展開エラー	展開の失敗につながった未完了のパッチ。各エントリには、パッチ ID、関連するサポート技術情報、パッチ名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコード」を参照）。パッチノードを展開して、障害が発生したデバイスを表示できます。

4. （**オプション**）スケジュールの詳細を確認した後、次のいずれかのアクションを実行できます。
   - パッチ適用スケジュールを編集するには、**編集** をクリックします。詳細については、「パッチスケジュールの設定」を参照してください。
   - パッチ適用スケジュールを実行するには、**今すぐ実行** をクリックします。
   - パッチ適用スケジュールのコピーを作成するには、**複製** をクリックします。
   - パッチ適用スケジュールを削除するには、**削除** をクリックします。

パッチ適用ステータスの定義

パッチ適用ステータスは、現在のタスクの状態を示します。この情報は、パッチスケジュールの概要 ページのスケジュールステータス セクションに表示されます。詳細については、「パッチスケジュールの詳細を確認」を参照してください。

パッチ適用ステータスの定義

パッチ適用ステータス	定義
警告しています	ユーザーに警告が送信され、確認の待機中です。
キャンセルされました	タスクはユーザーによってキャンセルされました。

パッチ適用ステータス	定義
クリーンアップ	過去 90 日間アクセスがないエージェントからのペイロードファイル。
完了しました	タスクが完了しました。
接続しています	エージェントが再起動後に再接続しています。
展開	パッチの展開が進行中です。
検出	パッチの検出が進行中です。
ダウンロード	パッチ展開はパッケージのダウンロードを待機しています。
エラー	タスクはタイムアウトまたは他のエラーのために完了していません。
スケジュールなし	このデバイスに対してタスクはまだ作成されていません。
事前検出	進行中のエージェントを使用した事前検出。
再起動を保留しています	パッチが展開されました。続行するには再起動が必要です。
再起動が再通知設定されました	パッチが展開されました。続行するには再起動が必要です。設定された間隔が経過すると、エンドユーザーには再起動するように求めるメッセージが表示されます。
ロールバックしています	パッチのロールバックが進行中です。
スケジュール済み	タスクはスケジュール済みで、実行を待機中です。
再通知設定されました	タスクは再通知になりました。設定された再通知間隔が過ぎるとユーザーにメッセージが表示されます。
ステージ	後で展開できるようにファイルをダウンロードしています。
中断されました	タスクは完了する前に停止されました。
ログをアップロードしています	事前検出、検出、展開、検証、またはロールバックログをアップロードしています。
確認しています	展開後の検証の検出が進行中です。
バージョンチェック	タスクがパッチバージョンを確認しています。

パッチ適用ステータス	定義
オンデマンド展開を待っています	タスクがユーザーアクションによりスケジュールが展開されるのを待機しています。
接続を待っています	デバイスが切断されました。
スケジュールを待っています	タスクはエージェントのタイムゾーンでスケジュールを待機しています。

パッチステータスの表示

パッチが展開されたデバイスのリストを含む、パッチのステータスを表示できます。

1. パッチの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **カタログ** をクリックします。
2. 導入ステータス 表までスクロールします。

    この表には、パッチが展開されたデバイスのリストを含む、パッチの詳細が表示されます。

デバイス別のパッチステータスの表示

管理対象デバイスごとにパッチのステータスを表示できます。

1. 組織の デバイスの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
    c. デバイスの名前をクリックします。
2. セキュリティ セクションまでスクロールし、**パッチ適用の検出/デプロイのステータス** リンクをクリックします。

デバイスにインストールされたパッチのリストが表示されます。

パッチ内のファイルの表示

各パッチに含まれているファイルを表示することができます。

1. パッチの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **カタログ** をクリックします。
2. 関連付けられたファイル 表までスクロールします。

パッチレポートの表示

パッチ適用に関連するレポートを参照することができます。

1. パッチ管理の レポート ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **レポート作成** をクリックします。

    特定基準で表示 ドロップダウンリストで選択した **パッチ適用** について、レポート ページが開きます。このページには、パッチ関連のレポートへのリンクが含まれています。

パッチロールバックの管理

パッチでロールバックがサポートされている場合は、パッチをロールバックして管理対象デバイスから削除できます。

ただし、一部のベンダーおよびパッチタイプではロールバックはサポートされていません。例えば、サービスパックのような大規模なソフトウェアパッチをロールバックすることはできません。

パッチがロールバック可能であるかどうかの確認

パッチカタログ ページを検索することで、管理対象デバイスにパッチが展開された後に、そのパッチをロールバックできるかどうかを確認することができます。

1. パッチの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **カタログ** をクリックします。
    d. パッチの名前をクリックします。
2. 右側のリストの上にある **高度な検索** タブをクリックして、高度な検索 パネルを表示します。
3. 次の検索条件を入力します。

    パッチリスト情報: ロールバックのサポート | は | True
4. **オプション** : 追加の検索条件を入力します。
5. **検索** をクリックします。

ロールバックをサポートするパッチが表示されます。

前回のパッチ適用ジョブを元に戻す

パッチベンダーがロールバックをサポートしている場合は、ロールバックのパッチスケジュール、または検出とロールバックのパッチスケジュールの作成と実行により、前回のパッチ展開を元に戻すことができます。

1. パッチスケジュールの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。

c. パッチ管理 パネルで **スケジュール** をクリックします。

d. パッチスケジュールの名前をクリックします。

2. アクション ドロップダウンリストで、**ロールバック** または **検出とロールバック** を選択します。

3. 元のスケジュールでパッチを指定したときと同様、Smart Labelを作成して、ロールバックするパッチを選択します。

   詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。

   このオプションは、1つのソフトウェアアプリケーションからの前回にインストールしたパッチの削除のみをサポートしています。詳細については、「パッチロールバックの管理」を参照してください。

4. 必要に応じて、パッチスケジュールのその他の設定を指定します。

   詳細については、「パッチスケジュールの設定」を参照してください。

パッチインベントリの管理

アプライアンスにダウンロードされたパッチは、パッチインベントリと呼ばれます。パッチインベントリに関する詳細と統計を表示し、パッチをアクティブまたは非アクティブとマークできます。さらに、ラベルを使用してパッチを管理できます。

パッチインベントリの管理に関する前提条件

パッチインベントリを管理するには、パッチをサブスクライブし、ダウンロードする必要があります。

詳細については、以下を参照してください。

- パッチのサブスクライブとダウンロード設定項目の設定
- パッチおよび機能更新プログラムのダウンロード設定の選択

パッチ情報の表示

必要に応じて、パッチに関する情報およびデバイスのパッチ情報を表示できます。

ダウンロードされたパッチの表示

パッチカタログ リストには、サブスクライブしているパッチ向けにダウンロードされたパッチ検出署名が表示されます。

1. パッチの カタログ ページに移動します。

   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。

   c. パッチ管理 パネルで **カタログ** をクリックします。

2. このドロップダウンリストを使用して、パッチを一覧表示します。

   - **特定基準で表示：選択したドロップダウンリストに基づいて、リストに表示されるパッチを制御します。**

列	説明
すべてのパッチ	すべてのパッチを表示します。
ラベル	ラベルを使用してタグ付けされたパッチを表示します。この情報は、ラベルが作成されている場合にのみ表示されます。
ステータス	「**アクティブ**」、「**無効**」、または「**非アクティブ**」というステータスのパッチを表示します。
ダウンロードステータス	「**ダウンロードされました**」または「**ダウンロードされませんでした**」というダウンロードステータスのパッチを表示します。
重要度	Microsoftなどのベンダーが指定している重要度に基づいて、パッチリストをフィルタリングします。重要度のレベルには、「**緊急**」、「**重要**」、「**低**」などがあります。
最近	最近追加されたパッチを表示します。**過去 1 か月**、**過去 6 か月**、**過去 1 年**、または **過去 2 年** に追加されたパッチを表示できます。
年	リリースされた年に基づいて、パッチリストをフィルタリングします。
オペレーティングシステム	オペレーティングシステムに基づいて、パッチリストをフィルタリングします。

3. パッチカタログ ページの列には、次の情報が表示されます。

列	説明
ステータス	パッチの状態：アクティブ、非アクティブ、または無効。 • **アクティブ**：サブスクライブしているパッチでダウンロードされたパッチ、および検出または展開の準備ができているパッチ。 • **非アクティブ**：サブスクライブしているパッチだが、「非アクティブ」とマークされていて自動的に検出または展開できないパッチ • **無効**: サブスクリプションに一致しないパッチ。これらのパッチは、パッチサブスクリプションで 無効なパッチの検出 オプションが有効になっている場合にのみ検出できます。サブスクリプション条件に合わない場合、これらのパッチは展開できません。
パッケージ	パッチ識別情報。パッチに適用されているラベルは、この列にも表示されます。
名前	パッチの名前。

列	説明
リリース済み	パッチが提供開始された日付。
発行元	パッチの発行元の名前。
重要度	発行元（Microsoftなど）が決定したパッチの重要度。
再起動	パッチ適用プロセスを完了するためにデバイスを再起動する必要があるかどうか。
コンプライアンス	スケジュールされたパッチに対するインストール済みのパッチの割合。
インストール済み	パッチを受け取ったデバイスの数。
不在	パッチが必要であると検出されたデバイスの数、および展開を待っているデバイスの数。
エラー	展開の最大試行回数失敗したデバイスの数。展開の最大試行回数はパッチスケジュールで設定します。詳細については、「パッチスケジュールの設定」を参照してください。
サイズ	パッチファイルのサイズ。 • **黒色**: 非アクティブまたは無効なパッチ。 • **赤色**: サブスクライブしているパッチ。ただし、このパッチに対して関連付けられたパッケージは今回はダウンロードされていません。不足している関連付けられたパッケージを確認するには、パッチの名前をクリックし、パッチの詳細 ページを表示します。 • **サイズ= 0**: ダウンロードされたパッチパッケージはありません。 • **実際のサイズ**（ゼロ以外）: パッチパッケージのうち最低1つがダウンロードされました。
廃止	他のパッチに置き換えられ、不要になったパッチ。

パッチの詳細の表示

パッチの詳細には、ベンダー情報、展開ステータス、およびメモが含まれます。また、パッチの詳細を表示するときに、パッチにラベルを割り当てることができます。

1. パッチの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **カタログ** をクリックします。

d. パッチ名をクリックします。

パッチの詳細 ページが表示され、パッチに関する完全な情報が表示されます。

パッチ展開の試行回数のリセット

パッチ展開が設定済みの最大回数試行された場合、再試行の回数をリセットすることができます。

展開の最大試行回数を設定するには、パッチスケジュールの設定を参照してください。

展開の試行回数は、カタログ リストと パッチの詳細 ページの 2 つの場所でリセットできます。

- パッチカタログリストからパッチ展開の試行回数をリセットするには、パッチのカタログからのパッチ展開の試行回数のリセットを参照してください。
- パッチの詳細ページからパッチ展開の試行回数をリセットするには、パッチの詳細 ページからのパッチ展開の試行回数のリセットを参照してください。

パッチのカタログからのパッチ展開の試行回数のリセット

パッチ展開が設定済みの最大回数試行された場合、パッチの カタログ ページから再試行の回数をリセットできます。

1. パッチの カタログ ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
   c. パッチ管理 パネルで **カタログ** をクリックします。
2. リストの1つまたは複数のパッチ/通知の隣のチェックボックスをオンにし、**アクションの選択 > 試行回数のリセット** を選択します。

   展開の試行回数が0にリセットされます。

パッチの詳細 ページからのパッチ展開の試行回数のリセット

パッチ展開が設定済みの最大回数試行された場合、パッチの詳細 ページから再試行の回数をリセットできます。

1. カタログ リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
   c. パッチ管理 パネルで **カタログ** をクリックします。
2. 次のいずれかを実行して、Patch Detail（ パッチの詳細 ）ページを表示します。
   - **表示** ドロップダウンリストが、**Applicable Packages**（ 適用可能なパッケージ ）または **All Packages**（ すべてのパッケージ ）に設定されている場合は、パッケージの名前をクリックし、次にパッケージ内のパッチの名前をクリックします。
   - **表示** ドロップダウンリストが、「**Individual Patches**」に設定されている場合は、パッチの名前をクリックします。
3. 導入ステータス セクションまでスクロールし、**試行回数のリセット** ボタンをクリックします。

   展開の試行回数が0にリセットされます。

インベントリ内のデバイスのパッチ情報の表示

インベントリ セクションには、管理対象デバイスについての詳細なパッチ情報が表示されます。

この情報には次のものが含まれます。

- デバイスに展開されたパッチのリスト
- デバイスに適用されるパッチスケジュールの詳細
- 成功および失敗したパッチ適用とロールバックの試行についての情報

1. 組織の デバイスの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
    c. デバイスの名前をクリックします。
2. セキュリティ セクションまでスクロールします。
3. **パッチ適用の検出/デプロイのステータス** をクリックして、「パッチ適用の検出/デプロイのステータス」の詳細を展開します。
4. 詳細については、スケジュール済みタスクのステータス および 導入ステータス の隣にある **ヘルプ** ボタンをクリックします：。

パッチ未適用のデバイスの表示

パッチが未適用のデバイスを表示して、更新されていない理由を確認することができます。

1. パッチカタログ リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
    c. パッチ管理 パネルで **カタログ** をクリックします。
2. カタログリストの上で、パッチ未適用のデバイス の後にある数字をクリックします。

    デバイス リストが開き、パッチ未適用のデバイスがすべて表示されます。

パッチ適の統計とログの表示

パッチの統計とログは、アプライアンスのパッチ適用タスクの概要を提供します。

パッチ適用の統計の表示

パッチの統計は、パッチ管理パネルで表示することができます。

1. パッチ管理 パネルに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。

パッチ管理 パネルが表示され、パッチの統計が表示されます。

パッチログの表示

パッチログを表示して、パッチのダウンロードプロセス中のエラーを確認できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**ログ** をクリックして、ログ ページを表示します。
3. Log（ ログ ）ドロップダウンリストで、**パッチダウンロードのログ** を選択します。

パッチログが表示されます。

パッチの非アクティブのマーク付け

サブスクライブしているパッチを非アクティブにマークし、自動的に検出または展開できないようにすることができます。

1. パッチカタログ リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。
   c. パッチ管理 パネルで **カタログ** をクリックします。
2. パッチの隣のチェックボックスをオンにします。
3. **アクションの選択 > 次にステータスを変更 > 非アクティブ** を選択します。

表示 ドロップダウンリストが、**適用可能なパッケージ** または **すべてのパッケージ** に設定されている場合は、選択した掲示板を構成するすべてのパッチが非アクティブとマークされます。**表示** ドロップダウンリストが、**Individual Patches** に設定されている場合は、選択したすべてのパッチが非アクティブとマークされます。非アクティブとマークされたすべてのパッチは、次回のスケジュールされたパッチダウンロード中に、キャッシュから自動的に消去されます。

Mac OS Xデバイスへのパッチの適用

必要に応じて、パッチをMac OS Xデバイスに適用できます。

1. パッチカタログ リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**パッチ管理** をクリックします。

c. パッチ管理 パネルで **カタログ** をクリックします。

2. 次のいずれかを実行します。
   - **テーブルの上の** 特定基準で表示 **ドロップダウンリストで、オペレーティングシステム > Mac <OS X> を選択します。**
   - **テーブルの上に表示される高度な検索 タブをクリックして、Mac OS Xパッチを検索します。**
   - **Smart Label機能を使用すると、定義済み検索条件に基づいてパッチリストが自動的に検索されます。**
3. アプライアンスがMac用のAppleセキュリティ更新プログラムをダウンロードできるようにするには、パッチのサブスクリプション設定 ページで Macプラットフォーム リストから該当するオペレーティングシステムを選択します。

   複数のMacオペレーティングシステムを選択できます。詳細については、次を参照してください。 パッチのサブスクライブ

Windows 機能更新プログラムの管理

Windows 機能更新プログラムは、Microsoft Windows 10 の新しいバージョンで、毎年数回リリースされています。アプライアンスを使用すると、これらの更新プログラムのインストールプロセスを自動化して、管理対象の Windows 10 デバイスのパフォーマンスを向上させ、潜在的な OS 関連の脆弱性から保護することができます。

アプライアンスを使用して、アプライアンスによって管理されている Windows 10 デバイス用の最新の Windows Feature Update を検出して展開します。

注: この機能は、半年に 1 度のチャネルサブスクリプションを使用する Windows 10 デバイスでのみサポートされています。10 以外の OS バージョンを実行している Mac、Linux、または Windows デバイスでは使用できません。

Windows 機能更新プログラムのサブスクライブ

管理対象の Microsoft Windows 10 デバイスの Windows 機能更新プログラムをサブスクライブできます。

Windows 機能更新プログラムをサブスクライブしてダウンロードする前に、管理対象デバイスにインストールされているオペレーティングシステムを識別し、更新の要件を確認してください。ダウンロードできるのは、管理対象の Windows 10 デバイスの更新プログラムのみです。

1. Windows 機能更新プログラムのサブスクリプション ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの ー般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Windows 機能更新プログラム** をクリックします。
   c. Windows 機能更新プログラム パネルで **サブスクリプション** をクリックします。
2. 「サブスクリプション」設定を指定します。ダウンロードされるパッチは、サブスクリプションで指定されたオペレーティングシステムと口ケールによって制御されます。

オプション	説明
Windows 機能更新プログラムのバージョン	選択した Windows 機能更新プログラムをダウンロードします。編集 ボタンをクリックして、オペレーティングシステムのリストを管理します: をクリックします。**バージョンの選択** をクリックし、管理対象の Windows 10 デバイスにインストールす

オプション	説明
	る 1 つまたは複数の更新プログラムバージョンを選択します。Windows 機能更新プログラムを無視するには、**無効** を選択します。 選択したアイテムは、設定を保存した後に表示されます。
ロケール	選択された言語のパッチをダウンロードします。**編集** ボタンをクリックして、ロケールのリストを管理します: をクリックします。ロケールに関係なくパッチをダウンロードするには、**すべてのロケール** を選択するか、1つまたは複数の口ケールの横にあるチェックボックスをオンにします。 選択したアイテムは、設定を保存した後に表示されます。

注: Windows 機能更新プログラムサブスクリプションの少なくとも 1 つのバージョンと 1 つの口ケールを選択する必要があります。

3. **保存** をクリックします。

次回のスケジュールされたダウンロード時間に、選択した Windows 機能更新プログラムは自動的にダウンロードされます。

次に、Windows Feature Update のダウンロード設定を構成できます。詳細については、「パッチおよび機能更新プログラムのダウンロード設定の選択」を参照してください。

Windows 機能更新プログラムのスケジュールの設定

Windows 機能更新プログラムのスケジュールを作成および設定し、その実行時間をスケジュールすることができます。Windows 機能更新プログラムのスケジュールは、管理対象インストールやその他の配布には干渉しません。

1. Windows Feature Update のスケジュールの詳細 ウィザードの開始：
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Windows 機能更新プログラム** をクリックします。
   c. Windows 機能更新プログラム パネルで **スケジュール** をクリックします。
   d. Windows Feature Update スケジュール リストページで、次のいずれかを実行します。

   - スケジュールの詳細 ウィザード使用して新しい Windows Feature Update スケジュールを作成するには、**アクションの選択 > 新規作成（ウィザード）** の順にクリックします。
   - スケジュールの詳細 ページを使用して新しい Windows Feature Update のスケジュールを作成するには、**アクションの選択 > 新規作成（クラシック）** の順にクリックします。
   - 既存のスケジュールを編集するには、リスト内のスケジュール名をクリックし、表示される Windows Feature Update スケジュール概要 ページで **編集** をクリックします。

     選択した スケジュールの詳細 ページまたはウィザードが表示されます。各選択で同じオプションを使用できます。必要に応じて、右上隅にある **クラシックビュー** または **ウィザードビュー** をクリックして、ページとウィザードを切り替えることができます。

2. スケジュールに関する一般的な情報を設定します。

オプション	説明
名前	スケジュールを識別するための名前。この名前は、Windows 機能更新プログラムのスケジュールリストページに表示されます。
説明	Windows Feature Update スケジュールの簡単な説明。

3. Windows 機能更新プログラムの選択 セクションで、次のオプションを設定します。

オプション	説明
ビルドの選択	検出、ステージング、または展開する Windows 機能更新プログラムIのバージョンを選択します。このセクションには、サブスクリプションで選択した更新が一覧表示されます。
エディションの選択	選択したバージョンの 1 つまたは複数のエディションを選択します。このセクションでは、選択したバージョンのすべてのエディションが一覧表示されます。たとえば、異なるプラットフォーム（32 ビットと 64 ビット）の Business エディションと Consumer エディションなどです。

4. 次のいずれかのアクションを選択します。

   これらのアクションは、パッチスケジュールアクションと同じです。詳細については、「パッチスケジュールの設定」を参照してください。

アクション	説明
検出	互換性のある Windows 機能更新プログラムをスキャンします。
検出とステージ	互換性のある Windows 機能更新プログラムをスキャンし、後で展開できるように、該当するファイルをエージェントデバイスにダウンロードします。
検出、ステージ、およびオンデマンド展開	管理対象デバイスにインストールされている、または管理対象デバイスから欠落している Windows Feature Update を検出し、該当するファイルをエージェントデバイスにダウンロードして、Windows システムトレイアイコンでユーザーに警告します。 • これらのスケジュールは、バージョン 11.0 以降のエージェントを持つ Windows デバイスでのみ使用できます。 • エージェント通信設定で、デバイス上のエージェントステータスアイコン オプションが有効になっている必要があります。これらの設定は、組織の詳細 ページ、通信とエージェントの設定（1 つ以上の組織コンポーネントが有効になっている場合）の下、または 通信設定 ページ（組織コンポーネントがない場合）で確認できます。詳細については、「エージェント通信とログ設定の定義」を参照してください。

アクション	説明
検出と展開	互換性のある Windows 機能更新プログラムをスキャンし、該当するファイルをエージェントデバイスにダウンロードして、選択したデバイスに更新プログラムを展開します。

5. 次のオプションを使用してターゲットデバイスを選択します。

   これらのオプションは、パッチスケジュールアクションに表示されるオプションと同じです。詳細については、「パッチスケジュールの設定」を参照してください。

アクション	説明
全デバイス	このスケジュールをすべての管理対象デバイスに適用するには、このオプションを選択します。パッチアクションを特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
デバイスラベル	ここで選択したラベルを使用して機能更新へのアクションを制限します。これは、最も一般的に使用されるオプションです。 a. **関連ラベルの管理** をクリックします。 b. 表示された ラベルを選択 ダイアログボックスで、1 つ以上のラベルを 実行の制限対象 領域にドラッグし、**OK** をクリックします。 このオプションを使用するには、機能の更新に Smart Label が既に存在している必要があります。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
デバイス	選択したデバイスでパッチアクションを実行します。 • デバイスを検索するには、フィールドに入力し始めます。 • 指定されたすべてのデバイスを削除してから再起動するには、**すべて削除** をクリックします。 • スコープユーザーは、役割にラベルが割り当てられている場合に、自身の役割に関連付けられているデバイスだけを表示できます。ユーザーの役割の詳細については、ユーザーの役割の追加または編集を参照してください。

6. スケジュール セクションで、スケジュールに適用可能なオプションを指定します。

   これらのオプションは、パッチスケジュールアクションに表示されるオプションと同じです。詳細については、「パッチスケジュールの設定」を参照してください。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。このオプションは、サーバーに手動でパッチを適用するか、または定期的に実行しないパッチアクションを実行する場合に便利です。

オプション	説明
毎 _ 時間	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
毎月 / 特定月の n 日、HH:MM に実行	毎月n日（例えば、毎月1日または2日）、または特定の月、特定の時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。

オプション	説明
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。
タイムゾーン	アクションをスケジュールするときに使用するタイムゾーン。**サーバー** を選択すると、アプライアンスのタイムゾーンを使用します。**エージェント** を選択すると、管理対象デバイスのタイムゾーンを使用します。
オフラインの場合は次の接続時に実行	管理対象デバイスが現在オフラインである場合、次回管理対象デバイスがアプライアンスに接続するときにアクションを実行します。このオプションは、定期的にオフラインになるノートPCおよびその他のデバイスに対して役立ちます。このオプションが選択されていない場合でデバイスがオフラインのときは、次回のスケジュールされた時間までアクションは再度実行されません。
再接続後の実行を遅延	指定した時間、スケジュールを遅延させます。遅延時間は、パッチアクションの実行がスケジュールされている時間から開始されます。
次の時間の経過後に終了:	パッチ適用アクションの期限。 例えば、04:00にパッチが実行されるようスケジュールする場合、07:00にパッチ適用アクションをすべて停止し、ユーザーが業務を開始するときに帯域幅の問題が発生しないようにすることができます。これを行うには、分 ボックスで「**180**」を指定します。 期限に到達すると、進行中のパッチ適用タスクはすべて中断され、これらのタスクに対するセキュリティログのステータスは「中断されました」になります。 これらのパッチ適用タスクは次回実行で再開されず、スケジュール済みの毎回のパッチ適用アクションで最初から開始されます。

7. **保存** をクリックします。

   Windows Feature Update スケジュール概要 ページが表示され、新しく作成または更新されたスケジュールが表示されます。このページの詳細については、「Windows Feature Update のステータスの表示」を参照してください。

   - Smart Label の基準に一致するデバイスを追加した場合、それらのデバイスは更新スケジュールに自動的に含まれます。
   - 更新プログラムがエージェントデバイスにダウンロードされ、導入の準備が整ったら、Windows システムトレイとメニューで KACE エージェントアイコンが更新され、エージェントがアクションを使用できることが示されます。更新プログラムをインストールするには、エージェントデバイスの Windows システムトレイで KACE エージェントをクリックし、**Deploy staged patches**（ステージングされたパッチの展開）を選択します。KACE エージェントアイコンの詳細については、

「Windows システムトレイを使用して Windows デバイスで KACE エージェントを管理する」を参照してください。

Windows 機能更新プログラムのスケジュールの表示

アプライアンスに存在する Windows 機能更新プログラムのスケジュールの概要情報を表示できます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織の Windows Feature Update のスケジュールを個別に表示します。

1. Windows 機能更新プログラムのスケジュール ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Windows 機能更新プログラム** をクリックします。
2. Windows 機能更新プログラム パネルで **スケジュール** をクリックします。

    Windows 機能更新プログラムのスケジュール ページで使用できる列は、パッチスケジュール ページの列と同じです。パッチスケジュール ページに表示されるフィールドの詳細については、「パッチスケジュールのリストを表示する」を参照してください。
3. （ オプション ）列の表示を変更するには、右側の表の上部に表示される 表のオプション ドロップダウンリストから **列の表示・非表示** を選択します。

Windows Feature Update スケジュールの詳細を確認する

Windows Feature Update スケジュールを設定すると、このページにスケジュール設定とそのステータスに関する詳細が表示されます。

1. Windows Feature Update スケジュール概要 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Windows 機能更新プログラム** をクリックします。
    c. Windows 機能更新プログラム パネルで **スケジュール** をクリックします。
    d. Windows 機能更新プログラムスケジュールの名前をクリックします。
2. 構成 セクションの内容を確認します。

オプション	説明
作成済み	スケジュールが作成された日付と時刻。
修正日	スケジュールが最後に変更された日付と時刻。
前回の実行	スケジュールが最後に実行された日付と時刻。

オプション	説明
名前	スケジュールを識別するための名前。この名前は、Windows 機能更新プログラムのスケジュールリストページに表示されます。
アクション	スケジュールに関連付けられたアクション： • **検出**：互換性のある Windows 機能更新プログラムをスキャンします。 • **検出とステージング**：互換性のある Windows 機能更新プログラムをスキャンし、後で展開できるように、該当するファイルをエージェントデバイスにダウンロードします。 • **検出、ステージ、およびオンデマンド展開**：管理対象デバイスにインストールされている、または管理対象デバイスから欠落している Windows Feature Update を検出し、該当するファイルをエージェントデバイスにダウンロードして、エージェントデバイスの Windows システムトレイで、更新プログラムを展開する準備が整ったことをユーザーに警告します。その後、ユーザーは都合に合わせて展開プロセスを開始できます。 ◦ これらのスケジュールは、バージョン 11.0 以降のエージェントを持つ Windows デバイスでのみ使用できます。 ◦ エージェント通信設定で、デバイス上のエージェントステータスアイコン オプションが有効になっている必要があります。これらの設定は、組織の詳細 ページ、通信とエージェントの設定（1 つ以上の組織コンポーネントが有効になっている場合）の下、または 通信設定 ページ（組織コンポーネントがない場合）で確認できます。詳細については、「エージェント通信とログ設定の定義」を参照してください。 • **検出と展開：**互換性のある Windows 機能更新プログラムをスキャンし、該当するファイルをエージェントデバイスにダウンロードして、選択したデバイスに更新プログラムを展開します。
説明	Windows Feature Update スケジュールの簡単な説明。
デバイス	このフィールドは、すべてのデバイスに適用されるようにスケジュールが設定されている場合にのみ表示されます。
Windows Feature Update	Windows Feature Update の名前とバージョン。

オプション	説明
デバイスラベル	スケジュールが実行されるデバイスに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したデバイスに適用するようにスケジュールが設定されている場合にのみ表示されます。
デバイス名	スケジュールの実行対象である 1 つまたは複数の選択されたデバイス。このフィールドは、選択したデバイスに適用するようにスケジュールが設定されている場合にのみ表示されます。
ラベルの検出	スケジュールされたアップデートに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したアップデートを検出するようにスケジュールが設定されている場合にのみ表示されます。
警告	**検出と展開スケジュールのみ**。更新アクションの実行時にユーザーに表示される警告： • **OK**: すぐに実行されます。 • **キャンセル**: 次のスケジュールされた実行までキャンセルされます。 • **再通知**: 再通知間隔 の経過後に再度プロンプトが表示されます。 **注:** アラートは、検出、および検出とステージスケジュールでは使用できません。
再起動	**検出と展開スケジュールのみ**。管理対象デバイスの再起動のオプション： • **再起動しない**：更新を有効にするために再起動が必要な可能性がある場合でも、デバイスを再起動しません。このオプションはお勧めしません。これは、再起動が必要な場合に、再起動しないで更新プログラムを展開するため、システムが不安定な状態のままになることがあるからです。さらに、再起動が必要な更新プログラムは、再起動後にのみ適用済みとして表示されます。 • **ユーザーにプロンプトを表示**：デバイスを再起動する前に、ユーザーが再起動に同意するまで待ちます。ユーザーが再通知を選択するか、または再起動をキャンセルすると、再起動されるまで更新は停止します。ターゲットデバイスに表示されるエージェントダイアログボックスで再通知間隔を選択すると、指定した再通知間隔の間、再起動プロンプトが一時停止します。 • **強制的に再起動**：再起動が必要なアップデートが展開されるとすぐに再起動されます。強制的な再起動はキャンセルできません。強

オプション	説明
	制的な再起動は、デスクトップとサーバーに対して効果的です。ノートPCの再起動を強制することはお勧めしません。通常サーバーには専属のユーザーがいないため、強制的な再起動はサーバーで効果的に機能します。ただし、サーバが更新され、再起動しているときにサービスが使用できなくなることをユーザーに警告するのは重要です。詳細については、「パッチ適用に関するベストプラクティス」を参照してください。
スケジュール	選択したアップデートスケジュール。**タスクスケジュールの表示** をクリックして、詳細なタスクスケジューラを表示します。表示されるダイアログボックスで、タスクの詳細を確認するタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。
オフラインの場合は次の接続時に実行	管理対象デバイスが現在オフラインである場合、次回そのデバイスがアプライアンスに接続するときにスケジュールがアクションを実行するかどうかを示します。
再接続後の実行を遅延	設定されている場合、このオプションはスケジュールが遅延する時間を示します。遅延時間は、更新アクションの実行がスケジュールされている時間から開始されます。
次の後に終了	設定されている場合、このオプションはスケジュールを実行できる最大時間を示します。この制限時間に達すると、進行中の更新タスクはすべて中断されます。

3. スケジュールステータス セクションで、次のいずれかのタブで全体的なスケジュールのステータスを確認します。

タブ	コンテンツ
マシン別	更新対象として選択されたデバイス。各エントリには、デバイス名、IP アドレス、更新ステータス（「パッチスケジュールの詳細 ページのフィールド」を参照）、更新の結果、更新の完了日が表示されます。デバイスノードを展開して、適用可能なアップデートを表示できます。各エントリには、更新 ID、関連する技術情報記事番号、更新名、および現在のステータス（インストール済み、未インストール、ステージング済み、および検出、ステージ、または展開の失敗）が表示されます。
Feature Update 別	検出、ステージング、および展開用に選択されたアップデート。各エントリには、更新 ID、関連するサポート技術情報記事番号、更新名、更新されるデバイスの数、更新されないデバイスの数、および検出または展開の失敗が発生したデバイスの数が表示されます。

タブ	コンテンツ
インストール済み	デバイスに正常にインストールされたアップデート。各エントリには、更新 ID、関連するサポート技術情報記事番号、および更新名が表示されます。アップデートノードを展開して、アップデートがインストールされるデバイスを表示できます。
インストールされませんでした	デバイスにインストールされていないアップデート。各エントリには、更新 ID、関連するサポート技術情報記事番号、および更新名が表示されます。アップデートノードを展開して、アップデートがインストールされるデバイスを表示できます。
ステージング済み	インストール用にステージングされたアップデート。ステージングとは、後で導入するためにエージェントデバイスにコピーされるアップデートファイルのことです。各エントリには、更新 ID、関連するサポート技術情報記事番号、および更新名が表示されます。アップデートノードを展開して、アップデートがインストールされるデバイスを表示できます。
検出エラー	検出の失敗につながった未完了のアップデート。各エントリには、更新 ID、関連するサポート技術情報、更新名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコード」を参照）。アップデートノードを展開して、障害が発生したデバイスを表示できます。
ステージエラー	ステージングの失敗につながった未完了のアップデート。各エントリには、更新 ID、関連するサポート技術情報記事番号、更新名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコード」を参照）。アップデートノードを展開して、障害が発生したデバイスを表示できます。
展開エラー	展開の失敗につながった未完了のアップデート。各エントリには、更新 ID、関連するサポート技術情報、更新名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコード」を参照）。アップデートノードを展開して、障害が発生したデバイスを表示できます。

4. （**オプション**）スケジュールの詳細を確認した後、次のいずれかのアクションを実行できます。
   - アップデートスケジュールを編集するには、**編集** をクリックします。詳細については、「Windows 機能更新プログラムのスケジュールの設定」を参照してください。
   - アップデートスケジュールを実行するには、**今すぐ実行** をクリックします。
   - アップデートスケジュールのコピーを作成するには、**複製** をクリックします。
   - 更新スケジュールを削除するには、**削除** をクリックします。

利用可能な Windows 機能更新プログラムの表示

Windows 機能更新プログラムをサブスクライブし、更新プログラムがダウンロードされたら、利用可能な更新プログラムを表示できます。

関連する更新プログラムを表示するには、Windows 機能更新プログラムのバージョンをサブスクライブし、機能更新プログラムのダウンロード設定を選択する必要があります。詳細については、以下を参照してください。

- Windows 機能更新プログラムのサブスクライブ
- パッチおよび機能更新プログラムのダウンロード設定の選択

1. Windows 機能更新プログラム リストページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Windows 機能更新プログラム** をクリックします。
    c. Windows 機能更新プログラム パネルで **カタログ** をクリックします。
2. Windows 機能更新プログラムを検索します。
    a. 検索ボックスに検索条件を入力します。

    例えば、「1909」と入力します。

    b. **Enter** を押します。

    リストページが更新され、バージョンが 1909 の Windows 機能更新プログラムのみが表示されます。

Windows Feature Update のステータスの表示

Windows Feature Update の詳細には、ベンダー情報と展開ステータスが含まれます。

1. Windows Feature Update の詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Windows 機能更新プログラム** をクリックします。
    c. Windows 機能更新プログラム パネルで **カタログ** をクリックします。
    d. Windows Feature Update 名をクリックします。

    Windows Feature Update の詳細 ページが表示され、選択した Windows Feature Update に関する完全な情報が表示されます。

Dellデバイスおよびアップデートの管理

アプライアンスを使用して Dell からのデバイスの更新を管理できます。

これらの更新には、以下が含まれます。

- サーバー用のソフトウェアおよびファームウェア
- クライアントデバイス用のソフトウェアおよびファームウェア
- デルが提供する一部のアプリケーション

注: サーバおよびクライアントデバイスは、ユーザーのサーバまたはクライアント OS ではなく、Dell サーバおよびクライアントハードウェアを指します。

アップデートが必要な Dell デバイスには、クライアントまたはサーババージョンのいずれかの Dell Open Manage インベントリエージェントをインストールしておく必要があります（該当する場合）。このコンポーネントはデフォルトですべての Dell アップデートに含まれているため、手動で追加する必要はありません。Dell Open Manage インベントリクライアントがターゲットデバイスに存在しない場合、最初の導入プロセス中にインストールされます。

注: Dell ハードウェアアップデートは、KACE エージェントが 11.1 以上の場合にのみ機能します。古いエージェントのバージョンでは、この機能はサポートされません。

サポートされている Dell モデル レポートを実行して、どの Dell コンピュータの Dell クライアントアップデートがサポートされているかを確認します。詳細については、「各組織レポートと総合レポートの実行」を参照してください。

パッチ適用とDellアップデートの相違点

パッチ適用とDellアップデートの相違点には、サブスクリプションプロセス、アクション名、および管理プロセスの場所の違いがあります。

パッチ適用とDellアップデートの相違点は次の通りです。

- アップデートが必要な Dell デバイスには、クライアントまたはサーババージョンのいずれかの Dell Open Manage インベントリエージェントをインストールしておく必要があります（該当する場合）。
- Dell アップデートのサブスクリプションプロセスはアプライアンスのパッチサブスクリプションプロセスと異なる。Dell アップデートのサブスクライブ手順については、Dell アップデートのダウンロード設定の選択を参照してください。
- 以下のパッチ適用アクションに使用される名前が異なる。

アクション	パッチ適用の用語	Dellアップデートの用語	用語の使用場所
管理するデバイスにパッチまたは更新をインストールする。	展開	更新	Dellデバイスおよびアップデートの管理

- 次のように、パッチ適用と Dell アップデートを管理および実行する**管理者コンソール**内の場所が異なる。

アクション	検索場所
Dellアップデートを実行する。	**セキュリティ > Dellアップデート**
Dellアップデートを管理する。	アプライアンスで組織コンポーネントが**有効化されていない**場合： **管理者コンソール > 設定 > Dell アップデートのダウンロード設定** アプライアンスで組織コンポーネントが**有効化されている**場合：

アクション	検索場所
	システム管理コンソール > システム > 設定 > Dell アップデートのダウンロード設定
パッチスケジュールを実行する。	**セキュリティ > スケジュール**
パッチ適用を管理する。	**セキュリティ > サブスクリプション**

Dell アップデートのダウンロード設定の選択

デバイスのアップデートスケジュールを作成するには、カタログ更新の設定とスケジュール作成を事前に行う必要があります。

Dell アップデートパッケージは、**カタログ**形式で、サーバー用とクライアント用に 1 部ずつ提供されます。

1. Dell アップデートのダウンロード設定 ページに移動します。
   - **アプライアンスで組織コンポーネントが有効になっていない場合は**、セキュリティ **をクリックし、次に** Dellアップデート **をクリックします。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **Dell アップデートのダウンロード設定** をクリックします。

   Dellカタログの現在のステータスが表示されます。
3. ファイルダウンロードの設定 セクションで、次のオプションを選択します。

オプション	説明
無効	Dell アップデートパッケージのダウンロードを防ぎます。この予防措置の対象には、更新をインストールするために必要なインストーラも含まれます。
すべてのファイル	アプライアンス上でサブスクライブしたパッケージの完全キャッシュを保持します。このオプションを選択すると、展開パッケージがすべてダウンロードされます。展開パッケージが環境に必要かどうかを判断するためのチェックは行われません。
不足しているファイルのみ	アプライアンスが検出ジョブの結果に基づいてダウンロードするパッケージを決定できるようにします。管理対象デバイスのいずれかで Dell アップデート検出署名が「未インストール」として検出された場合は、パッケージがダウンロードされます。管理対象デバイスに「未インストール」として検出されたデバイスがない場合は、この更新のパッケージはダウンロードされません。
__日経過後に、未使用のファイルを削除する	指定した日数内に展開されなかった Dell アップデートパッケージを削除します。非アクティブ または 無効 とマークされた Dell アップデートは、ダウンロードプロセス中に自動的に削除されます。

オプション	説明
更新 **説明** **アクション**	各タイプの更新プログラム (署名 または アップデートファイル) について、説明と使用可能なアクションへのアクセスを提供します。 • **更新の確認**: クリックして Dell アップデート署名ファイルをダウンロードします。 • **削除**: クリックすると、アプライアンスからすべての Dell アップデートがただちに削除されます。このオプションは、今後更新が不要となり、使用したディスク領域をすぐに再利用する場合に便利です。 • **今すぐ実行**: クリックすると、サブスクリプションのスケジュールに関係なく、サブスクライブした Dell アップデートがすぐにダウンロードされます。

4. スケジュール セクションで Dell アップデート署名のスケジュールオプションを選択します。ファイル署名には、セキュリティ通知および Quest からダウンロードされる Dell アップデートを定義するその他のファイルが含まれています。

オプション	説明
署名のダウンロード	Dell アップデート署名がダウンロードされないようにするには、**なし** を選択します。
毎日、指定した時刻	**日** を選択して、Dell アップデート検出署名を毎日ダウンロードするか、または曜日を選択して週に 1 回ダウンロードします。 ダウンロードを開始する時間を選択します。時間は 24 時間形式で表示され、0 の場合は午前 0 時を、1 の場合は午前 1 時を、23 の場合は午後 11 時を表します。 **注:** Dell アップデートダウンロードを設定する場合、タイミングが重要です。アプライアンスのアクティビティログは午前 1 時 30 分に作成され、メンテナンスタスクは午前 1 時から 1 時 30 分の間に行われます。ログの作成とメンテナンスタスクが完了する午前 3 時頃よりも後に、Dell アップデートダウンロードが行われるようスケジュールすることをお勧めします。
毎月 / 特定月 n 日の HH:MM に実行	月の特定の日を選択して、1 か月ごとに Dell アップデート検出署名をダウンロードします。

5. Dell アップデートのスケジュールオプションを設定します。

オプション	説明
署名のダウンロード後	署名がダウンロードされた後で、パッケージをダウンロードします。このオプションは、ファイルダウンロードを設定する セクションで **無効** オプションがクリアになっている場合は使用できません。

オプション	説明
__分ごと	パッケージをダウンロードする頻度を指定します。ファイルのダウンロード設定 セクションの 不足しているパッチのみ が選択されている場合にのみ、このオプションは使用できます。
ダウンロードのブラックアウト: 開始: __、終了: __	ファイルがダウンロードできない時間帯を指定します。例えば、停止時間を早朝にして、通常の業務時間に多くのネットワーク帯域幅がプロセスによって使用されないようにします。 このオプションを選択すると、指定した時間にファイルダウンロードが停止します。次回の指定したファイルダウンロード時間になるまで、ダウンロードは開始されません。ダウンロードが再開されると、停止した時点からパッチダウンロードが開始されます。未完了のダウンロードは、Dell アップデートカタログ ページに表示されない可能性があります。

6. **保存** をクリックします。

Dell アップデートスケジュールの設定

アプライアンスでは、設定したスケジュールに従って、お使いの Dell クライアントとサーバに必要なファームウェアとドライバの更新を自動的に特定し、インストールすることができます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のDellアップデートのスケジュールを個別に作成します。

Dellアップデートとデバイスをグループ化するラベルを作成することを検討します。Dellアップデートスケジュールを作成するときに、これらのラベルを使用できます。例えば、ドライバやファームウェアなどのアプリケーションファミリで更新をグループ化するラベルを作成できます。または、Microsoft Windows 7 を実行するすべての Dell サーバを 1 つのラベルにグループ化して、Dell アップデートスケジュールを実行して、最新の状態にできます。更新とデバイスに対するラベルの作成の詳細については、パッチ適用に対する Smart Label の使用を参照してください。

1. Dellアップデート ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Dellアップデート** をクリックします。
2. **オプション**：使用可能な更新を確認し、インストールしない更新を非アクティブにします。

    アプライアンス設定がDellカタログ更新をダウンロードするよう設定されている場合のみ、更新は使用可能です。

    更新を確認し、非アクティブにするには

    a. Dellアップデート パネルで **カタログ** をクリックします。
    b. アップデートの隣のチェックボックスをオンにします。
    c. **アクションの選択 > 次にステータスを変更 > 非アクティブ** を選択します。
3. インベントリと更新をスケジュールします。

    これは、パッチ管理 セクションでのパッチスケジュールの作成方法と似ています。インベントリは単独で、またはインベントリと更新のスケジュールの一部として収集し、さらに更新のインストールも行うことができます。通常は、アップデートスケジュールの一環としてインベントリが自動的に実行されます。

インベントリと更新をスケジュールするには

a. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Dellアップデート** をクリックします。
b. Dellアップデート パネルで **スケジュール** をクリックします。
c. **アクションの選択 > 新規作成** を選択します。
d. Dell アップデートスケジュール リストページで、次のいずれかを実行します。

- スケジュールの詳細 ウィザード使用して新しい Dell アップデートスケジュールを作成するには、**アクションの選択 > 新規作成 (ウィザード)** の順にクリックします。
- スケジュールの詳細 ページを使用して新しい Dell アップデートスケジュールを作成するには、**アクションの選択 > 新規作成 (クラシック)** の順にクリックします。
- 既存のスケジュールを編集するには、リスト内のスケジュール名をクリックし、表示される Dell アップデートスケジュールの概要 ページで **編集** をクリックします。

  選択した スケジュールの詳細 ページまたはウィザードが表示されます。各選択で同じオプションを使用できます。必要に応じて、右上隅にある **クラシックビュー** または **ウィザードビュー** をクリックして、ページとウィザードを切り替えることができます。

e. スケジュールに関する一般的な情報を設定します。

オプション	説明
名前	スケジュールを識別するための名前。この名前は、Dell アップデートスケジュール リストページに表示されます。
説明	Dell アップデートスケジュールの簡単な説明。

f. 次のいずれかのアクションを選択します。

これらのアクションは、パッチスケジュールアクションと同じです。詳細については、「パッチスケジュールの設定」を参照してください。

アクション	説明
検出	互換性のある Dell アップデートをスキャンします。
検出と展開	互換性のある Dell アップデートをスキャンし、該当するファイルをエージェントデバイスにダウンロードして、選択したデバイスにアップデートを展開します。
展開	選択したデバイスにアップデートを展開します。

注: Dell アップデート展開アクションでは、該当する管理対象デバイスを再起動する必要があります。

g. 次のオプションを使用してターゲットデバイスを選択します。

これらのオプションは、パッチスケジュールアクションに表示されるオプションと同じです。詳細については、「パッチスケジュールの設定」を参照してください。

通常、ノート PC、ワークステーション、およびサーバについてそれぞれ異なるスケジュールを作成します。それは、これらの 3 つのタイプのデバイスの用途が大きく異なるためです。

アクション	説明
全デバイス	このスケジュールをすべての管理対象デバイスに適用するには、このオプションを選択します。更新ア

アクション	説明
	クションを特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
デバイスラベル	ここで選択したラベルを使用して Dell アップデートへのアクションを制限します。これは、最も一般的に使用されるオプションです。 a. **関連ラベルの管理** をクリックします。 b. 表示された ラベルを選択 ダイアログボックスで、1 つ以上のラベルを 実行の制限対象 領域にドラッグし、**OK** をクリックします。 このオプションを使用するには、機能の更新に Smart Label が既に存在している必要があります。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
デバイス	選択したデバイスで Dell アップデートを実行します。互換性のある Dell デバイスのみがリストに表示されます。 • デバイスを検索するには、フィールドに入力し始めます。 • 指定されたすべてのデバイスを削除してから再起動するには、**すべて削除** をクリックします。 • スコープユーザーは、役割にラベルが割り当てられている場合に、自身の役割に関連付けられているデバイスだけを表示できます。ユーザーの役割の詳細については、ユーザーの役割の追加または編集を参照してください。
オペレーティングシステム	更新するデバイスのオペレーティングシステムを選択します。デフォルトは、すべてのオペレーティングシステムです。このオプションが設定されている場合、スケジュールは選択したオペレーティングシステムを搭載したデバイスにのみ適用されます。 a. **オペレーティングシステムの管理** をクリックします。 b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**Windows**

アクション	説明
	> Windows 10 の順に選択し、**x64** を選択します。

h. スケジュール セクションで、スケジュールに適用可能なオプションを指定します。

これらのオプションは、パッチスケジュールアクションに表示されるオプションと同じです。詳細については、「パッチスケジュールの設定」を参照してください。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。このオプションは、サーバーに手動でパッチを適用するか、または定期的に実行しないパッチアクションを実行する場合に便利です。
毎 _ 時間	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
毎月 / 特定月の n 日、HH:MM に実行	毎月n日（例えば、毎月1日または2日）、または特定の月、特定の時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタ

オプション	説明
	リスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。
タイムゾーン	アクションをスケジュールするときに使用するタイムゾーン。**サーバー** を選択すると、アプライアンスのタイムゾーンを使用します。**エージェント** を選択すると、管理対象デバイスのタイムゾーンを使用します。
オフラインの場合は次の接続時に実行	管理対象デバイスが現在オフラインである場合、次回管理対象デバイスがアプライアンスに接続するときにアクションを実行します。このオプションは、定期的にオフラインになるノートPCおよびその他のデバイスに対して役立ちます。このオプションが選択されていない場合でデバイスがオフラインのときは、次回のスケジュールされた時間までアクションは再度実行されません。
再接続後の実行を遅延	指定した時間、スケジュールを遅延させます。遅延時間は、パッチアクションの実行がスケジュールされている時間から開始されます。
次の時間の経過後に終了:	パッチ適用アクションの期限。 例えば、04:00にパッチが実行されるようスケジュールする場合、07:00にパッチ適用アクションをすべて停止し、ユーザーが業務を開始するときに帯域幅の問題が発生しないようにすることができます。これを行うには、分 ボックスで「**180**」を指定します。 期限に到達すると、進行中のパッチ適用タスクはすべて中断され、これらのタスクに対するセキュリティログのステータスは「中断されました」になります。 これらのパッチ適用タスクは次回実行で再開されず、スケジュール済みの毎回のパッチ適用アクションで最初から開始されます。

注: エージェントのタイムゾーンは、タイムゾーン情報の取得元になるDellデバイスがインベントリ内にある場合にのみ使用可能です。

i. **保存** をクリックします。

Dellアップデートスケジュール ページにスケジュールが表示されます。このスケジュールは、デフォルトでは無効になっています。

ヒント: スケジュールを有効にするには、デバイスの小さなサブセットに対してスケジュールをテストして、すべてが想定した通りに機能することを確認します。

j. スケジュールを有効にするには、スケジュール名の隣のチェックボックスをオンにし、**アクション の選択 > 有効にする** を選択します。

インベントリと更新が、指定したスケジュールに従って実行されます。

Dell アップデートスケジュールの表示

アプライアンスに存在する Dell アップデートスケジュールの概要情報を表示できます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織の Dell アップデートのスケジュールを個別に表示します。

1. Dell アップデートスケジュール ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Dellアップデート** をクリックします。
2. Dellアップデート パネルで **スケジュール** をクリックします。

   Dell アップデートスケジュール ページで使用できる列は、パッチスケジュール ページの列と同じです。パッチスケジュール ページに表示されるフィールドの詳細については、「パッチスケジュールのリストを表示する」を参照してください。
3. （ オプション ）列の表示を変更するには、右側の表の上部に表示される 表のオプション ドロップダウンリストから **列の表示・非表示** を選択します。

Dell アップデートスケジュールの詳細の確認

Dell アップデートスケジュールを設定すると、このページにスケジュール設定とそのステータスに関する詳細が表示されます。

1. アップデートスケジュールの概要 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Dellアップデート** をクリックします。
   c. Dellアップデート パネルで **スケジュール** をクリックします。
   d. スケジュールの名前をクリックします。
2. 構成 セクションの内容を確認します。

オプション	説明
作成済み	スケジュールが作成された日付と時刻。
修正日	スケジュールが最後に変更された日付と時刻。

オプション	説明
前回の実行	スケジュールが最後に実行された日付と時刻。
名前	スケジュールを識別するための名前。この名前は、Dell アップデートスケジュール リストページに表示されます。
アクション	スケジュールに関連付けられたアクション： • **検出**：互換性のある Dell アップデートをスキャンします。 • **検出と展開**：互換性のある Dell アップデートをスキャンし、後で展開できるように、該当するファイルをエージェントデバイスにダウンロードします。 • **展開**：選択したデバイスにアップデートを展開します。
説明	Dell アップデートスケジュールの簡単な説明。
デバイス	このフィールドは、すべてのデバイスに適用されるようにスケジュールが設定されている場合にのみ表示されます。
デバイスラベル	スケジュールが実行されるデバイスに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したデバイスに適用するようにスケジュールが設定されている場合にのみ表示されます。
デバイス名	スケジュールの実行対象である 1 つまたは複数の選択されたデバイス。このフィールドは、選択したデバイスに適用するようにスケジュールが設定されている場合にのみ表示されます。
ラベルの検出	スケジュールされたアップデートに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したアップデートを検出するようにスケジュールが設定されている場合にのみ表示されます。
警告	**検出と展開スケジュールのみ**。更新アクションの実行時にユーザーに表示される警告： • **OK**: すぐに実行されます。 • **キャンセル**: 次のスケジュールされた実行までキャンセルされます。 • **再通知**: 再通知間隔 の経過後に再度プロンプトが表示されます。

オプション	説明
再起動	**検出と展開スケジュールのみ**。管理対象デバイスの再起動のオプション： • **再起動しない**：更新を有効にするために再起動が必要な可能性がある場合でも、デバイスを再起動しません。このオプションはお勧めしません。これは、再起動が必要な場合に、再起動しないで更新プログラムを展開するため、システムが不安定な状態のままになることがあるからです。さらに、再起動が必要な更新プログラムは、再起動後にのみ適用済みとして表示されます。 • **ユーザーにプロンプトを表示**：デバイスを再起動する前に、ユーザーが再起動に同意するまで待ちます。ユーザーが再通知を選択するか、または再起動をキャンセルすると、再起動されるまで更新は停止します。ターゲットデバイスに表示されるエージェントダイアログボックスで再通知間隔を選択すると、指定した再通知間隔の間、再起動プロンプトが一時停止します。 • **強制的に再起動**：再起動が必要なアップデートが展開されるとすぐに再起動されます。強制的な再起動はキャンセルできません。強制的な再起動は、デスクトップとサーバーに対して効果的です。ノートPCの再起動を強制することはお勧めしません。通常サーバーには専属のユーザーがいないため、強制的な再起動はサーバーで効果的に機能します。ただし、サーバが更新され、再起動しているときにサービスが使用できなくなることをユーザーに警告するのは重要です。詳細については、「パッチ適用に関するベストプラクティス」を参照してください。
スケジュール	選択したアップデートスケジュール。**タスクスケジュールの表示** をクリックして、詳細なタスクスケジューラを表示します。表示されるダイアログボックスで、タスクの詳細を確認するタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。
オフラインの場合は次の接続時に実行	管理対象デバイスが現在オフラインである場合、次回そのデバイスがアプライアンスに接続するときにスケジュールがアクションを実行するかどうかを示します。
タイムゾーン	このオプションが設定されている場合は、関連するアクションをスケジュールするときに使用するタイムゾーンを指定します。サーバに設定されている場合、スケジュールはアプライアンスのタイムゾーンを使用します。エージェントに設定されている場合は、管理対象デバイスのタイムゾーンが使用されます。

オプション	説明
再接続後の実行を遅延	設定されている場合、このオプションはスケジュールが遅延する時間を示します。遅延時間は、更新アクションの実行がスケジュールされている時間から開始されます。
次の後に終了	設定されている場合、このオプションはスケジュールを実行できる最大時間を示します。この制限時間に達すると、進行中の更新タスクはすべて中断されます。

3. スケジュールステータス セクションで、次のいずれかのタブで全体的なスケジュールのステータスを確認します。

タブ	コンテンツ
マシン別	更新対象として選択されたデバイス。各エントリには、デバイス名、IP アドレス、更新ステータス（「パッチスケジュールの詳細 ページのフィールド」を参照）、更新の結果、更新の完了日が表示されます。デバイスノードを展開して、適用可能なアップデートを表示できます。各エントリには、更新 ID、関連するサポート技術情報記事番号、更新名、現在のステータス（インストール済み、未インストール、または導入の失敗）、およびアップデートが検出された日付が表示されます。
アップデートごと	検出および展開用に選択されたアップデート。各エントリには、更新 ID、関連するサポート技術情報記事番号、更新名、更新されるデバイスの数、更新されないデバイスの数、および検出または展開の失敗が発生したデバイスの数が表示されます。
インストール済み	デバイスに正常にインストールされたアップデート。各エントリには、更新 ID、関連するサポート技術情報記事番号、および更新名が表示されます。アップデートノードを展開して、アップデートがインストールされるデバイスを表示できます。
インストールされませんでした	デバイスにインストールされていないアップデート。各エントリには、更新 ID、関連するサポート技術情報記事番号、および更新名が表示されます。アップデートノードを展開して、アップデートがインストールされるデバイスを表示できます。
検出エラー	検出の失敗につながった未完了のアップデート。各エントリには、更新 ID、関連するサポート技術情報、更新名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコード」を参照）。アップデートノードを展開して、障害が発生したデバイスを表示できます。
展開エラー	展開の失敗につながった未完了のアップデート。各エントリには、更新 ID、関連するサポート技術情報、更新名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコー

タブ	コンテンツ
	ド」を参照）。アップデートノードを展開して、障害が発生したデバイスを表示できます。

4. （**オプション**）スケジュールの詳細を確認した後、次のいずれかのアクションを実行できます。
   - アップデートスケジュールを編集するには、**編集** をクリックします。詳細については、「Windows 機能更新プログラムのスケジュールの設定」を参照してください。
   - アップデートスケジュールを実行するには、**今すぐ実行** をクリックします。
   - アップデートスケジュールのコピーを作成するには、**複製** をクリックします。
   - 更新スケジュールを削除するには、**削除** をクリックします。

利用可能な Dell アップデートの表示

Dell アップデートカタログで Dell アップデートのリストを確認できます。

関連アップデートを表示するには、Dell アップデートのダウンロード設定を選択する必要があります。詳細については、「Dell アップデートのダウンロード設定の選択」を参照してください。すべての Dell アップデート署名ファイルがダウンロードされると、Dell アップデートカタログに関連するアップデートが一覧表示されます。

注: このページの 重大度 列には、Dell の重大度レベルに一致しない Microsoft のセキュリティ標準が使用されます。

表示される重大度レベル	対応する Dell の重大度レベル
普通	オプション
重要	推奨
緊急	緊急

1. Dell アップデートカタログ リストページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Dellアップデート** をクリックします。
   c. Dellアップデート パネルで **カタログ** をクリックします。
2. Dell アップデートを検索します。
   a. 検索ボックスに検索条件を入力します。

   例えば、「2021」と入力します。

   b. **Enter** を押します。

   リストページが更新され、バージョンが 2021 の Dell アップデートのみが表示されます。

Dell アップデートステータスの表示

Dell アップデートの詳細には、ベンダー情報と展開ステータスが含まれます。

1. Dell アップデートカタログ ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Dellアップデート** をクリックします。

c. Dellアップデート パネルで **カタログ** をクリックします。

d. Dellアップデートの名前をクリックします。

Dell Update Detail（Dell アップデートの詳細）ページが表示され、選択したアップデートに関する完全な情報が表示されます。

Linux パッケージアップグレードの管理

Linux パッケージアップグレードにより、管理対象の Linux デバイスの全体的なパフォーマンスが向上し、潜在的な脆弱性から保護されます。

このアプライアンスを使用すると、Linux パッケージアップグレードのインストールと管理のプロセスを自動化できます。個々の Linux パッケージリポジトリに依存し、管理対象 Linux デバイスが適切なリポジトリを参照していることを前提としています。

また、アプライアンスはセキュリティ更新を含むパッケージのみを検出し、各 Linux リポジトリでそのように識別されます。すべてのパッケージを検出またはアップグレードしようしたり、管理対象デバイスの OS 全体を最新バージョンにアップグレードしようとしたりはしません。

注: Linux Raspbian では、定期的な更新とセキュリティ更新は区別されません。管理対象の Raspbian デバイスのパッケージを検出してアップグレードすると、デバイスにすべての更新済みパッケージがインストールされます。

注: KACE システム管理アプライアンスでの update という用語は、次のように仮定しています。ディストリビューションのリポジトリに新しいバージョンのパッケージがある場合、アプライアンスは標準のシステムコマンドを使用して、システムが可能な最新バージョンをインストールするようにします。これは、update（または upgrade）という語が基盤となるシステムコマンドで使用されるのとまったく同じ方法で使用されることを意味するものではありません。

Linux パッケージアップグレードスケジュールを表示する

アプライアンスに存在する Linux パッケージアップグレードスケジュールの概要情報を表示できます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織のスケジュールを個別に表示します。

1. Windows 機能更新プログラムのスケジュール ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Linux パッケージアップグレード** をクリックします。
2. Linux パッケージアップグレード パネルで **スケジュール** をクリックします。

   Linux パッケージアップグレードスケジュール ページで使用できる列は、パッチスケジュール ページの列と非常に似ています。パッチスケジュール ページに表示されるフィールドの詳細については、「パッチスケジュールのリストを表示する」を参照してください。
3. （オプション）列の表示を変更するには、右側の表の上部に表示される 表のオプション ドロップダウンリストから **列の表示・非表示** を選択します。

Linux パッケージアップグレードスケジュールを設定する

Linux パッケージアップグレードスケジュールを作成および設定し、その実行時間をスケジュールすることができます。

1. Linux パッケージアップグレードウィザードを起動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Linux パッケージアップグレード** をクリックします。
   c. Linux パッケージアップグレード管理 パネルで **スケジュール** をクリックします。
   d. Linux パッケージアップグレードスケジュール リストページで、次のいずれかを実行します。

   - 新しい Linux パッケージアップグレードスケジュールを作成するには、**アクションの選択 > 新規作成（ウィザード）** の順にクリックします。
   - 既存のスケジュールを編集するには、リスト内のスケジュール名をクリックし、表示される Linux パッケージアップグレード概要 ページで **編集** をクリックします。

   スケジュールの詳細 ウィザードが表示されます。
2. スケジュールの詳細 ウィザードの 一般的な情報 ページで、スケジュールに関する一般的な情報を設定します。

オプション	説明
名前	スケジュールを識別するための名前。この名前は、Linux パッケージアップグレードスケジュール リストページに表示されます。
説明	Linux パッケージアップグレードスケジュールの簡単な説明。

3. アクション ページで、次の手順を実行します。
   a. アクション で、以下のアクションのいずれかを選択します。

   選択したアクションの結果は、管理対象 Linux デバイスが適切なパッケージリポジトリに関連付けられているかどうかによって異なります。該当するすべてのデバイスを選択するには、それぞれの管理対象デバイスが適切なパッケージリポジトリを使用していることを確認します。

   注: アプライアンスは、Linux Raspbian を除く、各 Linux リポジトリで識別されるセキュリティ更新を含むパッケージのみをスキャンします。すべてのパッケージを検出またはアップグレードしようしたり、管理対象デバイスの OS 全体を最新バージョンにアップグレードしようとしたりはしません。ただし、Linux Raspbian リポジトリでは、定期的な更新とセキュリティ更新は区別されません。管理対象の Raspbian デバイスのパッケージを検出してアップグレードすると、それらのデバイスにすべての更新済みパッケージがインストールされます。

アクション	説明
すべて検出	セキュリティ更新を含むすべての Linux パッケージアップグレードをスキャンします。
すべて検出してアップグレード	セキュリティ更新を含むすべての Linux パッケージアップグレードをスキャンし、該当するファイルを

アクション	説明
	ダウンロードして、選択したデバイスにアップグレードを展開します。

b. すべて検出 で、検出アクションが完了するまでの時間を選択します。
c. **すべて検出してアップグレード アクションのみ**。すべてアップグレード で、アップグレードアクションが完了するまでの時間を選択します。

4. **次へ** をクリックします。
5. デバイス ページで、このスケジュールに関連付けるデバイスを指定します。

これらのオプションは、パッチスケジュールアクションに表示されるオプションと同じです。手順については、パッチスケジュールの設定を参照してください。

アクション	説明
全デバイス	このスケジュールをすべての管理対象デバイスに適用するには、このオプションを選択します。パッチアクションを特定のラベルまたはデバイスに制限するには、このチェックボックスをオフにします。
デバイスラベル	選択した関連付けられているラベルを使用して、アクションを機能更新プログラムに制限します。これは、最も一般的に使用されるオプションです。 a. **関連ラベルの管理** をクリックします。 b. 表示された ラベルを選択 ダイアログボックスで、1 つ以上のラベルを 実行の制限対象 領域にドラッグし、**OK** をクリックします。 このオプションを使用するには、機能の更新に Smart Label が既に存在している必要があります。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。
デバイス	選択したデバイスでパッチアクションを実行します。表示されるリストには、該当する Linux デバイスのみが表示されます。 • デバイスを検索するには、フィールドに入力し始めます。 • 指定されたすべてのデバイスを削除してから再起動するには、**すべて削除** をクリックします。 • スコープユーザーは、役割にラベルが割り当てられている場合に、自身の役割に関連付けられているデバイスだけを表示できます。ユーザーの役割の詳細については、ユーザーの役割の追加または編集を参照してください。
オペレーティングシステム	アップグレードするデバイスのオペレーティングシステムを選択します。ダイアログボックスには、該当する Linux オペレーティングシステムのみが表示されます。デフォルトは、すべてのオペレーティングシステムです。このオプションが設定されている場合、スケジュールは選択したオペレーティングシステムを搭載したデバイスにのみ適用されます。

アクション	説明
	a. **オペレーティングシステムの管理** をクリックします。 b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Linux Ubuntu x86_64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**Linux > Ubuntu** の順に選択し、**x64** を選択します。

6. **次へ** をクリックします。
7. スケジュール セクションで、スケジュールに適用可能なオプションを指定します。

   これらのオプションは、パッチスケジュールアクションに表示されるオプションと同じです。手順については、パッチスケジュールの設定を参照してください。

アクション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。このオプションは、サーバーに手動でパッチを適用するか、または定期的に実行しないパッチアクションを実行する場合に便利です。
毎 _ 時間	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
毎月 / 特定月の n 日、HH:MM に実行	毎月n日（例えば、毎月1日または2日）、または特定の月、特定の時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59)

アクション	説明
	値の指定は次の要領で行います。 • **スペース ( )**：各フィールドはスペースで区切ります。 • **アスタリスク (*)**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。
オフラインの場合は次の接続時に実行	管理対象デバイスが現在オフラインである場合、次回管理対象デバイスがアプライアンスに接続するときにアクションを実行します。このオプションは、定期的にオフラインになるデバイスで役立ちます。このオプションが選択されていない場合でデバイスがオフラインのときは、次回のスケジュールされた時間までアクションは再度実行されません。

8. **保存** をクリックします。

   Linux パッケージアップグレードスケジュール概要 ページが表示され、新しく作成または更新されたスケジュールが表示されます。このページの詳細については、「Linux パッケージアップグレードスケジュールの詳細を確認する」を参照してください。Smart Label の基準に一致するデバイスを追加した場合、それらのデバイスはアップグレードスケジュールに自動的に含まれます。

Linux パッケージアップグレードスケジュールの詳細を確認する

Linux パッケージアップグレードスケジュールを設定すると、このページにスケジュール設定とそのステータスに関する詳細が表示されます。

1. Linux パッケージアップグレードスケジュール概要 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Linux パッケージアップグレード** をクリックします。
    c. Linux パッケージアップグレード管理 パネルで **スケジュール** をクリックします。
    d. Linux パッケージアップグレードスケジュールの名前をクリックします。
2. 対象のデバイス フィールドを確認します。スケジュールで指定されているとおりに、この番号はアップグレード用に選択された Linux デバイスの数を指定します。
3. 構成 セクションの内容を確認します。

オプション	説明
作成済み	スケジュールが作成された日付と時刻。
修正日	スケジュールが最後に変更された日付と時刻。
前回の実行	スケジュールが最後に実行された日付と時刻。
名前	スケジュールを識別するための名前。この名前は、Linux パッケージアップグレードスケジュールリストページに表示されます。
アクション	スケジュールに関連付けられたアクション： • **すべて検出**：すべての Linux パッケージアップグレードをスキャンします。 • **すべて検出してアップグレード**：すべての Linux パッケージアップグレードをスキャンし、該当するファイルをダウンロードして、選択したデバイスにアップデートを展開します。
説明	Linux パッケージアップグレードスケジュールの簡単な説明。
デバイス	このフィールドは、すべてのデバイスに適用されるようにスケジュールが設定されている場合にのみ表示されます。
デバイスラベル	スケジュールが実行されるデバイスに関連付けられた 1 つ以上の Smart Label。詳細については、「パッチ適用に対する Smart Label の使用」を参照してください。このフィールドは、選択したデバイ

オプション	説明
	スに適用するようにスケジュールが設定されている場合にのみ表示されます。
デバイス名	スケジュールの実行対象である 1 つまたは複数の選択されたデバイス。このフィールドは、選択したデバイスに適用するようにスケジュールが設定されている場合にのみ表示されます。
スケジュール	選択したアップデートスケジュール。**タスクスケジュールの表示** をクリックして、詳細なタスクスケジューラを表示します。表示されるダイアログボックスで、タスクの詳細を確認するタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。
オフラインの場合は次の接続時に実行	管理対象デバイスが現在オフラインである場合、次回そのデバイスがアプライアンスに接続するときにスケジュールがアクションを実行するかどうかを示します。
再接続後の実行を遅延	設定されている場合、このオプションはスケジュールが遅延する時間を示します。遅延時間は、更新アクションの実行がスケジュールされている時間から開始されます。
次の後に終了	設定されている場合、このオプションはスケジュールを実行できる最大時間を示します。この制限時間に達すると、進行中の更新タスクはすべて中断されます。

4. スケジュールステータス セクションで、パッチスケジュールの全体的なステータスを次のいずれかのタブで確認します。

タブ	コンテンツ
マシン別	アップグレード対象として選択されたデバイス。各エントリには、デバイス名、IP アドレス、アップグレードステータス、アップグレード結果、および、該当する場合はアップグレードが完了した日付が表示されます。デバイスノードを展開すると、パッケージ名、バージョン、互換性のある OS 名、パッケージがデバイスにインストールされているかどうか、およびパッケージが検出された日付など、各パッケージに関する追加情報を表示できます。
パッケージごと	検出およびインストール用に選択されたアップグレード。各エントリには、パッケージ名、そのバージョン、互換性のある OS 名、パッケージ ID が表示され、パッケージがインストールされているかどうかが示されます。
アップグレードが必要	デバイスにインストールできるアップグレード。各エントリには、パッケージ名、バージョン、および互換性のある OS 名が表示されます。アップデートノードを展開して、アップデートがインストールされるデバイスを表示できます。

タブ	コンテンツ
展開エラー	展開の失敗につながった未完了のアップデート。各エントリには、更新 ID、関連するサポート技術情報、更新名、および関連するエラーコードが表示されます（「パッチとスクリプトによるエラーコード」を参照）。アップデートノードを展開して、障害が発生したデバイスを表示できます。

5. （**オプション**）スケジュールの詳細を確認した後、次のいずれかのアクションを実行できます。
   - スケジュールを編集するには、**編集** をクリックします。詳細については、「Windows 機能更新プログラムのスケジュールの設定」を参照してください。
   - スケジュールを実行するには、**今すぐ実行** をクリックします。
   - スケジュールのコピーを作成するには、**複製** をクリックします。
   - スケジュールを削除するには、**削除** をクリックします。

Linux パッケージアップグレードの確認

すべて検出 アクションを実行すると、アプライアンスはアップグレードに使用できるパッケージのリストを生成します。

パッケージ リストページを使用して、アップグレード可能な最新の Linux パッケージを表示し、管理対象デバイスにインストールします。まず、特定の Linux OS を選択し、リストの内容を確認して、アップデートが必要なデバイスプールの全体的な見積もりを取得します。

パッケージごとに、リストには、パッケージがインストールされているデバイスの数またはインストールされていないデバイスの数、および最新バージョンを実行しているデバイスの割合が表示されます。

1. パッケージ リストページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**Linux パッケージアップグレード** をクリックします。
   c. Linux パッケージアップグレード管理 パネルで **Package Upgrade History**（パッケージアップグレード履歴）をクリックします。
2. パッケージ リストページで、**特定基準で表示** をクリックして Linux OS を選択します。たとえば、RHEL や Ubuntu などです。

   リストが更新され、選択した OS で検出されたパッケージが表示されます。
3. リストの内容を確認します。以下の列が使用可能です。

列	説明
パッケージ名	検出されたパッケージの名前。
バージョン	最新パッケージのバージョン。
インストール済み	パッケージがインストールされている、選択した Linux OS を実行している管理対象 Linux デバイスの数。この列の番号をクリックすると、デバイス リストページにこれらのデバイスのリストが表示されます。

列	説明
アップグレードが必要	選択した Linux OS を実行している管理対象 Linux デバイスのうち、このパッケージの以前のバージョンがあり、アップグレードの候補となっているものの数。この列の番号をクリックすると、デバイス リストページにこれらのデバイスのリストが表示されます。
完了	このパッケージがインストールされているすべてのデバイスの割合。

デバイスとアプライアンスのセキュリティの維持

アプライアンスでは、標準の脆弱性テストとスキャンを使用して、エージェント管理対象デバイスのセキュリティをテストできます。アプライアンスセキュリティを維持するには、日次セキュリティレポートを確認し、使用可能になったアプライアンスソフトウェアの更新を適用します。

デバイスのセキュリティのテスト

デバイスのセキュリティをテストするには、OVAL脆弱性テストおよびSCAPスキャンがエージェント管理対象デバイスに対して実行されるようにスケジュールすることができます。

OVALセキュリティチェックについて

OVAL（Open Vulnerability and Assessment Language）は、デバイス上のセキュリティの脆弱性および設定の問題を検出するための、国際的に認定された標準です。

OVALセキュリティチェックは、コンプライアンスに準拠していない資産を判別し、セキュリティポリシーをカスタマイズして、ルールの施行、テストのスケジュールによる自動実行、結果に基づくレポートの作成を行えます。

OVALはCVE（Common Vulnerabilities and Exposures）リストと互換性があります。CVEコンテンツは、国際的な情報セキュリティコミュニティからのエキスパートで構成されるCVE Editorial Boardによって決定されます。コミュニティフォーラムで審議されたセキュリティの脆弱性に関する新しい情報は、リストに追加可能かを確認するためにCVEイニシアチブに送信されます。CVE、MITRE Corporation、または OVAL Board の詳細については、http://cve.mitre.orgを参照してください。

脆弱性と危険性について一般的な言葉で説明できることにより、他のCVE互換のデータベースおよびツールとセキュリティデータを共有することがさらに容易になります。

注: OVAL セキュリティチェックは、サポートされている Windows、macOS、または Linux オペレーティングシステムを実行しているデバイスに対して実行できます。Java 1.7 以降を管理対象の macOS および Linux デバイスにインストールする必要があります。

OVALテストと定義の理解

OVAL定義には、OVALテストを実行するために必要な情報が含まれています。この情報には、レジストリエントリ、ファイルバージョン、およびWMI（Windows Management Instrumentation）データの確認を含めることができます。

OVALテスト定義は、リリース前に一連のフェーズを経て処理されます。このプロセスでの定義の状態に応じて、次のいずれかのステータス値が割り当てられます。

ステータス	説明
ドラフト	定義にOVAL ID番号が割り当てられており、コミュニティフォーラムおよびOVAL Boardで審議中であることを示します。
暫定処置中	定義はOVAL Boardによる調査中であり、コミュニティフォーラムで審議可能であることを示します。さらなる変更または審議が必要でない場合、定義は一般的に2週間、このステータスが割り当てられます。
容認済み	定義は暫定処置中のステージを通過し、 OVAL定義ページに掲載されたことを示します。このステータスの定義に関する審議のすべての履歴はOVAL定義からリンクされています。

その他に、次のステータス値が使用できることがあります。

- 初期送信
- 非推奨

OVAL 定義のステージの詳細については、http://cve.mitre.orgを参照してください。

OVALテストが有効になっていると、使用可能なすべてのOVALテストがターゲットデバイスに対して実行されます。

OVALテストの詳細には、脆弱性の重要度は示されません。特定の脆弱性の存在についてネットワークをテストするかどうかを独自に判断します。

OVALテストと定義の表示

管理者コンソールで OVAL テストと定義を表示することができます。

1. OVALカタログ リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**OVALスキャン** をクリックします。
    c. OVALスキャン パネルで **カタログ** をクリックします。
2. **オプション**：特定基準で表示 ドロップダウンリストを使用して、表示されるテストを絞り込みます。または、検索 フィールドを使用して、OVAL ID、CVE番号、オペレーティングシステム、またはテキストに基づいてOVALテストを検索します。
3. OVALカタログ リストで **名前** リンクをクリックします。

    OVAL定義の詳細 ページに次の情報が表示されます。

フィールド	説明
OVAL-ID	脆弱性のステータスは OVAL-ID の後に続きます。可能な値は ドラフト、暫定処置中、または 容認済み です。

フィールド	説明
クラス	脆弱性のタイプ。可能な値は、compliance、deprecated、patch、およびvulnerabilityです。
参照ID	脆弱性についての追加の詳細へのリンク。
説明	CVEリストに登録されている脆弱性の一般的な定義。
定義	脆弱性が存在するかどうかをテストするために使用する手順。

OVAL テスト：定義 ページの下部にある表には、脆弱性のあるネットワーク内のデバイスのリストが表示されます。便利なように、このデータの印刷用バージョンが使用可能です。

OVALテストの実行

アプライアンスは、OVAL 設定で指定したスケジュールに基づいて、OVAL テストを自動的に実行します。

OVALテストの実行には約1時間かかります。また、OVALテストは大量のメモリとCPUリソースを消費するため、ターゲットデバイスのパフォーマンスに影響が出る場合があります。ユーザー作業の中断を最小限に抑えるには、毎週または毎月、ユーザーにとって不都合となる可能性が最も低い時間帯にOVALテストを実行します。

また、OVALテストを手動で実行するには、管理者としてデバイスにログインし、debug.batを実行します。このファイルは、通常、プログラムデータディレクトリにあります。例：C:\ProgramData\Quest\KACE\kbots_cache\packages\kbots\9

ラベルを使用したOVALテストの制限

OVALテストを定期的に実行する場合、または、少数のデバイスについてのみOVALテスト結果を取得する場合は、それらのデバイスにラベルを割り当てることができます。その後、「今すぐ実行」機能を使用して、それらのデバイスに対してのみOVALテストを実行できます。

ラベルの使用の詳細については、ラベルについてを参照してください。

OVALの更新プログラムの理解

アプライアンスは毎晩、新しい OVAL 定義を確認しますが、新しい定義が追加されるのは月毎となります。OVALテストが有効になっている場合、新しいパッケージが使用可能になるたびに、アプライアンスは、OVALのスケジュール設定には関係なく、次のスクリプト更新時に、すべての管理対象デバイスに新しいOVAL定義をダウンロードします。

OVAL更新プログラムのZIPファイルは30 MBを超える場合があります。このサイズでは、接続の遅いデバイスのパフォーマンスに影響が出る可能性が高くなります。ZIPファイルにはOVALインタープリターの32ビットと64ビットの両方のバージョンが含まれており、デバイスに対して正しいバージョンが使用されます。OVALインタープリターには、Microsoft .NET Frameworkが必要で、フル（「Extended」）バージョンとClient Profileバージョンの両方がサポートされている必要があります。

OVAL設定項目の設定

OVALテストを実行するには、OVALを有効にし、ターゲットデバイスとオペレーティングシステムを選択して、実行スケジュールを確立する必要があります。

OVALテストは多大なリソースを必要とするため、ターゲットデバイスのパフォーマンスに影響が出る可能性があります。そのため、OVAL設定項目を設定するときは、注意してください。

1. OVALスケジュールの詳細 ページに移動します。

a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**OVALスキャン** をクリックします。

c. OVALスキャン パネルで **スケジュール** をクリックします。

2. 設定 セクションで、各設定を次のように指定します。

設定	説明
有効	ターゲットデバイス上で実行します。有効になっている設定のみ実行できます。 OVALテストが無効になっている場合、更新は、アプライアンスには保存されますが、OVALテストを有効化し、スケジュール設定しないかぎり、ターゲットデバイスにはプッシュアウトされません。
ログオフされている間の実行を許可	ユーザーがログインしていない場合でも実行します。ユーザーがデバイスにログインしている場合にのみこの項目を実行するには、このチェックボックスをオフにします。

3. 展開 セクションで、各設定を次のように指定します。

設定	説明
ラベル	指定したラベルに属するデバイスだけに展開を制限します。ラベルを選択するには、**編集** をクリックしてラベルを 展開の制限対象 ウィンドウにドラッグし、**保存** をクリックします。 レプリケーション共有または代替のダウンロード場所が指定されているラベルを選択した場合、デジタル資産は、アプライアンスから直接ダウンロードされるのではなく、指定されたレプリケーション共有または代替のダウンロード場所からコピーされます。 **注:** アプライアンスがKACE代替の場所を使用する前にレプリケーション共有を使用することが明らかになりました。
デバイス	展開対象を特定のデバイスのみに限定します。ドロップダウンリストから、アプリケーションの展開先のデバイスを選択します。リストをフィルタリングするには、デバイス フィールドに数文字入力します。フィールドの横の数字は、使用可能なデバイスの数を示しています。スコープユーザーは、役割にラベルが割り当てられている場合に、自身の役割に関連付けられているデバイスだけを表示できます。ユーザーの役割の詳細については、ユーザーの役割の追加または編集を参照してください。
オペレーティングシステム	展開先のオペレーティングシステムを選択します。 a. **オペレーティングシステムの管理** をクリックします。

設定	説明
	b. 表示される **オペレーティングシステム** ダイアログボックスで、必要に応じてナビゲーションツリーで OS バージョンを選択します。 ファミリ、製品、アーキテクチャ、リリース ID、またはビルドバージョンで OS バージョンを選択するオプションがあります。必要に応じて、特定のビルドバージョンまたは親ノードを選択できます。ツリーで親ノードを選択すると、関連付けられている子ノードが自動的に選択されます。この動作により、管理対象の環境でデバイスを追加またはアップグレードするときに、将来の OS のバージョンを選択できます。例えば、Windows 10 x64 アーキテクチャに関連付けられているビルドの現在および将来のバージョンをすべて選択するには、**すべて** > **Windows** > **Windows 10** の順に選択し、**x64** を選択します。

4. スケジュール セクションで、OVALを実行する時間と頻度を指定します。

設定	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 分 / 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。

設定	説明
	例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

5. **保存** をクリックします。
6. **今すぐ実行** をクリックすると、スクリプトがすぐに実行されます。

   展開 セクションで選択したデバイス上でテストが実行されます。

OVAL脆弱性レポートの表示

OVAL Report (OVAL レポート) ページには、OVAL 定義が前回更新された後に実行された OVAL テストが表示されます。

OVAL定義が更新されると、OVAL結果はこのページから削除されます。結果を保存するには、OVALデバイスレポートを定期的に実行するようにスケジュールします。詳細については、「レポートスケジュールの追加」を参照してください。

1. OVALスキャン ページに移動します。
   a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**OVALスキャン** をクリックします。
   c. レポート作成 セクションで、**概要結果の表示** をクリックします。

反映先のデバイスに対するラベルの適用

テストの詳細 ビューから、OVALテストに不合格になったすべてのデバイスを確認できます。また、それらのデバイスにラベルを割り当てて、後でパッチを適用できるようにすることができます。

1. OVALスキャンの概要 ページに移動します。
    a. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**OVALスキャン** をクリックします。
    b. レポート作成 の下にある **デバイスのコンプライアンスの表示** をクリックします。
2. 1つまたは複数のテストの隣のチェックボックスをオンにします。
3. **アクションの選択** を選択し、反映先のデバイスにラベルを適用 の下で該当するラベルを選択します。

    また、右側のテーブルの上に表示される 特定基準で表示 ドロップダウンリストを適切に選択し、テストを検索することもできます。

OVALレポートの表示

OVAL デバイスのコンプライアンス ページには、OVAL テスト結果と共にデバイスのリストが表示されます。ここでは、特定のデバイスで実行されたテストの概要を表示できます。

OVAL コンピュータレポート ページにある デバイス 列の下のラベルは、アプライアンスインベントリコンポーネントによって割り当てられたインベントリ ID です。

レポート上の任意のデバイスに関する詳細を確認するには、該当するデバイス名（リンク）をクリックしてください。デバイスの詳細ページに移動します。

1. OVAL デバイスのコンプライアンス ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**OVALスキャン** をクリックします。
    c. レポート作成 の下の **概要結果の表示** をクリックします。

        OVAL デバイスのコンプライアンス ページが表示され、OVAL レポートのリストが一覧されます。

SCAPについて

SCAP（Secure Content Automation Protocol）は、Windowsデバイス上で、ソフトウェアの脆弱性の列挙、セキュリティ関連の設定および製品名の監視、システムの検査による脆弱性の検出と検出されたセキュリティ問題のインパクトの評価（スコア付け）を行う、一連のオープンスタンダードです。

SCAPはNational Institute of Standards and Technology（NIST）によって管理されており、US OMB（米国行政管理予算局）などの政府系機関によってSCAPの使用が義務付けられています。

SCAPでは、基準ベースの脆弱性管理データリポジトリである米国政府のNational Vulnerability Database（NVD）を利用します。NVDには、セキュリティチェックリスト、セキュリティ関連ソフトウェアの脆弱性、構成ミス、製品名、およびインパクトメトリックのデータベースが含まれます。SCAP および NVD の詳細については、NIST のウェブサイト（http://scap.nist.gov/index.html および http://nvd.nist.gov/）を参照してください。

SCAPがサポートするバージョンとプラットフォーム

アプライアンスは、SCAP 1.0、1.1、1.2、および 1.3 をサポートしています。SCAP は、Windows 7 以降のプラットフォーム（32 ビットおよび 64 ビットシステム）で動作することが認定されています。

アプライアンスは、管理対象デバイスにインストールされている KACE エージェントソフトウェアを使用して SCAP スキャンを実行します。SCAP は、エージェント不要デバイスなどの、KACE エージェントソフトウェアがインストールされていないデバイスでは使用できません。

アプライアンスの SCAP スキャンの実行方法

アプライアンスは、National Checklist Repository からのセキュリティ設定チェックリストを使用して、選択したエージェント管理対象デバイスでスクリプトを実行することによって、SCAP スキャンを実行します。

SCAPバージョン1.0および1.1では、スクリプトは、次に示すSCAP標準を使用して、XML形式で書き込まれたSCAPデータストリームをチェックします：CCE、CPE、CVE、CVSS、OVAL、およびXCCDF。詳細については、「SCAP標準の定義」を参照してください。

SCAP 1.2 および 1.3 では、個々の結果ファイルがすべて 1 つの XML ファイルに結合される データストリームの概念が追加されます。また、これらのバージョンでは、ARF（Asset Report Format 1.1）と呼ばれる新しい出力形式が追加されます。詳細については、http://scap.nist.gov/specifications/arf/を参照してください。

アプライアンスは、エージェントソフトウェアを使用して SCAP スキャンコンプライアンスチェックを実行します。結果ファイルはアプライアンスまたは組織データベースにアップロードされ、政府機関に報告するための1つのファイルにまとめられます（必要な場合）。結果はアプライアンスの SCAPスキャン結果 ページにも各デバイスについて表示されます。

アプライアンス上で組織コンポーネントが有効化されている場合は、組織ごとにSCAPスキャン結果を個別に表示できます。

SCAPではOVALインタープリターバージョン5.10.1を使用して次を提供します。

- オペレーティングシステムおよびソフトウェアアプリケーションが異なるデバイスに対するセキュリティ設定の監視
- 任意の時点におけるシステムのセキュリティステータス
- さまざまな一連のセキュリティ要件に対するコンプライアンス
- セキュリティタスクを実行する標準化かつ自動化された方法
- セキュリティツール間の相互運用性

このような特長により、ソフトウェアのセキュリティ、脅威評価、および脆弱性修正が向上します。

注: 現在、アプライアンスではカスタマイズはサポートされていません。

SCAP標準の定義

SCAPスキャンでは、指定したプロトコルおよび標準を使用して、デバイスのセキュリティを監視します。

標準	定義
CCE	Common Configuration Enumerationは、システム設定の問題に一意の識別子を付与し、複数の情報源およびツールに対する設定データを素早く正確に関連付けます。 アプライアンスの SCAP スキャンが生成するコンプライアンスチェックの結果には、XCCDF に対する関連する CCE ID のリファレンスと、チェックリスト定義での指定に従ってチェックされた各ルールの OVAL 定義が含まれます。 CCE情報は、XCCDF結果ファイルおよびアプライアンスの SCAPスキャン結果 ページで確認できます。

標準	定義
CPE	Common Platform Enumerationは、情報技術システム、プラットフォーム、パッケージ向けの構造化された命名規約です。CPEはURI（ユニフォームリソースアイデンティファイア）の汎用構文に基づき、公式名前形式、複雑なプラットフォームを記述するための言語、システムに対する名前チェックの方法、テキストとテストを名前にバインドするための記述形式が含まれています。本質的には、CPEはセキュリティチェックリストが正しいプラットフォームに適用されるようにするものです。 この情報は、XCCDF結果ファイルおよびアプライアンスの SCAPスキャン結果 ページで確認できます。
CVE	Common Vulnerability and Exposuresは、一般に知られたセキュリティの脆弱性とソフトウェアの脆弱性に標準の識別子（共通名）を付与するリストまたは辞書です。 アプライアンスの SCAP スキャンが生成するコンプライアンスチェックの結果には、関連する CVE ID のリファレンスと、チェックリスト定義でチェックされた各ルールの OVAL 定義が含まれます。 各パッチまたは脆弱性について、CVE IDリファレンスがアプライアンスの SCAPスキャン結果 ページに表示されます。 CVE情報は、スキャンで生成されるパッチ結果XMLファイルに保存されます。ファイルは、エージェントの作業ディレクトリおよびサーバーの SCAPスキャン結果 ページで、調査と検証に使用できます。
CVSS	Common Vulnerability Scoring Systemは、ITの脆弱性の特性とインパクトを通知するためのオープンなフレームワークを提供します。その定量的モデルによって、正確な測定を繰り返し行うことができると同時に、スコアを生成するために使用された、基になる脆弱性の特性をユーザーが確認できるようにします。CVSSは、脆弱性のインパクトの正確かつ一貫したスコアを必要とする業種、組織、および政府に適しています。特に、CVSSは、脆弱性修復活動の優先順位を決め、脆弱性の重大度を計算するために役立ちます。National Vulnerability Database（NVD）では、ほとんどすべての既知の脆弱性に対してCVSSスコアを提供しています。
OVAL	Open Vulnerability and Assessment Languageは、一般に公開されているオープンなセキュリティコンテンツを普及させるための情報セキュリティコミュニティの国際標準です。セキュリティツールとサービス全体に渡ってこれらの情報の転送を標準化します。 各OVALテストの結果はターゲットデバイスの複数のファイルに書き込まれた後、アプライアンスの1つの結果ファイルにまとめられ、SCAPスキャン結果 ページに表示されます。

標準	定義
SCAP	SCAP（Secure Content Automation Protocol）は、ソフトウェアの脆弱性の列挙、セキュリティ関連の設定および製品名の監視、デバイスの検査による脆弱性の検出と検出されたセキュリティ問題のインパクトの評価（スコア付け）を行う、一連のオープンスタンダードです。詳細については、「SCAPについて」を参照してください。
XCCDF	eXtensible Configuration Checklist Description Formatは、セキュリティチェックリスト、ベンチマーク、関連ドキュメントを作成するための仕様言語です。XCCDFファイルには、一連のターゲットデバイスに関する構造化されたセキュリティ設定ルール一式が含まれています。仕様は、情報の交換、ドキュメント生成、組織および状況へのカスタマイズ、コンプライアンスの自動テストおよびコンプライアンスのスコアをサポートするよう、設計されています。詳細については、「SCAPスキャンの仕組み」を参照してください。

ベンチマークについて

SCAPベンチマークは、特定の運用環境でデバイスの脆弱性を評価するための一連のルールを含む、セキュリティ設定チェックリストです。

NIST（National Institute of Standards and Technology）が管理するNational Checklist Repositoryには、特定のIT製品とIT製品のカテゴリに関するさまざまなセキュリティ設定チェックリストが格納されています。

USGCB（米国政府共通設定基準）ベンチマーク基準は、FDCC（Federal Desktop Core Configuration）から発展したもので、現在、Windows OS に対応しています。

SCAP 1.0 および 1.1 のみ。チェックリストは、SCAPストリームという複数のXMLファイルが格納されたZIPファイルで構成されています。ストリーム内の主要ファイルはXCCDFファイルです。XCCDFファイルは、一連のターゲットデバイスに関する構造化されたセキュリティ設定ルール一式です。基本的に、実行する必要のあるOVALテストのリストです。その他のXMLファイルには、XCCDFファイルで指定されているOVALテストが格納されています。XCCDF 仕様に関する詳細については、http://scap.nist.gov/specifications/xccdf/を参照してください。

SCAP 1.2 以降のみ。これらのバージョンでは、必要なすべてのストリームを含む単一のファイルが使用されます。

ベンチマークには、1つ以上のプロファイルが含まれる場合があります。プロファイルは、特定の種類のデバイスに対して実行されるルールを指定します。例えば、ベンチマークには、デスクトップに関するルール一式と、サーバーに関する別のルール一式が含まれる場合があります。

SCAPスキャンの仕組み

SCAP スキャンを実行する前に、アプライアンスは、ベンチマークのインポートと検証を行います。インポートと検証の完了後、ベンチマークはアプライアンスに読み込まれ、XCCDFファイルは解決と呼ばれるプロセスに渡されます。

解決中に、oval-command.zipファイルが生成されます。このZIPファイルには、特定のプロファイルの実行に必要な入力ファイルが格納されています。このファイルは Script Detail（スクリプトの詳細）ページで確認できます。詳細については、「SCAPスケジュールの設定」を参照してください。

SCAPスキャンはKScriptによって制御されます。スキャンの実行時、次のファイルがスクリプト依存関係としてターゲットデバイスにダウンロードされます。

- benchmark.zip：ベンチマークファイル（アプライアンスにアップロードされた SCAP ストリーム）が格納されています（XCCDFファイルはデバイスによって実際には使用されません）。
- oval-command.zip：XCCDF によって生成された入力ファイルが格納されています。
- ovalref.zip：OVAL スキャンエンジン（ovaldi.exe）が格納されています。

KScriptは、ターゲットデバイス上でOVALスキャンを開始し、複数の結果ファイルを生成します。OVALスキャンエンジンは、2回または3回実行されます。

- 最初の実行では、ターゲットデバイスがそのベンチマークプロファイルに対して正しいプラットフォームであることを、ベンチマークに含まれるCPEファイルを使用してチェックします。
- 2回目の実行では、ベンチマークに定義されたルールを使用して、デバイスの脆弱性をチェックします。また、CCE標準を実装します。
- 3回目の実行では、セキュリティパッチが最新であることをチェックします。また、CVE標準を実装します。

各実行で、結果ファイルが生成されます。これらのファイルは実行に従って名前が付けられます。例えば、最初の実行で生成されたファイルの名前はscap-profile-10-result-1.xml、2回目のファイルはscap-profile-10-result-2.xmlとなります。これらのファイルは、次のディレクトリに配置されます。C:\Documents and Settings\All Users\Quest\KACE\kbots_cache\packages\kbots**<working directory>**.

KACE エージェントの作業ディレクトリを探すには、**インベントリ > デバイス > デバイスの詳細 > ログ** に移動します。

その後、これらの結果ファイルはアプライアンスにアップロードされ、1 つの結果ファイル（xccdf-results.xml）にまとめられます。このファイルは、US OMB（米国行政予算管理局）のような政府系機関への結果のレポートに使用できます。アプライアンスおよび管理対象デバイスには最新の結果ファイルのみが保持されます。

実行の最終の手順で、結果ファイルのサブセットは、「組織」データベースに抽出されて格納され、各デバイスの SCAPスキャン結果 ページでのレポートの作成と表示に使用できるようになります。

この情報が格納されるデータベーステーブルは、SCAP_RESULT、SCAP_RESULT_RULE、および SCAP_RESULT_SCOREです。詳細については、「SCAPスキャン結果の表示」を参照してください。

SCAPスキャン情報へのアクセス

SCAPスキャン情報は、セキュリティ セクションからアクセスできます。

1. SCAPスキャン ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**SCAPスキャン** をクリックします。
    c. このページには次の3つのリンクがあります。

    - **カタログ**：SCAPベンチマークのステータスが表示されます。さらに、このページから、チェックリストをインポートしたり、削除したり、CSV形式でエクスポートしたりできます。
    - **スケジュール**：ベンチマークの名前とそれらの実行スケジュールが表示されます。さらに、このページから、ベンチマークを追加/削除したり、有効/無効にしたり、CSV形式でエクスポートしたりできます。
    - **レポート作成**：SCAPスキャンの全般的な結果が表示されます。

    このページには、ベンチマークごとの結果を示すダッシュボードも表示されます。デバイスがベンチマークに合格するには、100 %のスコアを獲得する必要があります。

ベンチマークの表示と管理

アプライアンスにインポートされたプロファイルとチェックリストを含むSCAPベンチマークを表示および管理することができます。

さらに、SCAPカタログ ページで **アクションの選択** を選択して、ベンチマークのインポート、ベンチマークの削除、およびベンチマークのCSV形式へのエクスポートを行うことができます。

1. SCAPカタログ リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**SCAPスキャン** をクリックします。
    c. SCAPスキャン パネルで **カタログ** をクリックします。
2. **オプション**：特定基準で表示 ドロップダウンリストまたは 検索 フィールドを使用して、表示されるベンチマークを指定します。

    タイトルまたは識別子内の文字列の一部に基づいて検索できます。
3. **オプション**：ベンチマークを並べ替えるには、列見出しをクリックします。
4. ベンチマークの名前をクリックして、詳細を表示します。

    「SCAPカタログ」には、選択したベンチマークの一般情報と、SCAPデータがアプライアンスにアップロードされた日時が表示されます。詳細については、「アーカイブからのベンチマークのダウンロード」を参照してください。

ベンチマークのインポートと修正

必要に応じて、National Checklist Repositoryからベンチマークをインポートして修正できます。

National Checklist Repository（https://web.nvd.nist.gov/view/ncp/repository）からベンチマークまたはチェックリストをダウンロードします。

1. SCAPカタログ リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**SCAPスキャン** をクリックします。
    c. SCAPスキャン パネルで **カタログ** をクリックします。
2. **アクションの選択 > 新しいチェックリストのインポート** を選択します。

    SCAP設定のスキャン設定 ページが表示され、インポートウィザードの手順1が表示されます。
3. **参照** または **ファイルの選択** をクリックして、ベンチマークZIPファイルをインポートします。
4. **次へ** をクリックします。

    ダイアログボックスが表示されて、ファイルをアップロード中であることが示されます。ファイルのアップロード後、インポートの成功を通知するメッセージが SCAP設定のスキャン設定 ページに表示されます。

    注: アプライアンスによって、ZIPファイルに有効なベンチマークが格納されてることが検証されます。有効なベンチマークが格納されていない場合、エラーメッセージが表示され、ファイルはアップロードされません。
5. スキャンするプロファイルの選択 ドロップダウンリストでベンチマークを選択し、**次へ** をクリックします。

手順2が表示されます。

6. 既存のエンジンを使用したスキャン ドロップダウンリストで、使用するOVALエンジンを選択します。

   注: デフォルトのエンジンはMITREのOVALインタープリター（ovaldi.exe）です。Quest によってエンジンと OVAL 定義の新しいバージョンが認定されてリリースされると、アプライアンスはこのエンジンに対するそれらの更新を自動的にダウンロードします。

7. **オプション**：**参照** または **ファイルの選択** をクリックして、カスタムエンジンとその設定ファイルを見つけてアップロードします。

   ダイアログボックスが表示され、ファイルをアップロード中であることが示されます。アップロード後、エンジンのインポートの成功を通知するメッセージが SCAP Configuration Scan Settings（SCAP 設定のスキャン設定）ページに表示されます。

   ヒント: OVALエンジンのローカル制御が必要な場合や、エンジンを変更するための自動更新が不要な場合は、カスタムエンジンを使用します。カスタムエンジンは、カスタム ovaldi.exe と共に、エンジンの実行に必要な設定ファイルを格納したフォルダの ZIP ファイルであることが必要です。SCAP スキャンスクリプト内の ovalref.zip 依存関係ファイルをこの ZIP ファイルに置き換えます。詳細については、「解決されたXCCDFファイルの表示」を参照してください。

8. **次へ** をクリックします。

ダイアログボックスが表示されて、ベンチマークファイルを読み込み中であることが示され、続いて Script Detail（スクリプトの詳細）ページが表示されます。詳細については、「SCAPスキャンスケジュールの編集」を参照してください。

SCAPスケジュールの設定

SCAPスケジュールを設定することにより、ベンチマークまたは定義をインポートしたり、SCAPスキャンの設定を変更したりできます。

1. SCAPスキャンスケジュール リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**SCAPスキャン** をクリックします。
   c. SCAPスキャン パネルで **スケジュール** をクリックします。
2. **アクションの選択** を選択し、実行するアクション（ベンチマークの追加/削除、有効化/無効化、またはCSV形式でのエクスポート）を選択します。
3. スクリプトの詳細 ページで、スケジュールを編集するベンチマークをクリックします。
4. このページで、スケジュール セクションまで下へスクロールし、必要な変更を行います。

SCAPスキャンスケジュールの編集

Script Detail（スクリプトの詳細）ページからベンチマークスケジュールを表示したり編集したりできます。このページでは、SCAPスキャンを設定したり、スケジュールしたり、SCAPスキャンを実行するデバイスを指定したりするスクリプトを管理およびカスタマイズできます。SCAP用のスクリプトは標準のKScriptです。

注: このセクションでは、Script Detail（スクリプトの詳細）ページで使用できる機能に関する情報をすべて提供するわけではありません。SCAP スキャンの使用と理解に関係のある情報のみを提供します。

注: KScript の編集の詳細については、スクリプトの追加と編集を参照してください。

Script Detail（スクリプトの詳細）ページには、ベンチマークウィザード（SCAPスキャン情報へのアクセスを参照）、または SCAP Scan Schedules（SCAP スキャンスケジュール）ページ（SCAPスキャン結果の表示を参照）からアクセスできます。

解決されたXCCDFファイルの表示

SCAPスキャン解決プロセスで生成された入力ファイルを表示できます。

ベンチマークはサーバーに読み込まれ、XCCDFファイルは解決と呼ばれるプロセスに渡されます。それにより、特定のプロファイルの実行に必要な入力ファイルが生成されます。

1. スクリプトの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
    c. スクリプトの名前をクリックします。
2. （オプション）スクリプトの実行に必要な実行可能サポートファイルを追加するには、依存関係 セクションまでスクロールして、**新しい依存関係の追加** をクリックし、**参照** または **ファイルの選択** をクリックします。
3. **オプション**：これらのファイルの詳細を表示するには、選択したZIPファイルをクリックしてダウンロードします。
4. これらの依存関係ファイルがどのように実行されるかを確認するには、タスク セクションを表示します。

OVALタイムスタンプの表示

OVALタイムスタンプ（OVALドキュメントが作成された時刻）を表示できます。

1. スクリプトの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
    c. スクリプトの名前をクリックします。
2. 依存関係 セクションまでスクロールして、**benchmark.zip**をクリックし、OVAL XMLファイルを展開します。

    例えば、fdcc-winxp-oval.xmlとなります。
3. OVALファイルで、**<oval:timestamp>**を探します。

スクリプトタスクの表示

特定のスクリプトに関連付けられたタスクを表示できます。

1. スクリプトの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**スクリプト作成** をクリックして、**スクリプト** をクリックします。
    c. スクリプトの名前をクリックします。
2. タスク セクションまでスクロールします。

タスク セクションが スクリプトの詳細 ページに表示されます。

SCAPスキャン結果の表示

Scan Results（スキャン結果）ページには、SCAP スキャンの結果がデバイス別に表示されます。このページから、各スキャンに関する詳細情報にアクセスできます。

1. SCAPスキャン ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**SCAPスキャン** をクリックします。
    c. SCAPスキャン パネルで **レポート作成** をクリックします。
2. **オプション**：特定のベンチマークに関する結果を表示するには、右側のテーブルの上に表示される 特定基準で表示 ドロップダウンリストで必要なベンチマークを選択します。

    結果ページには、次の情報が表示されます。

セクション	説明
デバイス名	スキャンが実行されたデバイスです。
ベンチマーク - プロファイル	ベンチマークで使用された特定のプロファイルです。
スキャンされました	スキャンが実行された日時です。
成功	デバイスが合格したルールの数です。
失敗	デバイスが不合格となったルールの数です。
その他	error、unknown、not checked、not applicable、informationalのようなその他の値が返されたルールの数です。 XCCD仕様では、「not selected」も定義されていますが、結果からは除外されます。
合計	実行されたルールの合計数です。
コンプライアンス	合格したルールの割合（%）です。
スコア	ベンチマークによって定義されているデフォルトのスコアです。
結果	スキャンの結果（成功または失敗）。

3. 特定のデバイスに関する詳細を表示するには、デバイス 列でそのデバイスの名前をクリックします。

    ページが開き、選択したデバイスに関するスキャン結果の詳細が表示されます。次の表では、各セクションについてより詳細に説明します。

セクション	説明
概要	ベンチマークに関する一般的な情報です。

セクション	説明
テスト結果	ツリー構造で表示されるテスト結果で、ルールをグループ化して表示します。アイコンは、ルールの合否のステータスを示します。ルールをクリックすると、ダイアログボックスが開き、ルールの詳細が表示されます。
スコア	ベンチマーク用に定義されているスコアモデルごとのコンプライアンススコアです。
CCEによる結果	CCEに基づいた合否の結果です。FDCCでは、コンプライアンスがCCEに基づいてレポートされることが必要です。
結果のXMLファイル	XMLファイルへのリンクです。 • **XCCDFベンチマーク**: XCCDFファイルによって処理されたファイルであり、OVALスキャンエンジンの各実行から生成された結果ファイルが1つの結果ファイル（xccdf-results.xml）にまとめられたファイルです。 • **CPEインベントリ**: OVALスキャンエンジンの最初の実行によるファイル出力で、ベンチマークがスキャン対象のデバイスに適用されるかどうかをテストします。 • **OVALコンプライアンス**: OVALスキャンエンジンの2回目の実行によるファイル出力で、ベンチマークに定義されたルールに対してデバイスをテストします。 • **OVALパッチ**: OVALスキャンエンジンの3回目の実行によるファイル出力で、セキュリティパッチが最新であることが検証されます。 詳細については、「SCAPスキャンの仕組み」を参照してください。

4. ルールの詳細を表示するには、ルールのアイコンをクリックします。

   そのルールの「詳細の表示」が開きます。このページには、ルールに対するデバイスの合否にかかわらず、XCCDF定義からのルールの説明と、ルールのXMLが表示されます。

アーカイブからのベンチマークのダウンロード

毎日、アプライアンスは、デバイスから SCAP スキャン結果を収集し、各ベンチマークのアーカイブを作成します。ベンチマークアーカイブは、US OMB（米国行政管理予算局）のような該当する政府系機関に送信できるZIPファイルで構成されています。

1. SCAPカタログ リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**SCAPスキャン** をクリックします。

c. SCAPスキャン パネルで **カタログ** をクリックします。

2. ダウンロードするベンチマークの名前をクリックします。
3. 結果のアーカイブのダウンロード フィールドで、ZIPファイルをクリックしてアーカイブをダウンロードします。

   このファイルには、選択したベンチマークを使用してスキャンされたすべてのデバイスに関する結果が格納されています。

エージェントのプロビジョニングを妨げる Windows のセキュリティに関する問題の解決

Windows のセキュリティ設定によって、アプライアンスによる Windows デバイスへのエージェントのプロビジョニングが妨げられる場合は、コマンドプロンプトを使用して設定を変更できます。

プロビジョニングを許可するには、ファイアウォールを開いてセキュリティ設定を行う必要があります。

1. デバイスでコマンドプロンプトを開きます。
2. ファイアウォールを開いてセキュリティ設定を行います。

   reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v ForceGuest /t REG_DWORD /d 0 /f

   reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f

   reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v FdenyTSConnections /t REG_DWORD /d 0 /f

   netsh.exe firewall set service type=FILEANDPRINT mode=ENABLE scope=ALL

   netsh.exe firewall set service type=REMOTEADMIN mode=ENABLE scope=ALL

アプライアンスのセキュリティの維持

アプライアンスセキュリティを維持するには、日次セキュリティレポートを確認し、使用可能になったアプライアンスソフトウェアの更新を適用します。

アプライアンスソフトウェアの更新が公開された場合は、アプライアンスのダッシュボードで通知されます。

セキュリティの実行出力

アプライアンスのセキュリティステータスは、**セキュリティの実行出力**の E メールに示されます。

アプライアンスの **セキュリティの実行出力** は毎日、午前 2:00 に E メールでシステム管理者に自動的に送信されます。

以下の例は、**セキュリティの実行出力**の内容を示します。

```
Checking setuid files and devices:
Checking for uids of 0:
root 0
toor 0
Checking for passwordless accounts:
MyK1 kernel log messages:
+++ /tmp/security.G1jFJvQh 2013-04-21 02:01:01.000000000 -0700
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
```

+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
MyK1 login failures:
MyK1 refused connections:
-- End of security output --

隔離された添付ファイルを管理する

アプライアンスは、サービスデスクファイルの添付ファイルに対するマルウェアスキャン機能を搭載しています。アプライアンスの自動プロセスにより、ウイルス定義リストが定期的に更新されます。サービスデスクチケットに添付されたファイル、およびチケット関連の E メールの添付ファイルは、チケットに追加される前にスキャンされます。

隔離されたファイルは、ウイルス対策の検疫 ページにリストされます。このページを使用して、隔離されたサービスデスクの添付ファイルを確認および管理します。脅威が検出されると通知が表示され、ファイルに関連付けられたデバイスへのリンクが示されます。また、特定の種類の脅威が検出された場合や、そのステータスの変更に基づいて通知を作成することもできます。

1. ウイルス対策の検疫 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**セキュリティ** をクリックして、**ウイルス対策の検疫** をクリックします。

    デフォルトでは、ウイルス対策の検疫 ページには、検疫から拒否または解放されていない新しい脅威が表示されます。これらの項目は、常にアプライアンスのバックアップに含まれます。必要に応じて、特定基準で表示 メニューを使用してこのリストをフィルタできます。
2. ファイルのリストを確認し、該当するアクションを実行します。

    隔離されたファイルごとに、リストには、名前、ファイルが最初に表示された時刻と最後に表示された時刻、マルウェアの変種の名前、およびファイルの解放または拒否に関する追加情報が表示されます（ 該当する場合 ）。

    - 関連付けられたサービスデスクチケット内の隔離されたファイルへのアクセスを有効にするには、リストでそのファイルを選択し、**アクションの選択 > リリース** をクリックします。
    - サービスデスクチケット内の隔離されたファイルへのアクセスをブロックするには、リストでそのファイルを選択し、**アクションの選択 > 拒否** をクリックします。
    - サービスデスクチケットから隔離されたファイルを削除にするには、リストでそのファイルを選択し、**アクションの選択 > 削除** をクリックします。

    アクションの選択 メニューでは、リストをエクスポート、またはレポートを作成することもできます。

レポートの使用と通知のスケジュール

レポートを実行し、指定した条件を満たした場合に管理者に通知を送信するように、アプライアンスを設定できます。

レポートと通知について

アプライアンスを使用すると、さまざまなレポートと通知を作成およびスケジュールできます。レポートではインベントリアイテムに関する情報を収集し、通知では指定した条件を満たした場合にEメールで警告を送信できます。

レポートについて

アプライアンスには、ソフトウェア、ハードウェア、サービスデスク、およびその他のアイテムの標準レポートが多数用意されています。

アプライアンス上で組織コンポーネントが有効化されている場合は、各組織およびシステムレベルのレポートを個別に作成して実行できます。システムレベルのレポートには、すべての組織からの情報を集約した総合レポートと、各種のアプライアンスコンポーネントの標準レポートが含まれます。

通知について

通知は、デバイス、スキャン結果、および資産が指定された条件を満たす場合に、アプライアンスから管理者宛てに送信されるEメールメッセージです。

例えば、デバイスがディスク領域の制限に近づいたときに管理者に通知する場合は、ディスク使用量に基づき警告をセットアップできます。通知は、デバイスが指定された条件を満たす場合に送信されます。

アプライアンスは、指定された頻度で実行される通知スケジュールに従って、インベントリと条件を照合します。アイテムが基準を満たした場合、指定された受信者にEメールが送信されます。

インベントリのチェックは、デフォルトでは1時間ごとに行われます。頻度を変更するには、通知スケジュールを編集します。詳細については、「通知スケジュールの編集」を参照してください。

注: 通知および日次レポートは、デフォルトのアドレスである Charlie Root（root@**appliance_hostname**）から送信されます。このアドレスを変更することはできません。

レポート設定の変更追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

レポートの作成と変更

SQLクエリを使用してリストページからレポートを作成できます。また、レポートウィザードを使用して レポート作成 セクションからもレポートを作成できます。

レポートの作成

インベントリ情報などのデータを収集して分析するレポートを作成できます。

レポートを作成するには、いくつかの方法があります。

- レポート ページのレポートウィザードを使用します。詳細については、「レポートウィザードを使用したレポートの作成」を参照してください。
- レポート ページのSQLレポートフォームを使用します。詳細については、「SQLクエリを使用したレポートの作成」を参照してください。
- デバイス、資産、管理対象インストール などのリストページのメニューオプションを使用します。詳細については、「リストページからのレポートの作成」を参照してください。

また、XSL（Microsoft Excel）形式またはCSV（コンマ区切り値）形式でレポートを生成し、Microsoft Excelなどのツールにデータをインポートして、チャートおよびグラフを作成できます。

注: CSVファイルをExcelにインポートすると、マルチバイト文字（日本語および中国語の文字セットをサポートするために使用される文字）が「文字化け」として表示される場合があります。詳細については、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。

レポートウィザードを使用したレポートの作成

レポートウィザードを使用して、SQLクエリを作成せずにデータベースから収集する情報を識別できます。

1. 次のいずれかの操作を行って、Reports（レポート）リストに移動します。
   - **アプライアンスの組織コンポーネントが有効で、システムレベルのレポートにアクセスする必要がある場合：**

     アプライアンスシステム管理コンソール（https://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。次に、**レポート作成** をクリックします。
     システムレベルのレポートには、すべての組織からの情報を集約した総合レポートと、各種のアプライアンスコンポーネントの標準レポートが含まれます。
   - **アプライアンスで組織コンポーネントが有効化されていない場合、または組織レベルレポートにアクセスする場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。次に、レポート作成 をクリックします。**

     組織レベルのレポートには、各種のアプライアンスコンポーネントの標準レポートが含まれます。アプライアンスで組織コンポーネントが有効になっている場合、これらのレポートは選択された組織に固有の情報を提供します。

   レポート リストが表示されます。
2. **アクションの選択 > 新規作成（ウィザード）** を選択して、タイトルとトピック ページを表示します。
3. 次の設定を指定します。

オプション	説明
タイトル	レポートリストに表示されるレポートの表示名。リスト内の他のレポートと区別できるように、できるだけ分かりやすいタイトルを入力してください。
カテゴリ	レポートのカテゴリ。そのカテゴリがまだない場合は、Reports（レポート）ページのドロップダウンリストに追加されます。
説明	レポートの説明。
行番号の表示	レポートの行番号がある列を表示します。
トピック	レポートのトピック。この設定に基づいて、レポートで使用可能なフィールドが決定されます。
サブトピックの追加	このリンクをクリックして、関連トピックを最大2つまでレポートに追加します。これにより、同じレポート内で最大3つまでのデータタイプの関係を表示できます。 HTML形式でレポートを生成すると、各行の展開や折り畳みを行うことで、必要に応じて情報の詳細を掘り下げることができます。 **サブトピックの追加** をクリックすると、選択するトピックに応じて追加オプションが使用可能になります。例えば、**デバイス**、**ソフトウェア**、および **ファイル同期** を選択すると、次の 2 つのチェックボックスが表示されます。 • **デバイス** からの行のみを表示します（少なくとも1つの **ファイル同期** の行を含む）。 • **ファイル同期** からの行のみを表示します（少なくとも1つの **ソフトウェア** の行を含む）。 これらのチェックボックスをオンにすることで、少なくとも1つの子行を含む「デバイス」と「ソフトウェア」のみをレポート対象にすることができます。「デバイス」の行は、対応する「ソフトウェア」の行が少なくとも1つ以上含まれている場合にのみ、レポートに表示されます。「ソフトウェア」の行は、対応する「ファイル同期」の行が少なくとも1つ以上含まれている場合にのみ、レポートに表示されます。 これらのチェックボックスをオフにすると、「デバイス」行および「ソフトウェア」行は、それぞれ「ソフトウェア」の行または「ファイル同期」の行

オプション	説明
	が含まれているかどうかにかかわらず、すべて表示されます。

4. **次へ** をクリックして、表示するフィールド ページを表示します。
5. レポートに含めるフィールドを選択します。
6. **次へ** をクリックして、列の順番 ページを表示します。
7. フィールドをドラッグして列見出しが表示される順序（上から下へ）を設定します。レポート出力では、列見出しは左から右の順序で表示されます。
8. **次へ** をクリックして、並べ替えとブレーク ページを表示します。
9. 行をどのように編成するかを設定します。
   - **優先順位キー**: 結果をどのように並べ替えるかを指定します。レポートデータは、1つ目のフィールド、2つ目のフィールド、3つ目のフィールドの順にそれぞれの選択内容に基づいて編成されます。1つ目の並べ替えフィールドには、レポート出力ページに表示することを選択した1つ目のフィールドが表示されます。
   - **シーケンス**: 英数字の昇順または降順のどちらで結果を表示するか指定します。
   - **区切りヘッダー**: 優先順位キー で選択したフィールドの名前を使用して、結果を小見出しでグループ化するかどうかを選択します。
10. **次へ** をクリックして、フィルタ ページを表示します。
11. **オプション**：レポートで返されるデータセットを限定する場合は、フィルタ基準を追加します。
    a. **レコードをフィルタリングするルールの指定** をクリックします。

       ルールセットと次のすべての条件に一致 が表示されます。これらのルールはブール論理の **AND** ステートメントに相当します。アイテムがレポートに表示されるには、このセクションのすべてのルールに一致する必要があります。

    b. フィルタ条件を指定し、**保存** をクリックします。
    c. ルールを現在のルールセットに追加するには、**追加** ボタン（ ）をクリックします。
    d. フィルタ条件を選択し、行の右側にある **保存** をクリックします。
    e. ルールのサブセットを追加するには、**サブセットの追加** ボタン 。

    最初にネストされたサブセットは、「**次のいずれかの条件に一致**」ルールセットに追加されます。これらのルールはブール論理の **OR** ステートメントに相当します。これにより、最上位の **AND** 基準の下に、**OR** 基準をネストすることができます。アイテムがレポートに表示されるには、「**次のすべての条件に一致**」ルールセットの基準を満たし、かつ、「**次のいずれかの条件に一致**」ルールセットの基準の少なくとも1つを満たす必要があります。

    f. ルールセットの隣の**保存** をクリックします。
    g. 必要に応じて、他のルールおよびルールのサブセットを追加します。
12. **保存** をクリックします。

    レポート ページが開き、新しいレポートがリストに表示されます。右側のテーブルの上に表示される 特定基準で表示 リストが、自動的に新しいレポートのカテゴリに設定されます。
13. レポートを実行するには、レポートの生成 列の形式をクリックします。

    出力が生成されます。HTML 形式のレポートでは、最初のデータ列が**管理者コンソール**のアイテムの詳細ページに自動的にリンクされます。

ヒント: チャートおよびグラフは、アプライアンスのレポート作成ツールでは作成できません。チャートまたはグラフを作成するには、レポートを **XLS**（Microsoft Excel）形式または **CSV**（コンマ区切り値）形式で生成し、チャート機能またはグラフ機能を持つツール（Microsoft Excel など）にデータをインポートします。

SQLクエリを使用したレポートの作成

レポートフォームにSQLクエリを入力して、レポートを作成することができます。

使用するSQLクエリが不明の場合は、レポートウィザードの使用を検討してください。詳細については、「レポートウィザードを使用したレポートの作成」を参照してください。

1. 次のいずれかの操作を行って、Reports（レポート）リストに移動します。
   - **アプライアンスの組織コンポーネントが有効で、システムレベルのレポートにアクセスする必要がある場合：**

     アプライアンスシステム管理コンソール（https://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。次に、**レポート作成** をクリックします。
     システムレベルのレポートには、すべての組織からの情報を集約した総合レポートと、各種のアプライアンスコンポーネントの標準レポートが含まれます。
   - **アプライアンスで組織コンポーネントが有効化されていない場合、または組織レベルレポートにアクセスする場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。次に、レポート作成 をクリックします。**

     組織レベルのレポートには、各種のアプライアンスコンポーネントの標準レポートが含まれます。アプライアンスで組織コンポーネントが有効になっている場合、これらのレポートは選択された組織に固有の情報を提供します。

   レポート リストが表示されます。
2. **アクションの選択 > 新規作成（SQL）** を選択して、レポートの詳細 ページを表示します。
3. レポート設定を指定します。

オプション	説明
タイトル	レポートリストに表示されるレポートの表示名。リスト内の他のレポートと区別できるように、できるだけ分かりやすいタイトルを入力してください。
説明	レポートの説明。
カテゴリ	レポートのカテゴリ。そのカテゴリがまだない場合は、Reports（レポート）ページのドロップダウンリストに追加されます。
列の区切り	SQL列名のコンマ区切りリスト。レポートには、区切りヘッダーと、これらの列についての小計が生成されます。
行番号の表示	レポートの行番号がある列を表示します。
SQL	レポートデータを生成するクエリステートメントです。詳細については、MySQL のドキュメント（http://dev.mysql.com/doc/refman/5.0/en/）を参照してください。 サービスデスクのHD_Ticketテーブルに対してレポートまたはクエリを書き込むと、ユーザー カスタムフィールドには、HD_TICKETテーブル内のUSERテーブルに基づくユーザーIDが保存されます（HD_TICKETテーブルはチケットレコードが保持

オプション	説明
	されるテーブルです）。レポートにユーザーIDではなく、ユーザー名を表示する場合は、USERテーブル上で連結する必要があります。 詳細については、「データベーステーブル名」を参照してください。
組織の設定	これらの設定は、組織コンポーネントが有効になっているアプライアンス上のシステムレベルでのみ使用可能です。オプションは次の通りです。 • **すべての組織**: すべての組織で繰り返し参照するようSQL Selectステートメントが変更されます。レポートにはすべての組織の情報が含まれます。 • **結果の集計**: すべての組織のレコードを結合するようSQL Selectステートメントが変更されます。レポートには、すべての組織の概要情報が含まれます。このタイプの標準レポートは、総合レポートに分類されます。

4. **保存** をクリックします。

   アプライアンスでレポートの構文がチェックされ、エラーが見つかった場合はその エラーが表示されます。
5. 新しいレポートを実行するには、レポートの生成 列の形式をクリックします。

   ヒント: チャートおよびグラフは、アプライアンスのレポート作成ツールでは作成できません。チャートまたはグラフを作成するには、レポートを **XLS**（Microsoft Excel）形式または **CSV**（コンマ区切り値）形式で生成し、チャート機能またはグラフ機能を持つツール（Microsoft Excel など）にデータをインポートします。

リストページからのレポートの作成

デバイス ページなどのリストページを表示中に、レポートを作成できます。

1. リストページに移動します。例えば、デバイス ページに移動するには、次のことを行います。
   a. 必要に応じて、ページの右上隅のドロップダウンリストで組織を選択します。
   b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. **アクションの選択 > レポートの作成** を選択して、レポートの詳細 ページを表示します。
3. レポート設定を指定します。

オプション	説明
タイトル	レポートリストに表示されるレポートの表示名。リスト内の他のレポートと区別できるように、できるだけ分かりやすいタイトルを入力してください。
説明	レポートの説明。
カテゴリ	レポートのカテゴリ。そのカテゴリがまだない場合は、Reports（レポート）ページのドロップダウンリストに追加されます。

オプション	説明
列の区切り	SQL列名のコンマ区切りリスト。レポートには、区切りヘッダーと、これらの列についての小計が生成されます。
行番号の表示	レポートの行番号がある列を表示します。
SQL	レポートデータを生成するクエリステートメントです。詳細については、MySQL のドキュメント（ http://dev.mysql.com/doc/refman/5.0/en/ ）を参照してください。 サービスデスクのHD_Ticketテーブルに対してレポートまたはクエリを書き込むと、ユーザー カスタムフィールドには、HD_TICKETテーブル内のUSERテーブルに基づくユーザーIDが保存されます（ HD_TICKETテーブルはチケットレコードが保持されるテーブルです ）。レポートにユーザーIDではなく、ユーザー名を表示する場合は、USERテーブル上で連結する必要があります。

4. **保存** をクリックします。

レポートが レポート ページに表示されます。

レポートの複製

アプライアンスに付属している標準レポートを含め、あらゆるレポートを複製することができます。既存のレポートに類似したレポートを作成する場合は、既存のレポートを複製するほうが、レポートを最初から作成するよりも短時間で済みます。

1. 次のいずれかの操作を行って、Reports（ レポート ）リストに移動します。

   - **アプライアンスの組織コンポーネントが有効で、システムレベルのレポートにアクセスする必要がある場合：**

     アプライアンスシステム管理コンソール（ https://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。次に、**レポート作成** をクリックします。
     システムレベルのレポートには、すべての組織からの情報を集約した総合レポートと、各種のアプライアンスコンポーネントの標準レポートが含まれます。

   - **アプライアンスで組織コンポーネントが有効化されていない場合、または組織レベルレポートにアクセスする場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。次に、レポート作成 をクリックします。**

     組織レベルのレポートには、各種のアプライアンスコンポーネントの標準レポートが含まれます。アプライアンスで組織コンポーネントが有効になっている場合、これらのレポートは選択された組織に固有の情報を提供します。

   レポート リストが表示されます。
2. レポートのタイトルをクリックします。

   レポートのタイプに応じて、Report Detail（ レポートの詳細 ）ページまたはレポートウィザードの最初のページが表示されます。
3. ページの一番下で**複製** をクリックします。

レポートのタイプに応じて、Report Detail（レポートの詳細）ページまたはレポートウィザードの最初のページが表示されます。

4. 必要に応じてレポートの詳細を修正し、**保存** をクリックします。

レポートウィザードで作成したレポート上でのSQLステートメントの編集

レポートウィザードで作成した単一トピックのレポート上でSQLステートメントを編集できます。

この編集オプションは、SQLステートメントを変更するときや、新しいレポートにコピーするときに便利です。この編集オプションは、複数トピックのレポート上では使用できません。

1. 次のいずれかの操作を行って、Reports（レポート）リストに移動します。
   - **アプライアンスの組織コンポーネントが有効で、システムレベルのレポートにアクセスする必要がある場合：**

     アプライアンスシステム管理コンソール（https://**appliance_hostname**/system）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。次に、**レポート作成** をクリックします。
     システムレベルのレポートには、すべての組織からの情報を集約した総合レポートと、各種のアプライアンスコンポーネントの標準レポートが含まれます。
   - **アプライアンスで組織コンポーネントが有効化されていない場合、または組織レベルレポートにアクセスする場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。次に、レポート作成 をクリックします。**

     組織レベルのレポートには、各種のアプライアンスコンポーネントの標準レポートが含まれます。アプライアンスで組織コンポーネントが有効になっている場合、これらのレポートは選択された組織に固有の情報を提供します。

   レポート リストが表示されます。
2. レポートウィザードで作成した単一トピックレポートのタイトルをクリックします。

   レポートウィザードが表示されます。
3. フォーム下部の **SQLの編集** をクリックして、レポートの詳細 ページを表示します。
4. 必要に応じて、SQL フィールドのテキストを編集またはコピーして、**保存** をクリックします。

注: 異なるタイプのレポート間でSQLステートメントをコピーする場合、SQLステートメントの使用前に、修正が必要になる可能性があります。例えば、SQLステートメントをアプリケーションコンプライアンスレポートからコピーして、組織の 結果の集計 オプションが選択されているレポートに貼り付けた場合、SQLステートメントのエラーが報告されます。エラーが解決されるまで、レポートを保存できません。

履歴リストからのレポートの作成

履歴リストからレポートを作成できます。

1. 設定、資産、またはオブジェクトの履歴リストに移動します。
   - 資産履歴の表示
   - オブジェクト履歴の表示
   - 設定履歴の表示
2. **アクションの選択 > レポートの作成** を選択します。

   Report Detail（レポートの詳細）ページが表示されます。詳細については、「リストページからのレポートの作成」を参照してください。

レポートの変更

レポートは、必要に応じて編集または削除できます。

レポートの編集

カスタムレポートについては、どれでも編集することができます。ただし、アプライアンスに付属している標準レポートは編集できません。

標準レポートを編集するには、レポートをいったん複製してから編集します。詳細については、「レポートの複製」を参照してください。

1. 次のいずれかを実行します。
   - **組織レベルのレポートを編集するには、ページの右上隅にあるドロップダウンリストから組織を選択し（組織が存在する場合）、レポート作成 をクリックします。**
   - **システムレベルのレポートを編集するには、システム管理コンソール（http://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。次に、レポート作成 をクリックします（組織コンポーネントが有効になっているアプライアンスのみ）。**

   レポート ページが表示されます。
2. レポートのタイトルをクリックして、レポートの詳細 ページを表示します。

レポートの削除

カスタムレポートについては、どれでも削除することができます。ただし、アプライアンスに付属している標準レポートは削除できません。

1. 次のいずれかを実行します。
   - **組織レベルのレポートを削除するには、ページの右上隅にあるドロップダウンリストから組織を選択し（組織が存在する場合）、レポート作成 をクリックします。**
   - **システムレベルのレポートを削除するには、システム管理コンソール（http://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。次に、レポート作成 をクリックします（組織コンポーネントが有効になっているアプライアンスのみ）。**

   レポート ページが表示されます。
2. 1つまたは複数のレポートの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

レポートに使用する口ゴのカスタマイズ

レポートには、Quest口ゴがデフォルトで使用されますが、独自の口ゴに置き換えることができます。

独自の口ゴをアップロードするには、次の Logo Overrides（口ゴのオーバーライド）セクションを参照してください。

- 組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定
- 組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定

レポートと通知のスケジュール

アプライアンス上のアクティビティを監視するレポートおよび通知をスケジュールできます。

各組織レポートと総合レポートの実行

アプライアンス上で組織コンポーネントが有効化されている場合に、アプライアンス上に複数の組織が存在する時には、各組織の組織レポートを個別に実行できます。

また、すべての組織の情報を単一レポートに表示する総合レポートも実行できます。

各組織レポートの実行

単一組織レポートには、単一組織に固有の情報が表示されます。

アプライアンス上で組織コンポーネントが有効化されていない場合、または単一組織しか存在しない場合には、これらのレポートには「Default」組織に関する情報が表示されます。

1. レポート リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**レポート作成** をクリックして、**レポート** をクリックします。
2. レポートの生成 列で、次のいずれかのレポートの形式をクリックします。

    HTML形式のレポートは、新しいウィンドウに表示されます。他の形式の場合は、レポートのファイルを開くか、デバイスに保存できます。

> **注:** チャートおよびグラフは、アプライアンスのレポート作成ツールでは作成できません。チャートまたはグラフを作成するには、レポートを **XLS**（Microsoft Excel）形式または **CSV**（コンマ区切り値）形式で生成し、チャート機能またはグラフ機能を持つツール（Microsoft Excel など）にデータをインポートします。
>
> **注:** CSVファイルをExcelにインポートすると、マルチバイト文字（日本語および中国語の文字セットをサポートするために使用される文字）が「文字化け」として表示される場合があります。詳細については、**Questサポート**（ https://support.quest.com/contact-support ）にお問い合わせください。

総合組織レポートの実行

アプライアンス上で組織コンポーネントが有効化されている場合は、すべての組織の情報を単一レポートに統合するレポートを実行できます。

1. レポート リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**レポート作成** をクリックして、**レポート** をクリックします。
2. レポートの生成 列で、次のいずれかのレポートの形式をクリックします。

    HTML形式のレポートは、新しいウィンドウに表示されます。他の形式の場合は、レポートのファイルを開くか、デバイスに保存できます。

注: チャートおよびグラフは、アプライアンスのレポート作成ツールでは作成できません。チャートまたはグラフを作成するには、レポートを **XLS**（Microsoft Excel）形式または **CSV**（コンマ区切り値）形式で生成し、チャート機能またはグラフ機能を持つツール（Microsoft Excel など）にデータをインポートします。

注: CSVファイルをExcelにインポートすると、マルチバイト文字（日本語および中国語の文字セットをサポートするために使用される文字）が「文字化け」として表示される場合があります。詳細については、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。

レポートのスケジュール

環境を監視するために、指定した時間と間隔でレポートを実行して管理者にレポートを送信するようスケジュールできます。これはソフトウェア、デバイス、およびシステムの正常性を追跡する場合に便利です。

レポートスケジュールの追加

指定した時間にレポートを自動的に実行できるようにするレポートスケジュールを追加できます。これは、ソフトウェアライセンスコンプライアンスレポートなど、定期的な実行が必要なレポートに役立ちます。

1. 次のいずれかを実行します。
   - **組織レベルのレポートをスケジュールするには、ページの右上隅にあるドロップダウンリストから組織を選択し（組織が存在する場合）、レポート作成 をクリックします。**
   - **システムレベルのレポートをスケジュールするには、システム管理コンソール（http://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。次に、レポート作成 をクリックします（組織コンポーネントが有効になっているアプライアンスのみ）。**

   レポート ページが表示されます。
2. 次のいずれかを実行します。
   - **スケジュール ボタンをクリックします。このボタンはレポートの横にあります**。
   - **左側のナビゲーションバーで レポートスケジュール をクリックし、アクションの選択 > 新規作成を選択して、レポートスケジュールの詳細 ページを表示します。**
3. 次の設定を指定します。

オプション	説明
名前	スケジュールの表示名です。他のスケジュールからこのスケジュールを区別できるように、できる限り分かりやすい名前を入力してください。
レポート	スケジュールするレポートの名前。レポート ページのレポートの隣にある **スケジュール** アイコンをクリックすると、この名前が自動的に入力されます。
形式	レポートの形式。
説明	スケジュールの説明。この説明は、レポートのスケジュール ページに表示されます。

4. 通知 セクションで、各設定を次のように指定します。

オプション	説明
件名	レポートが含まれるEメールメッセージの件名行。

オプション	説明
受信者	レポートの送信先のEメールアドレス。アドレスが複数ある場合は、コンマで区切ります。
空のレポートを送信しない	レポートを毎回送信するか、または結果が見つかったときのみ送信するかを指定します。このオプションを選択すると、空のレポートが送信されるのを防ぐことができます。
メッセージ	Eメールメッセージの本文に記載する情報。
添付ファイルのオプション	レポートの形式。「**添付ファイル**」を選択してEメールメッセージにファイルを添付するか、「**圧縮された添付ファイル**」を選択してZIPアーカイブとしてファイルを添付します。

5. スケジュール セクションで、各設定を次のように指定します。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。

オプション	説明
	例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ (,)**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン (-)**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ (/)**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク (*) は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

6. **保存** をクリックします。

レポートスケジュールの削除

レポートスケジュールを使うと、指定した時間と間隔でレポートを実行できます。レポートスケジュールを削除すると、レポートの基準およびスケジュール設定もアプライアンスから削除されます。

レポートスケジュールは、必要に応じていつでも削除できます。

1. 次のいずれかを実行します。
   - **組織レベルのレポートスケジュールを削除するには、ページの右上隅にあるドロップダウンリストから組織を選択し (組織が存在する場合)、レポート作成 をクリックします。**
   - **システムレベルのレポートのスケジュールを削除するには、システム管理コンソール (http://appliance_hostname/system) にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択します。次に、レポート作成 をクリックします (組織コンポーネントが有効になっているアプライアンスのみ)。**

レポート ページが表示されます。

2. 左側のナビゲーションバーで、**レポートスケジュール** をクリックして、レポートスケジュール ページを表示します。
3. 1つまたは複数のレポートスケジュールの隣のチェックボックスをオンにします。
4. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

通知のスケジュール

環境の監視を管理するために、指定した基準を満たした場合に管理者にEメールで通知するようスケジュールできます。このアクティビティはシステムの正常性およびデバイスのプロパティを監視する場合に便利です。

通知スケジュールを追加、編集、および削除することができます。

レポート作成 セクションでの通知スケジュールの追加

レポート作成 セクションから、デバイス、検出スキャン、および資産に対する通知スケジュールを追加できます。

1. 通知スケジュール リストページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**レポート作成** をクリックして、**通知** をクリックします。
2. **アクションの選択** を選択して、次のいずれかを選択します。
    - **新規作成 > デバイス通知**
    - **新規作成 > 検出通知**
    - **新規作成 > 資産通知**
    - **新規作成 > 警告の監視の通知**

    通知 パネルが表示されます。

3. 通知基準を選択します。例えば、Windows 7 を搭載したデバイスが 24 時間以内にアプライアンスに接続されなかった場合に送信される通知を作成する場合は、次のように指定します。
    a. 次のように、Windows 7オペレーティングシステムがインストールされているデバイスを検出するために必要な条件を指定します。

    オペレーティングシステム: 名前 | 次の値を含む | Windows 7

    b. 演算子ドロップダウンリストで **および** を選択した状態で、**行の追加** をクリックします。
    c. 以下のように、24 時間以内にアプライアンスに接続されなかったデバイスを検出するために必要な条件を指定します。

    デバイスID情報：前回の同期時刻 | > | 24時間

4. 通知条件の下に、次の情報を入力します。

フィールド	説明
タイトル	Eメールの 件名 行に表示する情報。このタイトルは、通知の名前として 通知スケジュール ページにも表示されます。
受信者	対象とする受信者のEメールアドレス (複数可) 。Eメールアドレスは、完全修飾Eメールアドレスでなくてはなりません。複数のアドレスにEメールを送信するには、コンマを使用して各アドレスを区切るか、またはEメール配布リストを使用します。
頻度	選択した条件とインベントリのアイテムを比較するクエリがアプライアンスによって実行される間隔。条件に一致した場合、通知が送信されます。

5. **オプション**：条件を検証するには、**テスト** をクリックします。

   リストが更新されて、検索条件に一致するアイテムが表示されます。テスト中は通知は送信されません。
6. **保存** をクリックします。

通知が作成され、通知スケジュール ページに表示されます。通知の頻度のスケジュールの詳細については、通知スケジュールの編集を参照してください。

リストページからの通知スケジュールの追加

通知スケジュールを、デバイス、ソフトウェア、ソフトウェアカタログ、検出、または 資産 などのリストページから追加できます。

1. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. デバイス リストなどのリストページに移動し、リストの右上の **通知** タブをクリックします。

   通知 パネルが表示されます。

3. 通知スケジュールで使用する基準を選択します。

   詳細については、「例：高度な検索条件を使用した管理対象デバイスの検索」を参照してください。
4. 通知条件の下に、次の情報を入力します。

フィールド	説明
タイトル	Eメールの 件名 行に表示する情報。このタイトルは、通知の名前として 通知スケジュール ページにも表示されます。
受信者	対象とする受信者のEメールアドレス (複数可) 。Eメールアドレスは、完全修飾Eメールアドレスでなくてはなりません。複数のアドレスにEメールを送信するには、コンマを使用して各アドレスを区切るか、またはEメール配布リストを使用します。

フィールド	説明
頻度	選択した条件とインベントリのアイテムを比較するクエリがアプライアンスによって実行される間隔。条件に一致した場合、通知が送信されます。

5. **オプション**：条件を検証するには、**テスト** をクリックします。

   リストが更新されて、検索条件に一致するアイテムが表示されます。テスト中は通知は送信されません。
6. **保存** をクリックします。

通知が作成され、Notification Schedules（通知スケジュール）ページに表示されます。通知はデフォルトで有効になっています。通知を無効にしたり、説明を追加するには、通知スケジュールの編集を参照してください。

通知スケジュールの編集

必要に応じて、通知スケジュールの有効化と無効化、通知スケジュールの頻度の変更、および通知スケジュールの変更を行うことができます。

1. 通知スケジュール リストページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**レポート作成** をクリックして、**通知** をクリックします。
   c. 通知の名前をクリックします。
2. 必要に応じてプロパティを修正します。

フィールド	説明
有効	通知がアクティブか非アクティブかを示します。アプライアンスが選択した頻度でクエリを実行して、適切な通知を送信するようにする場合は、**有効** を選択します。アプライアンスがクエリの実行と通知の送信をしないようにする場合は、**無効** を選択します。
名前	Eメールの 件名 行に表示する情報。通知を 通知 パネルで作成する際に、この情報を タイトル フィールドに入力します。
受信者	対象とする受信者のEメールアドレス（複数可）。Eメールアドレスは、完全修飾Eメールアドレスでなくてはなりません。複数のアドレスにEメールを送信するには、コンマを使用して各アドレスを区切るか、またはEメール配布リストを使用します。
説明	任意の追加情報を入力します。
頻度	選択した条件とインベントリのアイテムを比較するクエリがアプライアンスによって実行される間隔。条件に一致した場合、通知が送信されます。

3. **オプション**：ウィザードを使用してレポートを編集するには、**保存** ボタンの上にある元の工ディタを使用して通知を再編集するには の隣の **ここをクリックします** を選択します。
4. **オプション**：通知がトリガされるSQL条件を変更するには、**保存** ボタンの上にあるこの工ディタを使用して通知を編集するには というラベルの付いたチェックボックスをオンにします。

SQLクエリを編集する場合、以下のようなasステートメントは必ずそのまま使用してください。

MACHINE.NAME AS SYSTEM_NAME

MACHINE.ID as TOPIC_ID

例：

SELECT MACHINE.NAME AS SYSTEM_NAME, SYSTEM_DESCRIPTION, MACHINE.IP, MACHINE.MAC, MACHINE.ID as TOPIC_ID FROM MACHINE WHERE ((SYSTEM_DESCRIPTION = 'Test Computer'))

5. **保存** をクリックします。

通知スケジュールの削除

通知スケジュールを削除すると、通知の基準およびスケジュール設定もアプライアンスから削除されます。

通知スケジュールは必要に応じていつでも削除できます。

1. 通知スケジュール リストページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**レポート作成** をクリックして、**通知** をクリックします。
2. 1つまたは複数の通知スケジュールの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

サーバーの監視

アプライアンスでは、インベントリ内のサーバに対して基本的なパフォーマンス監視を実行できるモジュールを提供しています。

サーバ監視について

アプライアンスの監視機能は、サーバクラスのオペレーティングシステムを対象とし、各オペレーティングシステムのパフォーマンス警告の基準を定義するデフォルトの監視プロファイルを提供します。同様の基準または別の基準を使用して、代替のイベントログまたはOSレベルログを参照する別のカスタムプロファイルを定義できます。

注: Raspbian Linux OS を実行している Raspberry Pi デバイスでは、サーバー監視はサポートされていません。

サーバー監視に対応したOSバージョンについては、**仕様に関するガイド**を参照してください。

注: Security-Enhanced Linux（SELinux）を実行している RHEL デバイスでエージェントベースの監視を使用するには、SELinux をオフにするか「許可モード」に切り替える必要があります。SELinux のモードを変更するには、ファイル /etc/selinux/config を変更してデバイスを再起動します。Red Hat Enterprise Linux での SELinux の有効化または無効化の詳細については、https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Working_with_SELinux-Enabling_and_Disabling_SELinux.htmlを参照してください。

アプライアンスのナビゲーションバーの 監視 タブでのインターフェイスコンポーネントの監視

セクション	説明
デバイス	監視対象デバイスごとに、最も重大な警告、警告数、バインドされているプロファイル数、バインドされているメンテナンスウィンドウ数、およびデバイスの設定を編集する詳細ページへのリンクが表示されます。また、このセクションでは、警告を作成および変更した時間、監視対象デバイスのIPアドレス、および設定変更警告が有効になっているかどうかを表示することもできます。
警告	警告レベル、警告の概要、警告の詳細へのリンク、警告作成の日時、最新の繰り返し時間、繰り返し回数、IPアドレス、およびステータスが表示されます。
プロファイル	プロファイル名、デフォルトのプロファイルと追加されたプロファイルのリスト、プロファイルがバインドされているデバイスの数、および特定のオペレーティングシステムタイプのデバイスにプロファイルが自動的に追加されるかどうかが表示されます。 プロファイルは、警告をトリガする基準を設定するものです。プロファイルでは、ログのパスとファイルが定義されており、ログ内で検索する検索テキスト、警告に割り当てられる重要度も定義されています。

セクション	説明
	監視対象のログが複数ある場合は、複数のプロファイルをデバイスにバインドできます。
メンテナンスウィンドウ	メンテナンスウィンドウ名、メンテナンスウィンドウがバインドされているデバイスの数、メンテナンスウィンドウがすべてのデバイスに自動的に追加されるかどうか、およびスケジュールとOSのデフォルトの設定を編集する詳細ページへのリンクが表示されます。また、このセクションでは、メンテナンスウィンドウの説明、およびメンテナンスウィンドウの作成と変更が行われた時間を表示することもできます。
Log Enablement Packages	Windows 信頼性およびパフォーマンスモニタ（ PerfMon ）テンプレートの基本セット、および Windows 以外のオープンソースの Perl スクリプトを表示します。そのため、監視機能を拡張し、システムおよびアプリケーションのパフォーマンス問題を特定できます。

監視プロファイル

デフォルトの監視プロファイルおよび独自にセットアップできるプロファイルを使用すると、アプライアンスでは次のことが可能になります。

- Windowsイベントログの監視
- Windows以外のファイルシステムログの監視
- 設定変更の監視

さらに、Log Enablement Package（ LEP ）を使用すると次のことが可能になります。

- しきい値の監視
- アプリケーションの監視

他のユーザーが使用できるように自分のプロファイルをダウンロードでき、他のユーザーが開発および使用可能にしたカスタムプロファイルをアップロードできます。

無料またはライセンスされたサーバーの監視

アプライアンスでは、標準ライセンスを使用して 5 台のサーバで監視が利用可能です。さらに、ライセンスを取得して利用可能な台数を増やすことができます。ライセンスで管理できるサーバ数を表示するには、ページの右上隅にある **サポートが必要な場合** をクリックすると表示されるページレベルのヘルプパネルで、**アプライアンスについて** をクリックします。容量使用率の管理 の行に 監視対象サーバー が表示され、既存のライセンスで監視できるデバイスの合計数に対して現在監視が有効になっているデバイス数も表示されます。

警告の操作

警告は**管理者コンソール**に表示されます。ここでは、警告が処理された後で、警告の確認および解除を行うことができます。アプライアンスには他にも機能があります。その中でも特に、次のことが可能です。

- 特定の警告でEメール通知をトリガします。
- 警告からサービスチケットを直接作成します。
- KACE GOアプリケーションを使用するモバイルデバイスに警告通知を送信できます。

アプライアンスには、警告をより効率的に操作できるようにするさまざまな機能があります。

- **警告統合 (繰り返し回数)**: 通知スパムを回避するために、アプライアンスでは警告が同じものかどうかを分析し、同じ警告に対して繰り返し回数を使用して警告が生成された回数を示します。
- **大量の警告の低減**: データの配信が大量に繰り返されないようにするため、アプライアンスでは 1 台のデバイスのコレクションを 1 つのコレクションにつき 50 の警告に制限します。さらに、アプライアンスは注意が必要な異常なアクティビティがあることを示す汎用の警告を構成します。
- **グルーミング**: ユーザーは警告を解除 (表示しないがデータベースには保持)、または設定した日数が経過した後で警告を手動や自動で削除できます。ただし、アプライアンスではデータベースから警告の削除を開始する前に、1 台のデバイスにつき保存する警告を 2000 に自動的に制限します。

サーバー監視の開始

アプライアンスでは、設定した数のサーバで監視が利用できるようになっています。サーバーがインベントリ内にある場合、そのデバイスの監視を有効にして、次のインベントリの後に警告のレポート作成を開始できます。

注: 製品ライセンス契約に従い、管理対象コンピュータ、コンピュータ以外のデバイス、および監視対象デバイスに分類された、指定された数のデバイスを管理できます。デバイスで監視が有効になっている場合、このデバイスは管理対象コンピューターとして 1 回カウントされ、監視対象デバイスとして 1 回カウントされます。

デバイスの監視の有効化

インベントリ内の対象となるサーバデバイスの監視を有効にすることができます。アプライアンスライセンスで指定されているように、最大で 200 台です。

対象のデバイスには、サーバークラスのオペレーティングシステムがあります。コンピューター以外のデバイスおよびサーバークラスのオペレーティングシステムが搭載されていないコンピューターを監視することはできません。

アプライアンスには、監視を有効にする 2 つの方法があります。

- デバイス インベントリリストからの 1 台または複数のサーバーの監視の有効化
- デバイスの詳細 ページからのサーバーの監視の有効化

サーバーが有効な場合、インベントリ セクションの デバイス ページの ステータス 列にあるアイコンは、有効なステータス、および監視がアクティブか一時停止かを示します。

-  : このエージェント管理対象デバイスでのサーバー監視は有効でアクティブです。
-  : このエージェント管理対象デバイスでのサーバー監視は一時停止しています。
-  : このエージェント不要管理対象デバイスでのサーバー監視は有効でアクティブです。
-  : このエージェント不要管理対象デバイスでのサーバー監視は一時停止しています。

関連トピック

1つ、または複数のデバイスの監視の無効化

デバイスの監視の一時停止

デバイス インベントリリストからの 1 台または複数のサーバーの監視の有効化

デバイス インベントリリストから、1 台のサーバーまたは複数のサーバーの監視を有効にすることができます。

1. デバイス インベントリページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
2. 監視を有効にする各デバイスのチェックボックスをオンにします。
3. **アクションの選択 > 監視を有効にする** を選択します。

    アクションの成功または失敗に関する情報がリスト上部に表示され、デバイスの ステータス が変わって監視アイコンが表示されます。

    監視を有効にできない原因として考えられるのは、デバイスの OS がサポートされていない、デバイスのタイプがサポートされていない、監視のライセンス数を超過している、などです。
4. **オプション**：左側のナビゲーションバーで、**監視 > デバイス** を選択し、デバイスの名前をクリックして Monitoring Detail（ 監視の詳細 ）ページでこのデバイスの監視設定に変更を加えます。
    - **監視を一時停止または再アクティブ化します。詳細については、「デバイスの監視の一時停止」を参照してください。**
    - **設定変更の監視を有効にします。詳細については、「デバイス設定の変更時の警告の受け取り」を参照してください。**
    - **監視プロファイルの追加またはプロファイルの変更を行います。詳細については、「監視プロファイルの操作」を参照してください。**
    - **メンテナンスウィンドウを追加します。詳細については、「その期間中デバイスから警告が収集されないメンテナンスウィンドウのスケジュール設定」を参照してください。**

    複数のデバイスを有効にしている場合は、必要に応じて繰り返します。

関連トピック

デバイスの詳細 ページからのサーバーの監視の有効化

デバイスの詳細 ページからのサーバーの監視の有効化

個々のサーバーでの監視は、その デバイスの詳細 ページから有効にすることができます。

1. デバイスの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
    c. デバイスの名前をクリックします。
2. 下へスクロールし、アクティビティ の下の **監視** をクリックしてセクションを展開します。

    デバイスにサーバークラスのオペレーティングシステムが搭載されていないため監視対象ではない場合、監視 セクションにはメッセージ（ **「オペレーティングシステムは、現在監視によってサポートされていません」** ）が表示されます。
3. **監視を有効にする** をクリックして監視を開始し、デバイスのデフォルトの監視設定の詳細も表示します。

監視が有効になっている場合、監視 セクションには、デバイスにバインドされている監視プロファイルの名前がデフォルトで表示されます。メンテナンスウィンドウがデフォルトとして定義されている場合は、その名前も表示されます。最近のアラートも 10 個まで表示されます。

4. **オプション**：**監視詳細の編集** をクリックして、監視の詳細 ページでこのデバイスの監視設定に変更を加えます。
   - **監視を一時停止または再アクティブ化します。詳細については、「デバイスの監視の一時停止」を参照してください。**
   - **設定変更の監視を有効にします。詳細については、「デバイス設定の変更時の警告の受け取り」を参照してください。**
   - **監視プロファイルの追加またはプロファイルの変更を行います。詳細については、「監視プロファイルの操作」を参照してください。**
   - **メンテナンスウィンドウを追加します。詳細については、「その期間中デバイスから警告が収集されないメンテナンスウィンドウのスケジュール設定」を参照してください。**

関連トピック

デバイスの監視の有効化

サーバー監視能力を上げるための新しいライセンスキーの取得

最大 200 台のサーバーで拡張監視機能を利用するには、新しいライセンスキーを取得する必要があります。キーを取得するには、Questの営業チームまでお問い合わせください。

1. 次のQuestウェブサイトの 購入方法 ページにアクセスします。https://quest.com/buy.
2. 購入方法 ページに記載されている3つの方法のいずれかで営業担当までお問い合わせください。
   - **ご使用の地域のフリーダイヤルにご連絡ください。**
   - **ご使用の地域のアドレスにEメールを送信してください。**
   - **お問い合わせフォーム に入力して送信してください。**

     コメント フィールドに、現在アプライアンスユーザーで、サーバ監視機能へのアクセスを希望するという内容を入力します。

アプライアンスでライセンスキー情報を更新します。

サーバー監視能力を上げるための新しいライセンスキーの追加

新しいライセンスキーを適用して、サーバー監視能力を上げることができます。

新しいライセンスキーを取得します。

1. アプライアンスの 設定 に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。
3. ライセンス情報 セクションで、新しいライセンスキーを入力して、**更新** をクリックします。
4. 確認 ダイアログで **はい** をクリックして、システムを再起動します。

再起動後のアプライアンスに再度サインインすると、すべての機能が使用できるようになります。

監視プロファイルの操作

監視プロファイルでは、デバイスのログ内を検索するテキストを識別し、そのテキストを定義した警告レベルに関連付けることで、警告作成の基準を示します。

アプライアンスには、サポートされているオペレーティングシステムを搭載したデバイス、および SNMP トラップデバイスのログ監視用に一連のデフォルトプロファイルが用意されています。さらに、既存の監視プロファイルの変更、独自のプロファイルの作成、および他のユーザーが作成したプロファイルのアップロードを行うことができます。また、アプリケーションとしきい値の監視を有効にする標準の Log Enablement Package（ LEP ）にアクセスできます。

使用可能な監視プロファイルは、監視 の プロファイル ページにリストで表示されます。

ヒント: ログ監視プロファイルだけを表示するには、右上隅で、**表示方法 > タイプ > ログ** の順にクリックします。SNMPトラップデバイスの監視プロファイルを表示するには、**表示方法 > タイプ > SNMPトラップ** の順にクリックします。

例えば、Mac OS Xデバイスの警告を作成するデフォルトのプロファイルでは、/var/log/system.logは、警告をトリガするテキストを検索する際に監視機能がスキャンするログであることを示しています。次の表は、Include Text（ 含まれるテキスト ）フィールドのデフォルトの検索テキストと、関連付けられた警告レベルを示しています。

ログ内で検索されるテキスト	警告レベル
緊急	**緊急**
エラー	**エラー**
致命的	**エラー**
失敗	**エラー**
アプライアンス監視警告	**エラー**
警告	**注意喚起**
使用不可	**注意喚起**

操作の必要性に応じてカスタマイズしたその他の警告を追加できます。

デフォルトのプロファイルには次のサポートされているオペレーティングシステムが含まれます。

- CentOS
- Debian
- FreeBSD
- Mac OS X
- Oracle Enterprise Linux
- Red Hat Enterprise Linux
- Solaris
- SUSE Linux
- Ubuntu
- Windows Server

Linux オペレーティングシステムを搭載したデバイスの場合、OS のバージョンに応じて、MySQL および Apache のログには複数の異なるログパスがあります。詳細については、「MySQL および Apache のプロファイルログのパス」を参照してください。

SNMPトラップメカニズムを使用して監視するエージェント不要デバイスの場合、トラップメッセージ形式および式を入力して特定のトラップ要素を取得する必要があります。詳細については、「SNMPトラップメッセージおよび警告基準の設定」を参照してください。

Log Enablement Packages リストページでは、QuestがWindows信頼性およびパフォーマンスモニタ（ PerfMon ）テンプレートの基本セット、およびWindows以外のオープンソースのPerlスクリプトを公開しています。そのため、ユーザーは監視機能を拡張し、システムおよびアプリケーションのパフォーマンス問題を特定できます。これらのテンプレートとスクリプトを入手できるため、ユーザーは最初から作成する必要はありません。アプライアンスでの監視はこれらの追加のテンプレートおよびスクリプトがなくても機能しますが、パフォーマンスしきい値監視を実行する場合はテンプレートおよびスクリプトから作成されたプロファイルが役立ちます。

また、便宜上、オプションの Windows 信頼性とパフォーマンスモニタ（ PerfMon ）テンプレートを管理対象 Windows Server 2003 デバイスにダウンロードした場合に使用できるデフォルトのプロファイルがあります。詳細については、「ITNinja監視Log Enablement Package（ LEP ）によるWindows Server 2003デバイスのセットアップ」を参照してください。

プロファイルの編集

既存のプロファイルの警告基準およびログパスを変更、追加、または削除できます。

プロファイルの作成に既存のプロファイルを使用する場合は、テンプレートとしてデフォルトプロファイルを使用した新規プロファイルの作成を参照してください。

警告を発生させるイベントを識別するには、Include Text（ 含まれるテキスト ）で文字列または正規表現を使用して、適切なメッセージ内容を指定します。例えば、文字列 Physical memory を入力する場合は、厳密にこの文字列が含まれるすべてのメッセージに対して警告が発生します。

複数の可能性に対応するには、正規表現を使用できます。例えば、「Drive /dev/[任意のドライブマウントポイント] has drive errors」という形式のドライブエラーがあるドライブマウントポイントに対して警告が必要な場合は、含まれるテキスト で Drive /dev/[a-z]{1,} has drive errors を使用できます。警告は、「Drive /dev/」、それに続く文字 a ～ z を含む任意の長さの単語、それに続く「has drive errors」を含むメッセージに対して発生します。

不要または煩雑と判断した場合は、特定のイベントを警告の発生から除外できます。受信しない警告をフィルタするには、Exclude Text（ 除外するテキスト ）を使用して、不要な警告を識別する内容を指定します。Exclude Text（ 除外するテキスト ）を使用して警告のカテゴリ全体をフィルタするか、Exclude Text（ 除外するテキスト ）を Include Text（ 含まれるテキスト ）と組み合わせて使用して、警告カテゴリのサブセットを絞り込むこと

ができます。詳細については、「監視プロファイルの含まれるテキストおよび除外するテキストの例」を参照してください。

1. プロファイル リストページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**監視** をクリックして、**プロファイル** をクリックします。
2. 編集する既存のプロファイルのチェックボックスをオンにし、**アクションの選択 > 編集** を選択して プロファイルの詳細 ページを表示します。
3. **オプション**：編集内容を表示するプロファイルの 名前 および 説明 を変更または修正します。

    注: デフォルトのプロファイルのいずれかを変更している場合は、自動で追加 フィールドを変更できません。

4. 必要に応じて、条件 設定を変更します。
    - **含めるフィルタ（SNMP トラップのみ）または** 含めるテキスト **（他のすべての監視プロファイル）を変更します。**
        1. 変更する含まれる検索テキスト（または SNMP トラップのフィルタ）がある行で、**編集** ボタンをクリックします。
        2. 新しい検索テキストまたはフィルタを入力します。
    - **（オプション）**除外するフィルタ **（SNMP トラップのみ）または** 除外するテキスト **（他のすべての監視プロファイル）を変更します。**
        1. 特定の警告を除外するために変更するテキスト（または SNMP トラップのフィルタ）がある行で、**編集** ボタンをクリックします。
        2. 新しい除外テキストまたはフィルタを入力します。
    - **入力した検索テキストが大文字と小文字を区別する場合は**、大文字と小文字を区別 **ドロップダウンリストから はい を選択します。**
    - **SNMP トラップのみ。アプライアンスが特定の SNMP 警告を受信するたびに、サービスデスクチケットを自動的に作成します。**
        - SNMP の含めるおよび除外するフィルタ（設定どおり）を含む行の チケットの作成 列で、**キューの選択** をクリックし、サービスデスクチケットの作成に使用するチケットキューを選択します。アプライアンスは、特定の含めるフィルタから生成された警告を受信したときに、指定されたチケットキューにサービスデスクチケットを作成します。警告に関連付けられているデバイスが、サービスデスクチケットで選択されます。SNMP 警告をトリガしたイベントの名前と概要が、チケットの詳細に表示されます。サービスデスクチケットの詳細については、「サービスデスクのチケット、プロセス、およびレポートの管理」を参照してください。
    - **警告レベルを変更します。**
        1. 変更する警告レベルがある行で、**編集** ボタンをクリックします。
        2. レベル ドロップダウンリストで、次の5つの選択肢からレベルを選択します。「**緊急**」、「**エラー**」、「**注意喚起**」、「**情報**」、および「**復旧済み**」。
    - **警告基準を追加します。**
        1. 条件 カテゴリヘッダーで、**追加** ボタンをクリックします。
        2. レベル、含めるテキスト、除外するテキスト（オプション）、および大文字と小文字の区別を設定します。
5. ページの一番下で **保存** をクリックします。

注: ページの一番下にある **出荷時設定にリセット** ボタンを使用して、デフォルトのプロファイルをオペレーティングシステムの出荷時の設定に戻すことができます。

関連トピック

Profile Details（プロファイル詳細）ページからの含まれるテキストおよび除外するテキスト機能を使用した警告のフィルタ

監視プロファイルの含まれるテキストおよび除外するテキストの例

SNMPトラップメッセージおよび警告基準の設定

SNMPトラップメッセージおよび警告基準は プロファイル ページを使用して設定できます。

- アプライアンスのSNMPトラップ監視を有効にします。詳細については、次を参照してください。 アプライアンスのセキュリティ設定の構成
- お使いのSNMPデバイスでの監視を有効にします。詳細については、次を参照してください。 1つ、または複数のデバイスの監視の有効化

SNMP（簡易ネットワーク管理プロトコル）は、ネットワーク上の管理対象デバイスを監視するためのプロトコルです。このプロトコルは、Dell Open Manageおよび多くのサードパーティ製品でサポートされています。アプライアンスでこの機能を有効にし、関連するデバイスの監視も有効にした場合、アプライアンスはプリンタ、プロジェクタ、ルーターなどの監視対象エージェント不要デバイスからSNMP接続を使用してSNMPトラップを受信できます。

SNMPトラップはネットワークデバイスから開始するメッセージであり、アプライアンス上のトラップレシーバに送信されます。例えば、ルーターの電源装置に障害が発生したときにルーターからメッセージを送信できます。また、プリンタで用紙切れが起こったときに、プリンタからメッセージを開始します。アプライアンスでは、これらのトラップを受信し、特定の事前定義のしきい値に到達するとアラートを生成します。

SNMPトラップメッセージおよび警告基準は プロファイルの詳細 ページを使用して設定できます。

必要に応じて、特定のイベントを検出対象にしたり除外したりできます。

1. プロファイル リストページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**監視** をクリックして、**プロファイル** をクリックします。
2. 次の手順のいずれかを実行します。
   - 新しい SNMP トラッププロファイルを作成するには、**アクションを選択 > 新規作成 > SNMP トラッププロファイル** の順に選択します
   - 既存のSNMPトラッププロファイルを編集するには、リストでそのプロファイルを選択し、**アクションを選択 > 編集** の順に選択します。
   - 既存のSNMPトラッププロファイルを複製するには、リストでそのプロファイルを選択し、**アクションの選択 > 複製および編集** の順に選択します。

   プロファイルの詳細 ページが表示されます。
3. **オプション**：編集内容を表示するプロファイルの 名前 および 説明 を変更または修正します。

   注: デフォルトのプロファイルのいずれかを変更している場合は、自動で追加 フィールドを変更できません。
4. 必要に応じて、トラップメッセージフォーマット 設定を変更します。

   例：%Td (%Tn => %To) %Vz

   SNMPトラップメッセージでは、次の要素を使用できます。

要素	説明
%Aa	エージェントのアドレス。

要素	説明
%Ah	エージェントのホスト名。
%d	ローカルの日。
%m	ローカルの月。
%y	ローカルの年。
%h	ローカルの時。
%i	ローカル分。
%s	ローカルの秒。
%u	Unixタイムスタンプ。
%Td	トラップの説明。
%Tm	トラップのMIB（管理情報ベース）。
%Tn	トラップの名前。
%To	トラップOID（オブジェクトID）。
%Tt	トラップタイプ（0 ー 5：汎用、6：エンタープライズ）。
%Tv	バージョンのトラップ（情報、トラップ {v1, v2, v3}）。
%Vd#	変数バインディング記述（ここで、「#」は、シーケンス内の要素の位置を表す番号）。
%Vn#	変数バインディング名（ここで、「#」は、シーケンス内の要素の位置を表す番号）。
%Vo#	変数バインディングOID（ここで、「#」は、シーケンス内の要素の位置を表す番号）。
%Vt#	変数バインディングタイプ（ここで、「#」は、シーケンス内の要素の位置を表す番号）。
%Vv#	変数バインディング値（ここで、「#」は、シーケンス内の要素の位置を表す番号）。
%Vz	すべての変数バインディングを表示（Name: Value、Name: Value、Name: Value）。Nameがない場合（MIBファイルが欠落しているため）、OIDが代わりに表示されます。

5. 必要に応じて、1つまたは複数の警告レベルを指定します。

次の警告レベルが使用可能です。「緊急」、「エラー」、「注意喚起」、「情報」、および「復旧済み」。

- 警告レベルを追加するには、条件 で  をクリックして新しい警告レベルを追加します。
- 既存の警告レベルを編集するには、編集する警告レベルを含む行で、  をクリックします。

6. レベルごとに、Include式やExclude式を指定します。また、その式で大文字と小文字が区別されるかどうかも示します。これらの式を使って、特定のイベントを検出に含めたり検出から除外したりできます。

   IncludeおよびExcludeの式の構文は次のとおりです

   <Field_Type> {TRAP_OID|TRAP_NAME|TRAP_DESCRIPTION|TRAP_TYPE|TRAP_MIB|VARBIND} {=|!=|>|<|>=|<=} **<Field_Value>** [<AND|OR> **<Condition_A>**] [<AND|OR> **<Condition_B>**] ...

   例：

   - TRAP_OID = ???.1.3.6.1.4.1.8072.2.3.2.1???: トラップOIDに「.1.3.6.1.4.1.8072.2.3.2.1」が含まれる場合、警告が生成されます。
   - TRAP_NAME = "acctngFileFull" AND VARBIND = "acctngFileName|ABC": トラップ名に「acctngFileFull」が含まれ、トラップの変数バインディングのいずれかが「ABC」の値を持つ「acctngFileName」の場合、警告が生成されます。

7. ページの一番下で **保存** をクリックします。

注: ページの一番下にある **出荷時設定にリセット** ボタンを使用して、デフォルトのプロファイルをオペレーティングシステムの出荷時の設定に戻すことができます。

テンプレートとしてデフォルトプロファイルを使用した新規プロファイルの作成

デフォルトまたは既存の監視プロファイルをコピーし、そのコピーを編集して新しいプロファイルを作成できます。

各デバイスに対するプロファイルは1つとは限りません。別の警告を生成する追加のプロファイルを作成して、既に1つ以上のプロファイルが関連付けられているデバイスにこのプロファイルをバインドできます。

1. プロファイル リストページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**監視** をクリックして、**プロファイル** をクリックします。
2. テンプレートとして使用する既存のプロファイルのチェックボックスをオンにし、**アクションの選択 > 複製および編集** を選択して プロファイルの詳細 ページを表示します。
3. プロファイルの名前を変更し、その説明を修正します。
4. **オプション**：編集内容を表示するプロファイルの 名前 および 説明 を変更または修正します。

   注: デフォルトのプロファイルのいずれかを変更している場合は、自動で追加 フィールドを変更できません。

5. ログパスには、オペレーティングシステムまたはアプリケーションに該当するパスを使用します。

   このパスは、表に示すようにオペレーティングシステムの基本的なパスになります。

オペレーティングシステム	ログのパス
CentOS	/var/log/messages

オペレーティングシステム	ログのパス
Debian	/var/log/syslog
Fedora	/var/log/messages
FreeBSD	/var/log/messages
Mac OS X	/var/log/system.log
openSUSE	/var/log/messages
Oracle Enterprise Linux	/var/log/messages
Red Hat Enterprise Linux	/var/log/messages
Solaris	/var/adm/messages
SUSE Enterprise Linux	/var/log/messages
Ubuntu	/var/log/syslog
Windows	Windowsアプリケーションのapplication **注:** イベントログのプロパティに表示されるそのログの「フルネーム」を使用する必要があります。正しいフルネームが使用されていることを確認するには、「イベントビューア」を開きます。「Windowsログ」を展開し、イベントログを右クリックして **プロパティ** を選択します。ログのプロパティ ダイアログのフィールドに表示されるフルネームのバージョンを使用します。 Windowsタスクスケジューラ関連のMicrosoft-Windows-TaskScheduler/Operational

または、基本的なイベントログ以外のデータを含むログを定義するパスを入力できます。例えば、SUSE上に/var/log/**<myapplog>**などの特定のログにデータを送信するアプリケーションがあった場合、この手順に従って新しいプロファイルにこのパスを使用し、検索テキストおよび警告レベルを定義できます。

Linux オペレーティングシステムを搭載したデバイスの場合、OS のバージョンに応じて、MySQL および Apache のログには多数の異なるログパスがあります。詳細については、「MySQL および Apache のプロファイルログのパス」を参照してください。

注: プロファイルには1つのログパスのみを定義できます。複数のログに対して複数のプロファイルを作成する必要があります。

6. 必要に応じて、条件 設定を変更します。
   - Include Text (**含まれるテキスト**) **を変更します。**
     1. 変更する含まれる検索テキストがある行で、**編集** ボタン をクリックします。
     2. 新しい検索テキストを入力し、必要に応じて 大文字と小文字を区別 ドロップダウンリストから **はい** を選択します。

3. 行の右側の **保存** をクリックします。

- **オプション：**Exclude Text **（除外するテキスト）を変更します。**

1. 特定の警告を除外するために変更するテキストがある行で、**編集** ボタン をクリックします。
2. 新しい除外するテキストを入力し、必要に応じて Case-sensitive（大文字と小文字を区別）ドロップダウンリストから **はい** を選択します。
3. 行の右側の **保存** をクリックします。

- **警告レベルを変更します。**

1. 変更する警告レベルがある行で、**編集** ボタン をクリックします。
2. レベル ドロップダウンリストで、次の5つの選択肢からレベルを選択します。「**緊急**」、「**エラー**」、「**注意喚起**」、「**情報**」、および「**復旧済み**」。
3. 行の右側の **保存** をクリックします。

- **警告を追加します。**

1. 条件 カテゴリヘッダーで、**追加** ボタン をクリックします。
2. レベル、検索テキスト、および大文字と小文字の区別を設定して、行の右側の **保存** をクリックします。
3. 追加する警告の数だけ繰り返します。
4. **オプション**：新しい警告基準を並べ替えます。それには **ドラッグ** ボタン をクリックします。

7. ページの一番下で **保存** をクリックします。

該当するデバイスの 監視の詳細 ページで、デバイスにプロファイルを割り当てることができます。

MySQL および Apache のプロファイルログのパス

Linux オペレーティングシステムを搭載したデバイスの場合、OS のバージョンに応じて、MySQL および Apache のログには多数の異なるログパスがあります。

注: プロファイルには1つのログパスのみを定義できます。複数のログに対して複数のプロファイルを作成する必要があります。

MySQL および Apache のログのログパスの最新の表については、http://www.itninja.com/blog/view/mysqland-apache-profile-log-path-locationsを参照してください。

別のユーザーが作成したプロファイルのアップロード

他のユーザーが使用できるカスタムプロファイルを別のユーザーが作成した場合、それをアプライアンスにアップロードできます。

別のユーザーが作成した XML プロファイルにアクセスできます。

1. プロファイル リストページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**監視** をクリックして、**プロファイル** をクリックします。

2. **アクションの選択 > プロファイルのアップロード** を選択して、プロファイルのアップロード ダイアログを表示します。
3. **ファイルの選択** をクリックしてアップロードするプロファイルに移動し、選択して **アップロード** をクリックします。

   複数のプロファイルを選択できます。

プロファイル リストの下部にプロファイルが表示されます。

必要に応じて、新しいプロファイルを編集できます。詳細については、「プロファイルの編集」を参照してください。

他のユーザーが使用できるようにするためのプロファイルのダウンロード

他のユーザーが使用できるようにするために、カスタムプロファイルをダウンロードできます。

1. プロファイル リストページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**監視** をクリックして、**プロファイル** をクリックします。
2. ダウンロードするプロファイルのチェックボックスをオンにし、**アクションの選択 > プロファイルのダウンロード** を選択して、プロファイルを ダウンロード フォルダに送信します。

   Profile Detail（ プロファイルの詳細 ）ページに表示されるように、プロファイルの XML ファイル名はプロファイル名から派生し、UNIX タイムスタンプが付加されます。

プロファイルを配布します。

デバイスへの追加プロファイルのバインド

デバイスでサーバ監視が有効になっている場合、アプライアンスでは、デバイスのオペレーティングシステムに適切なデフォルトのプロファイルとデフォルトのログのパスをデバイスに割り当てまたはバインドします。必要に応じて他のプロファイル（ 作成したカスタムプロファイルまたは他のソース（ ITNinjaなど ）から入手したプロファイル ）を追加できます。

1. 監視の詳細 ページに移動します。
   a. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。
   b. デバイスの名前をクリックして、監視の詳細 ページを表示します。
2. プロファイル フィールドをクリックして定義されたプロファイルのドロップダウンリストを表示し、適用するプロファイルを選択します。
3. **保存** をクリックします。

非標準のログ日付形式の定義

任意のオペレーティングシステムについて、アプライアンスでは、ログファイルのスキャン時のログの日時に、認識している標準形式を使用します。ただし、ログに一般的ではない形式が使用されている場合、サーバー監視でログを正常に解析できるようにその形式を定義する必要があります。

注: ほとんどの場合、このフィールドは空白にしておく必要があります。

注: ログ日付形式は、Windowsイベントログには関係しません。

1. プロファイル リストページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**監視** をクリックして、**プロファイル** をクリックします。
2. 編集する既存のプロファイルのチェックボックスをオンにし、**アクションの選択 > 編集** を選択して プロファイルの詳細 ページを表示します。
3. ログ日付形式 に、非標準のログ日付形式を入力します。

   サポートされている文字書式の設定および例は、Log Date Format（ ログの日付形式 ） の横にある をクリックすると表示できます。
4. ページの一番下で **保存** をクリックします。

Log Enablement Package を使用したアプリケーションおよびしきい値監視の設定

パフォーマンスしきい値監視および Exchange、Internet Information Services（ IIS ）などのアプリケーション監視には、Log Enablement Packages リストページからアクセスできる Log Enablement Package（ LEP ）と呼ばれるパッケージが必要です。

Log Enablement Packages リストページでは、QuestがWindows信頼性およびパフォーマンスモニタ（ PerfMon ）テンプレートの基本セット、およびWindows以外のオープンソースのPerlスクリプトを公開しています。そのため、ユーザーは監視機能を拡張し、システムおよびアプリケーションのパフォーマンス問題を特定できます。これらのテンプレートとスクリプトを入手できるため、ユーザーは最初から作成する必要はありません。アプライアンスでの監視はこれらの追加のテンプレートおよびスクリプトがなくても機能しますが、パフォーマンスしきい値監視を実行する場合はテンプレートおよびスクリプトから作成されたプロファイルが役立ちます。

Windows PerfMonテンプレート

アプライアンスでは、特定のイベントログ、およびイベントをトリガする PerfMon に対して Microsoft が使用する汎用基準を含むデフォルトの Windows OS およびアプリケーション LEP プロファイルをアプライアンスで事前定義しています。Log Enablement Packages リストページの LEP を介して Microsoft Server 2008 で使用できる基本の PerfMon テンプレートは、システム（ CPU、メモリ、ディスク ）、Exchange、SQL、IIS、Active Directory、および Hyper-V 用です。

注: Microsoft Server 2003 用の PerfMon テンプレートは ITNinja から入手できます。

Windows以外のPerlスクリプト

各パッケージは、組み込みのオペレーティングシステムスケジューラ（ cron、fcron など ）を使用して定期的に実行されるオープンソースの Perl スクリプトです。Perlスクリプトを実行すると、CPU、メモリ、およびローカルボリュームの使用を判断する一連のコマンドが実行されます。使用率がパッケージで定義されているしきい値を超えている場合、システムログ（ syslog ）ファイルに警告が書き込まれます。スクリプトは syslog に記録し、各イベントのプレフィックスメッセージを含むように構成されているため、アプライアンスでは設定の利便性を考えてすべての Windows 以外のプロファイルの syslog にデフォルトで基準を事前定義しています。

ITNinja から入手できるパッケージ

ITNinja は製品不問の IT コラボレーションコミュニティです。IT プロフェッショナルが情報を共有し、設定および展開のトピックに関する情報の主なリソースとして機能することを目的としています。特定のソフトウェアタイトルのトピックおよびその他のトピック（ 展開、管理、設定、およびトラブルシューティングなど ）を参照し

たり、提供したりできます。サーバ監視コミュニティは http://itninja.com/community/k1000-monitoring にあります。

ITNinja では、Log Enablement Packages リストページで入手できる標準的なテンプレート以外の PerfMon テンプレートを見つけることができます。例えば、Windows Server 2003 の多数のログの監視を設定するためのテンプレートがあります。アプライアンスの Log Enablement Package インストール機能では Windows Server 2003 はサポートされません。それらのサーバーについては、ITNinja に記載されている方法で、PowerShell を使用して LEP をインストールします。

ITNinja コミュニティのメンバーであるアプライアンス監視ユーザーは、利用可能な LEP ライブラリを拡充するために独自のテンプレートおよびスクリプトを提供できます。Windows Server 2003 パッケージと同様に、これらの LEP は標準パッケージで使用可能なインストールプロセスでは対応していないため、ITNinja に記載されている方法を使用してインストールする必要があります。

監視対象デバイスへの 1 つ、または複数の LEP のインストール

Windows デバイスおよび Windows 以外のデバイスにアプライアンスから直接 Log Enablement Package をインストールできます。

1. Log Enablement Packages リストページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**監視** をクリックして、**Log Enablement Packages** をクリックします。
2. デバイスにインストールするパッケージのチェックボックスをオンにし、**アクションの選択 > デバイスに追加** を選択して、Log Enablement Packages Install（ Log Enablement Package のインストール ）ページを表示します。

    複数のパッケージを選択する場合、Windows と Windows 以外の両方のパッケージを選択してインストールできます。この場合、Log Enablement Packages Install（ Log Enablement Package のインストール ）ページには、Windows パッケージ用のセクションと Windows 以外のパッケージ用のセクションが別々に表示されます。選択したすべてのパッケージが 1 つのタイプの場合、その特定のタイプ用のセクションのみが表示されます。
3. パッケージを追加するデバイスを選択します。
    a. デバイス テキストボックス内をクリックして、右側の Selected Packages（ 選択されたパッケージ ）に表示されているパッケージと互換性がある、インベントリ内のデバイスのリストを表示します。
    b. 必要なデバイスをリストから選択します。
4. **オプション**：Windows パッケージの場合、プロファイルが既にデバイスにバインドされていて、再インストールしない場合は、Add Windows OS and Application LEP Profile（ Windows OS およびアプリケーション LEP プロファイルの追加 ）チェックボックスをオフにします。
5. パッケージのいずれかが既にデバイスにインストールされている場合に、どのようにインストールするかを決定します。
    - **現在のパッケージを既存のバージョンよりも優先して再インストールする場合は**、Replace it **（ 置き換える ）を選択したままにします。**
    - **デバイスに現在インストールされている可能性があるパッケージを維持する場合は**、Skip it **（ スキップする ）を選択します。例えば、以前にパッケージを編集しており、その変更が失われないようにする場合があります。**
6. **インストール** をクリックします。
7. **オプション**：インストールの進行状況を表示します。
    a. 左側のナビゲーションバーの **監視** セクションで **デバイス** をクリックし、監視対象デバイスの名前を選択して、その Monitoring Detail（ 監視の詳細 ）ページを表示します。

LEP Installation Log（LEP インストールログ）セクションがページの一番下に表示され、この特定のデバイスのインストールプロセスの概要が表示されます。

b. **オプション**：詳細を表示するには、**このデバイスの LEP インストールログをすべて表示** をクリックします。

ITNinja監視Log Enablement Package（LEP）による Windows Server 2003デバイスのセットアップ

Windows Server 2003 の Log Enablement Package はアプライアンスの Log Enablement Packages リストページには表示されず、アプライアンスの LEP インストール機能では Windows Server 2003 はサポートされません。ただし、ITNinja から Windows 2003 デバイスを監視するためのパッケージを取得でき、それには異なるセットアッププロセスが必要です。

アプライアンスのインベントリに、エージェントによって管理される、またはエージェント不要管理によって管理される Windows Server 2003 デバイスを追加します。詳細については、「デバイスの管理について」を参照してください。

このプロセスには、監視対象のサーバデバイスでのアクション、およびアプライアンスのアクションが含まれます。サーバーデバイスで、ITNinjaからLog Enablement Packageをダウンロードしてperfmonを起動します。アプライアンスでデバイスの監視を有効にし、監視パッケージからプロファイルを定義してこのプロファイルをデバイスにバインドします。

注: この手順に従うと、1 つのパッケージが 1 台のデバイスにインストールされます。1 回の手順で複数のパッケージをインストールする場合は、PowerShell スクリプトを使用してそれを実行するための手順が ITNinja にあります。詳細については、「http://itninja.com/community/k1000-monitoring」を参照してください。

1. 適切な監視LEPをITNinjaから取得します。
   a. ITNinja Monitoring のコミュニティページにアクセスします。http://itninja.com/community/k1000-monitoring.
   b. **ダウンロード** タブから、調査対象のパフォーマンスカウンタが属するパフォーマンスカテゴリ用のパッケージを検索します。

   検索を使用して検索結果を絞り込むことができます。

   c. **ダウンロード** をクリックして、パッケージのHTMファイルをダウンロードします。
   d. HTMファイル（**<Performance_Category>**_Alerts.htm）を監視対象デバイスにコピーします。
2. 監視対象の Windows Server 2003 デバイスで、パフォーマンスモニタを起動し、**パフォーマンスのログと警告** フォルダを展開します。
3. **パフォーマンスのログと警告** で、**警告** を右クリックして **新しい警告の設定を取得** を選択します..
4. 開くダイアログで、パッケージの場所を参照して選択し、**開く** をクリックします。
5. 新しい警告の設定 ダイアログで、パッケージ名を確認して **OK** をクリックし、パッケージのプロパティページを表示します。
6. LEPのプロパティを確定または編集します。
   - **デフォルトの設定を変更せずに、OK をクリックしてページから移動します。**
   - **オプション：プロパティページの 全般 タブで、カウンタを追加または削除し、必要に応じてしきい値を変更して OK をクリックします。詳細については、「Windows Server 2003デバイス用監視Log Enablement Package（LEP）の編集」を参照してください。**
7. パフォーマンスウィンドウで、パッケージ名を右クリックして **開始** を選択し、監視を開始します。

   処理対象のデバイスを使用して、アプライアンスに移動して監視機能を有効にし、プロファイルを作成し、プロファイルをデバイスにバインドします。
8. アプライアンスで、このデバイスの監視を有効にします。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。

c. デバイスの名前をクリックして、デバイスの詳細 ページを表示します。

d. 下へスクロールし、アクティビティ の下の **監視** をクリックしてセクションを展開します。

e. **監視を有効にする** をクリックして監視を開始し、デバイスのデフォルトの監視設定の詳細も表示します。

監視が有効になっている場合、監視 セクションには、デバイスにバインドされている監視プロファイルの名前がデフォルトで表示されます。メンテナンスウィンドウがデフォルトとして定義されている場合は、その名前も表示されます。

9. プロファイルの詳細 ページで、監視パッケージプロファイルを作成します。

a. 左側のナビゲーションバーで、**監視** をクリックして、**プロファイル** をクリックします。

b. プロファイル リストページで、**Windows ITNinjaプラグインテンプレート** の横にあるチェックボックスをオンにし、**アクションの選択 > 複製および編集** を選択して プロファイルの詳細 ページを表示します。

c. 名前を編集して、監視プロファイルの説明を入力します。

d. Windows Server 2003の「ログのパス」、「Application」を使用します。

e. ログの日付形式 を空白のままにしておきます。

f. **オプション**：「**エラー**」以外のレベルを使用する場合は、**編集**（ ）をクリックして、レベルの下のドロップダウンメニューからレベルを選択します。

g. 基準行の最後にある **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

10. この新しいプロファイルをデバイスに追加します。

a. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。

b. デバイスの名前をクリックして、監視の詳細 ページを表示します。

c. プロファイル フィールドをクリックして、使用可能なすべてのプロファイルのドロップダウンリストを表示し、作成したプロファイルをクリックします。

d. **保存** をクリックします。

プロファイルがデバイスにバインドされます。

Windows Server 2008以上デバイス用監視Log Enablement Package（LEP）の編集

サーバーにインストールされた監視 LEP で、パフォーマンスカウンタを追加、削除、および設定できます。

Log Enablement Package がデバイスにインストールされています。詳細については、「監視対象デバイスへの 1 つ、または複数の LEP のインストール」を参照してください。

1. 監視対象デバイスで、パフォーマンスモニタを起動し、「**データ コレクタ セット**」フォルダを展開して「**ユーザー定義**」フォルダを展開します。
2. LEP定義のデータコレクタセットを選択します。
3. **オプション**：パッケージが実行されている場合は、セット名を右クリックして **停止** を選択します。
4. 右のペインで「DataCollector」を右クリックし、**プロパティ** を選択して プロパティ ダイアログを表示します。
5. プロパティ ダイアログのタブを使用して、パッケージを編集します。

オプション	説明
警告	**警告** タブを使用すると、パフォーマンスカウンタのしきい値属性および間隔属性を編集できます。ま

オプション	説明
	た、このタブを使用してカウンタの追加および削除を行うこともできます。 パフォーマンスカウンタを設定するには： a. パフォーマンスカウンタ でカウンタを選択します。 b. 警告する時期 ドロップダウンリストおよび 制限 フィールドを使用して警告トリガを編集します。 c. サンプルの間隔 および 単位 ドロップダウンメニューを使用してコレクション間隔を編集します。 d. **OK** をクリックして、変更を保存します。 パフォーマンスカウンタをこのLEPに追加するには： a. **追加** をクリックして、カウンタの追加 ダイアログを表示します。 ローカルにインストールされているアプリケーションのパフォーマンスカウンタが 使用可能なカウンタ に表示されます。また、次のコンピュータからカウンタを選んでください のリストまたは **参照** を使用する場合は、リモートシステムからオブジェクトおよびカウンタを選択することもできます。 b. 使用可能なカウンタ で、追加する1つ以上のカウンタを選択して **追加>>** をクリックします。 c. **OK** をクリックして、プロパティ ダイアログに戻ります。 パフォーマンスカウンタをこのLEPから削除するには： a. パフォーマンスカウンタ でカウンタを選択します。 b. **削除** をクリックします。 c. **OK** をクリックして、変更を保存します。
警告処理	パッケージの目的は、イベントログにイベントを記録することです。アプライアンスの監視機能では警告を検出できるため、アプリケーションイベントログにエントリを記録する のチェックボックスをオンにしておく必要があります。
警告のタスク	警告がトリガされた時に実行するタスクを設定する場合は、このタブで定義します。

6. プロパティ ダイアログの一番下にある **OK** をクリックして、パフォーマンスモニタ に戻ります。
7. **ユーザー定義** フォルダでパッケージを右クリックし、**開始** を選択して監視を開始します。

Windows Server 2003デバイス用監視Log Enablement Package（ LEP ）の編集

サーバーにインストールされた監視 LEP で、パフォーマンスカウンタを追加、削除、および設定できます。

Log Enablement Package がデバイスにインストールされています。詳細については、「監視対象デバイスへの 1 つ、または複数の LEP のインストール」を参照してください。

1. 監視対象デバイスで、パフォーマンスモニタを起動し、「**パフォーマンス ログと警告**」フォルダを展開します。
2. **警告** をクリックし、詳細ペインで編集するLEPを右クリックします。
3. **オプション**：パッケージが実行している場合、LEP名を右クリックして、**停止** を選択します。
4. 必要に応じてLEP名を再度右クリックし、**プロパティ** を選択して プロパティ ダイアログを表示します。
5. プロパティ ダイアログの **全般** タブを使用して、パッケージを編集します。
    a. カウンタ でパフォーマンスカウンタを選択して、現在の設定を表示します。
    b. 次の値になったら警告する ドロップダウンリストおよび 制限値 フィールドを使用して警告トリガを編集します。
    c. データのサンプル間隔 の 間隔 および 単位 ドロップダウンメニューを使用してコレクション間隔を編集します。
    d. 実行するアカウント名 でアカウント権限を設定します。

    - デフォルトでは、パッケージはシステムアカウント権限を使用して実行されます。システムアカウント権限を引き続き使用するには、実行するアカウント名 のエントリを<Default>のままにしておきます。
    - ビルトイングループは、次のパフォーマンスモニタ機能にアクセスできます。

グループ	機能
ローカルのAdministratorsグループのメンバー	すべてのパフォーマンスモニタ機能を使用できます
Usersグループのメンバー	• パフォーマンスモニタで表示されるプロパティを変更できます • パフォーマンスモニタでログファイルを表示できます • 警告の設定は作成できません
Performance Monitor Usersグループのメンバー	• Usersグループで使用可能なすべての機能を使用できます • パフォーマンスモニタでリアルタイムログを表示して、パフォーマンスモニタで表示されるプロパティをリアルタイムで変更できます • 警告の設定を作成または変更できません
Performance Log Usersグループのメンバー	• Performance Monitor Usersグループで使用可能なすべての機能を使用できます • グループにバッチユーザーとしてのログオンを割り当てると、警告の設定を作成および変更できます

6. **オプション**：パフォーマンスカウンタをLEPに追加するには：
    a. プロパティ ダイアログで、**追加** をクリックして カウンタの追加 ダイアログを表示します。

    ローカル コンピュータのカウンタ オブジェクトを使う が選択されている場合は、ローカルにインストールされているアプリケーションのパフォーマンスカウンタが 一覧からカウンタを選ぶ に表示されます。また、次のコンピュータからカウンタを選ぶ のリストを使用する場合は、リモートシステムからオブジェクトおよびカウンタを選択することもできます。

b. 次のコンピュータからカウンタを選ぶ で、追加する1つ以上のカウンタを選択して **追加** をクリックします。
c. **OK** をクリックして、プロパティ ダイアログに戻ります。

7. **オプション**：パフォーマンスカウンタをLEPから削除するには：
   a. プロパティ ダイアログの カウンタ で該当するカウンタを選択します。
   b. **削除** をクリックします。
   c. **OK** をクリックして、変更を保存します。
8. プロパティ ダイアログの一番下にある **OK** をクリックして、パフォーマンスモニタ に戻ります。
9. 詳細ペインでLEPを右クリックし、**開始** を選択して監視を開始します。

デバイスの監視の管理

デバイスの監視が有効になると、監視の実行方法および実行時期を設定してデバイスごとに監視を管理できます。

デバイスの監視の一時停止

デバイスでの作業中またはデバイスに変更を加える際に監視機能で警告が生成されないようにするには、監視を一時停止することができます。

注: 定期的なメンテナンスタスクに対応するために、設定済みのスケジュールに基づいた監視を一時停止する場合、メンテナンスウィンドウのスケジュールを設定できます。詳細については、「その期間中デバイスから警告が収集されないメンテナンスウィンドウのスケジュール設定」を参照してください。

複数のデバイスを同時に一時停止または再開する場合は、複数のデバイスの監視の一時停止または再開を参照してください。

1. 監視の詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。
   c. デバイス 列のデバイスをクリックして、監視の詳細 ページを表示します。
2. 一時停止 のオプションボタンを選択して、**保存** をクリックします。

インベントリ セクションの デバイス ページの ステータス 列にあるアイコンは、次の一時停止ステータスを示します。

-  ：このエージェント管理対象デバイスでのサーバー監視は一時停止しています。
-  ：このエージェント不要管理対象デバイスでのサーバー監視は一時停止しています。

複数のデバイスの監視の一時停止または再開

複数のデバイスの監視を同時に一時停止できます。同様に、複数のデバイスの監視を再開できます。

1. 監視対象デバイス リストページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。

2. 一時停止または再開するすべてのデバイスのチェックボックスをオンにします。
3. **アクションの選択 > 監視の一時停止** または **監視の再開** を選択します。

デバイスの 監視 列のエントリは、新しい状態（「一時停止しています」または「アクティブ」）の表示に変更されます。

ポーリング間隔および警告の自動解除または削除の設定

アプライアンスが警告のログをポーリングする頻度に関していくつかの一般的な監視設定を設定することができます。また、設定した日数が経過した後に自動的に警告を解除、および警告を削除するようにアプライアンスを設定できます。

警告を解除すると、警告 リストページのビューおよびダッシュボードウィジェットから警告が削除されます。警告を削除すると、データベースから警告が削除されます。解除した警告を回復することはできますが、削除した警告は回復できません。

1. 監視設定 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**設定** をクリックして、**監視設定** をクリックします。
2. ポーリング間隔を分単位で設定します。

   最小間隔は10分です。
3. **オプション**：指定した日数が経過した後に警告を解除するようにアプライアンスを設定します。
   a. 警告の自動解除 を選択します。
   b. 日数の値を入力します。
4. **オプション**：指定した日数が経過した後に警告を削除するようにアプライアンスを設定します。
   a. 警告の自動削除 を選択します。
   b. 日数の値を入力します。
5. **保存** をクリックします。

関連トピック

警告の解除

警告の削除

警告リストから解除された警告の取得と確認

Pingプローブの無効化

デバイスに対して監視を有効にすると、Pingプローブはデフォルトで有効になります。ただし、場合によっては Ping プローブは大量の警告を生成する可能性があるため、アプライアンスでは Ping プローブを無効にすることができます。

Pingは、インターネット制御通知プロトコル（ ICMP ）のecho requestパケットをターゲットに送信します。Ping プローブの頻度により、ICMPパケットをブロックするファイアウォールもあるため、拒否されるプローブから

大量の警告が生成される可能性があります。これらの場合、Pingプローブを無効にすると、監視結果が分かりやすくなります。

1. 監視設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**設定** をクリックして、コントロールパネル の **監視設定** をクリックします。
2. Pingプローブを有効にする をオフにします。
3. **保存** をクリックします。

デバイス設定の変更時の警告の受け取り

監視対象デバイスの設定が変更された場合に警告を作成するように監視を設定できます。

この機能を有効にすると、デバイス設定の変更が検出されるたびに、アラートが生成されます。デバイス資産について検出する変更のタイプを指定するには、資産履歴の設定 **ページからアクセスできる** デバイス **ダイアログボックスで選択します。**

設定変更には、例えば、ディスク、新しい論理ドライブの追加、メモリの増設または削減、パーティション変更などがあります。資産履歴の設定 ページの詳細、および設定変更の選択方法については 資産履歴サブスクリプションの設定参照してください。

1. 監視の詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。
    c. デバイスの名前をクリックします。
2. 設定変更警告を有効にする チェックボックスをオンにします。
3. **保存** をクリックします。

その期間中デバイスから警告が収集されないメンテナンスウィンドウのスケジュール設定

メンテナンスウィンドウを使用すると、システムに大量に送信される可能性がある必要以上の警告を生成する監視機能を使用せずに、サーバーのメンテナンスタスクを実行するある程度の時間帯を確保できます。

各監視対象デバイスに対して使用するメンテナンスウィンドウは1つとは限りません。メンテナンスウィンドウのライブラリを作成し、必要に応じて組み合わせたメンテナンスウィンドウを監視対象デバイスに適用できます。

1. メンテナンスウィンドウの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**監視** をクリックして、**メンテナンスウィンドウ** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. 次の情報を入力します。

オプション	説明
名前	メンテナンスウィンドウを識別する名前。名前は、メンテナンスウィンドウ リストに表示されます。
説明	ウィンドウの目的および対象を詳細に識別する情報。
自動で追加	• 「**なし**」：該当するデバイスで監視が有効になった場合に、このメンテナンスウィンドウはデバイスに自動的に追加されません。 • 「**すべて**」：該当するデバイスで監視が有効になった場合に、このメンテナンスウィンドウはデバイスに自動的に追加されます。

3. スケジュール セクションで、次のスケジュール設定を指定します。

オプション	説明
毎日/特定曜日　開始 HH:MM 終了HH:MM	毎日指定した時間および特定の時間帯、または特定曜日の指定した時間にウィンドウが開始されます。
実行基準 n 日 / 毎月 / 特定月 開始 HH:MM 終了 HH:MM	毎月または指定した月の同じ日かつ指定の時刻および時間帯に実行します。

注: スケジュールは24時間制を使用します。

4. **保存** をクリックします。
5. 監視の詳細 ページで、監視対象デバイスにメンテナンスウィンドウを適用します。
   a. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。
   b. デバイスの名前をクリックして、監視の詳細 ページを表示します。
   c. メンテナンスウィンドウ フィールドをクリックして、定義されたメンテナンスウィンドウのドロップダウンリストを表示し、適用するメンテナンスウィンドウを選択します。
6. **保存** をクリックします。

監視固有の役割の作成と割り当て

警告とプロファイルを操作する機能を制限するユーザーの役割を作成できます。

例えば、警告に対応して警告からサービスデスクチケットの作成はできるが、プロファイルをデバイスに追加したり、メンテナンスウィンドウを設定したりすることはできないスタッフメンバーの役割を作成できます。

アプライアンス上で組織コンポーネントが有効化されている場合、ユーザーの役割に使用できる権限は、組織に割り当てられた組織の役割によって異なります。詳細については、「組織の役割とユーザーの役割の管理」を参照してください。

注: 定義済みの次の役割は編集できません。管理者、アクセス権限なし、読み取り専用の管理者、およびユーザー。

1. 役割詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）に口グインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、口グイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左のナビゲーションバーで **設定**、**役割** の順にクリックします。
c. **アクションの選択 > 新規作成** を選択して、役割詳細 ページを表示します。

2. 名前 フィールドに、「警告の監視担当者」などの名前を入力します。
3. 説明 フィールドに、役割の簡単な説明を入力します（「警告に対応する責任があるサポートスタッフに使用」など）。

   この説明は、その名前と共に 役割 リストに表示されます。
4. 管理者コンソール の 権限 の下の **監視** リンクをクリックし、サーバ監視の権限設定を表示します。
5. 役割に割り当てるアクセスレベルに応じて権限を設定します。
   - **すべて書き込み**
   - **すべて読み取り**
   - **すべて非表示**
   - **カスタム:**

次の監視ページでは、書き込み、読み取り、または非表示の権限を組み合わせることができます。

カテゴリ	ページ（詳細ページを含む）	これらのアクションに適用される権限
監視	デバイス	• 警告の承認（解除） • 設定変更の監視の有効化 • 監視の一時停止または再開 • プロファイルの追加または削除 • メンテナンスウィンドウの追加または削除 • 監視の無効化 • 警告のエクスポート
	警告	• 警告の承認（解除） • サービスデスクチケットの作成 • 通知の設定 • 警告の取得 • 警告の削除 • 警告のエクスポート
	プロファイル	• プロファイルの作成 • プロファイルの編集 • プロファイルの削除 • すべてのデバイスからのプロファイルの削除 • プロファイルのアップロードとダウンロード
	メンテナンスウィンドウ	• メンテナンスウィンドウの作成 • メンテナンスウィンドウの編集 • メンテナンスウィンドウの削除 • すべてのデバイスからのメンテナンスウィンドウの削除 • メンテナンスウィンドウのエクスポート
	Monitoring LEP（監視 LEP）	• デバイスへの追加 • LEP のエクスポート

6. 必要に応じて、デバイスでの監視を有効にできる役割を割り当てます。

ユーザーはデバイスの デバイスの詳細 ページで監視を有効にできるため、権限は インベントリ セクションで設定する必要があります。

a. 管理者コンソール の 権限 の下の **インベントリ** リンクをクリックし、インベントリの権限設定を表示します。
b. デバイス を **書き込み** に設定します。

7. **保存** をクリックします。
8. ユーザーに役割を割り当てます。
   a. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
   b. 役割を割り当てるユーザーのチェックボックスをオンにします。
   c. **アクションの選択 > 役割の適用 > 役割の名前** を順に選択します。

1つ、または複数のデバイスの監視の無効化

デバイスの監視が不要になった場合は、そのデバイスがライセンス対象としてカウントされなくなった後で、この機能を無効にすることができます。

3 つの場所でデバイスの監視を無効にすることができます。そのうちの 2 つの場所は個々のデバイスに対して使用し、1 つの場所はデバイスのグループに対して使用します。

- デバイスの デバイスの詳細 ページから監視を無効にします。
  1. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
  2. デバイスの名前をクリックします。
  3. 下へスクロールし、アクティビティ の下の **監視** をクリックしてセクションを展開します。
  4. **監視の無効化** をクリックします。
  5. 確認ダイアログでアクションを確認します。
- デバイスの Monitoring Detail（ 監視の詳細 ）ページから監視を無効にします。
  1. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。
  2. デバイスの名前をクリックします。
  3. **監視の無効化** をクリックします。
  4. 確認ダイアログでアクションを確認します。
- デバイス リストから複数のデバイスの監視を無効にします。
  1. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。
  2. 監視を無効にするすべてのデバイスの前にあるチェックボックスをオンにします。
  3. **アクションの選択 > 監視の無効化** を選択します。
  4. 確認ダイアログでアクションを確認します。

監視を無効にしてもデバイスの警告は削除されません。無効化されたデバイスに関連する警告の場合、警告の監視 リストページの デバイス 列エントリに、「**デバイスが削除されたか、監視対象ではなくなりました**」と表示されます。ただし、このデバイスの監視を再度有効にすると、アプライアンスでは、このデバイスは新たな監視対象デバイスとして扱われます。この場合、デバイスの以前の警告は、「**デバイスが削除されたか、監視対象ではなくなりました**」のように表示されたままです。

警告の削除の詳細については、警告の削除を参照してください。

1つ、または複数のデバイスの監視の有効化

デバイスを監視する必要がある場合は、監視を開始できます。監視が有効化されているデバイスは、ライセンスの制限に対してカウントされます。

重要: SNMP管理デバイスの監視を有効にしても、ライセンスの制限に対してカウントされません。

3 つの場所でデバイスの監視を有効にすることができます。そのうちの 2 つの場所は個々のデバイスに対して使用し、1 つの場所はデバイスのグループに対して使用します。

- デバイスの デバイスの詳細 ページから監視を有効にします。
    1. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
    2. デバイスの名前をクリックします。
    3. 下へスクロールし、アクティビティ の下の **監視** をクリックしてセクションを展開します。
    4. **監視の有効化** をクリックします。
    5. 確認ダイアログでアクションを確認します。
- デバイス リストから複数のデバイスの監視を有効にします。
    1. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。
    2. 監視を有効にするすべてのデバイスの前にあるチェックボックスをオンにします。
    3. **アクションの選択 > 監視を有効にする** を選択します。
    4. 確認ダイアログでアクションを確認します。

デバイスの監視を有効にすることで、特定のしきい値条件が満たされたときに警告を生成できます。このデバイスの監視を再度有効にすると、アプライアンスでは、このデバイスは新たな監視対象デバイスとして扱われます。この場合、以前のデバイスの警告は、「**デバイスが削除されたか、監視対象ではなくなりました**」のように表示されます。警告の削除の詳細については、警告の削除を参照してください。

警告の操作

サーバー監視で警告が生成された場合、さまざまな応答を使用できます。

警告に基づいてサービスデスクチケットまたは自動Eメール通知を使用できます。手順に従って警告を処理した後に、警告を解除または完全に削除できます。

ダッシュボードに監視ウィジェットを追加している場合は、現在の主な警告が一目で分かります。警告には 警告の監視 リストページおよび Monitored Devices（監視対象デバイス）リストページへのリンクが示されています。

次のように、アイコンによって警告レベルが示されます。

- : **停止**
- : **エラー**
- : **警告**
- : **情報**
- : **完了**

関連トピック

ダッシュボードのウィジェットについて

警告の監視 リストページからの通知スケジュールの追加

デバイス、警告レベル、メッセージ、およびその他の警告情報に対する警告の監視通知スケジュールを追加できます。これらのスケジュールを使用することにより、アプライアンスは指定された条件が満たされた場合に、KACE GOモバイルデバイスへのEメールまたはプッシュ通知を介して管理者に通知することができます。

Eメール通知設定が設定されています。

1. 次のいずれかの方法で、警告の監視 リストページに移動します。
   - **警告の監視 ウィジェットが、開いている** ダッシュボード **にインストールされている場合は、警告の監視 をクリックします。**
   - **左側のナビゲーションバーで、監視 > 警告 を選択します。**
2. 警告メッセージが表示されている行のチェックボックスをオンにし、警告リストの右上の **通知** をクリックして 通知 パネルを表示します。
3. 通知基準を選択します。例えば、情報警告が生成された場合に通知を送信するには、次を指定します。

   レベル | は | 情報
4. 通知条件の下に、次の情報を入力します。

フィールド	説明
タイトル	Eメールの 件名 行に表示する情報。
Eメール受信者	対象とする受信者のEメールアドレス (複数可) 。Eメールアドレスは、完全修飾Eメールアドレスでなくてはなりません。複数のアドレスにEメールを送信するには、コンマを使用して各アドレスを区切るか、またはEメール配布リストを使用します。
頻度	選択した条件とインベントリのアイテムを比較するクエリがアプライアンスによって実行される間隔。条件に一致した場合、通知が送信されます。

5. **オプション** : KACE GOアプリケーションを使用しているモバイルデバイスに警告を送信する場合は、KACE Goに送信 のチェックボックスをオンにします。

   このオプションを使用できるようにするには、モバイルデバイスによるアクセスを有効にする必要があります。詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。
6. **オプション** : 条件を検証するには、**テスト** をクリックします。

   リストが更新されて、検索条件に一致するアイテムが表示されます。テスト中は通知は送信されません。
7. **保存** をクリックします。

通知が作成され、通知スケジュール ページに表示されます。通知の頻度のスケジュールの詳細については、通知スケジュールの編集を参照してください。

関連トピック

通知について

通知のスケジュール

警告からのサービスデスクチケットの作成

サーバー監視警告からサービスデスクチケットを作成できます。このチケットフォームのフィールドに警告からの情報が自動的に入力されます。

1. 次のいずれかの方法で、警告の監視 リストに移動します。
   - 警告の監視 **ウィジェットが、開いている** ダッシュボード **にインストールされている場合は、警告の監視 をクリックします。**
   - **左側のナビゲーションバーで、監視 > 警告 を選択します。**
2. 警告メッセージが表示されている行のチェックボックスをオンにし、**アクションの選択 > 新規チケット** を選択します。
   - キューに基づいてチケットを作成する場合で、組織内に複数のチケットキューがあるときは、**チケット** ドロップダウンリストからキューを選択します。
   - プロセステンプレートに基づいてチケットを作成する場合は、**プロセス** ドロップダウンリストからプロセスを選択します。

   タイトル、概要、送信者、および デバイス フィールドには、警告からの情報が表示されます。
3. **オプション**：企業の手順に適合させるには、「タイトル」および「概要」を変更します。
4. フォームの完成に必要な残りの情報を入力します。次に、**保存** をクリックしてチケットを保存し、チケット詳細 ページから移動するか、または **変更の適用** をクリックし、チケットを保存して編集を継続します。

オプション	説明
タイトル	（必須）問題についての簡単な説明。監視によって入力されたタイトルを自分が選択したいずれかのタイトルに置き換えることができます。
概要	問題についての詳細な説明。 このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションがすべて表示されます。 例： • 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。 • イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファイルパスを指定するか、指定された領域にイメージをドロップします。 ◦ スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。 ◦ この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。 ◦ テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイル

オプション	説明
	は、チケットページの 添付ファイル セクションで管理できます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。 • 外部リンクを追加するには、 をクリックします。 • 外部でホストされるビデオを埋め込むには、 をクリックします。
送信者	チケットを送信するユーザーのログイン名。ドロップダウンリストから別のログイン名を選択して送信者を変更できます。送信者の連絡先情報を表示するには、をクリックします。
資産	この資産の情報がチケットに含まれます。ドロップダウンリストから資産を選択します。資産の詳細を表示するには、をクリックします。
送信者に割り当てられている資産をフィルタリング	送信者に割り当てられている資産に基づいて資産リストをフィルタリングします。
デバイス	このデバイスの情報がチケットに含まれます。監視ではこの情報が提供されます。デバイスの詳細を表示するには、をクリックします。
送信者に割り当てられているデバイスをフィルタリング	送信者に割り当てられているデバイスに基づいて資産リストをフィルタリングします。
インパクト	不都合または作業不可の人数。
カテゴリ	問題の分類。
ステータス	チケットの現在の状態。チケットをプロセステンプレートから作成または編集している場合は、このフィールドは表示されません。
優先度	チケットの優先度の重要性。
所有者	ライフサイクルを通じてチケットを管理する責任があるユーザー。
期限	チケットが終了するようにスケジュールされている日時。 サービスレベル契約が有効になっていない場合、期日はデフォルトでは「なし」に設定されています。 サービスレベル契約が有効になっている場合、期日はSLA設定に従って自動的に計算されます。期日は、チケット送信時に設定された優先度に基づいて計算されます。チケットが最初に送信された後に優

オプション	説明
	先度が変更された場合、期日は新しい優先度に従って再計算されますが、この場合、元の送信日時に基づいた再計算になります。SLA解決時間の設定が変更された場合、その変更は新しいチケットにのみ適用されます。古いチケットは影響を受けません。詳細については、「サービスレベル契約の設定」を参照してください。 期限の日時を手動で設定するには、**手動日付** を選択します。この場合、サービスレベル契約が有効になっていると、期限の日時が計算されてオプションとして表示されますが、選択はされません。
「CC」リスト	チケットイベント発生時にEメール通知を受信するユーザーのリスト。CCリストには、キューの **イベント発生時にEメールを送信** 設定で指定されているチケットイベントと **チケットCC** に基づいて、Eメールが送信されます。
解決	チケットに関連付けられている問題の解決策。 このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションがすべて表示されます。 例： • 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。 • イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファイルパスを指定するか、指定された領域にイメージをドロップします。 ◦ スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。 ◦ この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。 ◦ テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイルは、チケットページの 添付ファイル セクションで管理できます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。 • 外部リンクを追加するには、 をクリックします。 • 外部でホストされるビデオを埋め込むには、 をクリックします。

オプション	説明
関連するチケットの情報	プロセステンプレートからチケットを作成している場合には、このセクションは表示されません。
チケットの追加	クリックしてこのチケットの関連情報にチケットを追加します。
参照元	**参照元** は読み取り専用フィールドで、**関連参照** セクションを介してこのチケットを参照しているすべてのチケットへのチケット参照が保持されます。
マージされたチケット	このセクションでは、必要に応じて、このチケットとマージされたチケットのリストを編集できます。マージするチケットは、同じキューに属している必要があります。チケットの詳細 ページを使用してチケットをマージする場合、開いているチケットがプライマリチケットになります。マージされたその他のすべてのチケットは、マージするとアーカイブされます。詳細については、「チケットのマージ」を参照してください。 マージされたチケットを追加するには、**チケットを追加してマージする / マージされたチケットを編集する** をクリックし、表示されるリストからチケットを選択します。
プロセス情報	プロセステンプレートからチケットを作成している場合にのみ、このセクションが表示されます。このセクションに表示されるすべての設定は読み取り専用です。プロセステンプレートの作成および設定の完全な情報については、次を参照してください。 プロセステンプレートの追加、編集、および有効化
プロセス	このチケットに関連付けられたプロセステンプレートの名前。
プロセスタイプ	プロセスのタイプ。
プロセスステータス	このプロセステンプレートに関連付けられたワークフローのステータス。例えば、保留中の承認。
親	親のチケットの名前。このチケットに関連付けられたプロセステンプレートで定義されます。
プロセスの承認	このチケットに対する承認者として割り当てられているユーザーのリスト（該当する場合）。承認者は、プロセステンプレートで定義されたステージのリストに表示されます。各ステージには、必要に応じて、1人または複数の承認者を設定できます。各承認者およびステージに関連した設定（承認のタイムアウトや通知など）も、このセクションのリストに表示されます。プロセスチケットを作成すると、最初の承認者に対するタイムアウト期間が開始します。そのユーザーがチケットを承認すると、次の承認者に対するタイムアウト期間が開始し、その後も同じことが繰り返されます。

オプション	説明
プロセスのアクティビティ	プロセスのアクティビティのリスト。それぞれが子チケットを表し、プロセステンプレートでの定義のとおりに、ステージのリストに表示されます。必要に応じて、複数のチケットを同じステージに割り当てることができます。例えば、最初のステージが新入社員の機器とサプライを入手することである場合、注文するデバイス、オフィス機器、およびサプライにそれぞれ別個の子チケットを用意し、そのすべてをステージ1に割り当てることができます。プロセスチケットを作成すると、ステージ 1 に割り当てられたすべての子チケットが自動的に作成されます。すべてのステージ 1 チケットが終了するとステージ 2 チケットが作成され、すべてのステージ 2 チケットが終了するとステージ 3 チケットが作成され、以下同様に続きます。
チケットの追加	クリックしてこのチケットの関連情報にチケットを追加します。
参照元	**参照元** は読み取り専用フィールドで、**関連参照** セクションを介してこのチケットを参照しているすべてのチケットへのチケット参照が保持されます。
Comments	チケットに追加するコメント。チケットのコメントとして、添付ファイルやスクリーンショットを追加したり、自動応答やサポート技術情報の内容を提供したりできます。詳細については、次を参照してください。 • チケットへのコメントの追加 • サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除 このチケットに対する解決策として自動応答を追加する場合は **事前定義された応答** をクリックし、応答テンプレートを選択します。 選択した応答テンプレートが **解決** フィールドに表示されます。複数の応答テンプレートを解決策のエントリとして追加できます。これらは、選択した順序で表示されます。 **ヒント:** 応答テンプレートを作成または編集するには、変更を保存し **管理** をクリックします。これにより、応答テンプレート ページが表示されます。応答テンプレートの詳細については、「応答テンプレートの表示および編集」を参照してください。
サポート技術情報記事	サポート技術情報記事を参照し、その内容をチケットのコメントに追加します。サポート技術情報記事の詳細については、「サポート技術情報記事の管理」を参照してください。

関連トピック

高度な検索条件を使用した警告の検索

高度なページレベル検索を使用すると、さまざまな条件の組み合わせを使用して、現在のページの情報を検索することができます。

この例では、高度な検索を使用して接続の問題に関連する重大な警告を検索する方法について示します。

1. 次のいずれかの方法で、警告の監視 リストページに移動します。
   - 警告の監視 **ウィジェットが、開いている** ダッシュボード **にインストールされている場合は、警告の監視 をクリックします。**
   - **左側のナビゲーションバーで、監視 > 警告 を選択します。**
2. 警告の監視 リストの右上にある **高度な検索** をクリックします。

   高度な検索 パネルが開きます。

3. 次のように、警告レベルの検索に必要な条件を指定します。

   警告の監視の情報: レベル | は | 緊急
4. 演算子ドロップダウンリストで **および** を選択した状態で、**行の追加** をクリックして新しい行を追加します。次に、メッセージに **接続できません** が含まれる警告の検索に必要な条件を指定します。

   警告の監視の情報: メッセージ | 次の値を含む | 接続できません
5. **検索** をクリックします。

リストが更新されて、検索条件に一致するデバイスが表示されます。

含まれるテキストおよび除外するテキスト機能を使用した警告のフィルタ

特定のタイプの警告の受信が多すぎる場合や、特定の警告を追跡する場合は、メッセージテキストおよび重大度レベルに基づいて警告をフィルタできます。

不要または煩雑と判断した場合は、特定のイベントを警告の発生から除外できます。受信しない警告をフィルタするには、Exclude Text（除外するテキスト）を使用して、不要な警告を識別する内容を指定します。テキストを含む と テキストを除外 を使用して、アラートカテゴリのサブセットを絞り込みます。

監視機能によって報告される警告をフィルタする方法は 2 つあります。1 つは Profile Details（プロファイル詳細）ページで作業する必要があり、もう 1 つは 警告の監視 リストページから **アクションの選択** ドロップダウンメニューを使用する必要があります。

Profile Details（プロファイル詳細）ページからの含まれるテキストおよび除外するテキスト機能を使用した警告のフィルタ

メッセージテキストおよび重大度レベルに基づいて、受信する警告をフィルタできます。

テキストを含む と テキストを除外 を使用して、アラートカテゴリのサブセットを絞り込みます。

注: 基準一致テキスト（error など）は、Windows イベントログ内で、重大度レベルとメッセージ自体の両方に対して照合されます。

1. プロファイル リストページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**監視** をクリックして、**プロファイル** をクリックします。
2. 編集する既存のプロファイルのチェックボックスをオンにし、**アクションの選択 > 編集** を選択して プロファイルの詳細 ページを表示します。
3. 必要に応じて、包含および除外の 条件 設定を変更します。
    - Include Text（**含まれるテキスト**）**を変更します。**
        1. 変更する含まれる検索テキストがある行で、**編集** ボタン をクリックします。
        2. 新しい検索テキストを入力します。
    - Exclude Text（**除外するテキスト**）**を変更します。**
        1. 特定の警告を除外するために変更するテキストがある行で、**編集** ボタン をクリックします。
        2. 新しい除外テキストを入力します。
    - **必要に応じて**、大文字と小文字を区別 **ドロップダウンリストで はい を選択します。**
    - **警告基準を追加します。**
        1. 条件 カテゴリヘッダーで、**追加** ボタン をクリックします。
        2. レベル、含めるテキスト、除外するテキスト、および大文字と小文字の区別を設定します。
4. ページの一番下で **保存** をクリックします。

関連トピック

監視プロファイルの含まれるテキストおよび除外するテキストの例

プロファイルの編集

警告の監視 リストページからの除外するテキスト機能を使用した警告のフィルタ

特定のタイプの警告の受信が多すぎる場合は、メッセージテキストに基づいてそれらをフィルタできます。

完全なメッセージ、メッセージの一部、および基本的な正規表現を Exclude Text（除外するテキスト）フィールドで使用して、受信する警告をフィルタするための基準を定義できます。

1. 警告の監視 リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. ダッシュボードまたはナビゲーションバーから警告リストにアクセスします。
    - 警告の監視 **ウィジェットが、開いている** ダッシュボード **にインストールされている場合は、警告の監視 をクリックします。**
    - **左側のナビゲーションバーで、監視 > 警告 を選択します。**
2. 警告の隣のチェックボックスをオンにします。
3. **アクションの選択 > このような警告をフィルタリング** を選択します。

このような警告をフィルタリング ダイアログが表示され、警告メッセージの内容が Exclude Text（除外するテキスト）フィールドに入力されます。

4. Exclude Text（除外するテキスト）フィールド内のテキストを編集して、フィルタを絞り込みます。

   例：断片化されたディスクのエラーを除くディスクエラーについて警告を発生させるには、次のように入力します。

Include Text（含まれるテキスト）の入力	Exclude Text（除外するテキスト）の入力
Error code.*Disk /dev/sd[a-z]	is fragmented

5. **保存** をクリックします。

   警告を発生させたプロファイルは、この除外情報によって変更されます。

関連トピック

監視プロファイルの含まれるテキストおよび除外するテキストの例

Profile Details（プロファイル詳細）ページからの含まれるテキストおよび除外するテキスト機能を使用した警告のフィルタ

監視プロファイルの含まれるテキストおよび除外するテキストの例

基準を定義するために、完全なメッセージ、メッセージの一部、および基本的な正規表現を Include Text（含まれるテキスト）および Exclude Text（除外するテキスト）フィールドで使用できます。

文字列フォーマットと一致するフィールド入力の例

文字列フォーマット（一致対象）	?? データの例	?? Include Text（含まれるテキスト）	?? Comments
[任意のテキスト]Error 32768 Physical memory running low[任意のテキスト]	Error 32768 Physical memory running low	Error 32768 Physical memory running low	一致： 「Error 32768 Physical memory running low」
Drive /dev/[任意のドライブマウントポイント] has drive errors	Drive /dev/sdi has drive errors	Drive /dev/[a-z]{1,} has drive errors	一致： 「Drive /dev/」 それに続く文字 a ～ z を含む任意の長さの単語 それに続く「has drive errors」
Error nnnn: Disk is [任意のテキスト]	2014-06-28: Error 4567: Disk is full	Error [0-9]{4}: Disk is	一致： 「Error」 それに続く任意の 4 桁の数字 それに続く「: Disk is」
Error nnnnnn [エラーメッセージ]	Error 4096 Drive has errors	Error [0-9]{1,8}	一致： 「Error」

文字列フォーマット（一致対象）	?? データの例	?? Include Text（含まれるテキスト）	?? Comments
			それに続く任意の 1 ～ 8 桁の数字
[FATAL] [エラーメッセージ]	[FATAL] General exception occurred	[FATAL].*	一致： 「[FATAL]」 それに続く任意のメッセージ
error reading [テキスト] on [ボリューム]:	error reading swap label on /dev/VolGroup00: [Errno 21] Is a directory	error reading.* on /dev/[a-zA-Z0-9]*:	一致： 「error reading」 それに続く任意のテキスト それに続く「on /dev/」 それに続く任意の長さの文字 a ～ z、A ～ Z、0 ～ 9 を含む任意のマウントポイント それに続くコロン

警告の出力を絞り込むために、含まれるテキストと除外するテキストを組み合わせて使用する例

例 A：除外するテキストとしての文字列

この例では、特定のドライブマウントポイントから断片化されたディスクに関するディスクエラーの警告を受信したくありませんが、その他のすべてのエラーは届くようにする必要があります。

2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 4: Disk /dev/sda has errors
2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 5: Disk /dev/sda is fragmented
2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 6: Disk /dev/sda has a bad block

ディスクエラーと不良ブロックについては警告を発生させ、断片化されたディスクについては発生させないようにするには、次のように入力します。

Include Text（含まれるテキスト）の入力	Exclude Text（除外するテキスト）の入力
Error code.*Disk /dev/sd[a-z]	is fragmented

注: Include Text（含まれるテキスト）では、テキストボックス内の改行は認識されません。つまり、次のように入力した場合

code 5
code 7

注: 検索では code 5code 7 について一致を見つけようとします。この場合、**追加** を使用して、2 つ目が含まれるように別の行を作成する必要があります。

注: ただし、Exclude Text（除外するテキスト）では、テキストボックス内の改行は認識されます。つまり、次のように入力した場合

code 5
code 7

注: 検索では code 5 と code 7 について一致を見つけようとします。この場合は、**追加** を使用して、2 つ目を除外するために別の行を作成する必要はありません。

例 B：除外するテキストとしての基本的な正規表現

この例では、特定のドライブマウントポイントから断片化されたディスクに関するディスクエラーまたは有効期限情報の警告を受信したくありませんが、その他のすべてのエラーは届くようにする必要があります。

2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 4: Disk /dev/sda has errors
2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 5: Disk /dev/sda is fragmented
2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 6: Disk /dev/sda has a bad block
2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 7: Disk /dev/sda is more than 3 years old

エラーコード5またはエラーコード7を含むイベントを無視して、優先されるイベントについて警告を発生させるには、次のように入力します。

Include Text（含まれるテキスト）の入力	Exclude Text（除外するテキスト）の入力
Error code.*Disk /dev/sd[a-z]	Error code [5|7]

包含または除外基準テキストフィールドでの特殊文字のエスケープ

除外または包含基準テキストフィールドに文字を入力する際に、一重引用符や二重引用符などの特殊文字を入力することもできます。ただし、これらの特殊文字を使用する場合は、検索が正しく機能するようにバックスラッシュ文字（\）を使用してエスケープする必要があります。

文字	説明
'	一重引用符
"	二重引用符
`	バックティック
\	バックスラッシュ

例えば、**Received 'redoubt started' message** を検索するには、「Received \'redoubt started\' message」と入力します。

警告の解除

警告を処理した場合、アクティブな警告のリストに表示されないように警告を解除することができます。

警告を解除しても、データベースから警告は削除されません。警告をデータベースから削除する場合は、警告の削除を参照してください。

1. 次のいずれかの方法で、警告の監視 リストページに移動します。
   - 警告の監視 **ウィジェットが、開いている** ダッシュボード **にインストールされている場合は、警告の監視 をクリックします。**
   - **左側のナビゲーションバーで、監視 > 警告 を選択します。**
2. 警告メッセージが表示されている行のチェックボックスをオンにし、**アクションの選択 > 解除** を選択します。

   警告リストにその警告が表示されなくなりました。

関連トピック

警告リストから解除された警告の取得と確認

警告リストから解除された警告の取得と確認

解除された警告はデータベースに残っているため、警告リストに取得して確認することができます。

注: 削除した警告は取得できません。

1. 次のいずれかの方法で、警告の監視 リストページに移動します。
   - **警告の監視 ウィジェットが、開いている** ダッシュボード **にインストールされている場合は、警告の監視 をクリックします。**
   - **左側のナビゲーションバーで、監視 > 警告 を選択します。**
2. **アクションの選択 > 解除された警告を包含** を選択します。

   警告リストに、解除されたすべての警告が再度読み込まれます。これらの警告では、ステータス 列に「解除されました」というステータスが表示されます。

警告の削除

警告を問題なく処理した後はデータベースから警告を削除することができます。

1. 警告の監視 リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**監視** をクリックして、**デバイス** をクリックします。
2. 1つまたは複数の警告の隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

サービスデスクの使用

サービスデスクとは、アプライアンスに用意されているエンドユーザーのトラブルチケット追跡システムです。サービスデスクを利用すると、Eメール、管理者コンソール、およびユーザーコンソールを介してトラブルチケットを送信できます。

サービスデスクの設定

サービスデスクの設定では、役割、ユーザー認証、ラベル、チケットとEメールの設定、キュー、およびカスタマイズの設定を行う必要があります。

システム要件

サービスデスクを使用するには、アプライアンス、E メールサーバ、およびユーザーアカウント情報が必要です。

- **アプライアンス要件**：サービスデスクを使用するには、アプライアンスを設定および構成しておく必要があります。アプライアンスサーバーの設定の詳細については、アプライアンスの設定を参照してください。
- **Eメールサーバー要件**: サービスデスクのEメールを送受信するため、次のいずれかのタイプのEメールサーバーが必要です。
  - POP3 Eメールサーバー。詳細については、POP3 Eメールアカウントについてを参照してください。
  - Microsoft Exchange ServerなどのEメールサーバー。このサーバとアプライアンスとの接続設定の手順については、「SMTP Eメールサーバーの設定」を参照してください。
- **ユーザーアカウント情報**: ユーザーアカウント情報は、LDAP準拠のディレクトリサービス（Microsoft Active Directoryなど）に保存できます。ユーザーアカウント情報を保存すると、サービスデスクはユーザーを承認したり、その他の追跡対象を識別したりするうえで使用するデータの検索およびインポートを効率的に行うことができます。LDAP属性（組織単位、ドメインコンポーネント、相対識別名など）を参照して、ユーザーやその他のエンティティのグループをフィルタリングすることができます。詳細については、「ユーザーアカウント、LDAP認証、およびSSOの設定」を参照してください。

小規模な組織であれば、この要件を割愛し、必要なユーザーアカウント情報をユーザーごとに手動で作成しても構いません。手動でのユーザーの作成の詳細については、サービスデスクの設定を参照してください。

サービスデスクについて

サービスデスクはエンドユーザーのトラブルチケット追跡システム（アプライアンス**ユーザーコンソール**の一部）のデフォルト名です。サービスデスクを利用すると、エンドユーザーが E メールを使用して、または**ユーザーコンソール**を介してトラブルチケットを送信できます。

ヘルプデスクチームは、E メール、**管理者コンソール**（http://**appliance_hostname**/admin）、または KACE GO アプリケーションを使用してこれらのチケットを管理します。必要に応じて、チケットに関連付けられたカテゴリやフィールドをカスタマイズできます。

注: 以前のバージョンのアプライアンスでは、**サービスデスク**は**ヘルプデスク**と呼ばれていました。以前のリリースからアップグレードした場合は、**管理者コンソール**のタブに、**ヘルプデスク**またはカスタム指定の文字列が表示される場合があります。この表示を変更する方法については、サービスデスクのタイトル名とラベル名の変更を参照してください。

設定作業の概要

会社のポリシーとブランド設定の要件を満たすようにサービスデスクを設定できます。

セットアップタスクには、以下が含まれます。

- **ユーザーの役割とラベルの設定**：権限ベースの役割を作成し、ユーザーのアクセスを管理します。詳細については、「ユーザーアカウントの役割の設定」を参照してください。
- **ユーザーアカウントの設定**：サービスデスクのユーザーおよび管理者にはすべて、認証済みのユーザーアカウントが必要です。詳細については、「ユーザーアカウント、LDAP認証、およびSSOの設定」を参照してください。
- **チケット情報のカスタマイズ**：必要に応じて、チケットのカテゴリ、ステータス、インパクト、および優先度のプロパティを追加します。チケットに含める追加情報を確認します。詳細については、「チケット設定の構成」を参照してください。
- **E メールテンプレートのカスタマイズ**：通知を送信するために使用されるサービスデスク E メールテンプレートを設定します。詳細については、「Eメールテンプレートの設定」を参照してください。
- **Eメール通知の設定**：E メール通知をトリガするイベントを設定します。詳細については、「Eメール設定の設定」を参照してください。
- **キューとプロセスの設定**：
  - **キュー**：チケットを整理したり、種類の異なるタスク（ハードウェアタスクやソフトウェアタスクなど）を処理したりするには、キューを使用します。詳細については、「サービスデスクチケットキューの設定」を参照してください。
  - **プロセス**：主要なタスクまたは連続するタスクに含まれるチケット間の関係を設定するには、プロセスを使用します。また、チケット内で親子関係を利用することで、関係を確立することもできます。詳細については、「サービスデスクプロセスの使用」を参照してください。
- **チケットルールのセットアップ**：サービスデスクがチケットを処理するために使用するルールを設定します。詳細については、次を参照してください。 チケットルールについて
- **満足度調査を実施するかどうかの決定**：詳細については、「満足度調査の利用」を参照してください。
- **会社の営業時間と休業日の設定**：会社の営業時間および認識されている休業日を定義します。これらの時間と休業日は、チケットの期日とサービスレベル契約違反を決定する際に使用されます。詳細については、「サービスデスクの営業時間と休業日の設定」を参照してください。
- **サービスレベル契約（SLA）の設定**：チケットの期日と SLA 違反を計算する際に使用される SLA を設定します。詳細については、「サービスレベル契約の有効化」を参照してください。
- **ユーザーコンソールホームページの設定**：**ユーザーコンソール**ホームページのロゴとようこそ情報を変更します。また、クイックアクションおよび告知や、サポート技術情報記事、チケット、およびその他のアイテムへのリンクを表示または非表示にします。詳細については、以下を参照してください。
  - ユーザーコンソールのロゴおよびログインテキストの管理者レベルでの変更
  - ユーザーコンソールホームページのアクションボタンおよびウィジェットの表示または非表示
  - ユーザーコンソールの告知の追加、編集、非表示、または削除
  - ユーザーコンソールホームページでのカスタムリンクの追加、編集、または削除
  - ユーザーコンソールホームページのサポート技術情報記事へのリンクの表示または非表示

別のシステムからのチケットのインポート

準備済みの CSV (カンマ区切り値) ファイルを使用して、別のシステムからチケットをインポートできます。チケットを CSV ファイルにエクスポートしてから、チケットのインポート ウィザードを使用してそのコンテンツをアプライアンスにインポートします。ウィザードは、関連するレコードが拒否されるのを防ぐために、インポートされているデータを検証し、特定のフィールドが事前定義された形式に従う必要があります。

1. チケットデータを CSV ファイルにエクスポートします。
2. チケットのインポート ウィザードに移動します。
    a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルの インポート セクションで、**チケットのインポート** をクリックします。
3. チケットのインポート ウィザードの チケットインポートファイルの選択 ページで、必要に応じて CSV ファイルと関連オプションを指定します。

    ヒント: ページの下部にあるリンクをクリックすると、最新のチケットインポートのステータスを確認できます。

    a. ファイル (.csv) のアップロード セクションで、**ファイルの選択** をクリックし、インポートするチケットデータを含む CSV ファイルを選択します。
    b. CSV ファイルにヘッダー行がある場合は、**ファイルヘッダー行** チェックボックスをオンにします。
    c. インポート先 セクションで、チケットデータをインポートするキューとテンプレートを指定します。
    d. チケットデータにアプライアンスデータベースに存在しない 1 人以上のユーザーが含まれていて、チケットのインポート時にそれらのユーザーを自動的に作成する場合は、**ユーザーの自動作成** チェックボックスをオンにします。
    e. **次へ** をクリックします。
4. チケットのインポート ウィザードで、表示される フィールドマッピング ページで、チケットテンプレートフィールドを CSV ファイルで指定されたチケットフィールドにマッピングします。

    チケットフィールドをマッピングする場合は、次のガイドラインに従ってください。

    - チケットフィールドを指定するには、**CSV フィールド** 列をクリックして、適切な値を選択します。
    - **コメント** フィールドでは、次の構文を使用する必要があります。"<datetime>";"<user_name>";"<comment>";"<owners_only_flag>".1 つの **コメント** フィールドに複数のコメントを入力する場合は、|EOL| で区切る必要があります。例 : "01/01/2019 10:10";"Admin";"これはサンプルコメントです";"Y"|EOL|"01/02/2019 11:20";"ユーザー A";"これはサンプルコメント 2 です";"Y"|EOL|"01/02/2019 12:00";"Admin";"これはサンプルコメント 3 です";"Y"|EOL|.また、プライマリキーを使用して、同じチケットフィールド内の複数の列エントリを結合することもできます。Table 33およびTable 34を参照してください。
    - **作業詳細** フィールドでは、次の構文を使用する必要があります。"<user_name>";"<start_datetime>";"<end_datetime>";"[adjustment_time];[<note>].1 つの **コメント** フィールドに複数のコメントを入力する場合は、|EOL| で区切る必要があります。例 : "Admin";"01/01/2019 08:10";"01/01/2019 10:30";"10";"Work Note"|EOL|"User B";"01/01/2019

11:20";"01/01/2019 12:30".また、プライマリキーを使用して、同じチケットフィールド内の複数の列エントリを結合することもできます。Table 33およびTable 34を参照してください。

- サブカテゴリを含む **カテゴリ** フィールドでは、サブカテゴリを区切るために二重コロン「::」を使用する必要があります。例：Hardware::Printer::Paper.アプライアンスにまだ存在しないカテゴリが検出された場合、それらのレコードは自動的に拒否されます。
- **インパクト** フィールドと **優先度** フィールドには、アプライアンスで事前定義された有効な内容が含まれている必要があります。
- ユーザー名フィールド（ **登録者** など ）は、ユーザー E メール、ユーザー名、ユーザー ID、および表示名を受け入れます。同じユーザー名を持つ複数のレコードが自動的に拒否されます。
- 特定のデータ形式（ リンクなど ）を想定するカスタムフィールドの内容は検証され、データが無効な場合は拒否されます。
- **PK** 行を使用して、行がデータレコードのプライマリキーであるかどうかを示します。プライマリキーとしてマークされた行の値が同じレコードは、1 つのサービスデスクチケットにまとめられます。たとえば、**タイトル** 列をチケットテーブルのプライマリキーとしてマークし、CSV ファイル内のすべてのレコードに完全に同じ **タイトル** 列がある場合（ 例：マイチケット ）、インポートによって単一のサービスデスクチケットが作成され、複数のエントリが同じ列に結合されます。または、コメント 列と 作業詳細 列 をインポートする場合は、|EOL| を使用してエントリを区切ることもできます。次の例では、複数のエントリを同じチケットフィールドに結合する場合に、|EOL| 区切り記号（ コメント および 作業詳細 列のみ ）または プライマリキー（ PK ） 設定（ 任意の列 ）を使用して、入力 CSV ファイルを構造化する方法を示します。

例：複数の列エントリを結合するには、|EOL| 区切り記号を使用します (コメント 列と 作業詳細 列のみ)

タイトル	ステータス	優先度	所有者	コメント
タイトル A	新規	中	管理者	「2021/6/15 3:15:44 コメント AAA」|EOL| 「2021/6/17 5:17:25 コメント BBB」|EOL| 「2021/6/19 7:21:42 コメント CCC」|EOL|
タイトル B	閉じられた	高	管理者	「2021/7/21 2:18:31 コメント DDD」|EOL| 「2021/6/17 4:56:56 コメント EEE」|EOL| 「2021/6/19 6:28:32 コメント FFF」|EOL|

注: |EOL| 区切り記号は、これらのエントリを 1 つの コメント フィールドに結合するようにウィザードに指示します。タイトル 列をプライマリキー（ PK ）として宣言する必要はありません。同じ構文が 作業詳細 コンテンツにも適用されます。

例：プライマリキー 設定を使用して、複数の列エントリを結合する

タイトル	ステータス	優先度	所有者	コメント
タイトル A	新規	中	管理者	「2021/6/15 3:15:44 コメント AAA」
タイトル A				「2021/6/17 5:17:25 コメント BBB」
タイトル A				「2021/6/19 7:21:42 コメント CCC」
タイトル B	閉じられた	高	管理者	"7/21/2021 2:18:31 コメント DDD
タイトル B				「2021/6/17 4:56:56 コメント EEE」
タイトル B				「2021/6/19 6:28:32 コメント FFF」

注: タイトル 列をプライマリキー（PK）として宣言すると、同じタイトル（タイトル A と タイトル B）を持つすべてのエントリが 1 つの コメント フィールドに結合されます。|EOL| 区切り記号を使用する必要はありません。作業詳細 を含む他の列にも同じメカニズムが適用されます。

- **PK** 設定を使用して、既存のチケットを更新することもできます。たとえば、Table 35 に記載されているデータでチケット A をアップロードした場合、Table 36 で説明されている更新された CSV ファイルをアップロードすることで簡単に置き換えることができますが、設定で タイトル 列をプライマリキー（**PK**）として設定する必要があります。

例：初期 CSV データ

タイトル	ステータス	優先度	所有者
タイトル A	新規	高	ユーザー A

例：更新済み CSV データ

タイトル	優先度	所有者
タイトル A	低	ユーザー B

- 完了したら、**プレビュー** をクリックします。

5. インポートしようとしているデータが、表示された 確認 ページで有効であることを確認します。

a. 以下のセクションを確認してください。

- **挿入対象のレコード**：サービスデスクチケットとして作成される CSV ファイルからのすべてのチケットレコードがリスト表示されます。
- **更新対象のレコード**：既存のサービスデスクチケットを更新しようとしているすべてのチケットレコードが CSV ファイルからリスト表示されます。
- **拒否されたレコード**：エラーのためにサービスデスクチケットとして作成されないすべてのチケットレコードが CSV ファイルからリスト表示されます。拒否されたレコードごとに、このセクションの 理由 列にエラーの原因が表示されます。関連するチケットフィールドが赤でハイライトされます。このフィールドの内容を確認して、問題をより深く理解します。たとえば、CSV ファイルにアプライアンスに存在しないユーザーが存在し、**ユーザーの自動作成** チェックボックスを選択しなかった場合、そのユーザーごとにエラーが発生します。インポート CSV ファイルを編集するか、チケットのインポートファイルの選択 ページで該当するインポートオプションを変更することで、エラーを解決できます。

b. チケットデータのインポートを続行する準備ができたら、**インポート** をクリックします。

注: インポートを開始すると、プロセスを停止または元に戻すことはできませんが、インポートが完了すると任意のチケットを削除できます。

チケットのインポート - ステータス ページが表示され、チケットレコードがインポートされていることが示されます。インポートの完了に必要な時間は、インポートするチケットデータの量によって異なります。完了すると、ステータス 行にインポート操作の結果が表示されます。インポート中にエラーが検出された場合は、エラーレコード 行に表示されます。**詳細の表示** をクリックして詳細を確認します（該当する場合）。

6. インポートの結果に問題がなく、追加のレコードをインポートする必要がない場合は、**完了** をクリックします。さらにチケットをインポートするには、**追加のインポート** をクリックし、必要に応じてインポートプロセスを繰り返します。

サービスデスクの営業時間と休業日の設定

営業時間と休業日を設定することで、サービスデスクキューでサービスレベル契約（SLA）を効果的に追跡し、満たすことができます。アプライアンス上で組織コンポーネントが有効化されている場合は、各組織の営業時間と休業日を個別に設定します。

営業時間と休業日を設定した後、各サービスデスクチケットキューの SLA 設定でそれらの営業時間と休業日を使用できるようにする必要があります。

サービスデスクの営業時間の設定

チケットの期日を計算する際に営業時間を考慮するようにサービスデスクを設定できます。組織が複数ある場合は、組織ごとに個別に営業時間を設定します。

サービスデスクの営業時間を設定した後、サービスレベル契約（SLA）設定で、チケットキューでそれらの時間を使用できるようにする必要があります。

1. Business Hours（営業時間）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。

c. **設定** パネルの Business Hours and Holidays（営業日と休業日）セクションで、**営業日を定義** をクリックします。

2. **24時間オープン** チェックボックスまたは **休業** チェックボックスをオンにして、開始時間と終了時間を指定し、曜日ごとに営業時間を指定します。
3. **保存** をクリックします。

SLA で営業時間を使用するようにキューを設定します。詳細については、「チケットキューの設定」を参照してください。

サービスデスクの休業日の設定

チケットの期日を計算する際に会社の休業日を考慮するようにサービスデスクを設定できます。組織が複数ある場合は、組織ごとに個別に休業日スケジュールを設定します。

サービスデスクの休業日を設定した後、サービスレベル契約（SLA）設定で、チケットキューでそれらの休業日を使用できるようにする必要があります。

1. Holidays（休業日）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルの Business Hours and Holidays（営業日と休業日）セクションで、**休業日を定義** をクリックします。
2. **休業日を追加** をクリックして、新しい休業日をリストに追加します。編集する休業日の隣にある **編集** ボタンをクリックします: をクリックします。削除する休日の隣にある **削除** ボタンをクリックします: をクリックします。リスト内の休業日は、**年でフィルタリング** ドロップダウンリストで年を選択して、年でフィルタリングできます。
3. **保存** をクリックします。

SLA で休業日を使用するようにキューを設定します。詳細については、「チケットキューの設定」を参照してください。

サービスレベル契約の設定

サービスレベル契約（SLA）は、チケットの優先度に基づいてサービスデスクチケットの想定解決時間（または期日）を計算するために使用されるルールです。

各チケット優先度の想定解決時間を設定でき、期日を計算する際に定義済みの営業時間と休業日を SLA で考慮できるようにすることができます。例えば、優先度が **低** のチケットが 2 日間で解決されるように設定されており、低優先度のチケットが休業日の前日に発行された場合、期日を計算する際に休業日は 2 日間の解決時間から除外されます。

また、通知および E メールイベントが有効な場合、チケットが期限超過になると、SLA 違反 E メールイベントに指定されているユーザーに E メールが送信されます。E メール通知の頻度は SLA 設定で設定され、その頻度に非営業時間や休業日が含まれている場合でも、通知はその頻度に従って送信されます。

サービスレベル契約の有効化

サービスレベル契約（SLA）では、各キューのチケットの解決に使用できる時間を定義します。サービスデスクキューが複数ある場合は、各キューの SLA 設定を個別に設定します。

SLA はキューで定義された優先度値に基づくため、これらの値を定義してから SLA を設定する必要があります。詳細については、「チケット優先度値のカスタマイズ」を参照してください。また、SLA では、営業時間と

休業日が定義されている場合にのみ、それらの時間と休業日を使用できます。詳細については、「サービスデスクの営業時間と休業日の設定」を参照してください。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。
   - キューの名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。
2. Service Level Agreement（ サービスレベル契約 ）セクションまでスクロールします。キューに定義されている各優先度値に対して1行が表示されます。詳細については、「チケット優先度値のカスタマイズ」を参照してください。
3. 優先度（ **高**、**中**、**低**など ）ごとに、次の設定を指定します。

オプション	説明
有効	優先度について SLA が有効かどうか。SLA を有効にする場合はチェックボックスをオンにし、無効にする場合はチェックボックスをオフにします。 **注:** サービスレベル契約が優先度に対して有効になっている場合、その優先度に対して定義されている解決時間に基づいてチケットの期日が自動的に計算されます。DUE_DATE フィールドに対する変更権限を持つユーザーは、この自動的に計算される日付をオーバーライドできます。
解決時間	有効にした優先度の時間（ 時間または分単位 ）。この期間は、チケットが送信される日付と時刻に基づいてチケットの期日と時刻を自動的に計算するために使用されます。
営業時間/休日を使用	各優先度のチケットの期日を計算する際に、設定した営業時間と休業日を使用するかどうか。これらの設定を使用する場合は、チェックボックスをオンにします。詳細については、「サービスデスクの営業時間と休業日の設定」を参照してください。
通知パターン	E メール通知が送信される時間（ 時間または分単位 ）。チケットの期日が過ぎても解決されない場合は、Eメール通知が繰り返し送信されます。Eメールは、「SLA違反」Eメールイベントで指定されているユーザーに送信されます（ イベント発生時にEメールを送信 セクションで設定されている場合 ）。詳細については、「EメールトリガとEメールテンプレートの設定」を参照してください。 **注:** E メール通知を繰り返し送信せず、1 回送信する場合は、0 を入力します。

4. **保存** をクリックします。

サービスデスクチケットキューの設定

サービスデスクチケットは、アプライアンスのキューに格納されます。ほとんどの組織では、チケットキューは1つだけで十分です。必要に応じて、この1つのキューをカスタマイズしたり、追加のキューを作成して管理したりできます。

詳細については、「サービスデスクチケットキューの管理」を参照してください。

チケットキューの設定

チケットキューの設定は必要に応じて変更することができます。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。
   - キューの名前をクリックします。
   - **アクションの選択** > **新規作成** を選択します。
2. 次の設定を指定します。

フィールド	説明
名前	サービスデスクキューの名前。ユーザーがサービスデスクからEメールメッセージを受信すると、この名前が 要求元 フィールドに表示されます。
Eメールアドレス	サーバーの完全修飾Eメールアドレス。ユーザーは通常、このアドレスに返信しません。 ユーザーがアプライアンスの E メールに返信できるようにするには、代替の E メールアドレス フィールドに E メールアドレスを指定します。
チケット番号プレフィックス	このキューのカスタムチケットプレフィックスを指定します。各キューに異なるプレフィックスを使用してサービスデスクのワークフローを整理し、ヘルプデスクに対する HD やハードウェアとソフトウェアの要求に対する REQ などの適切なカテゴリに関連付けることができます。
代替のEメールアドレス	**Support@mydomain.com** ユーザーがEメールの送信先として使用するプライマリEメールアドレス。アプライアンスもこのアドレスを使用して、サービスデスクから E メールを送信します。Eメールサービスに対し、ドメイン名が正しいことを確認します。

フィールド	説明
	注: 有効なEメールアドレスとして、このアドレスは他のEメールアドレス同様、スパムとセキュリティ上の脆弱性に注意する必要があります。

3. **オプション**：SMTP/POP3 サーバーの設定を行います。**キューの E メールの設定** をクリックし、必要に応じて、サービスデスクキュー E メール設定 ページで SMTP/POP3 オプションを指定します。詳細については、「キュー固有の E メールの設定」を参照してください。
4. **保存** をクリックしてキューを作成し、追加設定を行います。
5. ユーザー基本設定を指定します。

フィールド	説明
送信者としてすべてのユーザーを許可	アプライアンス上の任意のユーザーが、現在のサービスデスクキューを通じてチケットを送信できるようにします。
Restrict Submitters by Label（ラベル別に送信者を制限）	ラベルのみで送信者を選択します。「**送信者としてすべてのユーザーを許可**」がオフの場合にのみ指定可能になります。
承認者としてすべてのユーザーを許可	アプライアンスの登録ユーザーに、現在のサービスデスクキューを通じたチケットの承認を許可します。
Restrict Approvers by Label（ラベル別に承認者を制限）	ラベルのみで承認者を選択します。「**承認者としてすべてのユーザーを許可**」がオフの場合にのみ指定可能になります。
所有者のラベル:	すべてのユーザーがチケットを承認できるようにするには、「**承認者としてすべてのユーザーを許可**」を選択します。 チケットを所有および管理できるユーザー（一般にはITスタッフ）を識別します。ライフサイクル全体を通してチケットを管理する責任を持つチケット所有者を指定する必要があります。 これを行うには、**関連ラベルの管理** をクリックします。表示される ラベルを選択 ダイアログボックスで、チケット所有者として選択するユーザーに関連付けられている 1 つまたは複数のラベルを選択します。ダイアログボックスを閉じます。
不明なユーザーからのEメールを許可	不明なユーザーがチケットを作成できるようにします。 キュー設定でこのオプションが有効になっている場合、サービスデスクキューに送信されるすべての E メールで、チケットの 送信者 フィールドを設定することができます。送信者は、ユーザーコンソールのみ の役割を持つユーザーとしてアプライアンスに追加されます。デフォルトでは、この役割はサービスデスクチケットの作成、表示、および修正を行い、**ユーザーコンソール**からアプライアンスを操作する権限を持ちます。必要に応じて、この役割および他の役割に関連付けられている許可のレベルを調

フィールド	説明
	整できます。詳細については、「ユーザーアカウントの役割の設定」を参照してください。 無効になっている場合、送信者の E メールアドレスが既にサービスデスクのユーザーアカウントと関連付けられている場合に限り、上記のプロセスが実行されます。
チケットの削除を許可	チケット所有者および管理者がチケットを削除できるようにします。この設定は、スタッフがチケットを削除できないようにする場合に役立ちます。管理者は定期的にこのチェックボックスをオンにし、古いチケットを整理した後、再度オフにすることで、チケットが削除されるのを防ぐことができます。
親チケットが子チケットを閉じることを許可	親チケットを閉じた時点で、子チケットを自動的に閉じることができます。
最後の子チケットが親チケットを閉じるのを許可する	最後の子チケットを閉じた時点で、親チケットを自動的に閉じることができます。
Allow users with an Administrator role to read and edit tickets in this queue (管理者コンソール only) (管理者役割のユーザーがこのキューでチケットを表示および編集するのを許可 (管理者コンソールのみ))	管理者役割を持つすべてのユーザーに読み取り/書き込み権限を付与します。
所有者のみに表示されるデフォルトのチケットの所有者コメント	チケットにコメントが追加されたときに 所有者のみ チェックボックスを自動的にオンにします。
Enable ticket conflict warning for ticket owners (チケット所有者に対するチケットコンフリクト警告の有効化)	管理者とチケット所有者に対して、送信している変更と他のユーザーが同時に送信している変更との間のコンフリクトの概要を示すダイアログを表示します。管理者およびチケット所有者が Ticket Detail (チケットの詳細) ページで **保存** または **変更の適用** をクリックしたときに、チケットを編集用に開いていた間に他のユーザーがチケットを編集して保存した場合は、ダイアログが表示されます。これにより、管理者およびチケット所有者は、コンフリクトがある場合に、変更を破棄するか他のユーザーが行った変更を上書きするかを選択できます。 **注:** デフォルトでは、この警告は新しいキューでは有効であり、アプライアンスバージョン 6.3 以前で作成されたキューでは無効です。 このダイアログは、他のユーザーがチケットを変更した場合にのみ表示され、管理者とチケット所有者のみに表示されます。他のユーザーにはダイアログは表示されません。 **注:** ダイアログには他のユーザーが行ったすべての変更の概要が示されます。ただし、現在のユーザーの変更は、他のユーザーが行った変更とコンフリクトする場合にのみ概要が示されます。

フィールド	説明
マネージャが従業員のチケットを表示してコメントできるようにする	従業員が提出したチケットを、マネージャアカウントで表示し、コメントを編集できるようにします。詳細については、「チケットコメントの表示」を参照してください。
チケット CC リストでチケットを表示してコメントできるようにする	チケット CC リストのユーザーが、チケットにコメントを追加できるようにします。
チケットでコメントするときにユーザーをチケット CC リストに追加する	チケットにコメントするすべてのユーザーを、そのチケットの CC リストに追加し、今後チケットに変更が行われたときに E メールでそのユーザーに通知できるようにします。
すべてのユーザーが自身のコメントを編集 / 削除できる (添付ファイルを含む)	すべてのユーザーが、添付ファイルを含め、自身のコメントを編集または削除できるようにします。
ユーザーラベル	特定のユーザーがラベルを使用して自身のコメントや添付ファイルを編集または削除できるようにするには、**関連ラベルの管理** をクリックします。表示される ラベルを選択 ダイアログボックスで、選択するユーザーに関連付けられている 1 つまたは複数のラベルを選択します。ダイアログボックスを閉じます。
すべての技術者が、他のユーザーによって入力されたコメントを編集 / 削除できる (添付ファイルを含む)	すべての技術者が、添付ファイルを含め、他のユーザーによって追加されたコメントを編集または削除できるようにします。
技術者ラベル	特定の技術者が、ラベルを使用して、自身のコメントおよびファイル添付を編集または削除できるようにするには、**関連ラベルの管理** をクリックします。表示される ラベルを選択 ダイアログボックスで、選択する技術者に関連付けられている 1 つまたは複数のラベルを選択します。ダイアログボックスを閉じます。
強力な HTML サニタイズを有効にする	HTML を受け入れるすべてのフィールドですべての悪意のあるコードを削除します。
サポート技術情報記事の提案を許可する	チケットタイトルの入力中に KB 記事の提案を表示します。 **注:** このオプションが無効になっていて、パスワード管理者がブラウザにリンクされている場合、ブラウザは関連するサービスデスクチケットフィールドを自動的に入力できなくなります。

フィールド	説明
チケットへの添付ファイルの制限	必要に応じて、添付ファイルの制限をどのように処理するかを指定します。 • 「**なし**」：ユーザーが任意のタイプのファイルを添付ファイルとして追加できるようにします。 • **画像のみを許可**：画像のみを添付ファイルとして追加できるようにします。 • **カスタム**: 添付ファイルとして許可するファイル拡張子を指定します。拡張子のないすべてのファイルを許可することもできます。 • **すべての添付ファイルを禁止**：ユーザーが添付ファイルを追加できないようにします。

6. Archive Preferences（アーカイブの基本設定）セクションで、チケットのアーカイブの設定を選択します。**設定** リンクをクリックして、チケットのアーカイブを有効にします。

   注: チケットのアーカイブがオフになっている場合は、チケットのアーカイブの有効化を参照してください。

オプション	説明
Archive closed tickets older than（次の期間を経過した終了チケットをアーカイブ）	アーカイブの対象となるチケットの期間。例えば、**3 か月** を選択した場合、チケットが閉じられてから 3 か月経過するとチケットはアーカイブされます。キュー内のチケットがアーカイブされないようにするには、**無効** を選択します。必要に応じて、アーカイブされたチケットをキューに復元できます。詳細については、「アーカイブしたチケットの復元」を参照してください。
Delete archived tickets older than（次の期間を経過したアーカイブチケットを削除）	アーカイブから永続的に削除される対象となるチケットの期間。例えば、**6ヶ月** を選択した場合、チケットが開かれてから 6 ヶ月経過すると、アーカイブされたチケットはアーカイブから削除されます。キュー内のチケットがアーカイブから削除されないようにするには、**無効** を選択します。削除されたチケットをキューに復元することはできません。

7. チケットのデフォルト セクションで、新しいチケットのデフォルト値を選択します。例：
   - **カテゴリ**: ソフトウェア
   - **ステータス**: 新規
   - **インパクト**: 1人が作業不可です
   - **優先度**: 中
8. イベント発生時にEメールを送信 セクションで、指定されたイベントの発生時に E メールを受信するユーザーのカテゴリを選択します。各列はサービスデスクユーザー（役割）のタイプを表し、各行はチケットイベントを表します。詳細については、「Eメールトリガの設定」を参照してください。
9. **オプション**：Service Level Agreement Settings（サービスレベル契約設定）を設定します。ここでは、チケットの優先度に基づいてサービスレベル契約（SLA）設定を有効にできます。有効にした場合、チケッ

トの期日で解決時間、業務時間、および休業日が自動的に考慮されます。詳細については、「サービスレベル契約の設定」を参照してください。

10. チケットルール セクションで、キュー内のチケットに適用するルールを有効にします。いずれかの定義済みのルールを使用することも、独自にカスタマイズすることもできます。チケットルールを使用およびカスタマイズする方法の詳細については、チケットルールの使用を参照してください。
11. **保存** をクリックします。

キュー固有の E メールの設定

チケットキューごとに個別の E メール設定をセットアップできます。

デフォルトでは、サービスデスクはチケット関連 E メールの送信に内部 SMTP サーバーを使用するように設定されています。外部 SMTP サーバーを使用するオプションはありますが、アプライアンスネットワーク設定で設定する必要があります。詳細については、「アプライアンスのネットワーク設定の変更」を参照してください。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. キュー固有の サービスデスクキュー E メール設定 ページに移動します。
    a. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    b. **設定** パネルの E メール設定 セクションで、**サービスデスクキューの E メール設定** をクリックします。
    c. 表示された サービスデスクキュー E メール設定 ページでキューを選択します。

    または

    a. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    b. **設定** パネルで **キュー** をクリックします。
    c. キューの E メールアドレスの右側で、**キューの E メールの設定** をクリックします。

    サービスデスクキュー E メール設定 ページが表示されます。
3. ビルトイン E メール設定 セクションで、次のオプションを指定します。

フィールド	説明
Eメールアドレス	サーバーの完全修飾Eメールアドレス。ユーザーは通常、このアドレスに返信しません。 ユーザーがアプライアンスの E メールに返信できるようにするには、代替の E メールアドレス フィールドに E メールアドレスを指定します。
代替のEメールアドレス	**Support@mydomain.com** ユーザーがEメールの送信先として使用するプライマリEメールアドレス。アプライアンスもこのアドレスを使用して、サービスデスクから E メールを送信します。Eメールサービスに対し、ドメイン名が正しいことを確認します。 **注:** 有効なEメールアドレスとして、このアドレスは他のEメールアドレス同様、スパムとセキュリティ上の脆弱性に注意する必要があります。
不明なユーザーからのEメールを許可	不明なユーザーがチケットを作成できるようにします。 キュー設定でこのオプションが有効になっている場合、サービスデスクキューに送信されるすべての E メールで、チケットの 送信者 フィールドを設定す

フィールド	説明
	ることができます。送信者は、ユーザーコンソールのみ の役割を持つユーザーとしてアプライアンスに追加されます。デフォルトでは、この役割はサービスデスクチケットの作成、表示、および修正を行い、**ユーザーコンソール**からアプライアンスを操作する権限を持ちます。必要に応じて、この役割および他の役割に関連付けられている許可のレベルを調整できます。詳細については、「ユーザーアカウントの役割の設定」を参照してください。 無効になっている場合、送信者の E メールアドレスが既にサービスデスクのユーザーアカウントと関連付けられている場合に限り、上記のプロセスが実行されます。

4. 受信 E メールの設定 セクションのオプションを使用して、受信 E メールを受信する方法を選択して設定します。

   - **受信 E メールに SMTP サーバーを使用：受信メールに内部 SMTP サーバーを使用する場合は、このオプションを選択します。必要な資格情報は、下の** 送信 E メール設定 **セクションで指定できます。詳細については、「5」を参照してください。**
   - **受信 E メールに POP3 サーバーを使用：受信メールに POP3 サーバーを使用する場合は、このオプションを選択します。次のオプションを指定します。**

オプション	説明
POP3サーバー	キューに使用するPOP3サーバーの名前を入力します。たとえば、「**pop.example.com**」と入力します。
SSLを使用	POP3 サーバーでセキュアな接続を使用する場合は、このオプションを選択します。
POP3 ユーザー名（E メールアドレス） **POP3 Password（POP3 パスワード）**	POP3サーバーへのアクセス権を持つアカウントのユーザー名とパスワードを入力します。

テスト接続 をクリックして、POP3 設定をテストします。接続テスト POP3 ダイアログボックスが開き、テスト結果を示す複数のログメッセージが表示されます。テストが成功すると、これらのメッセージには例えば、ユーザーアカウントが認証されたかどうか、未開封メッセージの数、および最新の E メールの件名行が示されます。テストに失敗した場合は、設定を確認し、もう一度試してください。

- **受信 E メールに IMAP サーバーを使用：受信メールに IMAP サーバーを使用する場合は、このオプションを選択します。次のオプションを指定します。**

オプション	説明
IMAPサーバ	キューに使用する IMAP サーバーの名前を入力します。たとえば、「**imap.example.com**」と入力します。
SSLを使用	IMAP サーバーでセキュアな接続を使用する場合は、このオプションを選択します。
IMAP サーバーユーザー名（E メールアドレス） **IMAP サーバーパスワード**	IMAP サーバーへのアクセス権を持つアカウントのユーザー名とパスワードを入力します。

テスト接続 をクリックして、IMAP 設定をテストします。接続テスト IMAP ダイアログボックスが開き、テスト結果を示す複数のログメッセージが表示されます。テストが成功すると、これらのメッセージには例えば、ユーザーアカウントが認証されたかどうか、未開封メッセージの数、および最新の E メールの件名行が示されます。テストに失敗した場合は、設定を確認し、もう一度試してください。

- **受信 E メールに Gmail を使用：受信メールに Google Gmail を使用する場合は、このオプションを選択します。資格情報の選択 をクリックします。**
  - 既存の Google OAuth 資格情報を使用するには、リストで選択します。

    注: E メールを取得するための専用の Google OAuth 資格情報を作成する必要があります。たとえば、Chrome デバイスへのアクセスとメールのダウンロードに同じアカウントを使用することはできません。

  - 新しい Google OAuth 資格情報を作成するには、**資格情報の追加** をクリックします。資格情報の追加 ダイアログボックスが表示されます。必要に応じて、必要なオプションを指定します。詳細については、「Google Workspace 資格情報の追加および編集」を参照してください。
- **受信 E メールに Office365 を使用：受信メールに Office 365 を使用する場合は、このオプションを選択します。次のオプションを指定します。**

オプション	説明
資格情報の選択	• 既存の Office 365 OAuth 資格情報を使用するには、リストで選択します。 • 新しい Office 365 OAuth 資格情報を作成するには、**資格情報の追加** をクリックします。資格情報の追加 ダイアログボックスが表示されます。必要に応じて、必要なオプションを指定します。詳細については、「Microsoft Office 365 OAuth 資格情報の追加および編集」を参照してください。
Microsoft 365 API サービス	使用する環境に適した Microsoft 365 API サービスを選択します。 • 米国にある Azure AD アプリの場合は、必要に応じて次のいずれかのオプションを選択します。 ◦ **Microsoft 365 GCC**：引き続き、Azure の世界中のエンドポイント：https://graph.microsoft.com および https://portal.azure.com を使用して登録できます。 ◦ **Microsoft 365 GCC High**：https://portal.azure.us および https://graph.microsoft.us を使用して登録します。 ◦ **Microsoft 365 DoD**：https://portal.azure.us および https://dod-

オプション	説明
	graph.microsoft.us を使用して登録します。 • ドイツにある Azure AD アプリの場合は、**Microsoft 365 Germany** を選択します。 • 中国にある Azure AD アプリの場合は、**Microsoft 365 China** を選択します。

5. このキューに関連付けられた E メールに外部 SMTP サーバを使用する場合、送信 E メール設定 セクションの設定を使用してください。
   a. キュー固有の SMTP 設定の指定 チェックボックスをオンにします。
   b. 次のオプションを指定します。

オプション	説明
SMTPサーバ	外部 SMTP サーバーのホスト名（**smtp.gmail.com** など）または IP アドレスを指定します。外部 SMTP サーバでは、匿名（認証なし）のアウトバウンド E メール転送を許可する必要があります。ネットワークポリシーで、アプライアンスがSMTPサーバに直接問い合わせられることを確認します。また、メールサーバは、アプライアンスからのEメールのリレーを、認証なしで許可するように設定する必要があります。
SMTPポート	外部 SMTP サーバーに使用するポート番号を入力します。標準的な SMTP にはポート 25 を使用します。セキュアな SMTP にはポート 587 を使用します。
SMTP Username（SMTP ユーザー）	外部 SMTP サーバーにアクセスするアカウントのユーザー名を入力します（「**your_account_name**@gmail.com」など）。
SMTP パスワード	指定したサーバーアカウントのパスワードを入力します。

6. 送信 E メールへの添付ファイルの設定 セクションで、チケットの詳細を E メールで送信するときの添付ファイルの処理方法を指定します。

オプション	説明
画像埋め込みを許可する	チケット関連の E メールにグラフィックファイルを含める場合は、このオプションを選択します。このオプションを選択すると、グラフィックは埋め込み画像として表示されます。
E メールあたりの合計画像サイズ制限（MB）	チケット関連の E メールに埋め込むことができる、チケットに関連付けられているすべての画像ファイルの最大サイズを指定します。
ファイル添付を許可する	ファイルリンクを提供せずにチケットに添付されたファイルを送信する場合は、このオプションを選択します。

オプション	説明
E メールあたりの合計ファイルサイズ制限（MB）	E メールで送信できるすべての添付ファイルの最大ファイルサイズを指定します。

7. サービスデスクキュー E メール設定 ページの イベント発生時に E メールを送信 セクションで、指定されたイベントが発生したときに E メールを送信するオプションを選択します。各列はサービスデスクユーザー（役割）のタイプを表し、各行はチケットイベントを表します。

サービスデスクユーザー（役割）	説明
所有者	チケットを解決すべきユーザー。
送信者	チケットの元となる問題を提起したユーザー。
承認者	処理するチケットを承認または拒否できるユーザー。
チケットCC	チケットの CC フィールドに保存されている 1 つ以上の E メールアドレス。
カテゴリCC	チケットの Category Value（カテゴリ値）の CC リスト に保存されている 1 つ以上の E メールアドレス。詳細については、「チケットカテゴリのための CC リストの設定」を参照してください。
キューの所有者	所有者 ラベルで指定されたチケットキューの 1 人または複数の所有者。これは、E メールを使用した新しいチケット イベントと ポータル経由の新規チケット イベントにのみ適用されます。

チケットイベントが発生すると、選択した役割またはユーザーに E メールが送信されます。例えば、所有者 列で **任意の変更** ボックスを選択した場合、チケットが変更されるたびにチケット所有者に E メールが送信されます。コメント および Ticket Closed（チケット終了）トリガの場合、E メールが直ちに送信されます。一方、その他のチケットの変更の場合、E メールのオーバーロードを回避するため、数分ごとに E メールが送信されます。

注: スマートフォンまたはタブレットにKACE GOモバイルアプリケーションがインストールされている場合、システムは、選択したサービスデスクチケットイベントのプッシュ通知を送信します。

オプション	説明
任意の変更	チケットに関する任意の情報が変更されます。
所有者の変更	チケットの 所有者 フィールドが変更されます。
ステータスの変更	チケットの ステータス フィールドが変更されます。
コメント	情報、添付ファイル、またはスクリーンショットがチケットの コメント セクションに追加されます。ユーザーがチケットフォームでコメントを追加し、**送信** をクリックすると、コメントの E メール通知が送信されます。一方、ユーザーがチケットフォームでコメントを追加し、**保存** をクリックすると、任意の変更 通知のみが送信されます。

オプション	説明
承認の変更	チケットの承認ステータスが変更されました。
解決の変更	チケットの解決が変更されました。
エスカレーション	チケットは、チケット優先度で定義されるエスカレーション時間内に停止または閉じられたステータスに更新されていません。
SLA違反	チケットは、その期日までに解決されていません。
Ticket Closed（チケット終了）	チケットの ステータス フィールドが **閉じられた** に変更されます。このイベントは、送信者に満足度調査を提示するために使用します。詳細については、「満足度調査の利用」を参照してください。
E メールを使用した新しいチケット	ユーザーがサービスデスクに E メールメッセージを送信し、チケットが作成されます。
ポータル経由の新規チケット	チケットは**ユーザーコンソール**を通じて作成されます。

8. **保存** をクリックします。

   アプライアンスが、指定した SMTP サーバーに E メールを転送するように設定されました。複数のキューがある場合、それぞれのキューについて前の手順を繰り返します。

サービスデスクのタイトル名とラベル名の変更

必要に応じて、**管理者コンソール**および**ユーザーコンソール**で使用される、サービスデスクのタイトル名とラベル名を変更できます。

1. サービスデスクの 設定 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. 設定 パネルで **設定** をクリックします。
2. 次の設定を指定します。

設定	説明
メインタブ	**管理者コンソール**のコンポーネントレベルタブ、および**ユーザーコンソール**のタブ上に表示されるテキスト。デフォルトは「**サービスデスク**」です。ただし、以前のバージョンのアプライアンスをアップグレードしている場合は、デフォルトで **Help Desk**（ヘルプデスク）と表示される場合があります。
キュー **キュー（複数）**	**管理者コンソール** の サービスデスク設定 ページおよび キュー リストで、**キュー** および **キュー（複数）** の代わりに表示するテキスト。このテキストは、アクションの選択 メニューのオプション

設定	説明
	と、**ユーザーコンソール**の チケット ページの見出しにも使用されます。
チケット **チケット (複数)**	**管理者コンソール**の チケット タブおよび チケット ページで、**チケット** および **チケット (複数)** の代わりに表示するテキスト。このテキストは、**ユーザーコンソール**の チケット ページにも使用されます。
プロセス **プロセス (複数)**	**管理者コンソール**の サービスデスク設定 ページおよび プロセス リストで、**プロセス** および **プロセス (複数)** の代わりに表示するテキスト。

3. **保存** をクリックします。

コンフリクト警告の有効化または無効化

キューに対してコンフリクト警告ダイアログが有効な場合、複数のユーザーがチケットを同時に編集していると、管理者およびチケット所有者に通知ダイアログが表示されます。ダイアログによって、ユーザーは他のユーザーが行った変更を表示し、どちらの変更を保持するかを決定できます。

管理者コンソールで管理者権限を持っています。

管理者は、キューごとに個別にコンフリクト警告ダイアログを有効または無効にすることができます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの詳細 ページを表示するには、次のいずれかを実行します。
    - キューの名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. User Preferences (ユーザー基本設定) セクションで、コンフリクト警告を有効または無効にします。

フィールド	説明
Enable ticket conflict warning for ticket owners (チケット所有者に対するチケットコンフリクト警告の有効化)	管理者とチケット所有者に対して、送信している変更と他のユーザーが同時に送信している変更との間のコンフリクトの概要を示すダイアログを表示します。管理者およびチケット所有者が Ticket Detail (チケットの詳細) ページで **保存** または **変更の適用** をクリックしたときに、チケットを編集用に開いていた間に他のユーザーがチケットを編集して保存した場合は、ダイアログが表示されます。これにより、管理者およびチケット所有者は、コンフリクトがある場合に、変更を破棄するか他のユーザーが行った変更を上書きするかを選択できます。 このダイアログは、他のユーザーがチケットを変更した場合にのみ表示され、管理者とチケット所有者のみに表示されます。他のユーザーにはダイアログは表示されません。

フィールド	説明
	注: ダイアログには他のユーザーが行ったすべての変更の概要が示されます。ただし、現在のユーザーの変更は、他のユーザーが行った変更とコンフリクトする場合にのみ概要が示されます。

3. **保存** をクリックします。

応答テンプレートの表示および編集

応答テンプレートを使用すると、サービスデスクチケットにコメントまたは解決策として共通の応答を保存できます。

各応答テンプレートは、特定のチケットキューに関連付けられ、作成したユーザーに属しています。チケットの詳細 ページで、該当する応答テンプレートを選択できます。

テンプレートテキストは、E メールトークンの使用をサポートします。トークンの値は、それらが参照されているチケットのフィールド値を使用して動的に更新されます。E メールテンプレートで使用できる同じトークンを使用できます。詳細については、「Eメールテンプレートの設定」を参照してください。

応答テンプレートはパブリックにもプライベートにもできます。プライベート応答テンプレートは、作成したユーザーだけが、該当するチケットで更新および参照できます。パブリック応答テンプレートは、他のユーザーによって関連付けられたチケットキューでの選択に使用できますが、応答メッセージの内容を編集できるのは、それを作成したユーザーに限られます。他のユーザーは、パブリック応答テンプレートの内容を表示できますが、編集することはできません。

1. サービスデスクの 応答テンプレート ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルの **キュー** の下で、**応答テンプレート** をクリックします。
    d. 応答テンプレートの詳細 ページを表示するには、次のいずれかを実行します。
    - 応答テンプレートの名前をクリックします。
    - **アクションの選択** > **新規作成** を選択します。

注: キュー 設定ページへのアクセス権のないキュー所有者は、チケットの詳細 ページの 事前定義された応答 オプションのすぐ上に表示される 管理 リンクをクリックすることによって、応答テンプレート ページにアクセスできます。

2. 次の設定を指定します。

フィールド	説明
名前	応答テンプレートの名前。この名前は、該当するサービスデスクチケットへの自動化された応答を設定する時に、事前定義された応答 フィールドでの選択肢として使用できるものとして表示されます。
パブリックにする	この応答テンプレートを、他のユーザーの選択肢として使用できるようにする場合、このチェックボックスをオンにします。他のユーザーは、パブリック応答テンプレートの内容を表示できますが、編集することはできません。

フィールド	説明
テンプレート	応答メッセージの内容。このフィールドは、プレーンテキストとトークンをサポートしています。

3. 応答テンプレートを変更した場合は、**保存** をクリックします。
4. 応答テンプレートのリストに戻るには、**キャンセル** をクリックします。

応答テンプレートは、サービスデスクチケットの照会に対する事前定義された応答として使用できます。詳細については、「チケットへのコメントの追加」を参照してください。

チケット設定の構成

サービスデスクのチケットキューにはそれぞれ、新しいチケット用のデフォルト設定があります。必要に応じてこれらの設定を構成し、カスタムフィールドを追加できます。

一般的なカスタムフィールドには、以下のようなものがあります。

- **問題に関する情報**: 問題の症状、問題の継続時間、問題の原因だと考えられるその他のコンポーネントなど。
- **ソフトウェアに関する情報**: ソフトウェアの製造元、バージョン、目的、およびインストール日。
- **サービスデスクスタッフ専用の情報**: 診断、レポート、または計画のために使用できる情報 (エスカレーションを行う際のベンダーの連絡先、根本原因、過去に修正されたことがあるか、など) 。
- **カスタム定義のチケット特性**: カテゴリ、ステータス、優先度、およびインパクト。

これらのフィールドはいつでも追加または変更できます。フィールドの数は、データベーステーブル内で使用可能な列数によってのみ限定されます。しかしながら、チケットによって使用されているフィールドを削除することはできません。使用中のフィールドを削除するには、チケットが使用するフィールドを別のフィールドに変更してから、目的のフィールドを削除します。

チケット詳細 ページのカスタマイズ

必要に応じて、キューの チケットの詳細 ページをカスタマイズします。キューが複数ある場合は、それぞれのキューの チケットの詳細 ページを個別にカスタマイズできます。

サービスデスクでは、次のチケット設定を変更できます。

設定	使用可能な値
カテゴリ	• ソフトウェア • ハードウェア • ネットワーク • その他（デフォルト）
ステータス	• 新規作成（デフォルト） • オープン • 閉じられた • 要追加情報
インパクト	• 複数人が作業不可です • 複数人が不都合です • 1人が作業不可です（デフォルト） • 1人が不都合です
優先度	• 高 • 中（デフォルト） • 低
状態	• オープン（デフォルト） • 閉じられた • 停止済み

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。
   - キューの名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。
2. 「**すべてのチケット所有者**」ラベルを 所有者のラベル フィールドに追加します。
   a. 所有者のラベル フィールドで **関連ラベルの管理** をクリックします。
   b. ラベルの選択 ダイアログで **すべてのチケット所有者** を 所有者の制限対象 フィールドにドラッグし、**OK** をクリックします。

   このラベルの詳細については、「すべてのチケット所有者」ラベルの追加を参照してください。

c. **保存** をクリックします。

3. チケットのデフォルト セクションで、**これらの値のカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
4. カテゴリ値 セクションで、列見出しにある **追加** ボタンをクリックしてカテゴリを追加します をクリックします。

   新しい値について、編集可能なフィールドが表示されます。
5. 次の設定を指定します。

フィールド	説明
名前	ドロップダウンリストに表示されるテキスト。デフォルトでは、このテキストは「**カテゴリを選択してください**」と表示され、ユーザーにチケットのカテゴリの選択を求めます。
デフォルト所有者	**DefaultTicketOwners** を選択します。
「CC」リスト	**なし** を選択し、チケット上にCCリストが表示されないようにします。「**DefaultTicketOwners**」がデフォルト所有者であるため、チケットが作成されると、すべての潜在的なチケット所有者にEメール通知が送信されます。
ユーザー設定可能	このカテゴリをユーザーが参照できるようにします。オフにした場合は、サービスデスクスタッフユーザーだけがこのカテゴリを参照できるようになります。 この設定を使用すると、ユーザーには簡易的な値のリストが表示されますが、管理者やサービスデスクスタッフには包括的なリストが表示されます。ユーザーのチケットを処理する際、ユーザーは状況に応じてこれらのカテゴリを参照できますが、カテゴリを設定したり変更したりすることはできません。

6. **保存** をクリックします。

   注: 管理者は、チケットのカテゴリを随時追加できます。詳細については、「チケットカテゴリとサブカテゴリの作成」を参照してください。
7. 「カテゴリ値」の残りのカテゴリについて、**編集** ボタンをクリックします。
8. 次の変更を行います。
   a. Default Owner（デフォルト所有者）列で **DefaultTicketOwners** を選択し、このユーザーアカウントをこれらの全カテゴリのデフォルト所有者に指定します。

   このアカウントの詳細については、DefaultTicketOwnersアカウントの作成を参照してください。
   b. 「**CC**」**リスト**の中身を削除します。
   c. **保存** をクリックします。
9. その他のステータス値を作成します。
   a. ステータス値 セクションで、**追加** ボタンをクリックします。

      新しい値について、編集可能なフィールドが表示されます。
   b. 名前 列に「エンドユーザー待ち」と入力した後、状態 列で **停止済み** を選択します。
   c. **保存** をクリックします。
   d. ステータス値 セクションで、**追加** ボタンをクリックします。

e. 名前 列に「サービスデスクスタッフ待ち」と入力した後、状態 列で **停止済み** を選択して、**保存** をクリックします。

f. ステータス値 セクションで、**追加** ボタンをクリックします。

g. 名前 列に「再オープン」と入力した後、状態 列で **オープン** を選択して、**保存** をクリックします。

注: 「**未解決**」状態のチケットのみ、エスカレーションできます。詳細については、「チケットのエスカレーションプロセスの使用」を参照してください。

10. エスカレーション時間が15分の優先度、「**緊急**」を作成します。

a. 優先度値 セクションで、**追加** ボタンをクリックします。

新しい値について、編集可能なフィールドが表示されます。

b. 名前 列に「緊急」と入力し、エスカレーション時間 列で「**15分**」を選択します。

c. **保存** をクリックします。

11. 「**高**」優先度のエスカレーション時間を 1 時間に変更し、高優先度チケットを特定するための色を選択します。

12. ページの一番下で **保存** ボタンをクリックします。

ユーザーコンソールホームページのカスタマイズ

会社のブランド設定、ポリシー、および通信の要件に合わせて、**ユーザーコンソール**ホームページに表示されるロゴ、タイトル、ようこそメッセージ、告知、およびリンクをカスタマイズできます。

ユーザーコンソールのロゴおよびテキストのシステムレベルでの変更

アプライアンス上で組織コンポーネントが有効化されている場合は、**ユーザーコンソール**のタイトル、ようこそテキスト、およびロゴをシステムレベルで変更できます。

システムレベルで選択したロゴは、管理者レベルで個別に組織設定を行わない限り、すべての組織に対して使用されます。詳細については、「ユーザーコンソールのロゴおよびログインテキストの管理者レベルでの変更」を参照してください。

1. システムレベルの 一般設定 ページに移動します。

a. アプライアンスシステム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択します。

b. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。

c. コントロールパネル で **一般設定** をクリックします。

2. ユーザーコンソール セクションで、次のフィールドのテキストをカスタマイズします。

オプション	説明
タイトル	**ユーザーコンソール**のログインページに表示される見出し。
ようこそメッセージ	**ユーザーコンソール**のようこそメッセージまたは説明。このテキストは、**ユーザーコンソール**のログインページのタイトルの後に表示されます。

3. カスタムユーザーコンソールロゴと背景色を使用するには、ログイン画面オプション セクションに次の情報を入力します。

オプション	説明
ユーザーコンソールログインの背景色	色選択機能をクリックして使用し、**ユーザーコンソールログイン**画面の背景に表示する色を指定します。必要に応じて、マウスを使用して色を選択するか、RGB 値を指定できます。色選択機能を閉じると、右側の HTML カラーコード フィールドに、選択した色の HTML コードが表示されます。選択を元に戻すには、**リセット** をクリックして最初からやり直します。 **注:** 色選択機能は、Internet Explorer 11 ではサポートされていません。
ユーザーコンソールロゴ	該当する各セクションで、**ファイルの選択** をクリックし、**ユーザーコンソール**でカスタムロゴとして使用するグラフィックファイルを指定します。 サポートされているグラフィックファイル形式は、.bmp、.gif、.jpg、および .png です

4. **保存してサービスを再起動** をクリックします。

デフォルトのホームページとカスタマイズバージョンを次の図に示します。

デフォルトのロゴのユーザーコンソールホームページ

ユーザーコンソールホームページのカスタムロゴ

レポートのデフォルトロゴ

カスタムレポートのロゴ

ユーザーコンソールのロゴおよびログインテキストの管理者レベルでの変更

会社のブランド設定のニーズに合わせて、**ユーザーコンソール**のタイトル、ようこそテキスト、およびロゴを変更できます。

アプライアンスで組織コンポーネントが有効化されている場合は、カスタムロゴをシステムレベルだけでなく管理者（組織）レベルでも指定できます。ただし、管理者レベルのロゴ設定はシステムレベルのロゴ設定よりも優先されます。そのため、組織ごとに異なるロゴを指定できます。組織のカスタムロゴを選択しない場合は、システムレベルの設定が使用されます。詳細については、「ユーザーコンソールのロゴおよびテキストのシステムレベルでの変更」を参照してください。

1. 管理者レベルの 一般設定 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    b. 左のナビゲーションバーで **設定**、**コントロールパネル** の順にクリックします。
    c. コントロールパネル で **一般設定** をクリックします。
2. ユーザーコンソール セクションで、次のフィールドのテキストをカスタマイズします。

> **注:** アプライアンス上で組織コンポーネントが有効化されている場合、これらの**ユーザーコンソール**設定はシステムレベルで利用可能になります。詳細については、「ユーザーコンソールのロゴおよびテキストのシステムレベルでの変更」を参照してください。

オプション	説明
タイトル	**ユーザーコンソール**のログインページに表示される見出し。
ようこそメッセージ	**ユーザーコンソール**のようこそメッセージまたは説明。このテキストは、**ユーザーコンソール**のログインページのタイトルの後に表示されます。

3. カスタムユーザーコンソールロゴと背景色を使用するには、ログイン画面オプション セクションに次の情報を入力します。

オプション	説明
ユーザーコンソールログインの背景色	色選択機能をクリックして使用し、**ユーザーコンソールログイン**画面の背景に表示する色を指定します。必要に応じて、マウスを使用して色を選択するか、RGB 値を指定できます。色選択機能を閉じると、右側の HTML カラーコード フィールドに、選択した色の HTML コードが表示されます。選択を元に戻すには、**リセット** をクリックして最初からやり直します。 **注:** 色選択機能は、Internet Explorer 11 ではサポートされていません。
ユーザーコンソールロゴ	該当する各セクションで、**ファイルの選択** をクリックし、**ユーザーコンソール**でカスタムロゴとして使用するグラフィックファイルを指定します。 サポートされているグラフィックファイル形式は、.bmp、.gif、.jpg、および .png です

4. **保存してサービスを再起動** をクリックします。

   デフォルトのホームページとカスタマイズバージョンを次の図に示します。

デフォルトのロゴのユーザーコンソールホームページ

ユーザーコンソールホームページのカスタムロゴ

レポートのデフォルトロゴ

カスタムレポートのロゴ

ユーザーコンソールホームページのアクションボタンおよびウィジェットの表示または非表示

ユーザーコンソールのホームページに表示されるアクションボタンおよびウィジェットを表示または非表示にすることができます。アクションボタンによって、ユーザーはサービスデスクチケットの提出や**ユーザーコンソール**を介したソフトウェアのダウンロードを実行できるページに迅速にアクセスできます。ウィジェットでは、カスタマイズしたリンクおよび告知を**ユーザーコンソール**ホームページに追加できます。

アクションボタンは、ユーザーのチケットキュー権限とは関係なく、各サービスデスクについて**ユーザーコンソール**にグローバルに表示されます。ただし、システムで組織コンポーネントが有効化されている場合は、各組織のサービスデスクのアクションボタンおよびウィジェットを個別に管理します。

1. User Console Home Page Settings（ユーザーコンソールホームページの設定）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルの User Console Home Page（ユーザーコンソールのホームページ）セクションで、**ユーザーコンソールのホームページの設定** をクリックします。
2. 各アイテムの表示オプションを選択します。アイテムを表示する場合はチェックボックスをオンにし、アイテムを非表示にする場合はチェックボックスをオフにします。

オプション	説明
Display Quick Actions（クイックアクションの表示） • チケットクイックアクション • Downloads Page Quick Action（ダウンロードページクイックアクション）	**ユーザーコンソール**ダウンロードページに表示されるクイックアクションリンクを表示または非表示にします。これらのリンクのテキストは次のとおりです。 • **チケットクイックアクション**：何かにお困りですか？報告 • **Downloads Page Quick Action**（ダウンロードページクイックアクション）：ソフトウェ

オプション	説明
	アが必要ですか? ダウンロードのページにアクセスしてください **注:** リンクテキストは変更できません。ただし、サービスデスクチケットのラベルを変更した場合は、そのラベルがこのリンクで使用されます。例えば、**チケット**ではなくラベル**インシデント**を使用するようにサービスデスクを変更した場合、クイックアクションリンクは Incident Quick Action（インシデントクイックアクション）になります。詳細については、「サービスデスクのタイトル名とラベル名の変更」を参照してください。
Main Panel Widgets（メインパネルウィジェット） • チケットウィジェット • サポート技術情報のウィジェット	次のウィジェットを表示または非表示にします。 • **チケット**：ユーザーが提出したチケットへのリンク、およびユーザーが チケット（複数）リストに移動できる View My Tickets（マイチケットの表示）リンク。 • **サポート技術情報**：ユーザーが利用可能なサポート技術情報記事へのリンク。
Right Panel Widgets（右パネルウィジェット） • Announcements Widget（通知ウィジェット） • Helpful Links Widget（役立つリンク集ウィジェット）	次のウィジェットを表示または非表示にします。 • **通知**：ユーザーに表示するメッセージ。 • **役立つリンク集**：会社のイントラネット、wiki、クラウドアプリケーション、またはその他のウェブリソースへの HTML リンク。

3. **保存** をクリックします。

   クイックアクションおよびウィジェットは、**ユーザーコンソール**ホームページですぐに表示または非表示になります。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、リンクはページが更新されると表示されます。

   注: 告知、リンク、またはサポート技術情報記事が追加されるまで、ウィジェットは空です。

告知、リンク、およびサポート技術情報記事を追加します。詳細については、以下を参照してください。

- ユーザーコンソールの告知の追加、編集、非表示、または削除
- ユーザーコンソールホームページでのカスタムリンクの追加、編集、または削除
- サポート技術情報記事の追加、編集、または複製

ユーザーコンソールホームページのサポート技術情報記事へのリンクの表示または非表示

ユーザーコンソールのホームページに表示されるサポート技術情報記事へのリンクを表示または非表示にすることができます。また、ラベルを使用して、さまざまなユーザーグループに対してサポート技術情報記事を表示または非表示にすることができます。

サポート技術情報記事へのリンクを管理するには、サポート技術情報記事を少なくとも 1 つ作成する必要があります。詳細については、「サポート技術情報記事の追加、編集、または複製」を参照してください。

ラベルを使用してサポート技術情報記事へのリンクを表示または非表示にするには、ユーザーラベルを少なくとも 1 つ作成する必要があります。詳細については、「手動ラベルの追加または編集」を参照してください。

1. User Console Home Page Settings（ユーザーコンソールホームページの設定）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルの User Console Home Page（ユーザーコンソールのホームページ）セクションで、**ユーザーコンソールのホームページの設定** をクリックします。
2. Main Panel Widgets（メインパネルウィジェット）セクションで、**サポート技術情報のウィジェット** の横にあるチェックボックスをオンにします。
3. **保存** をクリックします。

    設定が保存され、Service Desk Configuration（サービスデスク設定）パネルが表示されます。
4. サポート技術情報記事へのアクセスを制御するには、Article Detail（記事の詳細）ページに移動して、ユーザーラベルを記事に適用します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**サポート技術情報** をクリックします。
    c. 記事の詳細 ページを表示するには、次のいずれかを実行します。
    - 記事の名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。

    d. Assign to Labels（ラベルへの割り当て）セクションで、記事に関連付けるラベルを選択して、**保存** をクリックします。

    サポート技術情報記事へのアクセスは、該当するラベルが適用されたユーザーに制限されます。
5. ユーザーが記事を表示できるようにするには、ユーザー リストに移動して、ラベルをユーザーアカウントに適用します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
    c. ユーザー リストで、記事を表示できるようにするユーザーの横のチェックボックスをオンにします。
    d. **アクションの選択 > ラベルの適用** を選択します。
    e. サポート技術情報記事に関連付けられたラベルを Apply these labels（これらのラベルを適用）ボックスにドラッグし、**ラベルの適用** をクリックします。

    ラベルが適用されたユーザーは、サポート技術情報記事にアクセスできます。

ユーザーコンソールの告知の追加、編集、非表示、または削除

ユーザーコンソールホームページに表示される告知を追加でき、必要に応じて既存の告知を非表示にしたり、編集または削除したりできます。

告知を表示するには、通知 ウィジェットが表示されるようにサービスデスクを設定する必要があります。詳細については、「ユーザーコンソールホームページのカスタマイズ」を参照してください。

告知は、ユーザーのチケットキュー権限とは関係なく、各サービスデスクについて**ユーザーコンソール**にグローバルに表示されます。ただし、システムで組織コンポーネントが有効化されている場合は、各組織のサービスデスクの告知を個別に管理します。

注: 各告知の最初の 140 文字が**ユーザーコンソール**ホームページに表示されます。告知が 140 文字を超える場合は、**詳細を表示** リンクによってユーザーは告知全体を読むことができます。

1. User Console Announcements（ユーザーコンソールの告知）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）に口グインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、口グイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**通知** をクリックします。
2. 告知を追加するには、次の手順を実行します。
   a. **通知の追加** をクリックします。
   b. 次の情報を入力します。

オプション	説明
Message Title（メッセージタイトル）	（必須）告知に対して使用するタイトル。 **注:** Message Title（メッセージタイトル）フィールドでリンクを使用することはできません。
Message Body（メッセージ本文）	（オプション）表示する追加情報（リンクを含む）。この情報はタイトルの下に表示されます。 告知メッセージのリンクを作成する際は、次のいずれかの形式を使用します。 • http://example.com • https://example.com • http://www.example.com • www.example.com
非表示	（オプション）**ユーザーコンソール**ホームページに告知を表示するかどうか。このアクションは、システムステータスや計画されているメンテナンスに関する告知など、定期的に表示または非表示にするメッセージがある場合に役立ちます。告知を非表示にするには、チェックボックスをオンにします。告知を表示するには、チェックボックスをオフにします。
Assigned to Labels（割り当て先ラベル）	（オプション）告知が適用されるユーザーラベル。ラベルを選択した場合、告知はラベルがユーザーアカウントに適用されている場合にのみユーザーに表示されます。このアクションは、地理的に異なる場所にいるユーザーなどのユーザーグループに告知を表示する必要があり、それらのユーザー用のラベルを作成して適用している場合に役立ちます。

   c. **保存** をクリックします。

サービスデスクに対して通知ウィジェットが有効になっている場合、選択した設定に従って、告知は**ユーザーコンソール**ホームページに表示されます。

3. 告知を編集するには、告知タイトルの下の **編集** をクリックしてから、**保存** をクリックします。

   変更は**ユーザーコンソール**ホームページにすぐに表示されます。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、告知はページが更新されると削除されます。
4. 告知を非表示にするには、次の手順を実行します。
   a. 告知タイトルの下の **編集** をクリックします。
   b. 非表示 の隣のチェックボックスをオンにします。
   c. **保存** をクリックします。

   告知は**ユーザーコンソール**ホームページですぐに非表示になります。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、告知はページが更新されると非表示になります。
5. 告知の優先度を変更するには、告知の左側にあるドラッグアイコンを使用します。詳細については、「ユーザーコンソールの告知の優先付け、または告知の緊急としてのマーク付け」を参照してください。

   告知は**ユーザーコンソール**ホームページですぐに非表示になります。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、告知はページが更新されると非表示になります。
6. 告知を削除するには、告知タイトルの下の **削除** をクリックしてから、確認ウィンドウで **はい** をクリックします。

   告知は**ユーザーコンソール**ホームページからすぐに削除されます。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、告知はページが更新されると削除されます。

ユーザーコンソールの告知の優先付け、または告知の緊急としてのマーク付け

ユーザーコンソールホームページに告知が表示される順序を設定できます。また、緊急の告知をハイライトしたバナーに表示して、視認性を高めることができます。

告知を優先付けするには、通知 ウィジェットが表示されるようにサービスデスクを設定する必要があり、告知を追加する必要があります。詳細については、以下を参照してください。

- ユーザーコンソールホームページのアクションボタンおよびウィジェットの表示または非表示
- ユーザーコンソールの告知の追加、編集、非表示、または削除

1. User Console Announcements（ユーザーコンソールの告知）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**通知** をクリックします。
2. 告知を優先付けするには、告知の左側にあるドラッグアイコン（☰）を次のように使用します。
   - 告知の優先度を変更するには、その告知をリスト内で上下にドラッグします。告知は、ユーザーコンソールの通知 ページに表示されている順序で**ユーザーコンソール**ホームページに表示されます。
   - 告知を緊急として設定するには、その告知を Urgent Announcement（緊急の告知）ボックスにドラッグします。緊急の告知は、**ユーザーコンソール**ホームページの上部のバナーに表示されます。

     注: Urgent Announcement（緊急の告知）バナーに表示できる告知は一度に 1 つのみです。
   - 緊急の告知を変更するには、別の告知を Urgent Announcement（緊急の告知）ボックスにドラッグします。
   - 緊急の告知を通常の告知に変更するには、その告知を Urgent Announcement（緊急の告知）ボックスからドラッグします。

告知は**ユーザーコンソール**ホームページですぐに適切に優先付けされます。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、告知の優先度はページが更新されると更新されます。

ユーザーコンソールホームページでのカスタムリンクの追加、編集、または削除

ユーザーコンソールホームページに表示されるカスタムリンクを追加でき、必要に応じて既存のカスタムリンクを編集または削除できます。

カスタムリンクを表示するには、役立つリンク集 ウィジェットが表示されるようにサービスデスクを設定する必要があります。詳細については、「ユーザーコンソールホームページのカスタマイズ」を参照してください。

カスタムリンクは、ユーザーのチケットキュー権限とは関係なく、各サービスデスクについて**ユーザーコンソール**にグローバルに表示されます。ただし、システムで組織コンポーネントが有効化されている場合は、各組織のサービスデスクのカスタムリンクを個別に管理します。

1. User Console Home Page Links（ユーザーコンソールホームページのリンク）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルの User Console Home Page（ユーザーコンソールのホームページ）セクションで、**役立つリンク集の定義** をクリックします。
2. リンクを追加するには、次の手順を実行します。
   a. ＋ をクリックします。
   b. 次の情報を入力します。

オプション	説明
タイトル	リンクテキストとして表示するテキスト。URL 自体またはテキスト文字列を使用できます。
URL	リンクの URL。次のようなリンクフォーマットを使用できます。 • http://example.com • https://example.com • http://www.example.com **注:** 同じ URL を複数のリンクで使用することはできません。

   c. URL フィールドの右にある **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

   リンクは**ユーザーコンソール**ホームページにすぐに表示されます。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、リンクはページが更新されると表示されます。
3. リンクを編集するには、次の手順を実行します。
   a. ✎ をクリックします。
   b. 必要に応じて Title（タイトル）または URL を変更します。
   c. URL フィールドの右にある **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

変更は**ユーザーコンソール**ホームページにすぐに表示されます。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、リンクはページが更新されると表示されます。

4. ユーザーコンソールホームページでリンクが表示される順序を変更するには、次の手順を実行します。
   a. リスト内で ☰ を使用してリンクを上下にドラッグします。
   b. ページの一番下で **保存** をクリックします。

   変更は**ユーザーコンソール**ホームページにすぐに表示されます。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、リンクの順序はページが更新されると変更されます。
5. リンクを削除するには、次の手順を実行します。
   a. 🗑 をクリックします。
   b. ダイアログウィンドウで、**はい** をクリックします。
   c. URL フィールドの右にある **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

      リンクは**ユーザーコンソール**ホームページからすぐに削除されます。ユーザーがログインしていて**ユーザーコンソール**ホームページを表示している場合は、リンクはページが更新されると削除されます。

ユーザーコンソールホームページへのチケットリンクの追加

ユーザーのチケットへのリンクを**ユーザーコンソール**ホームページに自動的に追加するようにサービスデスクを設定できます。このリンクによって、ユーザーはシングルクリックでチケットの詳細にアクセスできます。

チケットリンクは、ユーザーがチケットを少なくとも 1 つ作成している場合にのみ表示されます。

1. User Console Home Page Links（ユーザーコンソールホームページのリンク）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルの User Console Home Page（ユーザーコンソールのホームページ）セクションで、**ユーザーコンソールのホームページの設定** をクリックします。
2. Main Panel Widgets（メインパネルウィジェット）セクションで、**チケットウィジェット** の横にあるチェックボックスをオンにします。
3. **保存** をクリックします。

   設定が保存され、Service Desk Configuration（サービスデスク設定）パネルが表示されます。**ユーザーコンソール**ホームページに、ユーザーが提出したチケットと、**マイチケット** リンクが表示されます。このリンクによって、ユーザーは チケット（複数）ページに直接移動します。

   注: ユーザーがチケットを作成していない場合は、チケット（複数）ウィジェットが表示され、表示できるチケットがないことが示されます。

ユーザーコンソールホームページのレポート問題のクイックアクションリンクの追加

ユーザーコンソールホームページに 新規チケット ページへのクイックアクションリンクを追加できます。これにより、ユーザーはシングルクリックで新規チケットフォームにアクセスできます。

1. User Console Home Page Settings（ユーザーコンソールホームページの設定）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
c. **設定** パネルの User Console Home Page（ユーザーコンソールのホームページ）セクションで、**ユーザーコンソールのホームページの設定** をクリックします。

2. Display Quick Actions（クイックアクションの表示）セクションで、**チケットクイックアクション** の横にあるチェックボックスをオンにします。
3. **保存** をクリックします。

   設定が保存され、Service Desk Configuration（サービスデスク設定）パネルが表示されます。Have a problem? 報告 ボタンが**ユーザーコンソール**ホームページに表示されます。ユーザーがこのボタンをクリックすると、新規チケット ページが表示されます。

セッションタイムアウト期間について

デフォルトでは、非アクティブな状態で 1 時間が経過すると、アプライアンスは、**管理者コンソール**または**ユーザーコンソール**から自動的にユーザーをログアウトさせます。これを、**セッションタイムアウト**と呼びます。

セッションは、現在のページの再読み込み、変更の保存、新しいページへの移動など、サーバーとの通信が発生するたびに再開されます。まったく通信を行わないまま所定のセッションタイムアウト期間が経過すると、保存されていない変更はすべて失われ、ログインページが表示されます。タイムアウトセッションカウンタは、各コンソールの右上に表示されます。

セッションタイムアウトの変更手順については、以下を参照してください。

- 組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定
- 組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定

満足度調査の利用

満足度調査により、サービスデスクチケットの送信者が、チケットへの対処に関するフィードバックを提供できるようになります。

満足度調査が有効な場合、チケットが閉じられるとすぐに、調査について説明する E メールメッセージが送信者に送信されます。この E メールメッセージでは、**Ticket Closed**（チケットが閉じられた）E メールテンプレートが使用されます。

デフォルトでは、この調査は終了チケットが初めてアクセスされてから調査が完了するまで、送信者に表示されます。調査が完了すると、この調査は表示されなくなります。調査のスコアとコメントはチケットに保存され、サービスデスクスタッフはこれを編集できません。

さまざまなレポートを実行し、サービスデスクレポートを使用して調査データを表示したり、分析したりできます。また、調査について説明する Ticket Closed（チケットが閉じられた）E メールテンプレートを変更したり、調査ラベルを変更したり、調査が表示されないように設定したりできます。詳細については、以下を参照してください。

- サービスデスクレポートの実行
- Eメールテンプレートの設定
- 「満足度調査」ラベルの変更
- チケットからの 満足度調査 フィールドの削除

満足度調査のデフォルト動作の変更

満足度調査は、調査ボックスでデフォルトプロンプトを変更することによって変更できます。または、満足度調査を削除して、チケット送信者に表示されないようにすることができます。

「満足度調査」ラベルの変更

「満足度調査」概要ラベルをニーズに合わせて変更できます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの名前をクリックします。
2. ページ上部の フィールドとレイアウトのカスタマイズ をクリックして、キューのカスタマイズ ページを表示します。
3. チケットのレイアウトフィールド セクションで、SAT_SURVEY 行の **編集** ボタンをクリックします をクリックします。
4. ラベル セクションで、調査ボックスの新しいラベルを入力します。
5. このアイテムの右側の **保存** ボタンをクリックします。
6. ページの一番下で **保存** ボタンをクリックします。

チケットからの 満足度調査 フィールドの削除

満足度調査がチケット送信者に表示されないように設定できます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの名前をクリックします。
2. ページ上部の フィールドとレイアウトのカスタマイズ をクリックして、キューのカスタマイズ ページを表示します。
3. チケットのレイアウトフィールド セクションで、SAT_SURVEY 行の **編集** ボタンをクリックします。
4. 権限 セクションで、ドロップダウンリストから **非表示** を選択します。
5. このアイテムの右側の **保存** ボタンをクリックします。
6. ページの一番下で **保存** ボタンをクリックします。

    満足度調査が無効化され、チケットが閉じられたときにチケット送信者に表示されなくなります。

サービスデスクの添付ファイルのセキュリティの有効化または無効化

管理者コンソールまたは**ユーザーコンソール**の外部からファイルにアクセスされないように、サービスデスクの添付ファイルのセキュリティを有効または無効にすることができます。

デフォルトでは、サービスデスクの添付ファイルのセキュリティは有効になっています。**管理者コンソール**または**ユーザーコンソール**の外部のチケットリンクからユーザーがチケットの添付ファイルにアクセスできるようにする場合は、この機能を無効にします。また、サービスデスクの添付ファイルのセキュリティ設定は、アプライ

アンスレベルの設定です。システム上で組織コンポーネントが有効化されている場合、選択した設定がすべての組織に適用されます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **セキュリティ設定** をクリックして、セキュリティ設定 ページを表示します。
3. Secure Attachments in Service Desk（ サービスデスクの添付ファイルの保護 ）セクションで、サービスデスクチケットに添付されたファイルについてセキュリティを追加するかどうかを選択します。
   - **チケットに添付されたファイルについてセキュリティを有効にする場合は、チェックボックスをオンにします。このオプションを選択した場合、ユーザーはアプライアンス管理者コンソールまたはユーザーコンソール内からのみ、チケットに添付されたファイルにアクセスできます。**
   - **ユーザーがユーザーコンソールまたは管理者コンソールの外部からチケットリンクをクリックしてファイルにアクセスできるようにする場合は、チェックボックスをオフにします。**
4. **保存してサービスを再起動** をクリックして変更を保存し、アプライアンスを再起動します。

サービスデスクダッシュボードの使用

サービスデスクダッシュボードには、選択した組織（ 該当する場合 ）、またはアプライアンスのサービスデスクチケットの概要が表示されます。

アプライアンスで組織コンポーネントが有効化されており、管理者コンソール（ http://**appliance_hostname**/admin ）にログインしている場合は、サービスデスクダッシュボード には、選択した組織の情報が表示されます。システム管理コンソール（ http://**appliance_hostname**/system ）にログインしている場合は、このダッシュボードにすべての組織を含めたアプライアンス情報が表示されます。

ユーザーアカウントに関連付けられた 1 つまたは複数の役割によってこのダッシュボードへのアクセス権が与えられている場合は、サービスデスクダッシュボードにアクセスできます。非表示にする場合は、必要に応じて、ユーザーの役割を編集します。詳細については、「ユーザーの役割の追加または編集」を参照してください。

ヒント: アプライアンスは、概要ウィジェットを定期的に更新します。任意の時間にほとんどのウィジェットを更新するには、ページの右上にある 更新 ボタンをクリックします：。ほとんどのウィジェットを個々に更新するには、ウィジェットの上にマウスを置き、ウィジェットの上の 更新 ボタンをクリックします。一部のウィジェットでは、追加の手順が必要になる場合があります。

サービスデスクダッシュボードウィジェットについて

サービスデスクダッシュボードウィジェットでは、選択に応じて、組織またはアプライアンスのサービスデスクチケットの概要が示されています。

このセクションでは、サービスデスクダッシュボード で使用可能なウィジェットについて説明します。アプライアンス上で組織コンポーネントが有効化されている場合は、ウィジェットに選択した組織の情報が管理者レベルで表示され、アプライアンスの情報がシステムレベルで表示されます。

このダッシュボードでは、デバイスの使用率の高レベルな概要を示します。このダッシュボードを使用すると、デバイスの状態をすばやく確認し、チケット管理を改善するためのインジケータを見つけられます。例えば、所有者ごとにアクティブなチケットまたは期限超過チケットの数を確認できます。

一部のウィジェットのタイトル、グラフの種類、アイテムのグループ化を更新できます。グループ化オプションは、これらのウィジェットで多少異なります。

ウィジェット	説明
ショートカット	このウィジェットには、一般的なサービスデスクアクションへのリンクが含まれています。これらを使用して、新しい KB（サポート技術情報）記事の作成、レポートのスケジュール設定など、特定のタスクを迅速に開始します。
ビュー	このウィジェットには、作成したすべてのカスタムビューを含む、一般的なサービスデスクのページとウィザードへのリンクが含まれています。これらを使用して、自分の最近のチケット、未割り当てのすべてのチケット、本日期限のチケット など、特定のページにすばやく移動します。また、該当する場合は、カスタムビューへのリンクも表示されます。カスタムビューのリストはアルファベット順に並べられています。カスタムビューを特定の順序で表示する場合は、必要に応じて名前の前に数字を付けることができます。
レポート	このウィジェットには、一般的なサービスデスクレポートへのリンクが含まれています。これらを使用して、過去7日間の未解決チケット（所有者別）、停止済み/未解決のチケット（所有者別） など、特定のレポートをすばやく生成します。
本日開かれたチケット	このウィジェットには、本日開かれたサービスデスクチケットの数が含まれています。
所有者別のアクティブなチケット カテゴリ別のアクティブなチケット 優先度別のアクティブなチケット アクティブなチケット クローズチケット 期限超過チケット 所有者別の期限超過チケット 本日の期限超過チケット 本日期限のチケット 再度開かれたチケット	これらのウィジェットには、アクティブ、クローズ、期限超過、本日期限超過、期限、本日期限、または再度開かれたサービスデスクチケットが、次のカテゴリのいずれかにグループ化されます。 • カテゴリ • 優先度 • 所有者 • キュー • 範囲 結果のデータは、棒グラフ または ドーナツグラフで表示できます。 ウィジェットのタイトルを変更したり、チケットをグループ化する方法を選択したり、グラフのタイプを選択したりするには、ウィジェットで 🖉 をクリックします。表示されたダイアログボックスで、編集を行い、**保存** をクリックします。

ウィジェット	説明
チケットの平均解決時間	このウィジェットには、過去 30 日間でチケット解決に要した平均日数が表示され、次のカテゴリにグループ化されています。 • カテゴリ • 優先度 • 所有者 • キュー • 月 結果のデータは、棒グラフ または ドーナツグラフで表示できます。 ウィジェットのタイトルを変更したり、チケットをグループ化する方法を選択したり、グラフのタイプを選択したりするには、ウィジェットで をクリックします。表示されたダイアログボックスで、編集を行い、**保存** をクリックします。
期限超過したチケット	このウィジェットには、現在期限が超過しているサービスデスクチケットの数が表示されます。

サービスデスクダッシュボードのカスタマイズ

サービスデスクダッシュボードをカスタマイズして、必要に応じて、ウィジェットを表示または非表示にできます。

これらのウィジェットはすべて、インストールされている場合、ホームダッシュボードでも使用できます。

1. サービスデスクダッシュボードに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**ダッシュボード** をクリックします。
2. ウィジェットの上にマウスを置き、次のボタンのいずれかを使用します。
    - : ウィジェットの情報を更新します。
    - : ウィジェットに関する情報を表示します。
    - : ウィジェットを非表示にします。
    - : ウィジェットのサイズを変更します。
    - : ウィジェットをページ上の別の場所にドラッグできます。
3. 一部のウィジェットのタイトル、グラフの種類、アイテムのグループ化を更新できます。これを行うには、ウィジェットの をクリックします。表示されたダイアログボックスで、編集を行い、**保存** をクリックします。
4. ページの右上隅にある **カスタマイズ** ボタンをクリックすると、使用可能なウィジェットが表示されます。
5. 現在非表示のウィジェットを表示するには、**インストール** をクリックします。

サービスデスクのチケット、プロセス、およびレポートの管理

管理者コンソールを使用してサービスデスクのチケット、プロセス、およびレポートを管理します。チケットは、**ユーザーコンソール**および E メールを使用して管理することもできます。

チケットを管理するには、サービスデスクを設定する必要があります。詳細については、「サービスデスクの設定」を参照してください。

サービスデスクチケットのライフサイクルの概要

サービスデスクチケットは、ライフサイクルの間にいくつかのステージを経て進行します。

次のステージがあります。

1. チケットは、ユーザーコンソール、管理者コンソール、またはEメールによって送信されます。管理者コンソールおよびユーザーコンソールからのチケットの作成およびEメールによるチケットの作成と管理を参照してください。
2. チケットルールに従って、チケットが所有者に割り当てられます。チケット設定の構成およびチケットルールの使用を参照してください。
3. チケット所有者はチケットを確認し、必要に応じて影響を調整し、優先度を割り当てます。
4. チケットが存在するキューでサービスレベル契約が有効になっている場合は、優先度に基づいてチケットの期日が計算されます。
5. 問題が簡単なものであれば、所有者が問題を素早く解決して、チケットを閉じ、Eメール通知が送信されます。詳細については、「Eメール設定の設定」を参照してください。
6. 複雑なチケットの場合、チケットは一定期間、未解決のままになり、チケットの所有者が複数になる場合があります。
7. 所有者がエスカレーション時間内にチケットを解決できなければ、チケットはエスカレーションされます。詳細については、「チケットのエスカレーションプロセスの使用」を参照してください。
8. チケットがクローズされたら、ユーザーは満足度調査を記入し、チケットの処理方法に関するフィードバックを提供します。詳細については、「満足度調査の利用」を参照してください。
9. チケットがアーカイブされます。詳細については、「チケットのアーカイブ、復元、削除」を参照してください。

管理者コンソールおよびユーザーコンソールからのチケットの作成

管理者コンソールまたは**ユーザーコンソール**からサービスデスクチケットを作成できます。

チケットはEメールを使用して作成することもできます。詳細については、「Eメールによるチケットの作成と管理」を参照してください。

ユーザーコンソールからのチケットの作成

ユーザーコンソールを使用して、サービスデスクチケットを作成できます。

ユーザーコンソールからチケットを作成すると、ユーザー情報が 新規チケット ページの 送信者 フィールドに自動的に追加されます。

1. ユーザーコンソールの 新規チケット ページに移動します。
   a. ユーザーコンソール（http://**appliance_hostname**/user）に移動します。ここで、**appliance_hostname** は、アプライアンスのホスト名です。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
   c. 新規チケット ページを表示するには、次のいずれかを実行します。
   - **新規作成 > キューからの新規チケット > キュー名** の順に選択します。

     多数のキューがある場合は、検索ボックスを使用して特定のキューをすばやく検索します。
   - **新規作成 > キューからの新規チケット > キュー名 > チケットテンプレート名** の順に選択します。
   - **新規作成 > プロセスからの新規チケット > プロセス名** の順に選択します。
2. プロセスから新しいチケットを作成した場合で、プロセステンプレートがプロセスの説明ページを表示するように設定されているときは、表示される 説明 ページの情報を確認し、**続行** をクリックします。

   このページでは通常、チケットを作成する手順を続行する前に、完了する必要がある重要ないくつかの前提条件が表示されます。例えば、プロセステンプレートでシステムに新しい従業員を追加する方法を定義した場合に、従業員の取得プロセスが完了したかどうか、および従業員IDが作成されたかどうかをユーザーに確認するように指示できます。プロセステンプレートを作成および設定する方法の詳細については、プロセステンプレートの追加、編集、および有効化を参照してください。
3. **キューベースのチケットとプロセスチケットのみ**。次の情報を入力します。

オプション	説明
タイトル	（必須）問題についての簡単な説明。関連付けられているサービスデスクキューにこのフィールドが表示されている場合は、入力を中止してから数秒後に、このフィールドに入力した情報に関連付けられた技術情報記事のリストが表示されます。提案された記事は、サービスデスクチケットを作成する前に、発生している問題の詳細を確認し、問題を解決するために役立ちます。
概要	問題についての詳細な説明。 このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションがすべて表示されます。 例： • 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。 • イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファ

オプション	説明
	イルパスを指定するか、指定された領域にイメージをドロップします。 ◦ スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。 ◦ この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。 ◦ テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイルは、チケットページの 添付ファイル セクションで管理できます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。 • 外部リンクを追加するには、 をクリックします。 • 外部でホストされるビデオを埋め込むには、 をクリックします。
送信者	チケットを送信するユーザーのログイン名。送信者を変更するには、ドロップダウンリストで別のログイン名を選択します。
インパクト	不都合または作業不可の人数。
カテゴリ	問題の分類。
添付ファイル	チケットに追加するファイル。5つのファイルに貼り付けることができます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。
スクリーンショット	チケットに追加するスクリーンショット。チケットには最大5つのスクリーンショットを貼り付けることができます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。

4. **テンプレートベースのチケットのみ**。このチケットに関する情報を入力します。チケットフィールドは、関連付けられたチケットテンプレート内で定義されます。

   チケットテンプレートの詳細については、「チケットテンプレートの設定」を参照してください。

5. 次のいずれかを実行します。
   - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
   - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
   - **キャンセル** をクリックして、チケットの変更を破棄します。

他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

管理者コンソールのチケットページからのチケット作成

必要に応じて、**管理者コンソール**の チケット ページからサービスデスクチケットを作成できます。

管理者コンソールの チケット ページからチケットを作成すると、ユーザー情報が 新規チケット ページの 送信者 フィールドに自動的に追加されます。

1. サービスデスクの 新規チケット ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
   c. 新規チケット ページを表示するには、次のいずれかを実行します。
   - **アクションの選択 > 新規作成** を選択します。
   - **新規作成 > キューからの新規チケット > キュー名** の順に選択します。

     多数のキューがある場合は、検索ボックスを使用して特定のキューをすばやく検索します。
   - **新規作成 > キューからの新規チケット > キュー名 > チケットテンプレート名** の順に選択します。
   - **新規作成 > プロセスからの新規チケット > プロセス名** の順に選択します。
2. プロセスから新しいチケットを作成した場合で、プロセステンプレートがプロセスの説明ページを表示するように設定されているときは、表示される 説明 ページの情報を確認し、**続行** をクリックします。

   このページでは通常、チケットを作成する手順を続行する前に、完了する必要がある重要ないくつかの前提条件が表示されます。例えば、プロセステンプレートでシステムに新しい従業員を追加する方法を定義した場合に、従業員の取得プロセスが完了したかどうか、および従業員IDが作成されたかどうかをユーザーに確認するように指示できます。プロセステンプレートを作成および設定する方法の詳細については、プロセステンプレートの追加、編集、および有効化を参照してください。
3. **キューベースのチケットとプロセスチケットのみ**。次の情報を入力します。

オプション	説明
タイトル	（必須）問題についての簡単な説明。
概要	問題についての詳細な説明。 このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションがすべて表示されます。

オプション	説明
	例： • 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。 • イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファイルパスを指定するか、指定された領域にイメージをドロップします。 ◦ スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。 ◦ この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。 ◦ テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイルは、チケットページの 添付ファイル セクションで管理できます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。 • 外部リンクを追加するには、 をクリックします。 • 外部でホストされるビデオを埋め込むには、 をクリックします。
送信者	チケットを送信するユーザーのログイン名。ドロップダウンリストから別のログイン名を選択して送信者を変更できます。送信者の連絡先情報を表示するには、 をクリックします。 プロセステンプレートから子チケットを作成または編集する場合には、このフィールドを関連付けられた親チケットの 親の所有者 または 親の送信者 に設定するオプションもあります。
資産	この資産の情報がチケットに含まれます。ドロップダウンリストから資産を選択します。資産の詳細を表示するには、 をクリックします。
送信者に割り当てられている資産をフィルタリング	送信者に割り当てられている資産に基づいて資産リストをフィルタリングします。このチェックボックスは、デフォルトで選択されています。
デバイス	このデバイスの情報がチケットに含まれます。チケットの送信者に割り当てられた場合、デバイスはここにリスト表示され、デフォルトで選択された送信者のプライマリデバイスも一緒に表示されます。

オプション	説明
	必要に応じて、ドロップダウンリストでデバイスを選択します。デバイスの詳細を表示するには、  をクリックします。
送信者に割り当てられているデバイスをフィルタリング	送信者に割り当てられているデバイスに基づいてデバイスリストをフィルタリングします。デバイスがチケットの送信者に割り当てられた場合、このオプションはデフォルトで選択された状態でこのページに表示されます。ただし、チケットの詳細 ページでこのチケットをオープンにすると、このオプションは選択された状態になりません。また、チケットを最初に作成したときに選択したデバイスが、デバイス フィールドに表示されます。これはデフォルトの動作です。このチェックボックスをオフにしておくと、チケットに関連付けられた問題と関係のないデバイスを誤って選択してしまう事態を防止できます。
インパクト	不都合または作業不可の人数。
カテゴリ	問題の分類。
ステータス	チケットの現在の状態。チケットをプロセステンプレートから作成または編集している場合は、このフィールドは表示されません。
優先度	チケットの優先度の重要性。
所有者	ライフサイクルを通じてチケットを管理する責任があるユーザー。 プロセステンプレートから子チケットを作成または編集する場合には、このフィールドを関連付けられた親チケットの 親の所有者 または 親の送信者 に設定するオプションもあります。 ヒント: チケットを自分にすばやく割り当てるには、チケット リストページで、チケットを含む行で をクリックします。
期限	チケットが終了するようにスケジュールされている日時。 サービスレベル契約が有効になっていない場合、期日はデフォルトでは「なし」に設定されています。 サービスレベル契約が有効になっている場合、期日はSLA設定に従って自動的に計算されます。期日は、チケット送信時に設定された優先度に基づいて計算されます。チケットが最初に送信された後に優先度が変更された場合、計算済みの期日は新しい優先度に従って再計算されますが、この場合、元の送信日時に基づいた再計算になります。SLA解決時間の設定が変更された場合、その変更は新しいチケットにのみ適用されます。古いチケットは影響を受けません。詳細については、「サービスレベル契約の設定」を参照してください。

オプション	説明
	期限の日時を手動で設定するには、**手動日付** を選択します。この場合、サービスレベル契約が有効になっていると、期限の日時が計算されてオプションとして表示されますが、選択はされません。
「CC」リスト	チケットイベント発生時にEメール通知を受信するユーザーのリスト。CCリストには、キューの **イベント発生時にEメールを送信** 設定で指定されているチケットイベントと **チケットCC** に基づいて、Eメールが送信されます。
解決	チケットに関連付けられている問題の解決策。 このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションがすべて表示されます。 例： • 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。 • イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファイルパスを指定するか、指定された領域にイメージをドロップします。 ◦ スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。 ◦ この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。 ◦ テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイルは、チケットページの 添付ファイル セクションで管理できます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。 • 外部リンクを追加するには、 をクリックします。 • 外部でホストされるビデオを埋め込むには、 をクリックします。
事前定義された応答	このチケットに対する解決策として自動応答を追加する場合は **事前定義された応答** をクリックし、応答テンプレートを選択します。 選択した応答テンプレートが **解決** フィールドに表示されます。複数の応答テンプレートを解決策の工

オプション	説明
	ントリとして追加できます。これらは、選択した順序で表示されます。 **ヒント:** 応答テンプレートを作成または編集するには、変更を保存し **管理** をクリックします。これにより、応答テンプレート ページが表示されます。応答テンプレートの詳細については、「応答テンプレートの表示および編集」を参照してください。
関連するチケットの情報	プロセステンプレートからチケットを作成している場合には、このセクションは表示されません。
チケットの追加	クリックしてこのチケットの関連情報にチケットを追加します。
参照元	**参照元** は読み取り専用フィールドで、**関連参照** セクションを介してこのチケットを参照しているすべてのチケットへのチケット参照が保持されます。
マージされたチケット	このセクションでは、必要に応じて、このチケットとマージされたチケットのリストを編集できます。マージするチケットは、同じキューに属している必要があります。チケットの詳細 ページを使用してチケットをマージする場合、開いているチケットがプライマリチケットになります。マージされたその他のすべてのチケットは、マージするとアーカイブされます。詳細については、「チケットのマージ」を参照してください。 マージされたチケットを追加するには、**チケットを追加してマージする / マージされたチケットを編集する** をクリックし、表示されるリストからチケットを選択します。
プロセス情報	プロセステンプレートからチケットを作成している場合にのみ、このセクションが表示されます。このセクションに表示されるすべての設定は読み取り専用です。プロセステンプレートの作成および設定の完全な情報については、「プロセステンプレートの追加、編集、および有効化」を参照してください。
プロセス	このチケットに関連付けられたプロセステンプレートの名前。
プロセスタイプ	プロセスのタイプ。デフォルトのインストールでは、サービスデスク と ソフトウェアリクエスト：承認が必要 プロセスタイプだけが含まれます。必要に応じて、新しいプロセスタイプを作成できます。例えば、特定のアプリケーション、またはアプリケーションのグループにアクセスするためのプロセスタイプを作成できます。詳細については、「プロセスタイプの定義」を参照してください。
プロセスステータス	このプロセステンプレートに関連付けられたワークフローのステータス。例えば、保留中の承認。

オプション	説明
親	親のチケットの名前。このチケットに関連付けられたプロセステンプレートで定義されます。
プロセスの承認	このチケットに対する承認者として割り当てられているユーザーのリスト（該当する場合）。 • チケットのすべての承認が受信されると、このセクションはデフォルトで折りたたまれて表示されます。これらを表示するには **展開** をクリックします。 • このチケットの 1 つまたは複数の承認が保留されている場合、このセクションは表示されます。非表示にするには **折りたたむ** をクリックします。 承認者は、プロセステンプレートで定義されたステージのリストに表示されます。各ステージには、必要に応じて、1人または複数の承認者を設定できます。各承認者およびステージに関連した設定（承認のタイムアウトや通知など）も、このセクションのリストに表示されます。プロセスチケットを作成すると、最初の承認者に対するタイムアウト期間が開始します。そのユーザーがチケットを承認すると、次の承認者に対するタイムアウト期間が開始し、その後も同じことが繰り返されます。 このプロセスに関連付けられているプロセステンプレートが、チケット送信者のマネージャが 1 つまたは複数のステージの承認者になっており、ログオンしているユーザーにマネージャのアカウントが関連付けられていることを示している場合、マネージャのユーザー名がリストに表示されます。 ログオンしているユーザーのアカウントがマネージャに関連付けられておらず、関連付けられたプロセステンプレートで、送信者のマネージャが関連プロセスチケットを承認する必要があると指定されている場合、チケットを保存しようとするとエラーが表示されます。ただし、送信者のマネージャが承認者の 1 人に過ぎない場合は、プロセスの承認 セクションには他の承認者が一覧表示され、エラーが表示されることなくチケットを保存できます。
プロセスのアクティビティ	プロセスのアクティビティのリスト。それぞれが子チケットを表し、プロセステンプレートでの定義のとおりに、ステージのリストに表示されます。必要に応じて、複数のチケットを同じステージに割り当てることができます。例えば、最初のステージが新入社員の機器とサプライを入手することである場合、注文するデバイス、オフィス機器、およびサプライにそれぞれ別個の子チケットを用意し、そのすべてをステージ1に割り当てることができます。プロセスチケットを作成すると、ステージ 1 に割り当てられたすべての子チケットが自動的に作成されます。すべてのステージ 1 チケットが終了するとステージ 2 チケットが作成され、すべてのステージ 2 チケットが終了するとステージ 3 チケットが作成され、以下同様に続きます。承認の期限が切れると、

オプション	説明
	そのステージまたはそれ以降のステージに関連する子チケットは作成されません。
チケットの追加	クリックしてこのチケットの関連情報にチケットを追加します。
参照元	**参照元** は読み取り専用フィールドで、**関連参照** セクションを介してこのチケットを参照しているすべてのチケットへのチケット参照が保持されます。
Comments	チケットに追加するコメント。チケットのコメントとして、添付ファイルやスクリーンショットを追加したり、自動応答やサポート技術情報の内容を提供したりできます。詳細については、次を参照してください。 • チケットへのコメントの追加 • サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除 このチケットに対する解決策として自動応答を追加する場合は **事前定義された応答** をクリックし、応答テンプレートを選択します。 選択した応答テンプレートが **解決** フィールドに表示されます。複数の応答テンプレートを解決策のエントリとして追加できます。これらは、選択した順序で表示されます。 **ヒント:** 応答テンプレートを作成または編集するには、変更を保存し **管理** をクリックします。これにより、応答テンプレート ページが表示されます。応答テンプレートの詳細については、「応答テンプレートの表示および編集」を参照してください。
サポート技術情報記事	サポート技術情報記事を参照し、その内容をチケットのコメントに追加します。サポート技術情報記事の詳細については、「サポート技術情報記事の管理」を参照してください。

4. **テンプレートベースのチケットのみ**。このチケットに関する情報を入力します。チケットフィールドは、関連付けられたチケットテンプレート内で定義されます。

   チケットテンプレートの詳細については、「チケットテンプレートの設定」を参照してください。

5. 次のいずれかを実行します。
   - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
   - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
   - **キャンセル** をクリックして、チケットの変更を破棄します。

   他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効ま

たは無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

6. Update Notification（更新通知）ダイアログに報告された変更を確認します。

オプション	説明
Their Change(s)（他のユーザーの変更）	自分がチケットを編集している間に他のユーザーが送信した変更の概要です。
Your Change(s)（あなたの変更）	Their Changes（他のユーザーの変更）列にリストされたフィールドに自分が送信しようとしている変更の概要です。これらの変更は、他のユーザーが送信した変更とコンフリクトする可能性があります。 **注:** ダイアログには他のユーザーが行ったすべての変更の概要が示されます。一方で、自分の変更は、他のユーザーの変更とコンフリクトする場合にのみ表示されます。また、他のユーザーが、例えば Category（カテゴリ）などのフィールドを変更しているが、自分はそのフィールドを変更していない場合、変更は Modified!（変更されました!）セクションに表示されます。Your Changes（あなたの変更）列に表示される「--」は、内容を変更していないため、他のユーザーの変更が保持されることを示します。
Conflict!（コンフリクト!）	矛盾する変更です。例えば、チケットの Category（カテゴリ）を **ソフトウェア** に変更したときに、別のユーザーが Category（カテゴリ）を **Network**（ネットワーク）に変更した場合、変更は Conflict!（コンフリクト!）セクションにまとめられます。
Modified!（変更されました!）	コンフリクトしない変更の概要です。例えば、チケットの Summary（概要）に情報を追加したときに、別のユーザーが **Impact**（影響）を変更した場合は、両方の変更が Modified!（変更されました!）セクションにまとめられます。

7. 次のいずれかを実行します。
   - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
   - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
   - **キャンセル** をクリックして、チケットの変更を破棄します。

   他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

8. Update Notification（更新通知）ダイアログに報告された変更を確認します。

オプション	説明
Their Change(s)（他のユーザーの変更）	自分がチケットを編集している間に他のユーザーが送信した変更の概要です。

オプション	説明
Your Change(s)（あなたの変更）	Their Changes（他のユーザーの変更）列にリストされたフィールドに自分が送信しようとしている変更の概要です。これらの変更は、他のユーザーが送信した変更とコンフリクトする可能性があります。 **注:** ダイアログには他のユーザーが行ったすべての変更の概要が示されます。一方で、自分の変更は、他のユーザーの変更とコンフリクトする場合にのみ表示されます。また、他のユーザーが、例えば Category（カテゴリ）などのフィールドを変更しているが、自分はそのフィールドを変更していない場合、変更は Modified!（変更されました!）セクションに表示されます。Your Changes（あなたの変更）列に表示される「--」は、内容を変更していないため、他のユーザーの変更が保持されることを示します。
Conflict!（コンフリクト!）	矛盾する変更です。例えば、チケットの Category（カテゴリ）を **ソフトウェア** に変更したときに、別のユーザーが Category（カテゴリ）を **Network**（ネットワーク）に変更した場合、変更は Conflict!（コンフリクト!）セクションにまとめられます。
Modified!（変更されました!）	コンフリクトしない変更の概要です。例えば、チケットの Summary（概要）に情報を追加したときに、別のユーザーが **Impact**（影響）を変更した場合は、両方の変更が Modified!（変更されました!）セクションにまとめられます。

9. Update Notification（更新通知）ダイアログボックスでは、次のいずれかの操作を行います。
   - **変更を維持** をクリックして、自分が行った変更を保存します。このオプションは、自分の変更が他のユーザーの変更とコンフリクトしない場合に表示されます。

     注: 他のユーザーが、例えば Category（カテゴリ）などのフィールドを変更しているが、自分はそのフィールドを変更していない場合、変更は Modified!（変更されました!）セクションに表示されます。Your Changes（あなたの変更）列に表示される「--」は、内容を変更していないため、他のユーザーの変更が保持されることを示します。
   - **競合を上書き** をクリックして、自分がチケットに行った変更を保存します。**Conflict!**（コンフリクト!）とマーク付けされた変更については、他のユーザーが行った変更が自分の変更で上書きされます。
   - **キャンセル** をクリックして Ticket Detail（チケットの詳細）ページに戻り、チケットの編集を続行します。

デバイスの詳細 ページからのチケット作成

必要に応じて、デバイスの詳細 ページからデバイスに対してサービスデスクチケットを作成できます。

デバイスの詳細 ページからサービスデスクチケットを作成すると、ユーザー情報およびデバイス情報がチケットに自動的に追加されます。

1. デバイスの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**インベントリ** をクリックして、**ダッシュボード** をクリックします。

c. デバイスの名前をクリックします。

2. アクティビティ セクションで、**サービスデスクチケット** をクリックして、デバイスに関連するチケットを示すテーブルを表示します。
3. **新規作成** をクリックして、新規 ページを表示します。

- キューに基づいてチケットを作成する場合で、組織内に複数のチケットキューがあるときは、**チケット** ドロップダウンリストからキューを選択します。
- プロセステンプレートに基づいてチケットを作成する場合は、**プロセス** ドロップダウンリストからプロセスを選択します。

チケットの詳細 ページが表示されます。

4. 必要な情報を入力します。チケットフィールドの説明については、管理者コンソールのチケットページからのチケット作成を参照してください。
5. 次のいずれかを実行します。

- **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
- **変更の適用** をクリックしてチケットを保存し、編集を続行します。
- **キャンセル** をクリックして、チケットの変更を破棄します。

他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

Asset Detail（資産の詳細）ページからのチケットの作成

必要に応じて、Asset Detail（資産の詳細）ページから資産に対してサービスデスクチケットを作成できます。

Asset Detail（資産の詳細）ページからサービスデスクチケットを作成すると、ユーザー情報および資産情報がチケットに自動的に追加されます。

1. Asset Detail（資産の詳細）ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**資産管理** をクリックして、**資産** をクリックします。
   c. 資産の名前をクリックします。

サービスデスクチケット セクションに、資産に関連するチケットを示すテーブルが表示されます。

2. **新規作成** をクリックして、新規 ページを表示します。

- キューに基づいてチケットを作成する場合で、組織内に複数のチケットキューがあるときは、**チケット** ドロップダウンリストからキューを選択します。
- プロセステンプレートに基づいてチケットを作成する場合は、**プロセス** ドロップダウンリストからプロセスを選択します。

チケットの詳細 ページが表示されます。

3. 必要な情報を入力します。チケットフィールドの説明については、管理者コンソールのチケットページからのチケット作成を参照してください。
4. 次のいずれかを実行します。
   - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
   - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
   - **キャンセル** をクリックして、チケットの変更を破棄します。

   他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

警告からのサービスデスクチケットの作成

サーバー監視警告からサービスデスクチケットを作成できます。このチケットフォームのフィールドに警告からの情報が自動的に入力されます。

1. 次のいずれかの方法で、警告の監視 リストに移動します。
   - 警告の監視 **ウィジェットが、開いている** ダッシュボード **にインストールされている場合は、警告の監視 をクリックします。**
   - **左側のナビゲーションバーで、監視 > 警告 を選択します。**
2. 警告メッセージが表示されている行のチェックボックスをオンにし、**アクションの選択 > 新規チケット** を選択します。
   - キューに基づいてチケットを作成する場合で、組織内に複数のチケットキューがあるときは、**チケット** ドロップダウンリストからキューを選択します。
   - プロセステンプレートに基づいてチケットを作成する場合は、**プロセス** ドロップダウンリストからプロセスを選択します。

   タイトル、概要、送信者、および デバイス フィールドには、警告からの情報が表示されます。
3. **オプション**：企業の手順に適合させるには、「タイトル」および「概要」を変更します。
4. フォームの完成に必要な残りの情報を入力します。次に、**保存** をクリックしてチケットを保存し、チケット詳細 ページから移動するか、または **変更の適用** をクリックし、チケットを保存して編集を継続します。

オプション	説明
タイトル	（必須）問題についての簡単な説明。監視によって入力されたタイトルを自分が選択したいずれかのタイトルに置き換えることができます。
概要	問題についての詳細な説明。 このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションがすべて表示されます。

オプション	説明
	例： • 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。 • イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファイルパスを指定するか、指定された領域にイメージをドロップします。 ◦ スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。 ◦ この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。 ◦ テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイルは、チケットページの 添付ファイル セクションで管理できます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。 • 外部リンクを追加するには、 をクリックします。 • 外部でホストされるビデオを埋め込むには、 をクリックします。
送信者	チケットを送信するユーザーのログイン名。ドロップダウンリストから別のログイン名を選択して送信者を変更できます。送信者の連絡先情報を表示するには、 をクリックします。
資産	この資産の情報がチケットに含まれます。ドロップダウンリストから資産を選択します。資産の詳細を表示するには、 をクリックします。
送信者に割り当てられている資産をフィルタリング	送信者に割り当てられている資産に基づいて資産リストをフィルタリングします。
デバイス	このデバイスの情報がチケットに含まれます。監視ではこの情報が提供されます。デバイスの詳細を表示するには、 をクリックします。
送信者に割り当てられているデバイスをフィルタリング	送信者に割り当てられているデバイスに基づいて資産リストをフィルタリングします。
インパクト	不都合または作業不可の人数。

オプション	説明
カテゴリ	問題の分類。
ステータス	チケットの現在の状態。チケットをプロセステンプレートから作成または編集している場合は、このフィールドは表示されません。
優先度	チケットの優先度の重要性。
所有者	ライフサイクルを通じてチケットを管理する責任があるユーザー。
期限	チケットが終了するようにスケジュールされている日時。 サービスレベル契約が有効になっていない場合、期日はデフォルトでは「なし」に設定されています。 サービスレベル契約が有効になっている場合、期日はSLA設定に従って自動的に計算されます。期日は、チケット送信時に設定された優先度に基づいて計算されます。チケットが最初に送信された後に優先度が変更された場合、期日は新しい優先度に従って再計算されますが、この場合、元の送信日時に基づいた再計算になります。SLA解決時間の設定が変更された場合、その変更は新しいチケットにのみ適用されます。古いチケットは影響を受けません。詳細については、「サービスレベル契約の設定」を参照してください。 期限の日時を手動で設定するには、**手動日付** を選択します。この場合、サービスレベル契約が有効になっていると、期限の日時が計算されてオプションとして表示されますが、選択はされません。
「CC」リスト	チケットイベント発生時にEメール通知を受信するユーザーのリスト。CCリストには、キューの **イベント発生時にEメールを送信** 設定で指定されているチケットイベントと **チケットCC** に基づいて、Eメールが送信されます。
解決	チケットに関連付けられている問題の解決策。 このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションがすべて表示されます。 例： • 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。 • イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファ

オプション	説明
	イルパスを指定するか、指定された領域にイメージをドロップします。 ◦ スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。 ◦ この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。 ◦ テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイルは、チケットページの 添付ファイル セクションで管理できます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。 • 外部リンクを追加するには、 をクリックします。 • 外部でホストされるビデオを埋め込むには、 をクリックします。
関連するチケットの情報	プロセステンプレートからチケットを作成している場合には、このセクションは表示されません。
チケットの追加	クリックしてこのチケットの関連情報にチケットを追加します。
参照元	**参照元** は読み取り専用フィールドで、**関連参照** セクションを介してこのチケットを参照しているすべてのチケットへのチケット参照が保持されます。
マージされたチケット	このセクションでは、必要に応じて、このチケットとマージされたチケットのリストを編集できます。マージするチケットは、同じキューに属している必要があります。チケットの詳細 ページを使用してチケットをマージする場合、開いているチケットがプライマリチケットになります。マージされたその他のすべてのチケットは、マージするとアーカイブされます。詳細については、「チケットのマージ」を参照してください。 マージされたチケットを追加するには、**チケットを追加してマージする / マージされたチケットを編集する** をクリックし、表示されるリストからチケットを選択します。
プロセス情報	プロセステンプレートからチケットを作成している場合にのみ、このセクションが表示されます。このセクションに表示されるすべての設定は読み取り専用です。プロセステンプレートの作成および設定の

オプション	説明
	完全な情報については、次を参照してください。プロセステンプレートの追加、編集、および有効化
プロセス	このチケットに関連付けられたプロセステンプレートの名前。
プロセスタイプ	プロセスのタイプ。
プロセスステータス	このプロセステンプレートに関連付けられたワークフローのステータス。例えば、保留中の承認。
親	親のチケットの名前。このチケットに関連付けられたプロセステンプレートで定義されます。
プロセスの承認	このチケットに対する承認者として割り当てられているユーザーのリスト（該当する場合）。承認者は、プロセステンプレートで定義されたステージのリストに表示されます。各ステージには、必要に応じて、1人または複数の承認者を設定できます。各承認者およびステージに関連した設定（承認のタイムアウトや通知など）も、このセクションのリストに表示されます。プロセスチケットを作成すると、最初の承認者に対するタイムアウト期間が開始します。そのユーザーがチケットを承認すると、次の承認者に対するタイムアウト期間が開始し、その後も同じことが繰り返されます。
プロセスのアクティビティ	プロセスのアクティビティのリスト。それぞれが子チケットを表し、プロセステンプレートでの定義のとおりに、ステージのリストに表示されます。必要に応じて、複数のチケットを同じステージに割り当てることができます。例えば、最初のステージが新入社員の機器とサプライを入手することである場合、注文するデバイス、オフィス機器、およびサプライにそれぞれ別個の子チケットを用意し、そのすべてをステージ1に割り当てることができます。プロセスチケットを作成すると、ステージ 1 に割り当てられたすべての子チケットが自動的に作成されます。すべてのステージ 1 チケットが終了するとステージ 2 チケットが作成され、すべてのステージ 2 チケットが終了するとステージ 3 チケットが作成され、以下同様に続きます。
チケットの追加	クリックしてこのチケットの関連情報にチケットを追加します。
参照元	**参照元** は読み取り専用フィールドで、**関連参照** セクションを介してこのチケットを参照しているすべてのチケットへのチケット参照が保持されます。
Comments	チケットに追加するコメント。チケットのコメントとして、添付ファイルやスクリーンショットを追加したり、自動応答やサポート技術情報の内容を提供

オプション	説明
	したりできます。詳細については、次を参照してください。 • チケットへのコメントの追加 • サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除 このチケットに対する解決策として自動応答を追加する場合は **事前定義された応答** をクリックし、応答テンプレートを選択します。 選択した応答テンプレートが **解決** フィールドに表示されます。複数の応答テンプレートを解決策のエントリとして追加できます。これらは、選択した順序で表示されます。 **ヒント:** 応答テンプレートを作成または編集するには、変更を保存し **管理** をクリックします。これにより、応答テンプレート ページが表示されます。応答テンプレートの詳細については、「応答テンプレートの表示および編集」を参照してください。
サポート技術情報記事	サポート技術情報記事を参照し、その内容をチケットのコメントに追加します。サポート技術情報記事の詳細については、「サポート技術情報記事の管理」を参照してください。

関連トピック

サービスデスクのチケット、プロセス、およびレポートの管理

Eメールによるチケットの作成と管理

ユーザーがEメールでチケットを作成し管理できるようにできます。ユーザーに、アプライアンス**管理者コンソール**または**ユーザーコンソール**へのアクセス権がない場合、この機能を利用すると便利です。

Eメールを通じて作成されたチケットへの添付ファイルについて

ユーザーは、Eメールを通じて送信されるサービスデスクチケットにファイルを添付できます。最大8 MBのサイズのファイルを添付できます。

添付ファイルのサイズが8 MBを超える場合、Eメールメッセージは拒否されます。ユーザーにエラーメッセージは表示されません。

アプライアンスがサービスデスクチケットチケットに含まれている添付ファイル内の脅威を検出すると、ファイルへのアクセスがブロックされ、ウイルス対策の検疫 ページで管理できます。詳細については、「隔離された添付ファイルを管理する」を参照してください。

Eメールによるチケット作成を可能にする

ユーザーがEメールを使用してサービスデスクチケットを作成し管理できるようにできます。

1. サービスデスクの チケットの詳細 ページに移動します。

a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
c. **設定** パネルで **キュー** をクリックします。
d. キューの名前をクリックします。

2. ユーザーが E メールを送信してチケットを作成できるよう、有効な E メールアカウント（ Support@mydomain.com など ）を準備します。
3. Eメールアドレスを 代替のEメールアドレス フィールドに追加します。
4. **送信者としてすべてのユーザーを許可** チェックボックスをオンにします。
5. **不明なユーザーからのEメールを許可** チェックボックスをオンにします。

   キュー設定で「**不明なユーザーからのEメールを許可**」が有効になっている場合、チケットを作成するためにサービスデスクキューに送信されるすべてのEメールで、送信者 フィールドを設定することができます。この場合、ユーザー名は **@submitter** トークンで渡される必要があり、既存のユーザーのユーザー名であるか、不明なユーザーの場合は、現在の E メールアドレスである必要があります。

   「**不明なユーザーからのEメールを許可**」が無効になっている場合、送信者のEメールアドレスが既にサービスデスクのユーザーアカウントと関連付けられている場合に限り、上記のプロセスが実行されます。

6. **保存** をクリックします。

Eメールメッセージ経由で作成されたチケットには、キューの詳細 ページで設定したインパクト、カテゴリ、および優先度のデフォルト値が適用されます。Eメールメッセージの本文は、コメントとして追加されます。送信者 フィールドには、送信者の E メールアドレス情報が入力されます。

電子メールでチケットを作成する

電子メールの件名の行にチケットテンプレートの名前を指定すると、電子メールでチケットを簡単に作成できます。

チケットの作成に使用された元の E メールスレッド、またはチケットに関連付けられたサービスデスクから送信された E メールに送信された返信は、チケットの コメント タブに表示されます。詳細については、「チケットコメントの表示」を参照してください。

1. 電子メールアカウントにログインして、新しい電子メールメッセージを作成します。
2. 電子メールの件名の行で、チケットテンプレート名を波括弧で囲んで指定します。例：{Printer Issues}。

   チケットテンプレートを指定しない場合、アプライアンスではキューに関連付けられたデフォルトのチケットテンプレートを使用します。

3. 電子メールのメッセージに問題を記入して、指定されたチケットテンプレートが属するキューに関連付けられた電子メールアドレスに送信します。

   キューの電子メール設定を行う方法について詳しくは、「キュー固有の E メールの設定」を参照してください。

4. サービスデスクから確認の E メールを受信したら、E メール内のリンクをクリックしてチケットの内容を確認します。

   チケットの詳細 ページが表示され、新しく作成されたチケットが表示されます。

5. 必要に応じて変更を加えます。

   チケットページの編集の詳細については、管理者コンソールのチケットページからのチケット作成を参照してください。

Eメールを使用したチケット属性の修正

メッセージの最初に「@」記号を含む変数を使用することで、チケット属性をEメール経由で変更できます。

最後のEメール変数の後にテキストが入力されている場合、そのテキストはチケットの コメント フィールドに追加されます。

例えば、以下のEメールテキストを送信すると、チケットが閉じられ、チケット所有者が変更されて、コメントが追加されます。

@status=closed
@owner=joe
I fixed that problem.If it happens again, talk to Joe.

フィールドおよびフィールド値が無効な場合はエラーが生成され、E メールのエラーテンプレートを使用して、送信者宛てに E メールが返信されます。E メールテンプレートの詳細については、EメールトリガとEメールテンプレートの設定を参照してください。

Eメールを使用した、チケットフィールドのクリア

所定の構文を使用してEメールを送信すると、任意のフィールドを消去できます。

構文は、「@fieldname=」の形式を取ります。例えば、以下のように入力すると、「期日」フィールドがクリアされます。

@due_date=

Eメールを使用した、チケットフィールドの変更

チケットフィールドの値が「ユーザー修正」に設定されている場合は、Eメールメッセージを使用し、次のチケット属性を変更できます。

チケットフィールドの権限の変更については、チケット承認者の使用を参照してください。

フィールド	説明
@category	有効なカテゴリ。
@cc_list	Eメールアドレスまたは配布リストのコンマ区切りリスト。
@due_date	期日。日付は、どのような形式でもかまいません。例えば、4/3/2014、2014年4月3日、次の木曜日など。
@impact	有効なチケットのインパクト。
@owner	所有者のユーザー名、フルネーム、またはEメールアドレス。
@priority	有効なチケットの優先度。
@resolution	解決策。
@status	有効なチケットのステータス。
@submitter	送信者のユーザー名、フルネーム、またはEメールアドレス。Eメールアドレスは、ユーザー名とEメールアドレスのフィールドに使用されます。フルネームは、Eメールアドレスの名前の部分に設定されます。例：「**名前**@domain.com」。

フィールド	説明
@title	チケットのタイトル。
@summary	問題についての詳細な説明。
@asset	チケットに関連付けられている資産。
@machine	チケットに関連付けられているデバイス。
@approval	チケット承認プロセスの状態。このフィールドには、次のいずれかの値を設定できます。「承認されました」、「拒否されました」、「なし」、「追加の情報が必要です」。
@approval_note	承認に関連付けられたメモ。
@owners_only	Eメールでチケットにコメントできるのはオーナーだけかどうかを示します。1 に設定すると、フラグは True になります。その他の数値は、このインジケータを False に設定します。
@custom_<number>	カスタムチケットフィールドの値。<number> はカスタムフィールド ID です。たとえば、$custom_2=ABC は ABC の値を CUSTOM_2 チケットフィールドに割り当てます。

Eメールを使用した、チケット承認フィールドの変更

チケットの承認者に指定されたユーザーは、Eメールメッセージを使用して、複数の承認フィールドを変更することができます。

承認者は次の承認フィールドを変更できます。

フィールド	説明
@approval	チケットを修正します。次のいずれかを使用します。「**承認されました**」、「**拒否されました**」、「**なし**」、「**追加の情報が必要です**」。
@approver	チケット承認者を変更します。チケット承認ラベルからユーザー名を入力します。承認者のラベルを設定する手順については、チケット承認者の使用を参照してください。
@approval_note	コメントを入力します。

Eメールを使用した、カスタムフィールドの設定または変更

所定の構文を使用して、Eメールを通じてサービスデスクチケットのカスタムフィールドを設定できます。

構文は、「@custom_fieldname=newvalue」の形式を取ります。

カスタムフィールドではスペースを使用できません。単語の間にはアンダースコアを使用してください。例えば、「new_value」のようにします。

また、次のものも使用できます。

- @priority = high
- @priority = very_urgent

複数選択のカスタムフィールドの値には、コンマ区切りリストを使用してください。単一選択または複数選択のカスタムフィールドに無効な値を入力すると、エラーが生成されます。

チケットの表示およびコメントや作業や添付ファイルの管理

詳細ページのリンクを使用して、チケット、チケットに関連するデバイスおよび資産の間を移動することができます。また、チケットに作業情報、コメント、および添付ファイル（スクリーンショットなど）を追加できます。

Ticket Detail（チケットの詳細）ページでは、すばやくアクセスできるように関連するデバイスおよび資産がリストされ、リンクされています。同様に、デバイスの詳細 ページおよび 資産詳細 ページから、関連するチケットにアクセスすることができます。また、デバイスの詳細 および 資産詳細 ページからチケットを表示、作成することができます。

チケット、関連デバイス、および資産間の移動

チケット詳細ページのリンクを使用すると、関連するサービスデスクチケット、関連するデバイス、および資産間を移動できます。

1. サービスデスクの チケットの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
    c. チケットのタイトルをクリックします。
2. 送信者、資産、またはデバイスごとにチケットを表示します。
    - **送信者のチケットの履歴 をクリックします。**
    - **資産のチケットの履歴 をクリックします。**
    - **デバイスのチケットの履歴 をクリックします。**

    新しいウィンドウに、資産のすべてのチケットが、各チケットのチケット番号、タイトル、およびステータスと共に表示されます。

    チケットの詳細を表示するには、番号 列または タイトル 列のリンクをクリックして、チケットの詳細ページを表示します。
3. 関連するチケットの情報 セクションで関連するチケットを表示します。
    - 関連参照 **として参照されるチケットをクリックします。**
    - 参照元 **として参照されるチケットをクリックします。**
    - マージされたチケット **として参照されるチケットをクリックします。**
    - 子チケット **として参照されるチケットをクリックします。**
    - 親チケット **として参照されるチケットをクリックします。**

    選択したチケットの チケットの詳細 ウィンドウが表示されます。

チケットの作業情報の追加

サービスデスクチケットには、作業情報（作業開始日、作業終了日、チケットの合計作業時間、作業内容に関するメモなど）を追加することができます。この情報は、チケットの送信者および所有者に提供されます。

1. サービスデスクの チケットの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
    c. チケットのタイトルをクリックします。
2. ページの下部で **作業** タブを選択します。
3. **追加** をクリックします。
4. 次の情報を入力します。

オプション	説明
日付	作業を開始した日付。この日付を変更するには、日付 フィールドをクリックして別の日付を選択します。日付を削除するには、**クリア** をクリックします。
開始	作業を開始した時間（24時間制）。
終了	作業を終了した時間（24時間制）。
調整	記録された時間に追加する時間または記録された時間から差し引く時間数。この機能は、請求および追跡の用途に役立ちます。例えば、チケットの作業開始が08:00で作業終了が12:00とあっても、管理者が実際にチケットで作業した時間は2時間である場合があります。この場合は、このフィールドに「-2.0」と入力すると、実際に作業にかかった時間を正確にレポートできます。
メモ	任意の追加情報を入力します。

5. **作業の追加** をクリックします。

チケットのデフォルトビューの使用

チケット ページに表示されるチケットを制限するために使用できる、組み込みのシステムビューが複数あります。

1. サービスデスクの チケット（複数）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。

    チケット（複数）ページには、デフォルトキュー内のチケットが表示されます。
2. キューに表示されるチケットを制限するには、**特定基準で表示** ドロップダウンリストからビューを選択します。

使用可能な組み込みのビューは次の通りです。

グループ	ビュー
自分のチケット	すべての自分のチケット **注:** これには、自分が送信した、または自分が所有するすべてのチケット、あるいは自分が承認者であるすべてのチケットが含まれます。 自分のアクティブなチケット **注:** これには、自分が送信した、または自分に割り当てられた、「オープン」または「停止済み」状態のすべてのチケットが含まれます。 自分のチケットが今日送信されました 自分のチケット本日期限 自分の期限超過チケット 自分の最近のチケット
状態別自分のチケット	自分のオープン状態チケット 自分の停止済み状態チケット 自分のクローズ状態チケット 自分のクローズされていない状態チケット
ステータス別自分のチケット	**注:** このオプションは、特定のキューを表示している場合のみ表示されます。 自分の新規チケット 自分のオープンチケット 自分のクローズチケット 自分の要追加情報チケット
すべてのチケット	すべてのチケット すべてのアクティブな未割り当てチケット **注:** これには、所有者のいないチケットと、「オープン」および「停止済み」状態のチケットが含まれます。このビューは、ログインしているユーザーが選択されたキューの所有者である場合にのみ使用可能です。 すべてのチケットが今日送信されました すべてのチケット本日期限 すべての期限超過チケット
状態別のすべてのチケット	すべてのオープン状態チケット すべての停止済み状態チケット すべてのクローズ状態チケット すべてのクローズされていない状態チケット

グループ	ビュー
ステータス別のすべてのチケット	**注:** このオプションは、特定のキューを表示している場合のみ表示されます。 すべての新規チケット すべてのオープンチケット すべてのクローズチケット すべての追加の情報が必要なチケット
状態別自分の従業員のチケット	**注:** このオプションは、次の場合にのみ表示されます。 • ユーザーアカウントにマネージャの役割があり、1 つまたは複数の従業員アカウントが関連付けられている。 • **ユーザーコンソール**を使用している。 **注:** 管理者は キュー設定 ページでこの機能をオフにすることができます。 自分の従業員のチケット：開かれた 自分の従業員のチケット：停止済み 自分の従業員のチケット：閉じられた 自分の従業員のチケット：閉じられていない
送信者ラベル	<送信者ラベル>
カスタムビューカスタムビュウ	使用可能なカスタムビューのリスト。 **注:** このオプションは、ログインしているユーザーによって作成されたカスタムビューがある場合にのみ表示されます。

カスタムビューをデフォルトとして設定します。詳細については、「チケットのデフォルトビューとしてのビューの設定」を参照してください。

チケットのカスタムビューの作成

カスタムビューを作成して、チケット ページに表示されるサービスデスクチケットのタイプや数を制限します。こうすると、参照する必要のあるチケットのみを表示できるようになります。

注: カスタムビューは、カスタムビューが作成されたユーザーアカウントでのみ使用できます。複数のユーザーアカウントで使用することはできません。自分が作成したビューに他のユーザーがアクセスできるようにするには、カスタムビューのURLをそのユーザーに送信します。

1. サービスデスクの チケット（ 複数 ）ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）に口グインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
2. 右側のリストの上にある**カスタムビュー** タブを選択します。

   カスタムビュー パネルが表示されます。

3. カスタムビューで使用する基準を指定します。例えば、優先度が「高」の未解決チケットを表示するカスタムビューを作成できます。
4. **テスト** をクリックし、結果を確認します。
5. **作成** をクリックして、カスタムビューを保存します。

カスタムビューをデフォルトとして設定します。詳細については、「チケットのデフォルトビューとしてのビューの設定」を参照してください。

チケットのデフォルトビューとしてのビューの設定

ビューをサービスデスクの チケット（複数）ページのデフォルトビューとして設定できます。デフォルトビューはユーザー固有であり、ユーザーごとに個別に設定する必要があります。

1. サービスデスクの チケット（複数）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
2. **オプション**：右側のリストの上にある **カスタムビュー** タブをクリックし、カスタムビューの設定を選択します。詳細については、「チケットのカスタムビューの作成」を参照してください。
3. **アクションの選択 > デフォルトビューの設定 > デフォルトとして現在のビューを設定** を選択します。

    現在のビューがログインユーザーのデフォルトビューとして チケット（複数）リストに保存されます。

チケットへのコメントの追加

チケットに対して作業を行う際に、コメントを追加して、チケットにさらに情報を提供できます。

1. サービスデスクの チケットの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
    c. チケットのタイトルをクリックします。
2. まだ選択していない場合は、チケットの詳細 ページの一番下にある **コメント** タブをクリックします。
3. **コメント** テキストボックスにコメントを入力します。

    このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色のボタンなど、コンテンツをフォーマットするためのテキスト編集オプションがすべて表示されます。

例：

- 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。
- イメージを追加するには、 をクリックし、イメージファイルへの URL、ローカルファイルパスを指定するか、指定された領域にイメージをドロップします。
  - スクリーンショットをコピーしてテキストフィールドに直接貼り付けることもできます。
  - この方法で追加したイメージは、チケットに添付ファイルとして追加されます。また、必要に応じて E メール通信にも含まれます。
  - テキストフィールドからイメージを削除しても、関連付けられている添付ファイルは削除されません。添付ファイルは、チケットページの 添付ファイル セクションで管理できます。詳細については、「サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除」を参照してください。
- 外部リンクを追加するには、 をクリックします。
- 外部でホストされるビデオを埋め込むには、 をクリックします。

4. コメントが、所有者以外のユーザー (送信者など) には表示されず、チケットの所有者だけに表示されるように指定する場合は、**所有者のみ** チェックボックスをオンにします。
5. 添付ファイルをチケットに追加する場合は、**添付ファイルの追加** をクリックし、添付するファイルを選択します。

   チケットには 5 つまで添付ファイルを追加できます。詳細については、次を参照してください。 サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除
6. スクリーンショットをチケットに追加する場合は、**スクリーンショットの貼り付け** をクリックし、表示されるダイアログボックスにスクリーンショットを貼り付けます。

   チケットには最大5つのスクリーンショットを追加することができます。詳細については、次を参照してください。 サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除
7. このチケットにコメントとして自動応答を追加する場合は **事前定義された応答** をクリックし、応答テンプレートを選択します。

   選択した応答テンプレートが **コメント** フィールドに表示されます。複数の応答テンプレートをコメントとして追加できます。これらは、選択した順序で表示されます。

   ヒント: 応答テンプレートを作成または編集するには、変更を保存し **管理** をクリックします。これにより、応答テンプレート ページが表示されます。

   応答テンプレートの詳細については、「応答テンプレートの表示および編集」を参照してください。
8. このチケットにコメントとしてサポート技術情報記事の内容を追加する場合は、**サポート技術情報記事** をクリックして、該当するトピックを選択します。

   選択した記事の内容が、**コメント** フィールドに表示されます。

   サポート技術情報記事の詳細については、「サポート技術情報記事の管理」を参照してください。
9. すでにコメントを提供したチケットを表示しており、自身のコメントを編集する場合、そのチケットに関連付けられたキューで、ユーザーが自身のコメントを編集できるように設定されていれば編集できます。キューの基本設定を行う方法の詳細については、「チケットキューの設定」を参照してください。
10. 送信したチケットを表示しており、他のユーザーのコメントを編集する場合は、そのチケットに関連付けられたキューで、他のユーザーが送信したコメントを技術者が編集できるように設定されていれば編集できます。キューの基本設定を行う方法の詳細については、「チケットキューの設定」を参照してください。
11. アカウントにマネージャの役割があり、そのチケットに関連付けられているキューで、従業員のチケットへのコメントをマネージャが編集できるように設定されており、従業員が送信したチケットを表示している場合は、必要に応じて、コメントを追加または編集したり、チケットに添付ファイルやスクリーン

ショットを追加することができます。キューの基本設定を行う方法の詳細については、「チケットキューの設定」を参照してください。

12. チケットコメントに追加する関連のサポート技術情報記事がある場合は、ドロップダウンリストから記事を選択します。検索語を入力して、特定の記事を検索できます。
13. **送信** をクリックして、新しく追加したコメントを保存します。

> **注:** コメントは、他のすべてのチケット情報とは別に保存されます。コメントに基づいたEメール通知が有効になっている場合、サブスクライブされたユーザーは、コメントが追加されるとすぐにEメールを受信します。ユーザーが、既存のチケットについて送信されたEメール通知に応答する場合、ユーザーが返信行の上部に入力した新しいテキストのみがコメントとして追加されます。

チケットへの所有者限定コメントの追加

所有者以外のユーザー（送信者など）には表示されず、チケットの所有者だけに見えるチケットコメントを追加することができます。

ただし、所有者限定コメントを追加する場合は、他のチケット所有者にこの設定を変更する権限があることに注意してください。この設定が変更されると、所有者限定コメントは、他のユーザーにも見えるようになります。

Questでは、所有者限定コメントに関する次のベストプラクティスを推奨します。

- コメントを追加する際は、適切な内容を入力すること。
- 所有者のみ の設定を変更するポリシーは、明確、かつ明記されていること。

1. サービスデスクの チケットの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
    c. チケットのタイトルをクリックします。
2. まだ選択していない場合は、チケットの詳細 ページの一番下にある **コメント** タブをクリックします。
3. **所有者のみ** チェックボックスをオンにし、コメント、サポート技術情報記事への参照、または添付ファイルを追加します。

> **注:** キューの詳細 ページで **所有者のみに表示されるデフォルトのチケットの所有者コメント** を選択して、**所有者のみ** チェックボックスをデフォルトで有効にすることができます。詳細については、「チケットキューの設定」を参照してください。

4. **送信** をクリックします。

> **注:** コメントは、他のすべてのチケット情報とは別に保存されます。

チケットにコメントが追加されました。適切な権限を持つユーザーが 所有者のみ チェックボックスをオフにしない限り、コメントはチケット所有者にしか見えません。

チケットコメントの表示

チケットに対して作業を行う際に、**コメント** タブを選択すると、コメントが表示されます。これらのコメントは、**履歴**タブにも他の履歴アイテムと共に表示されます。

1. サービスデスクの チケットの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。

c. チケットのタイトルをクリックします。

2. チケットの詳細 ページの一番下で、**コメント** タブを選択します。

   コメント タブの下に、チケットに属するコメントのリストが表示されます。

3. コメントリストをフィルタリングして添付ファイルがあるコメントのみを表示するには、**添付ファイルのみを表示** チェックボックスをオンにします。

サービスデスクチケットに対するスクリーンショットおよび添付ファイルの追加または削除

各サービスデスクチケットに最大 5 つのスクリーンショットを貼り付けることができます。また、各チケットへの添付ファイルとして最大 5 つのファイルを追加できます。

スクリーンショットをチケットに貼り付けるには：

- キャプチャする内容が画面に表示され、スクリーンショットをコンピューターのクリップボードに保存できる必要があります。
- Safari 以外の対応ブラウザを使用して**管理者コンソール**にアクセスする必要があります。対応ブラウザの完全なリストについては、技術仕様を参照してください。

> **注:** 旧バージョンまたはサポートされていないブラウザを使用している場合には、スクリーンショット貼り付け機能が非表示になります。ただし、その場合でもスクリーンショットをファイルとしてチケットに添付できます。

ファイルを添付するには、**管理者コンソール**からファイルを参照できる必要があります。最大 8 MB のサイズのファイルを添付できます。

スクリーンショットと添付ファイルをチケットに追加すると、チケット画面の別のセクションに表示されます。また、イメージ（スクリーンショットを含む）を直接 概要 フィールドおよび コメント フィールドに追加することもできます。詳細については、「管理者コンソールのチケットページからのチケット作成」を参照してください。

1. キャプチャする内容が表示されている場合、スクリーンショットをコンピューターのクリップボードに保存するには、次のいずれかを行います。
   - Windows の場合、**Prnt Scrn** キーまたは **Print Screen** キーを押します。
   - Macでは、**Command**、**Shift**、および**3**キーを同時に押し続けます。

   スクリーンショットがコンピューターのクリップボードにコピーされます。
2. サービスデスクの チケットの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
   c. チケットの詳細 ページを表示するには、次のいずれかを実行します。
   - **アクションの選択 > 新規作成** を選択します。
   - **新規作成 > キューからの新規チケット > キュー名** の順に選択します。

     多数のキューがある場合は、検索ボックスを使用して特定のキューをすばやく検索します。
   - チケットの名前をクリックします。
3. ファイルをチケットに添付します。
   a. チケットの詳細 ページで、コメント タブの 添付ファイル セクションまで下にスクロールし、**添付ファイルの追加** をクリックします。

b. 表示されたファイルブラウザダイアログボックスで、チケットに添付するファイルを選択して開きます。

チケットには 5 つまで添付ファイルを追加できます。

アプライアンスがサービスデスクチケットチケットに含まれている添付ファイル内の脅威を検出すると、ファイルへのアクセスがブロックされ、ウイルス対策の検疫 ページで管理できます。ファイル名の横に 検疫 リンクが表示され、ウイルス対策の検疫 ページに移動できます。隔離されたファイルが解放されると、ファイルへのアクセスが復元されます。詳細については、「隔離された添付ファイルを管理する」を参照してください。

ファイルブラウザが閉じ、添付ファイルの名前が 添付ファイル セクションの **添付ファイルの追加** の下に表示されます。

c. ページの一番下で **送信** をクリックし、次に **変更の適用** をクリックします。

チケットに添付ファイルが追加されました。

4. スクリーンショットをチケットに追加します。
   a. チケットの詳細 ページで、ページの下部まで下にスクロールし、コメント タブの 添付ファイル セクションで **スクリーンショットの貼り付け** をクリックします。

   スクリーンショットの貼り付け ダイアログボックスが表示されます。

   b. スクリーンショットをキャプチャし、それをクリップボードにコピーします。
   c. 次のキーの組み合わせのいずれかを使用して、スクリーンショットをダイアログウィンドウに貼り付けます。

   - Windows の場合、**Ctrl** を押したまま、**V** を押します。
   - Mac の場合、**Command** を押したまま、**V** を押します。

   スクリーンショットが スクリーンショットの貼り付け ダイアログボックスに表示されます。

   d. **スクリーンショットの追加** をクリックします。

   スクリーンショットの貼り付け ダイアログボックスが閉じ、スクリーンショットに割り当てられたファイル名が、添付ファイル セクションの **スクリーンショットの貼り付け** に表示されます。チケットには 5 つまでスクリーンショットを追加できます。

   e. ページの一番下で、**変更の適用** をクリックします。

   チケットにスクリーンショットが追加されます。

5. チケットからスクリーンショットまたは添付ファイルを削除します。
   a. チケットの詳細 ページで、コメント タブの 添付ファイル セクションまで下にスクロールします。
   b. 添付ファイルを削除するには、**添付ファイルの追加** の下で、削除するファイルを探し、ファイル名の右側にある をクリックします。
   c. スクリーンショットを削除するには **スクリーンショットの貼り付け** の下で、削除するスクリーンショットを含むファイルを探し、ファイル名の右側にある をクリックします。
   d. ページの一番下で、**変更の適用** をクリックします。

   チケットからファイルが削除されます。

6. ページの一番下で **保存**をクリックし、チケットへの変更を保存します。

チケットアクティビティ履歴の表示

履歴 タブには、チケットについて実行されたすべてのアクティビティ履歴が表示されます。これには、すべてのチケットの詳細フィールドおよびコメントに対する更新が含まれます。

1. サービスデスクの チケットの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。

c. チケットのタイトルをクリックします。

2. チケットの詳細 ページの一番下で、**履歴** タブを選択します。

E メールを通じたチケット情報の送信

必要に応じて、サービスデスクチケット情報を手動による E メールで受信者に送信できます。

E メールの内容と形式は、Email Ticket Manually **(E メールでチケットを手動送信) 通知テンプレートによって制御されます。また、テンプレートの** $ticket_fields_visible **トークンには、E メールを送信中のログインユーザーに表示されるすべてのフィールドが表示されます。詳細については、「Eメールトリガと Eメールテンプレートの設定」を参照してください。**

1. サービスデスクの チケットの詳細 ページに移動します。

a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。

c. チケットのタイトルをクリックします。

2. **アクションの選択 > Eメールチケット** を選択します。
3. E メールチケット ページで、受信者の **E メールアドレス**を入力し、必要に応じて**件名**を更新します。
4. **送信** をクリックします。

チケット情報が指定の受信者に E メールで送信されます。

チケットからのデバイスのアクションの実行

サービスデスクチケットに割り当てられているデバイスの場合、Ticket Detail (チケットの詳細) ページからデバイスのアクションを実行できます。

- デバイスのアクションは既に追加されています。組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定の デバイスのアクション セクションを参照してください。
- デバイスは既にチケットに割り当てられています。
- 承認済みのブラウザを使用して**管理者コンソール**にアクセス中です。詳細については、「https://support.quest.com/kb/148787」を参照してください。

1. サービスデスクの チケットの詳細 ページに移動します。

a. アプライアンス管理者コンソール (https://**appliance_hostname**/admin) にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。

c. チケットのタイトルをクリックします。

2. デバイス ドロップダウンリストの下の Action (アクション) ドロップダウンリストから、デバイスアクションを選択します。

すぐにリモートデバイスでそのデバイスアクションの実行が自動的に試行されます。

チケットのマージ

関連するチケットで現在もアクティブなものが多数ある場合は、個別に管理するのではなく、それらを単一のチケットにマージし、マージされたすべてのチケットのチケット履歴を失うことなく、そのチケットを管理できます。

チケットをマージする場合は、プライマリチケットを選択する必要があります。残りのチケットは自動的にアーカイブされます。マージされたチケットに関連するすべての履歴は変更されません。チケット履歴には、チケットがいつマージされたかも示されます。

マージできるのは、同じキューに存在するチケットだけです。同じキューに属しているが異なるテンプレートを使用して作成されたチケットはマージできます。プライマリチケットテンプレートに関連付けられたフィールドは保持され、子チケットのフィールドは削除されてアーカイブされます。この機能は、チケットのアーカイブが有効になっている場合にのみ使用できます。

サービス、親、子、およびすでにマージされているチケットはマージできません。マージできるのは、親がなく子がないチケットだけです。

必要に応じてチケットのマージを解除できます。チケットの CC リストに含まれているユーザーのうち、マージプロセス中に追加されたユーザーは、そのチケットがマージ解除された場合でもリストに残ります。

チケットのマージの有効化

サービスデスクのチケットのマージ、または組織コンポーネントが有効になっている場合は、選択した組織のサービスデスクのチケットのマージを有効にすることができます。

1. Service Desk Settings（サービスデスクの設定）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **設定** をクリックします。
2. チケットのアーカイブ セクションで、**有効** チェックボックスをオンにします。

チケット リストページからチケットをマージ

チケット リストページを使用して、チケットをマージし、プライマリチケットを指定できます。

1. マージするチケットを選択します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. **サービスデスク** をクリックして、チケット ページを表示します。
    c. チケット リストページで、**キュー** をクリックし、マージしようとしているチケットを含むキューを選択します。
    d. マージするすべてのチケットを選択します。
2. 選択したチケットをマージします。
    a. アクションの選択 メニューで、**チケットのマージ** を選択します。

        チケットのマージ ダイアログボックスが表示されます。

    b. チケットのマージ ダイアログボックスで、プライマリチケットとして選択するチケットを指定し、**保存** をクリックします。

チケットのマージ ダイアログボックスが閉じ、確認 メッセージボックスが表示されます。このメッセージは、すべてのチケット（プライマリチケットを除く）がアーカイブされることを示します。

c. 確認 メッセージボックスで、**はい** をクリックしてマージを続行します。

チケットの詳細 ページからチケットをマージ

チケットの詳細 ページで表示しているチケットと 1 つ以上のチケットをマージできます。マージするチケットは、同じキューに属している必要があります。

チケットの詳細 ページを使用してチケットをマージする場合、開いているチケットがプライマリチケットになります。マージされたその他のすべてのチケットは、マージするとアーカイブされます。詳細については、「チケットのマージ」を参照してください。

1. 1 つまたは複数の他のチケットとマージするチケットを開きます。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
   c. チケットのタイトルをクリックします。

   チケットの詳細 ページが表示されます。
2. 1 つ以上のチケットを選択したチケットとマージします。
   a. チケットの詳細 ページの マージされたチケット の下で、**チケットを追加してマージする / マージされたチケットを編集する** をクリックし、表示されるリストからチケットを選択します。
   b. 必要に応じて、マージされたチケットをさらに追加します。
3. チケット履歴に、チケットのマージプロセスが表示されていることを確認します。
   a. チケットの詳細 ページで、履歴 タブを開き、**マージされたチケットの履歴の表示** チェックボックスをオンにします。
   b. 履歴 タブで、必要に応じてマージされたチケットに関連するエントリを確認します。

チケットのエスカレーションプロセスの使用

サービスデスクチケットのエスカレーションプロセスとは、チケットが一定期間無視されている場合に、サービスデスクスタッフやスーパーバイザに警告を行うためのメカニズムです。

チケットが特定の基準を満たすと、指定されたグループに対し、チケットが無視されていることを警告するEメールが送信されます。これにより、サービスレベル契約を監視し、チケットが適切に処理されていない場合に、適切なスタッフメンバーに自動的に通知できるようになります。

エスカレーションEメールは、次の条件を満たしたチケットについて、エスカレーション時間の終了時に送信されます。

- 「**未解決**」状態である。
- 優先度にエスカレーション時間が含まれている。

デフォルトのチケットのステータス、優先度、およびエスカレーションの設定について、以下に例を挙げます。これらの設定は、ステータスと状態が「**オープン**」で優先度が「**高**」のチケットが30分経過しても処理されない場合にエスカレーションEメールを送信するよう、サービスデスクに指示します。

次のことを行えます。

- 他の優先度を持つチケットについて、エスカレーションEメールを設定する。
- エスカレーション時間の制限を変更する。
- エスカレーションEメールの受信者を決定する。
- 必要に応じてEメールフォームを変更する。

注: チケットのエスカレーションとサービスレベル契約は、2つの別個の通知アクティビティです。チケットのエスカレーション通知はチケットが開かれていた期間に基づきますが、サービスレベル契約通知はチケットの期日に基づきます。チケットのエスカレーションでは、営業時間と休業日は考慮されません。

チケットの状態について

サービスデスクチケットの状態では、チケットの現在の状態が識別されます。状態には、「**オープン**」、「**停止済み**」、および「**クローズ**」があります。

チケットは、「**未解決**」状態の場合のみ、エスカレーションできます。この要件を設定することはできません。

注: デフォルト設定を使用して、チケットをエスカレーションするには、チケットの優先度が「**高**」で、ステータスが「**未解決**」である必要があります。

エスカレーション時間制限について

サービスデスクチケットに「**オープン**」状態が割り当てられるとすぐに、タイマーがエスカレーション時間制限に向けてのカウントを開始します。

チケットを変更すると、タイマーがリセットされます。タイマーが時間切れになると、エスカレーションEメールが送信され、再度タイマーが開始されます。チケットが変更されていない場合は、タイマーがリセットされます。エスカレーション時間制限に達するたびに、エスカレーションEメールが送信されます。デフォルトでは、エスカレーションEメールは、チケットが変更されるまで30分ごとに送信されます。

エスカレーションについて

サービスデスクチケットがエスカレーションされると、キュー設定で指定された受信者にEメールメッセージが送信されます。

エスカレーションEメールの送信先は、次から選択できます。

- チケット所有者
- チケット送信者
- 問題解決のためのテクニカルスキルを持つユーザー
- 問題解決のために投じられるリソースを調整する権限を持つユーザー

エスカレーションEメールメッセージの受信者は、キューの詳細 ページの イベント発生時にEメールを送信 セクション、および各チケットの **カテゴリCC** リストによって決定されます。

チケットのエスカレーション設定の変更

サービスデスクチケットのエスカレーション設定では、チケットの優先度やステータスが変更された場合に実行されるアクションが決定されます。

エスカレーション E メールは、優先度が **高** で、ステータスが **新規作成** から **Opened**（ 未解決 ）に変更されたチケットに対して送信されます。チケット所有者が30分以内にチケットに応答しない場合は、エスカレーション設定を変更して、そのチケットをエスカレーション対象にすることができます。

エスカレーションEメール受信者のリストの変更

必要に応じて、サービスデスクチケットのエスカレーションに使用するEメール受信者を変更できます。

デフォルト設定を使用している場合は、チケットステータスを「**新規作成**」から「**未解決**」に変更します。デフォルト設定を変更した場合は、ステータスの少なくとも1つが「**オープン**」状態であることを確認し、そのステータスをチケットに割り当てます。詳細については、「チケット設定の構成」を参照してください。

（オプション）デフォルトでチケットに「**オープン**」状態を割り当てたり、チケット所有者が所有権を得た時点でチケット所有者によるチケットステータスの変更を必要とするポリシーを作成したりできます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの名前をクリックします。
2. イベント発生時にEメールを送信 セクションで、該当するチェックボックスをオンにし、所有者、送信者、承認者、チケットCCメンバー、およびカテゴリCCメンバーをエスカレーションEメール受信者として追加します。
3. **保存** をクリックします。

エスカレーション時間の制限の変更

必要に応じて、チケットのエスカレーションに使用する時間制限を変更できます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの名前をクリックします。
2. チケットのデフォルト セクションで、**これらの値のカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. Priority Values（優先度値）セクションで、エスカレーション時間制限を変更する行の **編集** ボタンをクリックします（ をクリックします。
4. その行で **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

デフォルトのエスカレーションEメールメッセージの変更

サービスデスクチケットがエスカレーションされた場合に自動的に送信されるEメールメッセージのテキストを変更できます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。

d. キューの名前をクリックします。

2. イベント発生時にEメールを送信 セクションで、**Eメールのカスタマイズ** をクリックして、サービスデスクEメール通知 ページを表示します。
3. 必要に応じて、「エスカレーションされたチケット」メッセージを編集します。
4. **保存** をクリックします。

Ticket Escalation（チケットのエスカレーション）メッセージの詳細については、EメールトリガとEメールテンプレートの設定を参照してください。

サービスデスクプロセスの使用

サービスデスクプロセスとは、事前に定義された順序で表示されるチケットの集合です。これにより、複数の手順やアクティビティを完了する必要があるタスクを追跡できます。

例えば、新入社員向けにシステムや機器を準備する場合にどのようなタスクが必要になるかを考えてみます。

- オフィススペースおよび事務什器の要件を明確にする。
- 電話サービスを設定する。
- デバイスおよびソフトウェアを入手する。
- ネットワーク資格情報を設定する。
- 必要な雇用に伴う事務手続きを完了する。

これらの必要なタスクが子アクティビティとして含まれているプロセステンプレートを作成できます。その後、そのプロセステンプレートに基づいてチケットを作成すると、プロセスの各ステージで必要なすべてのタスクに対して子チケットが自動的に作成されます。

サービスデスクプロセスを設定するには、プロセステンプレートの追加、編集、および有効化を参照してください。

プロセステンプレートの追加、編集、および有効化

プロセステンプレートをサービスデスクに追加できます。プロセステンプレートを有効にして、そのプロセスに基づいてチケットを作成するためにエンドユーザーが使用できるようにするには、少なくとも1つの親チケットが含まれている必要があります。

1. サービスデスクの プロセステンプレートの作成 ウィザードに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **プロセステンプレート** をクリックします。
    d. 新しいプロセステンプレートを作成するには、プロセステンプレート ページで **アクションを選択 > 新規作成** の順に選択します。
    e. 既存のプロセステンプレートを編集またはコピーするには、プロセステンプレート ページでプロセステンプレート名をクリックします。

    プロセステンプレートの作成 ウィザードが表示され、同時に プロセステンプレートの定義 ページが開きます。
2. 既存のプロセステンプレートをコピーするには、プロセステンプレートの定義 ページで **複製** をクリックします。

    複製されたプロセステンプレートのコピーが表示されます。複製されたプロセステンプレートが無効になっている場合、他のすべてのオプションは、元のテンプレートと同じです。複製されたバージョンの更新が終了したら、発行のオプション ページで **有効** オプションを選択できます。
3. プロセステンプレートの定義 ページで、次の情報を指定します。

オプション	説明
名前	プロセス全体を説明する名前（例:「新規雇用」、「解雇」、「事務所移転」）。
説明	プロセスの説明。説明が長くなると、このフィールドは入力するときに自動的に拡張されます。
HTML/Markdown	説明にリッチテキストが含まれているかどうかを示します。一部のプロセスの説明は他のプロセスの説明より長い場合があります。そのため、特定のテキスト要素をフォーマットすることで全体的な読みやすさを向上させ、エンドユーザーがプロセスをよく理解するのに役立ちます。Markdownプロジェクト構文を使用して、説明 ボックスの内容をフォーマットできます。例： 処理前の確認事項： 新入社員採用プロセスが人事部門で 完了していることを確認します。 新入社員の社員番号がすでに用意 されているか確認します 社員番号がない場合は、 人事部門に問い合わせます。 Markdown構文の詳細については、http://daringfireball.net/projects/markdown/syntaxを参照してください。
プロセスタイプ	プロセスのタイプ。デフォルトのインストールでは、サービスリクエスト と ソフトウェアリクエスト：承認が必要 プロセスタイプだけが含まれます。必要に応じて、新しいプロセスタイプを作成できます。例えば、特定のアプリケーション、またはアプリケーションのグループにアクセスするためのプロセスタイプを作成できます。詳細については、「プロセスタイプの定義」を参照してください。
作成時に親チケットから子チケットがフィールドを継承できるようにする	同じキューに属する親チケットからフィールド値を継承するためのオプションを子チケットで有効にする場合は、このオプションを選択します。子チケットの作成時に親チケットに存在する値のみを継承できます。関連付けられた親チケットフィールドの値に対するその後の変更は、このオプションが選択されている子チケットには反映されません。継承されたフィールド値は、各チケットを設定するときにチケットごとに指定されます。

保存して続行 をクリックします。

4. プロセステンプレートの作成 ウィザードに表示される 親チケット ページで、親チケットをこのプロセステンプレートに関連付けます。
    a. **ソフトウェアリクエスト：承認が必要プロセスタイプのみ。**このプロセスタイプは、1 つまたは複数の承認を必要とするユーザーダウンロードを設定するために使用できる特別なプロセステン

プレートを作成するためのものです。選択した場合、親チケットはデフォルトでこのプロセスタイプから作成されます。

- チケットの内容を表示または編集するには、**ソフトウェアリクエスト：承認が必要** をクリックします。
- このタイプのチケットでは、タイトル、概要、デバイス、または 送信者 フィールドは編集できません。これらのフィールドには、プロセスを開始したリクエストの値が入力されます。
- このプロセスタイプの承認は必須です。

b. このプロセステンプレートに関連付ける親チケットを含むキューを選択し、**親チケットの追加** をクリックします。

c. 新しい親チケット ページで、次のプロセステンプレートの新しい親チケットを作成します。

- キューが複数ある場合は、1つのキューを選択します。親チケットおよび子チケットは、それぞれ異なるキューに配置することができます。複数のキューがない場合、キュー選択はできません。
- 1 つ以上のチケットテンプレートが関連付けられているキューを選択した場合、チケットテンプレートを選択します。
- フィールドのほとんどは、チケットの詳細 ページのフィールドと同じです。詳細については、「管理者コンソールのチケットページからのチケット作成」を参照してください。親チケットで、子チケットと同じカテゴリ、所有者などを使用する必要はありません。
- Due Date Offset（期日オフセット）は子チケットに関する作業を完了するために必要な時間で、この時間はチケットの期日の計算に使用されます。例えば、Due Date Offset（期日オフセット）を 4 日に設定した場合、子チケットの期日はチケットの作成日の 4 日後にオフセットされます。期日は適用されませんが、期日が経過した場合、チケットは チケット リストで期限超過とマーク付けされ、レポートに期限超過と表示されます。

チケットの作成についての追加情報は、管理者コンソールのチケットページからのチケット作成を参照してください。

d. **保存** をクリックして、プロセステンプレートの作成 ウィザードに戻ります。

5. （**オプション**）プロセスに親チケットを追加した後、そのプロセスの子チケットまたはアクティビティを設定できます。子チケットは、異なるキューに登録することも、異なるステージに割り当てることもできます。

a. プロセステンプレートの作成 ウィザードに表示される 親チケット ページの 子チケット で、子チケットに関連づけられたキューを選択します。

b. 選択したキューに 1 つ以上のチケットテンプレートが関連付けられている場合、チケットテンプレートを選択します。

キューに 1 つ以上のテンプレートが含まれている際に使用するテンプレートを指定しない場合、デフォルトのキューテンプレートが選択されます。

c. **子チケットの追加** をクリックします。

このプロセステンプレートに基づいたチケットの作成時に、ステージ1の子チケットが自動的に作成されます（承認され要件が満たされた後（必要な場合））。ステージ1での最後の子チケットがクローズされると、次のステージに定義されている子チケットが作成されます。

d. 子チケット ページで、以下の手順を実行して当該のプロセステンプレートの新しい子チケットを作成します。

- **ステージ**：チケットを作成するプロセスのステージ（1、2、3 など）。必要に応じて、複数のチケットを同じステージに割り当てることができます。例えば、最初のステージが新入社員の機器とサプライを入手することである場合、注文するデバイス、オフィス機器、およびサプライにそれぞれ別個の子チケットを用意し、そのすべてをステージ 1 に割り当てることができます。

プロセスチケットを作成すると、ステージ 1 に割り当てられたすべての子チケットが自動的に作成されます。すべてのステージ 1 チケットが終了す

るとステージ 2 チケットが作成され、すべてのステージ 2 チケットが終了するとステージ 3 チケットが作成され、以下同様に続きます。

- **タイトル**：子チケットのタイトル。
- **概要**：この子チケットに関連付けられているタスクの説明。
- **カテゴリ**、**所有者**、および **期日**：これらの値は、親チケットのものと一致する必要はありません。

プロセステンプレートの定義 ページで **作成時に親チケットから子チケットがフィールドを継承できるようにする** を選択した場合、**継承** チェックボックスが各フィールドに表示され、親チケットのこのフィールドの現在の値を入力できます。詳細については、ステップ「3」を参照してください。

チケットの作成についての追加情報は、管理者コンソールのチケットページからのチケット作成を参照してください。

e. **保存** をクリックして、プロセステンプレートの作成 ウィザードに戻ります。

6. このプロセステンプレートで作成したチケットで承認が必要な場合、表示される 承認 ページで、**このプロセスを開始するには、1件以上の承認が必要です。** を選択し、下の表にリストされた情報を指定します。

ソフトウェアリクエスト：承認が必要 プロセスタイプを選択した場合、このチェックボックスはデフォルトでオンになっており、オフにすることはできません。このプロセスタイプの承認は必須です。

承認を必要とするプロセスに対してプロセスチケットを作成した場合、すべての承認を受信するまで子チケットが作成されません。複数の承認ステージがある場合、承認を要求するEメールが最初にステップ1の承認者に送信されます。ステップ2の承認者は、すべてのステップ1の承認要件を満たされた後にのみをEメールを受信します。

承認者は、E メールトークンを使用して E メールでプロセスチケットを承認または拒否できます。例えば、必要に応じて、次の構文例を使用します。

- E メールでチケットを承認するには：

  @approval = 承認
  @approval_note = このリクエストは E メールで承認されます

- E メールでチケットを拒否するには：

  @approval = 拒否
  @approval_note = このリクエストは E メールで拒否されます

これらのトークンの詳細については、「Eメールを使用した、チケット承認フィールドの変更」を参照してください。

オプション	説明
承認ステップ	
承認ステップ1	1 人または複数の承認者。必要に応じて、承認者のリストを編集できます。 • **新しいプロセステンプレート**。このフィールドは空白で表示されます。 • **既存のプロセステンプレート**。1 人または複数の承認者がプロセステンプレートですでに定義されている場合、このフィールドにリストされます。 **注:** 送信者のマネージャがデフォルトで選択されて表示されます。
いずれかの承認が必要です	少なくとも1件のチケット承認が必要です。

オプション	説明
すべての承認が必要です	すべてのチケット承認が必要です。
すべて削除	リストからすべての承認者を削除します。
別のステップを追加	承認ステップを追加します。
承認のオプション	
承認タイムアウト期間	各承認者がチケットを承認または拒否する必要がある期間。期間は、このプロセステンプレートに基づいています。 承認タイムアウト期間は、複数の承認ステップにまたがることはありません。例えば、プロセスにが2つの承認ステップがあり、承認タイムアウト期間は8時間として定義されている場合です。 • ステップ1の承認者には、承認するまで8時間の期間があります。 • ステップ1のすべての承認が受信されたときに、承認要求に基づいてステップ2の承認者に処理のために8時間が与えられます。
承認通知の繰り返し	承認が保留中のチケットについて、各承認者に通知を送る頻度を示します。 この値をゼロ「0」のままにすると、通知は1度だけ送信され繰り返し送信されることはありません。
承認のタイムアウトおよび通知の頻度に、営業日および休業日を使用する	営業時間を使用して承認期間が計算されることを示します。
承認のオーバーライド	承認をオーバーライドすると、保留中の承認を待たずにプロセスチケットを次の処理に移行できます。オーバーライドした後、すべての保留中の承認がクローズされ、チケット履歴が書き込まれ、Eメール通知に定義されているように、承認は受信済みですというEメールが承認者に送信されます。
なし	承認のオーバーライドは許可されません。
すべての管理者にオーバーライドを許可する	管理者のアクセス権限を持つすべてのユーザーが承認をオーバーライドできます。
ラベルの指定	指定するラベルのグループに属するすべてのユーザーが承認をオーバーライドできます。

保存して続行 をクリックします。

7. 表示される E メール通知 ページで、チケットのライフサイクルの各ステージでの E メール通知の受信者を選択します。表示されたリンクをクリックして、サービスデスクキューE メール設定 ページでこれらのオプションを設定します。詳細については、「キュー固有の E メールの設定」を参照してください。

保存して続行 をクリックします。

8. 表示される 定期チケットのスケジュール ページで、チケットが作成される頻度を指定します。これは、システムの正常性の確認や定期的なファイルログの削除など、定期的にチケットを作成する場合に便利です。

オプション	説明
なし	特定の日付や時間ではなく、イベントと連携して実行します。
n 時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（ * ）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（ , ）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（ - ）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（ / ）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタリスク（ * ）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。

オプション	説明
	例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクが一覧表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

9. 表示される 発行のオプション ページで、必要に応じて、次のいずれかの発行のオプションを選択します。

オプション	説明
有効	プロセスを使用してプロセスチケットを作成するには、そのプロセスを有効にする必要があります。ユーザーがこのプロセステンプレートからチケットを作成できるようにする場合は、このチェックボックスを選択します。
所有者以外のユーザーから承認情報を隠す	ユーザーがチケットを所有して承認情報を表示しないようにする場合は、このオプションを選択します。
送信者からプロセスの手順を非表示にする	親のチケットの詳細ページでプロセスの手順（子チケット）を送信者に表示したくない場合は、このオプションを選択します。
すべてのユーザーにプロセスを表示	このオプションは、デフォルトで選択されています。エンドユーザーがこのプロセスにアクセスするのを制限する場合は、このオプションをクリアします。または、アクセスを付与するグループに関連付けられたラベルを選択します。
プロセスの説明ページを新しいプロセスリクエストを作成するときに表示	このプロセステンプレートに基づいて新しいチケットを作成するときに、プロセスの説明ページに表示する場合は、このオプションを選択します。
プロセスステータスワークフローをチケットステータスの代わりに使用	プロセステンプレートで利用可能な承認機能および通知機能を利用する場合は、このオプションを選択する必要があります。承認または通知をすでに設定している場合は、このオプションはデフォルトで選択されてクリアできません。プロセスステータスのワークフローの使用を選択すると、親チケットは各種プロセス特定のステータス（保留中の承認、承認が拒否されました、承認は期限切れです、進行中、プロセス完了）を自動的に移行します。

オプション	説明
	このオプションを選択しないでチケットステータスワークフローを代わりに継続して使用すること選択した場合、必要な承認機能と通知機能を実現するためのカスタムチケットルールを作成する必要があります。 プロセスステータスのワークフローを使用する場合は、ステータス フィールドは、関連キューに表示されるように設定されていても、チケットの詳細ページに表示されません。子チケットの ステータス フィールドは引き続き表示されます。
親チケットのクローズ済みステータス	このプロセスに関連付けられている親チケットがクローズされるときに使用するステータスを選択します。 最後の子アクティビティがクローズされると、親チケットは自動的にクローズしそのステータスがこのフィールドに表示されます。

終了 をクリックします。

プロセステンプレートの作成 ウィザードが閉じ、新規作成または更新したプロセステンプレートが プロセステンプレート ページに表示されます。

プロセスタイプの定義

デフォルトのインストールでは、サービスリクエスト と ソフトウェアリクエスト：承認が必要 プロセスタイプだけが含まれます。必要に応じて、新しいプロセスタイプを作成できます。例えば、特定のアプリケーション、またはアプリケーションのグループにアクセスするためのプロセスタイプを作成できます。

ソフトウェアリクエスト：承認が必要 プロセスタイプは、1 つまたは複数の承認を必要とするユーザーダウンロードを設定するために使用できる特別なプロセステンプレートを作成するためのものです。

親チケットを作成します。

1. サービスデスクの Process Detail（プロセスの詳細）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルの**プロセステンプレート** で、**プロセスタイプの定義** をクリックします。
2. 新しいプロセスタイプを追加するには、右上隅で ＋ をクリックします。表示されるテキストボックスで、プロセスタイプ名を入力し、**保存** をクリックします。
3. 既存のプロセスの名前を変更するには、編集するプロセスタイプを含む行で、✎ をクリックします。表示されるテキストボックスで、新しいプロセスタイプ名を入力し、**保存** をクリックします。

関連するタスクを管理するためのプロセスチケットの作成

キューにプロセステンプレートを追加し、有効にした場合は、プロセスチケットを作成して関連するタスクのセット（新入社員向けにシステムを設定するために必要なタスクなど）をグループとして管理できます。

プロセステンプレートを追加または有効にしました。詳細については、「プロセステンプレートの追加、編集、および有効化」を参照してください。

1. サービスデスクの 新規チケット ページに移動します。

a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
c. **新規作成 > プロセスからの新規チケット > プロセス名** の順に選択します。

新規チケット ページが表示されます。プロセスの各ステージに関連するアクティビティが プロセス情報 セクションに表示されます。

2. 必要なチケット情報を入力します。詳細については、「管理者コンソールのチケットページからのチケット作成」を参照してください。
3. 次のいずれかを実行します。
   - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
   - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
   - **キャンセル** をクリックして、チケットの変更を破棄します。

   他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

詳細については、「管理者コンソールのチケットページからのチケット作成」を参照してください。プロセスチケットが作成され、ステージ 1 に割り当てられたアクティビティの子チケットが自動的に作成されます。すべてのステージ 1 チケットが終了すると、ステージ 2 子チケットが作成され、以下同様に続きます。プロセスの承認が定義されている場合、子チケットは、プロセスチケットの承認の受領後に作成されます。

E メールでプロセスチケットを作成する

既存のプロセステンプレートのプロセスチケットを E メールですばやく作成できます。

E メールでプロセスチケットを作成する前に、次の情報を取得する必要があります。

- プロセス名
- プロセステンプレートの親チケットに関連付けられているチケットキューの E メールアドレス

1. 電子メールアカウントにログインして、新しい電子メールメッセージを作成します。
2. E メールの受信者行に、プロセステンプレートの親チケットに関連付けられているチケットキューの E メールアドレスを入力します。
3. E メールの件名の行で、プロセステンプレート名を中かっこで囲んで指定します。そのセグメントの後に追加したテキストがチケットタイトルに追加されます。例：{新規雇用} Jane Smith。
4. E メール本文はオプションです。E メール本文に追加したコンテンツは、チケットの説明に追加されます。
5. E メールを送信します。
6. サービスデスクの チケット リストページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
7. 新しく作成されたチケットを探し、チケットタイトルをクリックします。
8. 適用可能な変更を行います。

   チケットページの編集の詳細については、管理者コンソールのチケットページからのチケット作成を参照してください。

プロセス情報の表示

関連タスクセットを管理するためにプロセスチケットを作成している場合、これらのチケットの関連プロセス情報を表示できます。

プロセステンプレートに基づいてチケットを作成しました。詳細については、「関連するタスクを管理するためのプロセスチケットの作成」を参照してください。

1. サービスデスクの チケット ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
    c. チケットのタイトルをクリックします。

    チケット ページが表示されます。プロセスの各ステージに関連するアクティビティが プロセス情報 セクションに表示されます。このセクションに表示される情報レベルは、プロセステンプレートの作成 ウィザードの 発行 ページの設定によって決まります。例えば、関連するプロセステンプレートで承認とプロセスに関する情報を表示するように設定されている場合は、このセクションに表示されます。このウィザードの詳細については、プロセステンプレートの追加、編集、および有効化を参照してください。
2. 次のいずれかを実行します。
    - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
    - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
    - **キャンセル** をクリックして、チケットの変更を破棄します。

    他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（ 更新通知 ）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

プロセスチケットが作成され、ステージ 1 に割り当てられたアクティビティの子チケットが自動的に作成されます。すべてのステージ 1 チケットが終了すると、ステージ 2 子チケットが作成され、以下同様に続きます。

プロセスチケットのキャンセルまたは完了

関連タスクセットを管理するためにプロセスチケットを作成している場合、これらのチケットの関連プロセス情報を表示できます。プロセスの所有者または送信者のいずれかを指定することで、プロセスをキャンセル済みとしてマークできます。これは、所有者のみが完了としてマークできます。

プロセステンプレートに基づいて親チケットを作成しました。詳細については、「関連するタスクを管理するためのプロセスチケットの作成」を参照してください。

1. サービスデスクの チケット ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
    c. プロセスの親チケットのタイトルをクリックします。

チケット ページが表示されます。

2. 次のいずれかを実行します。
   - プロセスチケットをキャンセルするには、**アクションを選択 > プロセスのキャンセル** を選択します。
   - プロセスチケットを完了するには、**アクションを選択 > プロセスの完了** を選択します。
3. 表示されるダイアログボックスで、プロセスチケットの完了またはキャンセルを確定します。
4. 次のいずれかを実行します。
   - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
   - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
   - **キャンセル** をクリックして、チケットの変更を破棄します。

   他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

プロセステンプレートの削除

サービスデスクの プロセス リストを使用して、プロセスを削除することができます。特定のプロセスのチケットが存在する場合は、プロセスを無効としてのみマークできます。プロセスを削除するには、このプロセスを使用して作成したチケットを最初に削除する必要があります。

1. サービスデスクの プロセス リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **プロセステンプレート** をクリックします。
2. 1つ、または複数のプロセステンプレートを選択し、**アクションの選択 > 削除** を選択します。
3. 確認ページで、**はい** をクリックして選択したプロセステンプレートを削除します。

プロセスチケットから通常のチケットへの変換

必要に応じて、サービスデスクプロセスチケットを通常のチケットに変換できます。この変換は、チケットがプロセスチケットとして誤って作成され、そのチケットにはプロセスのどのステップも必要ない場合に便利です。

プロセスチケットの詳細については、サービスデスクプロセスの使用を参照してください。

1. サービスデスクの チケットの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
   c. チケットのタイトルをクリックします。
2. **アクションの選択 > プロセスProcess Nameを通常のチケットに変換** を選択します。

注: このメニューは、選択したチケットがプロセスから作成されたものである場合にのみ使用可能です。

確認ウィンドウが表示されます。

3. **はい** をクリックして、プロセスから通常のチケットへの変換を続行します。
4. 次のいずれかを実行します。
   - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
   - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
   - **キャンセル** をクリックして、チケットの変更を破棄します。

   他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

通常のチケットからプロセスチケットへの変換

通常のサービスデスクチケットをプロセスチケットに変換できます。この変換は、プロセス関連のチケットが E メールを通じて作成される場合に有益です。E メールを通じて作成されたチケットは常に単一のチケットとして作成されるからです。

また、プロセスをまだ理解していないため、またはプロセスにアクセスできないために、ユーザーが単一のチケットを作成する場合もあります。通常チケットをプロセスチケットに変更すると、管理者およびチケット所有者は、チケットが元々プロセスチケットとして送信されなかった場合でも、プロセスを利用できるようになります。プロセスチケットの詳細については、サービスデスクプロセスの使用を参照してください。

1. サービスデスクの チケットの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
   c. チケットのタイトルをクリックします。
2. **アクションの選択 > プロセス > Process Nameに変換** を選択します。

   確認ウィンドウが表示されます。
3. **はい** をクリックして、チケットからプロセスへの変換を続行します。
4. 次のいずれかを実行します。
   - **保存** をクリックしてチケットを保存し、チケット リストに戻ります。
   - **変更の適用** をクリックしてチケットを保存し、編集を続行します。
   - **キャンセル** をクリックして、チケットの変更を破棄します。

   他のユーザーが同時にチケットを変更した場合は、チケットの所有者または管理者に Update Notification（更新通知）ダイアログが表示されます。ただし、このダイアログがキューに対して有効化されている場合に限ります。このダイアログは、管理者およびチケットの所有者のみに表示されます。その他のユーザーには表示されません。管理者は、キューごとに個別にコンフリクト警告メッセージを有効または無効にすることができます。詳細については、「コンフリクト警告の有効化または無効化」を参照してください。

チケットルールの使用

チケットルールでは、サービスデスクチケットでクエリを実行し、返されたチケットのリストに対してアクションを実行できます。

例えばチケットルールを使用すると、所有者以外の誰かがチケットに応答した場合に、チケットのステータスを「クローズ」から「再オープン」に自動で変更することができます。デフォルトのチケットルールは4つあり、必要な数だけカスタムチケットルールを追加できます。

システムチケットルールの使用と設定

サービスデスク環境のニーズに合わせてシステムチケットルールを使用および設定できます。

オプションは次の通りです。

- デフォルトのチケットルールを有効にして、デフォルト設定を使用する
- カスタムチケットルールの作成
- カスタムチケットルールを複製する
- カスタムチケットルールを削除する
- キュー間でチケットルールを移動する

システムチケットルールの理解とカスタマイズ

指定した基準が満たされると、システムチケットルールによってサービスデスクチケットのステータスが自動的に変更されるか、Eメール通知が送信されます。

次の表に、システムチケットルールの名前、動作、使用法を示します。

チケットルール	デフォルト動作	コピーし、次の用途に使用可能
WaitingOverdue	休止状態が7日間続いているチケットを、期限超過ステータスに変更します。	設定可能な期間待機した後、チケットステータスを変更します。ステータスの変更が行われた場合に、Eメールメッセージを送信することもできます。
OverdueClose	7日間に渡り、何のアクションも行われず期限超過状態だったチケットを閉じます。	設定可能な期間待機した後、チケットステータスを変更します。ステータスの変更が行われた場合に、Eメールメッセージを送信することもできます。
EmailOnClose	チケットがクローズされたら、Eメールメッセージをチケット送信者に送信します。クローズチケットに対して応答が必要となるのは、そのチケットが再度開かれる場合のみです。	チケットがクローズされたら、Eメールメッセージを送信します。
CustomerResponded	ユーザーが、お客様のアクションを待機中のチケットに対応したときに、チケットを応答済みステータスに移動します。	未解決のチケットのステータスを変更し、それが更新された場合はEメールメッセージを送信します。
ReopenTicket	終了チケットに対して所有者以外の誰かが応答した場合は、そのチケットを再度開きます。	終了チケットが再び開かれた場合、このチケットルールによってチケットのステータスが変更され、Eメールメッセージが送信されることがあります。

カスタムチケットルールの作成

必要に応じて、サービスデスクチケットのカスタムチケットルールを作成することができます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの名前をクリックします。
2. ページの一番下にある チケットルール セクションで、**カスタマイズ** をクリックして、チケットルールページを表示します。
3. **アクションの選択 > 新規作成（ウィザード）** を選択して、チケットルールの定義 パネルを表示します。
4. カスタムチケットルールの対象チケットを選択するために必要な条件を入力します。例：

    優先度 | = | 中
5. **テスト** をクリックして、基準に一致するチケットを表示します。
6. **次へ** をクリックします。
7. 変更する値を選択します。例：

    優先度 | 変更後の値 | 高
8. **完了** をクリックして、チケットルールの詳細 ページを表示します。
9. 次の情報を入力します。

重要: **編集による影響が不明な場合は、SQLクエリを編集しないでください。不正なSQLステートメントによって、アプライアンスのパフォーマンスが低下する可能性があります。**

オプション	説明
名前	チケットルールの名前。
優先順位	評価優先順位レベルを指定する数字。チケットルールは、指定した評価優先順位に従って実行されます。数字の小さいものから順に実行されます。
キュー	（読み取り専用）チケットが属するキューの名前。
説明	任意の追加情報を入力します。
有効	チケットルールは使用可能です。有効になっている場合にのみ、チケットルールが実行されます。
Select SQL	必要に応じてSQLクエリを修正します。クエリは、チケットルール ページで指定した条件に基づき、チケットルールウィザードによって生成されます。このクエリによって、**更新クエリ**を実行する一連のチケットIDが返されます。 指定した頻度に従って**選択クエリ**が実行されます。 クエリの結果を表示するには、**チケット検索結果の表示** をクリックします。

オプション	説明
	重要: 編集による影響が不明な場合は、SQL クエリを編集しないでください。不正なSQL ステートメントによって、アプライアンスのパフォーマンスが低下する可能性があります。
Eメールで結果を送信	選択クエリの結果を、指定したEメールアドレスに送信します。選択クエリによって返されたすべての列は、Eメールに含まれます。 E メール フィールドに E メールアドレスを入力します。複数のアドレスは、コンマで区切ります。
コメントをチケットに追加	選択クエリによって返される各チケットにコメントを追加します。このアクションは、以降で指定される更新クエリで、その情報をログに記録しないでチケットが更新される場合に役立ちます。例えば、「チケットルール：優先度「高」への引き上げがトリガされます」などのメッセージを追加します。このメッセージを追加することで、どのチケットが変更されたかが分かります。 コメント フィールドに任意のコメントを入力します。
各受信者に E メールでクエリ結果を送信	選択クエリによって返された E メールアドレスにテキストを送信します。E メール 列の選択クエリによって返された各 E メールアドレスに、E メールが送信されます。 変数は、E メールの件名行か本文で評価されます。$Titleや$due_dateなどの文字列は、それぞれ TITLE 列と DUE_DATE 列の値で置き換えられます。選択クエリによって返された列はすべて、同じ方法で置き換え可能です。 チケットルールウィザードによって生成される SQL では、使用可能な値として **OWNER_**、**SUBMITTER_**、および **CC_LIST** が提供されます。 件名 フィールドに件名を入力します。 E メール フィールドに、Eメール列の名前を入力します (例：「OWNER_」)。E メールは、この E メール 列の選択クエリによって返された各 E メールアドレスに送信されます。 E メール本文 フィールドに、E メールメッセージを入力します。
更新クエリを実行	更新クエリ フィールドの結果を入力として使用し、別のデータベースクエリを実行します。 このフィールドでは、選択クエリによって返されたチケットのコンマ区切りリストを入力として使用し、別のSQL UPDATEステートメントを実行することができます。例えば、「update HD_TICKET set TITLE = 'changed' where HD_TICKET.ID in (<TICKET_IDS>)」は、「update HD_TICKET set

オプション	説明
	TITLE = 'changed' where HD_TICKET.ID in (1,2,3)」になります。 必要に応じてSQLクエリを修正します。クエリは、チケットルール ページで指定した条件に基づき、チケットルールウィザードによって生成されます。このクエリは、**選択クエリ**によって選択されたチケットに対して実行されます。 指定した頻度に従って更新クエリ が実行されます。 **重要: 編集による影響が不明な場合は、SQLクエリを編集しないでください。不正なSQLステートメントによって、アプライアンスのパフォーマンスが低下する可能性があります。**
期日の再計算	このオプションは、更新クエリに既存のチケットの優先度の更新が含まれる場合にのみ選択します。このオプションを選択すると、チケットルールによって設定された新しい優先度に基づいて期日が再計算されます。 **注:** いずれかのチケットに手動で上書きされた期日が含まれる場合、この期日はチケットルールによって上書きされません。
前回の実行ログ	最後のクエリの結果（障害やエラーを含む）。これらの結果は、チケットルールを実行するたびに更新されます。
頻度	チケットルールを実行する間隔。 **注:** チケット保存時 に実行されるチケットルールは、単一のチケットに対して実行され、単一のイベントをトリガするよう設計される必要があります。スケジュールに従って実行されるチケットルールは、複数のチケットに対して実行することが可能で、複数のイベントをトリガすることができます。
次回実行	チケットルールの次回の実行を予定している日付と時刻。

10. **今すぐ実行** をクリックして、すぐにチケットルールを実行します。
11. **保存** をクリックします。

カスタムチケットルールの複製

カスタムチケットルールを複製すると、プロパティが新しいルールにコピーされます。既存のルールとほぼ同じルールを作成する場合、チケットルールを複製することで、ルールをゼロから作成するよりも素早く作成できます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
c. **設定** パネルで **キュー** をクリックします。
d. キューの名前をクリックします。

2. ページの一番下にある チケットルール セクションで、**カスタマイズ** をクリックして、チケットルール ページを表示します。
3. チケットルールを選択し、開きます。
4. ページの一番下で **複製** ボタンをクリックします。

   チケットルール ページに、新しいルールが表示されます。デフォルトの名前は、「**original_ruleのコピー**」です。
5. 必要に応じて、複製されたチケットルールの名前を変更します。

   チケットルールのフィールドの詳細については、カスタムチケットルールの作成を参照してください。

カスタムチケットルールの削除

必要に応じて、サービスデスクからカスタムチケットルールを削除できます。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの名前をクリックします。
2. ページの一番下にある チケットルール セクションで、**カスタマイズ** をクリックして、チケットルール ページを表示します。
3. 次のいずれかを実行します。
   - **チケットルールの隣のチェックボックスをオンにし、アクションの選択 > 削除 を選択します。**
   - **チケットルールの名前をクリックし、**チケットルールの詳細 **ページで 削除 をクリックします。**
4. **はい** をクリックして確定します。

キュー間でのチケットルールの移動

サービスデスクチケットキューが複数ある場合は、必要に応じて、キュー間でチケットルールを移動できます。チケットルールを複数のキューで使用する場合は、ルールをコピーしてから、必要な変更を加えることができます。

1. サービスデスクの キュー リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
2. 移動するチケットルールが含まれるキューをクリックします。

   キュー詳細 ページが表示されます。
3. ページの一番下にある チケットルール セクションで、**カスタマイズ** をクリックして、チケットルール ページを表示します。

ヒント: チケットルール ページでキュー間の移動を実行するには、右側の表の上部に表示される 特定基準で表示 ドロップダウンリストを使用します。

4. 該当するチケットルールのチェックボックスをオンにします。
5. **アクションの選択 > 移動 > Queue Name** を選択します。

チケットルールが、選択したキューに移動します。このルールは、現在のキューのルール一覧に表示されなくなります。

サービスデスクレポートの実行

必要に応じて、サービスデスクアイテムでレポート作成を実行できます。

アプライアンスには、サービスデスクデータに対応する事前設定済みのレポート機能のセットが用意されています。

1. レポート リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**レポート作成** をクリックして、**レポート** をクリックします。
2. 右側のリストの上部に表示される 特定基準で表示 ドロップダウンリストで、**サービスデスク** を選択します。

    レポート ページにサービスデスクレポートが表示されます。
3. レポートの生成 列で、レポートを実行するフォーマットタイプをクリックします。

注: レポートの詳細については、レポートについてを参照してください。

チケットのアーカイブ、復元、削除

チケットをアーカイブすると、チケットデータは物理的にトランザクションテーブルから移動されますが、チケットデータには引き続きアクセスできます。アーカイブを実行しても、チケットデータが永続的にアプライアンスから削除されるわけではありません。古いチケットをまだ参照することがある場合は、アーカイブが効果的です。

チケットをアーカイブした場合、チケットを手動で削除するか、キューで設定された日付制限に基づいて削除されないかぎり、チケットは引き続き使用できます。この制限により、チケットが誤って削除される可能性を抑えられます。

チケットの標準的なライフサイクルは、作成、解決、アーカイブ、削除という形で構成されています。また、アーカイブしたチケットの復元で説明するように、チケットを「復元」することもできます。チケットを復元すると、そのチケットデータを使用できるようにアーカイブテーブルからトランザクションテーブルへとデータが戻され、チケット タブで再度チケットデータを利用できるようになります。

チケットを削除すると、チケットデータが永続的にアプライアンスから削除されます。

チケットのアーカイブの有効化

サービスデスクのチケットアーカイブ、または組織コンポーネントが有効になっている場合は、選択した組織のサービスデスクのチケットアーカイブを有効にすることができます。

1. Service Desk Settings（ サービスデスクの設定 ） ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。

c. **設定** パネルで **設定** をクリックします。

2. チケットのアーカイブ セクションで、**有効** チェックボックスをオンにして、スケジュールオプションを表示します。
3. 次の設定を指定します。

注: スケジュールに基づいてチケットをアーカイブしない場合は、**今すぐ実行** をクリックして、チケットのアーカイブおよび削除を適宜実行します。このオプションは、アーカイブが構成されているキューすべてに影響します。**今すぐ実行** は各キューからも利用でき、対象のキューの設定を使用して、チケットのアーカイブおよび削除を実行します。

オプション	説明
__時間ごと	指定した間隔で実行します。
毎日 HH:MM から	毎日または特定曜日の指定した時間に実行します。
実行基準 n 日 / 毎月 / 特定月 HH:MM から	毎月または指定月の、同じ日の指定した時刻に実行します。
実行基準 n 週 / 毎月 / 特定月 HH:MM から	毎月または指定月の、指定の週の指定した時刻に実行します。
カスタム	カスタムスケジュールに従って実行します。 標準の5つのフィールドからなるcron形式を使用します（拡張cron形式はサポート対象外）。 * * * * * | | | | +??????????????????????????day of week (0-6)(Sun=0) | | | +??????????????????????????month (1-12) | | +??????????????????????????day of month (1-31) | +??????????????????????????hour (0-23) +??????????????????????????minute (0-59) 値の指定は次の要領で行います。 • **スペース（ ）**：各フィールドはスペースで区切ります。 • **アスタリスク（*）**：アスタリスクを使用して、値の範囲全体をフィールドに含めます。例えば、時のフィールドに指定したアスタリスクは、毎時を示します。 • **コンマ（,）**：フィールド内の複数の値はコンマで区切ります。例えば、曜日フィールドに指定した 0,6 は日曜日と土曜日を示します。 • **ハイフン（-）**：フィールド内の値の範囲をハイフンで示します。例えば、曜日のフィールドに指定した 1-5 は 1,2,3,4,5 と同じになり、月曜日から金曜日までを示します。 • **スラッシュ（/）**：アクションを繰り返す間隔をスラッシュで指定します。例えば、時のフィールドに指定した */3 は、0,3,6,9,12,15,18,21 と同じです。アスタ

オプション	説明
	リスク（*）は毎時を指定しますが、/3 は 3 で割り切れる時刻に指定を制限します。 例: • 15 * * * * 毎日の毎時の15分後に実行します。 • 0 22 * * * 毎日22:00に実行します。 • 0 0 1 1,6 * 1月1日と6月1日の00:00に実行します。 • 30 8,12 * * 1-5 平日の08:30と12:30に実行します。 • 0 2 */2 * * 1日おきに02:00に実行します。
タスクスケジュールの表示	タスクスケジュールを表示する場合にクリックします。タスクスケジュール ダイアログボックスに、スケジュールされたタスクのリストが表示されます。タスクの詳細を確認するにはタスクをクリックします。詳細については、「タスクスケジュールの表示」を参照してください。

4. 次のいずれかを実行します。
   - **今すぐ実行 をクリックして、アーカイブが設定されたすべてのキューについてただちに処理を実行します。詳細については、「選択したチケットのアーカイブ」を参照してください。**
   - **保存 をクリックします。**

     サービスデスクのチケットアーカイブ、または組織コンポーネントが有効になっている場合は、選択した組織のサービスデスクのチケットアーカイブが有効になります。ただし、アーカイブ対象のチケットを選択するには、キューを個別に設定する必要があります。詳細については、「キューのアーカイブ設定の構成」を参照してください。
     左のナビゲーションバーに サービスデスク > アーカイブ リンクが表示されます。

キューのアーカイブ設定の構成

チケットのアーカイブが有効になっている場合、各キューのアーカイブ設定を構成できます。

サービスデスクのチケットのアーカイブが有効になっています。チケットのアーカイブを有効化する方法については、チケットのアーカイブの有効化を参照してください。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの名前をクリックします。
2. Archive Preferences（アーカイブの基本設定）セクションで、チケットのアーカイブの設定を選択し、**設定** リンクをクリックしてチケットのアーカイブを有効にします。

   注: チケットのアーカイブがオフになっている場合は、チケットのアーカイブの有効化を参照してください。

オプション	説明
Archive closed tickets older than（次の期間を経過した終了チケットをアーカイブ）	アーカイブの対象となるチケットの期間。例えば、**3 か月** を選択した場合、チケットが閉じられてから 3 か月経過するとチケットはアーカイブされます。キュー内のチケットがアーカイブされないようにするには、**無効** を選択します。必要に応じて、アーカイブされたチケットをキューに復元できます。詳細については、「アーカイブしたチケットの復元」を参照してください。
Delete archived tickets older than（次の期間を経過したアーカイブチケットを削除）	アーカイブから永続的に削除される対象となるチケットの期間。例えば、**6 か月** を選択した場合、チケットがアーカイブされてから 6 か月経過すると、アーカイブされたチケットはアーカイブから削除されます。キュー内のチケットがアーカイブから削除されないようにするには、**無効** を選択します。削除されたチケットをキューに復元することはできません。

3. ページの一番下で **保存** をクリックします。
4. **今すぐ実行** をクリックし、アーカイブの基本設定 で指定した基準と合致するチケットをアーカイブして削除します。

選択したチケットのアーカイブ

サービスデスクチケットのアーカイブが有効になっている場合、選択したチケットを必要に応じてアーカイブできます。

サービスデスクのチケットのアーカイブが有効になっています。チケットのアーカイブを有効化する方法については、チケットのアーカイブの有効化を参照してください。

ヒント: 特定のチケットをアーカイブする場合や、チケットのアーカイブの有効化のように、スケジュールに基づいてアーカイブを実行するように設定しない場合は、アーカイブするチケットの選択機能が役立ちます。

1. サービスデスクの チケット リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
2. 1つまたは複数のチケットの隣のチェックボックスをオンにします。
3. **アクションの選択 > アーカイブ** を選択します。
4. 確認ダイアログで、**はい** をクリックします。
5. アーカイブしたチケットにアクセスするには、**サービスデスク > アーカイブ** をクリックした後、表示するチケットへのリンクをクリックします。

アーカイブしたチケットの復元

必要に応じて、アーカイブしたチケットをチケットキューに復元することができます。

1. サービスデスクの アーカイブチケット リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**アーカイブ** をクリックします。

2. 1つまたは複数のアーカイブチケットの隣のチェックボックスをオンにします。
3. **アクションの選択 > 復元** を選択し、**はい** をクリックして確定します。

選択したチケットがすぐに復元され、チケット タブに表示されます。

アーカイブチケットの削除

アーカイブチケットを削除して、サービスデスクから永続的に消去することができます。削除したチケットは復元できません。

1. サービスデスクの アーカイブチケット リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**アーカイブ** をクリックします。
2. 1つまたは複数のアーカイブチケットの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

選択したチケットが、すぐにアプライアンスから削除されます。

チケット削除の管理

デフォルトでは、サービスデスク管理者やチケット所有者であれば、キューからチケットを削除できます。必要に応じて、この設定を変更できます。キューが複数ある場合、それぞれのキューに異なる設定を行うことができます。

チケットの削除設定の構成

キューのサービスデスクチケット削除設定を構成することができます。キューが複数ある場合、それぞれのキューに異なる設定を構成することができます。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの名前をクリックします。
2. User Preferences（ ユーザー基本設定 ） セクションで、次のいずれかを実行します。
   - **管理者およびチケット所有者によるチケットの削除を禁止するには**、チケットの削除を許可 **チェックボックスをオフにします。**
   - **管理者およびチケット所有者によるチケットの削除を有効にするには**、チケットの削除を許可 **チェックボックスをオンにします。**
3. **保存** をクリックします。

チケットの削除

サービスデスクのキュー設定でチケットの削除が有効になっている場合、必要に応じてチケットを削除できます。

キューのチケットの削除が有効になっています。詳細については、「チケットの削除設定の構成」を参照してください。

1. サービスデスクの チケット リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
2. 1つまたは複数のチケットの隣のチェックボックスをオンにします。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

サービスデスクチケットキューの管理

デフォルトでは、サービスデスクのチケットキューは1つだけです。基本的には、キューが1つあれば十分に機能します。ただし、必要に応じてキューを追加、複製、および削除することができます。また、キュー内に 1 つ以上のチケットテンプレートを作成できます。キュー内に複数のテンプレートがある場合、デフォルトテンプレートとしてチケットテンプレートを 1 つ選択する必要があります。

サービスデスクチケットキューについて

サービスデスクチケットは、アプライアンスの 1 つ以上のキューに格納されます。ほとんどの組織の場合、キューは1つのみで十分ですが、必要に応じて追加のキューを作成および管理できます。

次の場合にはチケットキューが複数あると便利です。

- **要件の異なる、別々のチケットセットがある場合。**例えば、一般的なサービスデスクタスク（ デバイス関連の問題の解決など ）に対してチケットを使用し、保有車両に関する問題の追跡にもチケットを使用する、というようなケースでは、問題のタイプごとに別々のキューを設定できます。
- **サービスデスクスタッフが特定のチケットセットに割り当てられる場合。**例えば、所属する企業のオフィスがさまざまな都市にあり、都市ごとに専任のサービスデスクスタッフがいる場合は、別々のキューでチケットを管理できます。ただし、企業のサービスデスクスタッフが、複数のオフィスの作業に1ヶ所から対応する場合、キューは1つで十分です。

チケットキューの設定に関する情報については、サービスデスクチケットキューの設定を参照してください。

キューの追加および削除

必要に応じてキューを追加、複製、および削除することができます。このアクティビティは、組織内のさまざまなグループに対して異なるタイプのチケットを設定する場合に役立ちます。

キューの追加

必要に応じてサービスデスクチケットキューを追加することができます。

キュー間でサービスデスクチケットを移動する予定がある場合、各キューでは必ず同じ値（カスタムフィールドなど）を使用します。同じ値を設定しなければ、古いキューのデータが、新しいキューに一致するよう変更されます。詳細については、「キュー間のチケットの移動」を参照してください。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. **アクションの選択 > 新規作成** を選択します。
2. 新しいキューの「名前」、「Eメールアドレス」、および「代替のEメールアドレス」の値を入力します。

    注意: アプライアンスに E メールを直接送信（アプライアンスに E メールを転送）する場合は、アプライアンスのアドレスと代替アドレスのローカル部分が一致していなければなりません。例えば、servicedesk@kboxとservicedesk@company.comのようにします。

    注意: 新しいキューは、それぞれ独自のEメールアドレスを使用する必要があります。アプライアンスは、新しいキューを保存する前に、この確認作業を行います。すでに別のキューに関連付けられている電子メールアドレスを指定すると、警告が表示されます。
3. POP3サーバーを設定している場合は、ユーザー/パスワード フィールドに、POP3メールのユーザーIDとパスワードを入力します。

    詳細については、「POP3 Eメールアカウントについて」を参照してください。

    ヒント: POP を使用してアプライアンスに E メールをダウンロードする場合、メールボックスは有効なものであれば、どのようなものでも使用可能です。
4. POP3認証については、SSL チェックボックスをオンにすることで、Secure Sockets Layer（SSL）をキューに適用できます。

    このチェックボックスをオンにするかどうかは、使用するPOP3アカウントの設定方法に応じて異なります。
5. **保存** をクリックします。
6. 必要に応じて、キューのその他の設定を選択します。詳細については、「サービスデスクチケットキューの設定」を参照してください。

既存キューの複製によるキューの追加

キューを複製するか、またはクローンを作成すると、既存のキューの全データが新しいキューにコピーされ、キューを最初から追加するよりも迅速に処理できます。複製されたキューにはチケットルールがコピーされますが、デフォルトでは無効化されています。

1. サービスデスクの キュー リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
2. キューの名前をクリックして、キュー詳細 ページを表示します。
3. ページの一番下で **複製** をクリックします。

    新しいキューの名前は、複製元のキューの名前の後に一意の識別番号が追加されたものになります。デフォルトでは、この新しいキューのチケットルールは無効化されています。
4. 必要に応じてキューの名前と設定を変更します。
5. **保存** をクリックします。

キューの削除

必要に応じてキューを削除することができます。

注意: キューを削除する前に、キュー内のデータをすべて削除してもよいか確認してください。これには、関連チケットと関連プロセスも含まれます。このアクションは元に戻すことができません。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの名前をクリックします。
2. ページの一番下で **削除** をクリックし、次に **はい** をクリックして確定します。

キューのチケットの表示

チケット ページを並べ替えて、すべてのキューのすべてのチケットを1つのリストに表示することができます。キューが複数ある場合は、チケット ページで表示するデフォルトのキューを指定することができます。

キューが複数ある場合は、チケット ページで表示するデフォルトのキューを選択することができます。デフォルトキューは次のレベルで指定できます。

- **システムレベル**: ユーザー設定が指定されていない場合に、この設定が使用されます。詳細については、「システムレベルでのデフォルトキューの設定」を参照してください。
- **ユーザーレベル**: この設定は、システムレベル設定よりも優先されます。ユーザー設定を変更する権限を持つ各ユーザーおよび管理者は、ユーザーレベルでデフォルトキューを指定することができます。詳細については、「ユーザーレベルでのデフォルトキューの設定」を参照してください。

すべてのキューのチケットの表示

キューが複数ある場合は、同じリストのすべてのキューからチケットを表示できます。

1. サービスデスクの チケット リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。 または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
2. 表の上部に表示される キュー ドロップダウンリストで、**すべてのキュー** を選択します。
3. キュー ドロップダウンリストの右側の 特定基準で表示 ドロップダウンリストで、表示するチケットのグループを選択します。

    多数のキューがある場合は、検索ボックスを使用して特定のキューをすばやく検索します。

デフォルトキューの設定

キューが複数ある場合は、チケット ページで表示するデフォルトのキューを選択することができます。

デフォルトキューは次のレベルで指定できます。

- **システムレベル**: ユーザー設定が指定されていない場合に、この設定が使用されます。詳細については、「システムレベルでのデフォルトキューの設定」を参照してください。
- **ユーザーレベル**: この設定は、システムレベル設定よりも優先されます。ユーザー設定を変更する権限を持つ各ユーザーおよび管理者は、ユーザーレベルでデフォルトキューを指定することができます。詳細については、「ユーザーレベルでのデフォルトキューの設定」を参照してください。

システムレベルでのデフォルトキューの設定

システムレベルのデフォルトキューの設定により、デフォルトで表示されるチケットキューが決定されます。ただし、ユーザーレベルの設定が指定されていない場合に限ります。

1. サービスデスクの 設定 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. 設定 パネルで **設定** をクリックします。
2. キュー基本設定 セクションで、チケットリストデフォルトキュー ドロップダウンリストのオプションを選択します。

オプション	説明
デフォルトなし	キューを表示する際にデフォルトを使用しません。これを選択した場合、**サービスデスク > チケット** を選択すると、システムに最初に追加されたキューがデフォルトで表示されます。ユーザーレベルで設定が指定された場合、この設定は無視されます。
すべてのキュー	デフォルトで すべてのキュー ビューが表示されます。これを選択した場合、**サービスデスク > チケット** を選択すると、すべてのキュー ビューが表示されます。ユーザーレベルで設定が指定された場合、この設定は無視されます。
<Queue Name>	選択したキューがデフォルトで表示されます。これを選択した場合、**サービスデスク > チケット** を選択すると、指定したキューが表示されます。ユーザーレベルで設定が指定された場合、この設定は無視されます。このリストにキューが表示されない場合は、キューを表示する権限があることを確認してください。

ヒント: これらの設定は、ユーザーレベルで上書きすることができます。詳細については、「ユーザーレベルでのデフォルトキューの設定」を参照してください。

3. **保存** をクリックします。

ユーザーレベルでのデフォルトキューの設定

ユーザーレベルのキュー設定により、デフォルトで表示されるチケットキューが決定されます。ユーザーレベルの設定は、システムレベルの設定よりも優先されます。ユーザー設定を変更する権限を持つ各ユーザーおよび管理者は、ユーザーレベルでデフォルトキューを指定することができます。

ユーザーレベルのデフォルトキューが指定されていない場合、システムレベルのデフォルトキューが使用されます。

1. ユーザー詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
    c. ユーザーの名前をクリックします。
2. デフォルトキュー ドロップダウンリストで、以下のオプションを選択します。

オプション	説明
デフォルトなし	キューを表示する際にデフォルトを使用しません。これを選択した場合、選択されたユーザーが**サービスデスク > チケット** を選択すると、システムに最初に追加されたキューがデフォルトで表示されます。
すべてのキュー	デフォルトで すべてのキュー ビューが表示されます。これを選択した場合、選択されたユーザーが**サービスデスク > チケット** を選択すると、すべてのキュー ビューが表示されます。
<Queue Name>	選択したキューがデフォルトで表示されます。これを選択した場合、選択されたユーザーが**サービスデスク > チケット** を選択すると、指定したキューが表示されます。このリストにキューが表示されない場合は、キューを表示する権限があることを確認してください。

3. **保存** をクリックします。

すべてのキュー チケットリストのデフォルトフィールドの設定

すべてのキュー ビューに表示するチケットフィールドを指定できます。

キューが複数ある場合に、システムのすべてのチケットを1つのリストに表示するには、すべてのキュー ビューが便利です。

例えば、各キューでは、チケットフィールドに異なる名前を使用できます。あるキューでは 優先度 チケットフィールドが使用され、別のキューで ビジネスインパクト チケットフィールドが使用される場合があります。すべてのキュー ビューに表示するフィールドは選択することができます。

フィールドは、以下の設定に従って表示されます。

- すべてのキューの表示 フィールドラベルのデフォルトキュー として選択されたキューで使用するフィールド名
- すべてのキューの表示 のリストレイアウトのカスタマイズ 設定で指定されたフィールド

1. サービスデスクの 設定 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
c. 設定 パネルで **設定** をクリックします。

2. キュー基本設定 セクションで、チケットリストレイアウト (すべてのキュー) ドロップダウンリストからキューを選択します。

   このキューのフィールド名が、チケット ページに表示されます。

3. **保存** をクリックします。
4. **すべてのキューの表示 のリストレイアウトのカスタマイズ** をクリックして、レイアウト ページを表示します。
5. 次のアイコンを使用してフィールドを変更します。

   - : フィールドを追加します。
   - : フィールド名またはフィールドの列幅を変更します。

     注: この幅は、フィールド列に割り当てられる使用可能なページ幅を示します。例えば、10 列あり、各列に幅として 10 が割り当てられている場合には、Width (幅) 列の数字すべての合計は 100 になります。したがって、各フィールド列には、使用可能なページ幅の 10 パーセントの幅が割り当てられることになります。幅 列の数値すべての合計が100より大きかったり小さかったりした場合には、幅を決定するためにパーセント値に標準化されます。例えば、3 列ある場合に、各列に割り当てられる幅が 10 とすると、Width (幅) 列のすべての数字の合計は 30 になります。ただし、パーセンテージに正規化されると、各列の幅は約 33.3 % になります。

     ヒント: すべてのキューの表示 で指定したフィールドの列幅は、各キューのプロパティよりも優先します。

   - : ドラッグし、フィールドの表示順を並べ替えます。
   - : フィールドを削除します。

6. 編集する各フィールドに対し、行の最後にある **保存** をクリックします。

   デフォルトキュー設定が保存されました。

7. 新しい設定を確認するには :
   a. **サービスデスク > チケット (複数)** を選択して、ページを表示します。
   b. キュー ドロップダウンリストで、**すべてのキュー** を選択します。特定基準で表示 ドロップダウンリストで、**すべてのチケット** を選択します。

      選択したキューのフィールドが、キュー設定で指定した並び順でリストに表示されます。

      注意: システムの すべてのキュー **ビューにアクティブなチケットまたはすべてのチケットが表示されると、**アクションの選択 **メニューと** 特定基準で表示 **ドロップダウンリストでデフォルト設定が使用されます。個々のキューに表示されるカスタム設定は、**すべてのキュー **ビューでは使用できません。**

キュー間のチケットの移動

キューが複数ある場合は、必要に応じてキュー間でチケットを移動できます。

チケットを別のキューに移動すると、そのチケットの元の設定 (ステータス、インパクト、優先度、カテゴリなど) が、移動先のキューの設定によって上書きされます。チケットの変更履歴には、元の値が保存されます。

次の例は、キュー間でチケットを移動した場合に、カスタムフィールドがどのように扱われるかを示したものです。

1. 移動されるチケットの CUSTOM_1 フィールドには、**パイロットエラー** という問題の根本原因がリストされるとします。

2. ターゲットキューの CUSTOM_1 フィールドには、**タンパ**、**ロサンゼルス**、**デンバー** などの地名がリストされるとします。

   「CUSTOM_1」の値「**パイロットエラー**」は、移動されるチケットで保持されます。
3. 「**タンパ**」に移動されたチケットの「CUSTOM_1」の値を変更した場合、「**パイロットエラー**」の値は、移動されたチケットでは使用できなくなります。

1. サービスデスクの チケットの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
   c. チケットのタイトルをクリックします。
2. **アクションの選択 > キューに移動 > キュー名** を選択します。

   多数のキューがある場合は、検索ボックスを使用して特定のキューをすばやく検索します。
3. **はい** をクリックして、チケットの移動を確定します。
4. **保存** をクリックして、新しいキューにチケットを保存します。

キュー内のチケットを一括編集する

一括チケット更新機能を使用すると、複数のチケットの 1 つまたは複数のフィールドを同時に編集できます。チケットは同じキューに属している必要があります。キューの所有者のみが、チケットを一括編集できます。

チケットセットに対して一括編集を実行しても、チケットルールには影響しません。一括編集するチケットに関連付けられたチケットルールは、設定に従って、引き続き実行されます。チケットルールの詳細については、チケットルールの使用を参照してください。

1. サービスデスクの チケット リストに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。

2. テーブルの上に表示される キュー ドロップダウンリストで、編集するチケットを含むキューを選択します。
3. チケット リストページで、一括編集するチケットを選択します。
4. **アクションの選択** > **一括チケット更新** を選択します。
5. 表示される 一括チケット更新 ダイアログボックスの フィールド名 列で、更新する値のフィールドを選択します。次に、フィールド値 列で、選択したフィールドに割り当てる値を設定します。
   - この一括編集にフィールドを追加するには、**更新するフィールドを追加** をクリックし、フィールドの名前と値を指定します。
   - リストからフィールドを削除するには、アクション 列で アイテムの削除 をクリックします。
   - この変更に関する該当するユーザーへの E メール通知を抑制するには、**通知を抑制** を選択します。
   - CC リスト フィールドを編集すると、追加した E メールアドレスが既存の CC リストに追加されます。CC リストのアイテムをここで指定した値に置き換えるには、**既存の CC リストに添付** チェックボックスがオフになっていることを確認します。
   - コメント フィールドを一括編集しても、既存のコメントは置換されず、単に既存のコメントに新しいコメントが追加されます。
   - 必須フィールドの値を指定しないと、エラーが発生します。
   - 一括更新では、チケットステータスを変更できません。このフィールドは、**アクションの選択** メニューのコマンドを使用して一括編集できます。
   - 完了したら、**保存** をクリックします。

ユーザーダウンロードおよびサポート技術情報記事について

ユーザーコンソールを使用して、ソフトウェア、スクリプト、その他のダウンロード可能なファイルをユーザーに配布できます。また、ユーザーが**ユーザーコンソール**内でサポート技術情報記事を参照できるようにすることができます。

ユーザーが**ユーザーコンソール**にアクセスできるようにするには、アプライアンス上でユーザーアカウントを作成するか、LDAP 認証を有効にする必要があります。詳細については、「ユーザーアカウントおよびユーザー認証について」を参照してください。

ユーザーダウンロードの管理

管理者コンソールを使用して、ユーザーダウンロード を作成、ラベル作成、および削除できます。

ユーザーコンソール内のアイテムを利用できるようにするには、アイテムを**管理者コンソール**の ユーザーダウンロード セクションにアップロードする必要があります。詳細については、「ユーザーダウンロードの追加」を参照してください。

インストーラやスクリプトを実行するために、ユーザーは KACE エージェントソフトウェアを自分のデバイスにインストールしておく必要があります。詳細については、「デバイスの管理について」を参照してください。

ダウンロード可能なアイテムへのユーザーのアクセスを制限するには、アイテムを適用するデバイスラベルを選択するか、ラベルをアイテム自体に適用します。詳細については、「ユーザーダウンロードへのラベルの適用」を参照してください。

ユーザーダウンロードの追加

ユーザーコンソールを使用して、ソフトウェア、スクリプト、その他のダウンロード可能なファイルを**管理者コンソール**に追加できます。

ユーザーコンソールに追加するすべてのアイテムが、アプライアンスの インベントリ セクションまたは スクリプト セクションに既に存在している必要があります。**管理者コンソール**を使用してソフトウェアまたはスクリプトを作成することはできません。

ヒント: ソフトウェアの配布は、ソフトウェア ページのアイテムおよびエージェントによって管理されるデバイスのみに実行できます。ソフトウェアカタログ ページのアイテムおよびエージェント不要デバイスでは実行できません。

1. User Downloads Detail（ユーザーダウンロードの詳細）ページに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**ユーザーダウンロード** をクリックします。
    c. **アクションの選択 > 新規作成** を選択します。
2. **有効** チェックボックスをオンにすると、アイテムがユーザーコンソールに表示され、オフにするとアイテムが非表示になります。
3. 設定 セクションで、タイプ を選択します。

オプション	説明
ダウンロード	次のいずれかのオプションを選択します。 • **カタログソフトウェア**: 1個または複数の関連ファイルが含まれるソフトウェアカタログからアイテムを選択するには、このオプションを使用します。最初にアプリケーションを選択し、次にダウンロードできるようにするファイルを選択します。ソフトウェアカタログ内のアプリケーションには、異なるアプリケーションバージョン用およびプラットフォーム用のインストーラーのような複数のファイルを含めることができます。 **ヒント:** ユーザーダウンロードにカタログソフトウェアを追加する場合は、ユーザーダウンロード（**管理者コンソール**）ページおよび ダウンロード（**ユーザーコンソール**）ページで、カテゴリ、ライセンスタイプ、プラットフォーム、ライフサイクル終了、一般公開、および 小売価格（￥）の各列にそのアプリケーションに関する追加情報が表示されます。 カタログソフトウェアの詳細については、「ソフトウェアカタログについて」および「ソフトウェアカタログのアプリケーションの詳細の表示」を参照してください。 • **ソフトウェア**：ドキュメント、ファイル、または自動的にインストールされない他のソフ

オプション	説明
	トウェアをダウンロードするアイテムを作成します。
インストール	ユーザーのデバイス上でソフトウェアプログラムを実行するアイテムを作成します。インストールを実行するには、デバイスにエージェントをインストールしておく必要があります。次のいずれかのオプションを選択します。 • **既存の管理対象インストールを使用**: 既存の管理対象インストール（MI）を選択するには、このオプションを選択します。各MIには、インストールまたは削除される特定のアプリケーションのタイトルおよびバージョンの情報（インストールコマンド、インストールファイル、ターゲットデバイス（ラベルによって識別）など）が含まれます。詳細については、「管理対象インストールの使用」を参照してください。 • **デフォルトのインストール**: **インベントリ > ソフトウェア** の順にクリックし、表示された中からプログラムを選択します。詳細については、「ソフトウェア ページについて」を参照してください。
スクリプト	ユーザーのデバイス上でスクリプトを実行するアイテムを作成します。**スクリプト > スクリプト** の順にクリックし、表示された中からスクリプトを選択します。スクリプトを実行するには、デバイスにエージェントソフトウェアをインストールしておく必要があります。

4. 前の手順で「**インストール**」パッケージタイプを選択した場合は、必要なインストールスイッチまたはパラメータも含め、インストールの実行に必要なパラメータを入力します。
5. 含める情報を指定します。

フィールド	説明
プロダクトキー	ユーザーがアプリケーションをダウンロードする際、ユーザーにプロダクトキーを送信します。「資産詳細」ライセンス情報を表示するには、**資産** をクリックします。
単価	（オプション）ユニット当たりのコスト。
インストール手順	アプリケーションと共に**ユーザーコンソール**にアップロードする指示、法的注意事項、またはその他の情報。
説明	任意の追加情報を入力します。
ベンダーライセンス	（オプション）ベンダー固有のライセンステキスト。

フィールド	説明
企業ライセンスポリシー	（オプション）企業固有のライセンステキスト。
エンドユーザーにプロダクトキーをEメールで送信	ユーザーがアプリケーションをダウンロードする際、ユーザーにプロダクトキーを送信します。「資産詳細」ライセンス情報を表示するには、**資産** をクリックします。
マネージャに通知	アプリケーションをダウンロードまたはインストールする前に、各自の管理者のEメールアドレスを入力するようユーザーに要求します。
添付ファイル	（オプション）ドキュメントとして含められるファイル。アイテムを保存すると、ファイルサイズが表示されます。

6. アクセス制御 セクションで、配布に関する制限を指定します。

フィールド	説明
ラベル	（オプション）**編集** をクリックしてラベルを選択し、アプリケーションの導入をラベルに含まれているユーザーに制限します。
デバイスを割り当てる制限ユーザーラベル	（オプション）ユーザーに割り当てられているデバイスでのみユーザーダウンロードをトリガできるように、ユーザーへのアクセスを制限します。
承認が必要	（オプション）ソフトウェアをダウンロードする承認を 1 つまたは複数、エンドユーザーに取得させる場合は、このチェックボックスをオンにして、次のフィールドを設定します。 • **承認プロセステンプレート**: 目的の承認プロセスを含むプロセステンプレートを選択します。プロセステンプレートは、ソフトウェアダウンロード要求に適用される ソフトウェアリクエスト：承認が必要 プロセスタイプに基づいている必要があります。 • **承認頻度**：選択したソフトウェアをダウンロードする権限をユーザーが要求する頻度を、ワンタイム承認 または すべてのダウンロード承認 から指定します。 **注:** 承認が必要なアイテムをエンドユーザーがダウンロードしようとすると、設定されているプロセステンプレートを使用してチケットが自動的に作成されます。承認者は自動的に通知されます。承認されると、ユーザーは通知を受信し、選択した項目をダウンロードすることができます。

7. **保存** をクリックします。

ユーザーダウンロードへのラベルの適用

ラベルを使用して、ユーザーダウンロードをグループ化できます。これは、一度に複数のアイテムを管理および配布したり、アイテムへのアクセスを制限したりする場合に役立ちます。

1. ユーザーダウンロード リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**ユーザーダウンロード** をクリックします。
2. 1 つまたは複数のアイテムの隣のチェックボックスをオンにします。
3. **アクションの選択 > ラベルの適用** を選択します。
4. これらのラベルを適用 フィールドにラベルをドラッグし、**ラベルの適用** をクリックします。

ラベルは、アイテムの隣の括弧内にリストされます。

ユーザーダウンロードからのラベルの削除

必要に応じて、ユーザーダウンロードからラベルを削除することができます。

1. ユーザーダウンロード リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**ユーザーダウンロード** をクリックします。
2. アイテムの隣のチェックボックスをオンにします。
3. **アクションの選択 > ラベルの削除** を選択します。
4. 削除するラベルの隣にある**削除** ボタンをクリックします をクリックします。
5. **ラベルの削除** をクリックします。

選択したラベルがアイテムから削除されます。

ユーザーダウンロードの削除

必要に応じてユーザーダウンロードを削除できます。

1. ユーザーダウンロード リストに移動します。
    a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**ユーザーダウンロード** をクリックします。
2. 1つまたは複数のアイテムの隣のチェックボックスをオンにします。
3. **アクションの選択 > 削除** を選択し、**はい** をクリックして確定します。

サポート技術情報記事の管理

管理者コンソールを使用して、サポート技術情報記事を追加、編集、複製、および削除することができます。

ユーザーコンソール内では、記事をキーワードで検索したり、記事番号、タイトル、カテゴリ、プラットフォーム、重要度などで分類したりすることができます。さらに、サポート技術情報記事の有用度を評価できます。

サービスデスクチケットにサポート技術情報記事のテキストを挿入するには、チケットページの **関連記事の検索** リンクをクリックします。

サポート技術情報記事の追加、編集、または複製

サポート技術情報記事は追加、編集、複製することができます。この記事は、**ユーザーコンソール**でユーザーに提供されます。

1. 記事の詳細ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**サポート技術情報** をクリックします。
    c. 記事の詳細 ページを表示するには、次のいずれかを実行します。
    - 記事の名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. 次の情報を入力します。

フィールド	説明
タイトル	サポート技術情報記事で取り上げる問題についての、具体的な説明。ユーザーが情報を見つけやすいように、分かりやすいタイトルを付けて、一般的な用語を使用してください。
カテゴリ	問題のタイプについての一般的な説明（ 例：「印刷」、「ネットワークアクセス」 ）。
プラットフォーム	このサポート技術情報記事が適用されるオペレーティングシステム。
重要度	このサポート技術情報記事の重要性。例えば「参考」、「低」、「緊急」、「高」など。
ラベルへの割り当て	記事へのアクセスを特定のユーザーセットに限定する場合は、リストから該当するユーザーラベルを選択します。このフィールドを空のままにした場合は、**ユーザーコンソール**にアクセスできるユーザーであれば、誰でもサポート技術情報記事を確認できます。
テキスト	このサポート技術情報記事のコンテンツ。 このフィールドには、太字テキスト、ハイパーリンク、リスト、テキストの色、埋め込み画像、およびビデオ用のボタンなど、コンテンツをフォーマット

フィールド	説明
	するためのテキスト編集オプションがすべて表示されます。 例： • 太字のテキストをテキスト文字列に適用するには、エディタでそのテキストを選択し、 をクリックします。 • 3 つの異なる方法を使用して、サポート技術情報記事に画像を追加できます。そのためには、 をクリックし、表示される画像パネルで、次のいずれかの手順を実行します。 ◦ コンピュータからファイルに移動して、そのファイルを記事にアップロードするには、 をクリックします。この方法で追加された画像は、添付ファイルとして KB 記事に自動的に保存されます。 ◦ 別の場所でホストされているファイル、または別の KB 記事の一部であるファイルにリンクするには、 をクリックします。 ◦ KB 文書にすでに添付されているファイルにリンクするには、 をクリックします。 • 外部リンク、または他の KB 記事へのリンクを追加するには、 をクリックします。 • ファイルを添付するには、 をクリックします。このオプションを使用してアップロードしたファイルは、この KB 記事の添付ファイルとして保存されます。 • 外部でホストされるビデオを埋め込むには、 をクリックします。 • 画像ファイルを記事のコンテンツから削除するが、添付ファイルは削除しない場合は、それらを記事のコンテンツに追加できます。これを行うには、 をクリックし、表示された画像パネルで をクリックします。 • 添付ファイルを削除するには、 をクリックします。

3. **オプション**：添付ファイル セクションで **追加** をクリックし、**参照** または **ファイルの選択** をクリックして添付ファイルを追加します。
4. **保存** をクリックします。

ヒント: チケットのコメントを流用してサポート技術情報記事を作成するには、**チケットの詳細** ページで KB記事の作成 をクリックします。

アプライアンスがそのサポート技術情報記事に記事番号を割り当てて、サポート技術情報記事 ページに表示します。サポート技術情報記事が**ユーザーコンソール**でユーザーにどのように表示されるかを確かめるには、サポート技術情報 ページでサポート技術情報記事のタイトルをクリックし、次に 記事の詳細 ページでユーザー URL をクリックします。

5. **オプション**：**複製** をクリックします。

サポート技術情報記事の削除

サポート技術情報記事を削除して、アプライアンスから永続的に消去することができます。

1. サポート技術情報記事 リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**サポート技術情報** をクリックします。
2. 1つまたは複数の記事の隣のチェックボックスをオンにします。
3. **アクションの選択** > **削除** を選択し、**はい** をクリックして確定します。

サポート技術情報記事のユーザー評価および表示回数の確認

サポート技術情報記事のユーザー評価および表示回数を確認することができます。

1. サポート技術情報の Article Detail（ 記事の詳細 ） ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**サポート技術情報** をクリックします。
    c. 記事の名前をクリックします。

    ページの一番下に、記事に関する現在のユーザー評価および表示回数が表示されます。
2. 表示されている星をマウスでポイントすると、5個の星による評価システムの定義が表示されます。

    この尺度では、星1つが低評価に、星5つが高評価になります。

    注: ユーザーは自分でつけた評価を変更できます。ただし、データベースでは、各記事に対するユーザーの最新の評価のみが維持されます。

サービスデスクチケット設定のカスタマイズ

ユーザーおよび環境のニーズに合わせてサービスデスクチケット設定をカスタマイズできます。キューが複数ある場合は、それぞれのキューのチケット設定を個別にカスタマイズできます。

サービスデスクチケット設定のカスタマイズについて

サービスデスクの要件に合わせて、チケット値のカスタマイズ、カスタムフィールドの追加、チケットカテゴリの作成、およびチケットサブカテゴリの作成を行うことができます。

デフォルトのチケット値には、「カテゴリ」、「ステータス」、「優先度」、「インパクト」があります。

- チケットの特性は次の通りです。
  - フィールド名
  - チケットに表示されるフィールドの並び順
  - フィールドの要否
  - フィールドを変更する権限を持つユーザー
- カスタムフィールド定義は次の通りです。
  - フィールドタイプ（チェックボックス、日付、タイムスタンプ、リンク、複数選択、メモ、数字、単一選択、テキスト、またはユーザー）
  - フィールドに入力可能な値
  - フィールドのデフォルト値

チケットカテゴリとサブカテゴリの作成

必要に応じてチケットカテゴリとサブカテゴリを作成できます。カテゴリとサブカテゴリはキュー固有のため、これらを作成すると、選択されたキューにある新規または既存のチケットに対して使用可能になります。

それぞれ1つ以上のサブカテゴリを持つチケットカテゴリを必要数追加できます。例えば、チケットカテゴリ「ハードウェア」に「モニタ」などのサブカテゴリを追加できます。これらのサブカテゴリは Ticket Detail（チケットの詳細）ページで次のように表示されます。

ユーザーが Monitor（モニタ）サブカテゴリを選択した場合、モデル情報といった追加のサブカテゴリの表示が必要になる場合もあるでしょう。

ほとんどの顧客は、カテゴリやサブカテゴリに対して、2層式のアプローチを用いており、一般的なカテゴリのほか、次のとおりユーザーのためのサブカテゴリを作成しています。

- ハードウェア-モニタ

さらに、サービスデスクスタッフ用として、モデル情報を盛り込んだ追加のサブカテゴリも作成しています。

- ハードウェア-モニタ-AceElectronics-V4500
- ハードウェア-モニタ-AceElectronics-V4600

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。

d. キューの詳細 ページを表示するには、次のいずれかを実行します。

- キューの名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

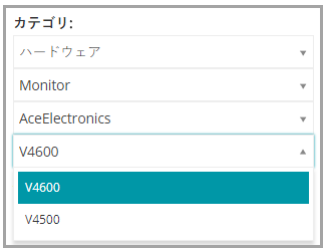
2. チケットのデフォルト セクションで、**これらの値のカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。

   キューのカスタマイズ ページの カテゴリ値 セクションでは、デフォルトで ツリー表示 タブが開き、チケットカテゴリとサブカテゴリを作成および管理できます。必要に応じて、リスト表示 タブのリスト フォームで既存のカテゴリとサブカテゴリを確認できます。

3. 必要に応じて、ツリーウィジェットを使用してチケットカテゴリとサブカテゴリノードを作成および編集します。

   - **新しいルートカテゴリ追加するには、 をクリックし、カテゴリ名を指定します。**
   - **新しいサブカテゴリを追加するには、親カテゴリノードを右クリックし、表示されるメニューで 作成 を選択します。**

     Queue Customization（ キューのカスタマイズ ）ページで、カテゴリとサブカテゴリが次のように表示されます。
     Ticket Detail（ チケットの詳細 ）ページで、カテゴリとサブカテゴリが次のように表示されます。

   - **カテゴリの名前を変更するには、カテゴリノートを右クリックし、メニューから 名前の変更 を選択して、新しい名前を入力します。**
   - **カテゴリを削除するには、カテゴリノートを右クリックし、メニューから 削除 を選択し、表示される 確認 ダイアログボックスで はい をクリックします。**
   - **カテゴリ内のすべてのサブカテゴリを並べ替えるには、カテゴリノートを右クリックし、メニューで、必要に応じて、並べ替え > 昇順 または 並べ替え > 降順 を選択します。**
   - **すべてのカテゴリとそのサブカテゴリを昇順で並べ替えるには、 をクリックし、表示される 確認 ダイアログボックスで はい をクリックします。**

     注: カテゴリを削除しても、そのサブカテゴリはツリーから削除されません。

   - **特定のカテゴリを検索するには、検索ボックスにカテゴリ名を入力します。入力すると、一致する結果がツリーウィジェットでハイライト表示されます。**
   - **カテゴリを移動するには、カテゴリノードをツリー内の目的の位置にドラッグします。**

4. カテゴリを編集するには、ツリーでカテゴリを選択し、右側の領域に次の情報を入力します。カテゴリの変更が完了したら、**追加** をクリックします。

フィールド	説明
デフォルト所有者	チケットが作成されるとき、ユーザーはチケットカテゴリまたはサブカテゴリの所有者として自動的に割り当てられます。既存のチケットを、異なるデフォルト所有者を持つカテゴリに移しても、チケットの所有者は自動的には変更されません。チケットの所有者は、手動で変更する必要があります。

フィールド	説明
「CC」リスト	このチェックボックスをオフにし、チケット上にCCリストが表示されないようにします。「**DefaultTicketOwners**」がデフォルト所有者であるため、チケットが作成されると、すべての潜在的なチケット所有者にEメールが送信されます。
ユーザー設定可能	対応するカテゴリの変更をユーザーに許可します。サービスデスクスタッフのみ変更できるようにするには、このチェックボックスをオフにしてください。ユーザーがカテゴリを変更できない場合でも、カテゴリを表示させることは可能です。

5. ページの一番下にある **保存**をクリックするか、チケット値の編集を続行します。

Ticket Detail（チケットの詳細）ページに新しいカテゴリとサブカテゴリが表示され、新規および既存のチケットに使用できるようになります。

チケット値のカスタマイズ

チケットのステータス、チケット優先度、およびチケットのインパクトに使用可能な値はカスタマイズすることができます。

チケットのステータス値のカスタマイズ

チケットのステータスを示す「オープン」または「クローズ」などの値はカスタマイズすることができます。

重要: ステータス値は多くの場合、チケットルールで使用されます。ステータス値を変更する前に、チケットルールを確認し、それらのルールでステータス値がどのように使用されているかを理解してください。詳細については、「チケットルールについて」を参照してください。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。
   - キューの名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。
2. チケットのデフォルト セクションで、**これらの値のカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. ステータス値 セクションで、カテゴリ値の隣にある **編集** ボタンをクリックして値を修正します（ ）。または、リストの上部にある **追加** ボタン（ ）をクリックして、新しい値を追加します。
4. ステータス値 フィールドを編集します。

フィールド	説明
名前	ステータス値の名前。

フィールド	説明
状態	ステータス値に割り当てられた状態。 • 未解決：チケットはアクティブです。この状態のみエスカレーションできます。詳細については、「チケットのエスカレーションプロセスの使用」を参照してください。 • クローズ：チケットは解決されました。 • 停止済み：チケットは期日を過ぎても開かれたままで、エスカレーションされていません。

5. 行で **保存** をクリックします。

   カテゴリを更新するには、各行の右側のアイコンを使用します。

   - : 列のソート順を変更します。
   - : フィールドを追加します。
   - : 値を変更します。
   - : 値の順序を変更します。
   - : 値を削除します。

     注: 値が使用中の場合や、デフォルトのチケット値として指定されている場合は、その値を削除できません。使用中の値を削除するには、その値が使用されているチケットに値を追加してから古い値を新規の値に変更します。古い値が現在は使用されていない場合は、値の隣に次の **削除** ボタンが表示されます：。

6. ページの一番下にある **保存**をクリックするか、チケット値の編集を続行します。

チケット優先度値のカスタマイズ

必要に応じて、チケットの優先度を示す値をカスタマイズできます。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。
   - キューの名前をクリックします。
   - **アクションの選択** > **新規作成** を選択します。
2. チケットのデフォルト セクションで、**これらの値のカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. 優先度値 セクションで、値の隣にある **編集** ボタンをクリックして値を修正します（ ）。または、リストの上部にある **追加** ボタン（ ）をクリックして、新しい値を追加します。
4. 優先度値 フィールドを次のように編集します。

フィールド	説明
名前	カスタムフィールドの名前を入力します。
色	（オプション）チケットリストページで、このステータスに使用する色を選択します。
エスカレーション時間	（オプション）期限を入力します。この期限を過ぎると、この優先度のオープンなチケットがエスカレーションされます。ドロップダウンリストから、時間の整数と単位を入力します。詳細については、「チケットのエスカレーションプロセスの使用」を参照してください。
営業時間/休日を使用	（オプション）キューのチケットの優先度を計算する際に営業時間と休業日の設定を使用するかどうか。営業時間と休業日がサービスデスクに対して設定されている場合、優先度に基づいてチケットをエスカレーションするかどうかを決定する際に、これらの時間と休業日を考慮するには、このチェックボックスをオンにします。このキューで営業時間と休業日の設定を無視する場合は、チェックボックスをオフにします。

5. 行で **保存** をクリックします。
6. 各行の右側のアイコンを使用して、その他の値を変更します。
   - : 列のソート順を変更します。
   - : フィールドを追加します。
   - : 値を変更します。
   - : 値の順序を変更します。
   - : 値を削除します。

     注: 値が使用中の場合や、デフォルトのチケット値として指定されている場合は、その値を削除できません。使用中の値を削除するには、その値が使用されているチケットに値を追加してから古い値を新規の値に変更します。古い値が現在は使用されていない場合は、値の隣に次の **削除** ボタンが表示されます：。
7. ページ下部の **保存** をクリックして、変更を保存し、キューの詳細 ページに戻ります。

チケットのインパクト値のカスタマイズ

チケットのインパクトを示す値をカスタマイズできます。

注: カテゴリ値と優先度値のフィールドを使用し、チケットを分類できるのは、チケット所有者だけです。チケット送信者がこのような評価をする場合は、チケットのインパクト フィールドを使用します。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。

c. **設定** パネルで **キュー** をクリックします。
d. キューの詳細 ページを表示するには、次のいずれかを実行します。
- キューの名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

2. チケットのデフォルト セクションで、**これらの値のカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. インパクト値 セクションで、値の隣にある **編集** ボタンをクリックして値を修正します ( ) 。または、リストの上部にある **追加** ボタン ( ) をクリックして、新しい値を追加します。
4. 必要に応じて 名前 フィールドを修正します。
5. 行で **保存** をクリックします。

各行の右側のアイコンを使用すると、カテゴリを更新できます。

- : 列のソート順を変更します。
- : フィールドを追加します。
- : 値を変更します。
- : 値の順序を変更します。
- : 値を削除します。

> **注:** 値が使用中の場合や、デフォルトのチケット値として指定されている場合は、その値を削除できません。使用中の値を削除するには、その値が使用されているチケットに値を追加してから古い値を新規の値に変更します。古い値が現在は使用されていない場合は、値の隣に次の **削除** ボタンが表示されます : 。

6. ページの一番下にある **保存**をクリックするか、チケット値の編集を続行します。

チケットレイアウトのカスタマイズ

各キューの チケット ページにチケットが表示される方法をカスタマイズすることができます。

カスタマイズオプションは次の通りです。

- ほとんどのデフォルトフィールドの順序を変えたり、非表示にしたりする。
- カスタムフィールドを1つ以上追加する。フィールドの数は、テーブル内で使用可能な列数によってのみ制限されます。これらのフィールドに対して静的な値を指定するか、データベースクエリを使用して、データベースから値を動的に引き出せます。
- ユーザー、チケット所有者、および管理者のチケットビューをカスタマイズし、読み取り/書き込み権限を設定する。これには、各役割について個々のチケットフィールドを非表示にする、表示する、表示するが変更しない、変更する、などの操作も含まれます。
- カスタマイズされたチケットページをプレビューするには、結果のレイアウトがニーズを満たしていることを確認します。
- チケット間で親/子チケット関係を設定し、すべての子チケットがクローズされるまで親をクローズしないようにする、または親チケットがすべての子チケットをクローズできるようにする。詳細については、「親/子チケット関係の利用」を参照してください。
- 必要な承認がない場合は、チケットの開閉を禁止する。または、チケットを閉じるときにのみ承認を要求する。詳細については、「チケット承認者の使用」を参照してください。

ヒント: ここで行われる変更は、このキュー内の既存のチケットすべてに自動的に伝播されます。

チケットのレイアウトフィールドと関連フィールドのカスタマイズ

チケットの詳細 ページでの チケットのレイアウトフィールド および チケットの関連フィールド の表示方法をカスタマイズできます。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。
   - キューの名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。
2. ページ上部の **フィールドとレイアウトのカスタマイズ** をクリックして、レイアウト および チケットの関連フィールド がある キューのカスタマイズ ページを表示します。

セクション	説明
Layout Ticket Fields（チケットのレイアウトフィールド）	このセクションには、アンケート、タイトル、および 概要 の各フィールド、送信者、資産、およびデバイス の各セクション、および チケットの関連フィールド セクションに表示されないすべての他のフィールドが含まれます。このセクションには、カスタムフィールドも含まれます。このセクション内のフィールドは、このセクション内で自由に移動することができ、指定した順番で Ticket（チケット）ページに表示されます。このセクション内のすべてのフィールドは、行全体を占める Resolution（解決）フィールドを除き、行あたり 2 フィールドの形式で表示されます。 注: 概要 フィールドが非表示の場合は、コメント フィールドが 新規チケット ページに表示されます。概要 フィールドに入力したテキストは、最初のコメントとして保存されます。この最初のコメントは下位互換性を維持するために、概要として格納されます。
チケットの関連フィールド	このセクションには、関連チケットに関する情報を取得するフィールドが含まれます。これらのフィー

セクション	説明
	ルドは非表示にすることはできますが、位置を変更することはできません。 • PARENT_INFO：選択されたチケットに対して親の関係を持つチケット。 • SEE_ALSO：選択されたチケットと同様の（追加情報を提供する）チケット。 • REFERERS：チケットを参照したユーザー。

3. カスタマイズするフィールドの隣にある **編集** ボタン（ ）をクリックします。
4. ラベル および Required（必須）フィールドで、使用するオプションを選択します。

セクション	説明
ラベル	Ticket Detail（チケットの詳細）ページのフィールドの隣に表示する名前。
必須	フィールドが必須かオプションか。 • **必須でありません**：このフィールドは必須ではありません。空白のままにすることができます。 • **常に必須**：このフィールドは空白のままにすることはできません。チケットを保存する前に入力する必要があります。 • **閉じるときに必須**：フィールドに入力するまでチケットを閉じることはできません。

5. 権限 フィールドで、使用する権限設定を選択します。

権限の設定	表示できるユーザー	変更できるユーザー	作成できるユーザー
非表示	なし	なし	なし
読み取り専用	ユーザー、チケット所有者、管理者*	なし	なし
所有者のみ - ユーザーから非表示	チケット所有者、管理者*	チケット所有者、管理者*	チケット所有者、管理者*
所有者のみ - ユーザーに表示	ユーザー、チケット所有者、管理者*	チケット所有者、管理者*	チケット所有者、管理者*
ユーザー作成	ユーザー、チケット所有者、管理者*	チケット所有者、管理者*	ユーザー、チケット所有者、管理者*
ユーザー修正	ユーザー、チケット所有者、管理者*	ユーザー、チケット所有者、管理者*	ユーザー、チケット所有者、管理者*

* デフォルト設定を示します。キュー詳細 ページで次のチェックボックスをクリアすることで、このデフォルト設定を削除できます。管理者役割のユーザーがこのキューでチケットを表示および編集するのを許可（管理者コンソールのみ）

6. **オプション**：次のコントロールを使用してフィールドの表示を変更します。
   - **：列のソート順を変更します。**
   - **: 値の順序を変更します。**
7. 行で **保存** をクリックします。
8. ページの一番下で **保存**をクリックし、変更を適用します。

コメント フィールドのオプションの設定

コメント フィールドのオプションでは、新規チケット ページの コメント フィールドおよび 添付ファイル セクションの外観を設定できます。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。
   - キューの名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。
2. ページ上部の **フィールドとレイアウトのカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. コメント フィールドのオプション セクションで、必要に応じてこれらのチェックボックスを選択またはクリアします。
   - **チケット入力フォームに コメント フィールドを表示する。コメント フィールドをチケット入力フォームに表示したい場合は、このチェックボックスを選択します。**
   - **チケット入力フォームに 添付ファイル フィールドを表示する。添付ファイル セクションをチケット入力フォームに表示する場合は、このチェックボックスを選択します。**

   これらのオプションが有効である場合は、新しいチケットの作成時に **コメント** フィールドと **添付ファイル** セクションが 新規チケット ページに表示されます。これらは、既存のチケットの変更時には、チケットの詳細 ページに表示されません。
4. ページの一番下で **保存**をクリックし、変更を適用します。

カスタムチケットフィールドの定義

サービスデスクチケットにはカスタムフィールドを追加できます。作成可能なカスタムフィールドの数は、テーブル内で使用可能な列数によってのみ制限されます。

カスタムフィールドを作成するには、キューのカスタマイズ ページの2つの領域を設定する必要があります。

- カスタム フィールドを使用して、カスタムフィールドの特性を設定する。
- チケットレイアウト セクションでカスタムフィールドの動作を設定する。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
   または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。

c. **設定** パネルで **キュー** をクリックします。

d. キューの詳細 ページを表示するには、次のいずれかを実行します。

- キューの名前をクリックします。
- **アクションの選択** > **新規作成** を選択します。

2. ページ上部の **フィールドとレイアウトのカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. カスタムフィールド セクションで、次のいずれかを行います。

- **フィールドを変更するには、編集 ボタンをクリックします** をクリックします。
- **フィールドを作成するには、追加 ボタンをクリックします**。

編集可能なフィールドが表示されます。

4. フィールドタイプ ドロップダウンリストから、フィールドタイプを選択します。

オプションは次の通りです。

- **チェックボックス**: チケットに、チェックボックスフィールドタイプを追加します。
- **日付**: チケットに、書式付き日付タイプのフィールドを追加します。
- **タイムスタンプ**: チケットに、タイムスタンプタイプのフィールドを追加します。
- **リンク**: 内部/外部URLへのリンクを定義し、チケットに追加します。
- **複数選択**: チケットに、複数値選択タイプのフィールドを追加します。複数のエントリはコンマで区切ります。
- **メモ**: チケットに、メモタイプのフィールドを追加します。
- **数字**: チケットに、整数選択タイプのフィールドを追加します。
- **単一選択**: チケットに、単一選択タイプのフィールドを追加します。
- **テキスト**: チケットに、テキストタイプのフィールドを追加します。
- **ユーザー**: フィルタリングおよび検索が可能で、ユーザーテーブルのユーザーが表示されるドロップダウンリストを追加します。

> **注:** ユーザー カスタムフィールドには、HD_TICKETテーブル内のUSERテーブルに含まれるユーザーIDが入力されます。HD_TICKETは、チケットのレコードを保持するためのテーブルです。HD_TICKETテーブルを対象とするレポートやクエリを記述する場合、レポート内にユーザーIDではなくユーザー名を表示するには、USERテーブルを結合（JOIN）する必要があります。

5. Select Values（値の選択）フィールドで、許容される値を指定します。

Select Values（値の選択）フィールドは、単一選択 または 複数選択 カスタムフィールドタイプに使用します。複数の値は、コンマ区切りの文字列として入力します。

データベースクエリを使用し、次の構文を持つフィールドでフィールドに値を指定できます。query:**query_instructionsカスタムフィールド** の隣にある、次の ヘルプ ボタンを選択すると例を表示できます：。

6. デフォルト フィールドに値を入力します。

この値は、チケットが作成されるときにデフォルトで入力されます。

> **注:** カスタムフィールドの名前を削除すると、そのフィールドの値がすべてのチケットから削除されます。カスタムフィールドの名前を変更すると、そのカスタムフィールドの値は保持されます。

データベースクエリを使用し、次の構文を持つフィールドでフィールドに値を指定できます。query:**query_instructionsカスタムフィールド** の隣にある、次の ヘルプ ボタンを選択すると例を表示できます：。

7. **保存** をクリックします。
8. チケットのレイアウトフィールド セクションまでスクロールし、先ほど設定したカスタムフィールドの隣の **編集** ボタンをクリックします。

   カスタムフィールドの動作オプションが編集可能になります。
9. ラベル フィールドの名前を入力します。
10. 必須 フィールドで、使用するオプションを選択します。
    - **「必須でありません」。このフィールドは必須ではありません。**
    - **「常に必須」。このオプションが指定されたフィールドは、チケットを保存し、送信する前に入力を完了する必要があります。**
    - **「閉じるときに必須」。このオプションが指定されたフィールドは、チケットをクローズする前に入力を完了する必要があります。**
11. 権限 フィールドで、使用する権限設定を選択します。

権限の設定	表示できるユーザー	変更できるユーザー	作成できるユーザー
非表示	なし	なし	なし
読み取り専用	ユーザー、チケット所有者、管理者*	なし	なし
所有者のみ - ユーザーから非表示	チケット所有者、管理者*	チケット所有者、管理者*	チケット所有者、管理者*
所有者のみ - ユーザーに表示	ユーザー、チケット所有者、管理者*	チケット所有者、管理者*	チケット所有者、管理者*
ユーザー作成	ユーザー、チケット所有者、管理者*	チケット所有者、管理者*	ユーザー、チケット所有者、管理者*
ユーザー修正	ユーザー、チケット所有者、管理者*	ユーザー、チケット所有者、管理者*	ユーザー、チケット所有者、管理者*

   * デフォルト設定を示します。このデフォルト設定は、キューの詳細 ページで、管理者役割のユーザーがこのキューでチケットを表示および編集するのを許可（管理者コンソールのみ）チェックボックスのチェックを外すと無効にできます。

12. **オプション**：列の上部の **ソート** ボタン（）を使用するか、移動 アイコン（）をドラッグして、フィールドの表示順を並べ替えます。
13. 行で **保存** をクリックします。
14. ページの一番下で **保存**をクリックし、変更を適用します。

チケットリストレイアウトのカスタマイズ

サービスデスクチケットリストのレイアウト（フィールド名、フィールドの順番、列の幅など）をカスタマイズすることができます。これは、キューで チケット リストが表示される方法です。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。
      または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効に

なっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。

c. **設定** パネルで **キュー** をクリックします。

d. キューの詳細 ページを表示するには、次のいずれかを実行します。

- キューの名前をクリックします。
- **アクションの選択** > **新規作成** を選択します。

2. ページ上部の **フィールドとレイアウトのカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. **チケットリストレイアウト** セクションまで下にスクロールします。レイアウトをカスタマイズするには、以下のボタンを使用します。

- : フィールドの表示順を並べ替えます。
- : 表示するフィールドと、列の幅を編集します。

> **注:** この幅は、フィールド列に割り当てられる使用可能なページ幅を示します。例えば、10 列あり、各列に幅として 10 が割り当てられている場合には、Width（ 幅 ） 列の数字すべての合計は 100 になります。したがって、各フィールド列には、使用可能なページ幅の 10 パーセントの幅が割り当てられることになります。幅 列の数値すべての合計が100より大きかったり小さかったりした場合には、幅を決定するためにパーセント値に標準化されます。例えば、3 列ある場合に、各列に割り当てられる幅が 10 とすると、Width（ 幅 ） 列のすべての数字の合計は 30 になります。ただし、パーセンテージに正規化されると、各列の幅は約 33.3 % になります。

- : チケットレイアウトにチケットフィールドを追加します。
- : チケットリストからフィールドを削除します。

4. ページの一番下で **保存** をクリックします。

チケットテンプレートの管理

チケットテンプレートを使用すると、同じキュー内に異なる複数のチケットタイプを作成できます。この仕組みにより、別々のキューを作成しなくても、さまざまなリクエストシナリオに対してエンドユーザーから提供する情報をより適切に制御できるようになります。

各キューには、1 つ以上のチケットテンプレートを入れられます。キュー内に複数のテンプレートがある場合、デフォルトテンプレートとしてチケットテンプレートを 1 つ選択する必要があります。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。

d. キューの詳細 ページを表示するには、次のいずれかを実行します。

- キューの名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

2. ページ上部の **フィールドとレイアウトのカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. チケットテンプレート セクションまで下にスクロールします。
4. 新しいチケットテンプレートをキューに追加するには、チケットテンプレート セクションで ＋ をクリックします。新しいチケットテンプレートを作成する方法の詳細については、「チケットテンプレートの設定」を参照してください。
5. 選択したキューのデフォルトテンプレートとしてあるチケットテンプレートとして設定するには、目的のテンプレートを含む行の デフォルト 列で、**デフォルトにする** をクリックします。1 つ以上のチケットテンプレートを持つキューには、デフォルトテンプレートが必要です。

   あるチケットテンプレートがキューのデフォルトテンプレートとして設定されている場合、チケットテンプレートを指定せずにそのキューでチケットを作成するたびに、デフォルトのテンプレートが適用されます。必要に応じて、テンプレートを切り替えられます。詳細については、「管理者コンソールのチケットページからのチケット作成」を参照してください。

チケットテンプレートの設定

チケットテンプレートには、チケットの詳細 ページに表示されるフィールドセットが指定されています。各キューには、1 つ以上のチケットテンプレートを入れられます。

チケットテンプレートの詳細 ページを使用して、新規または既存のテンプレートを設定します。

1. サービスデスクの キューの詳細 ページに移動します。
   a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
   c. **設定** パネルで **キュー** をクリックします。
   d. キューの詳細 ページを表示するには、次のいずれかを実行します。

   - キューの名前をクリックします。
   - **アクションの選択 > 新規作成** を選択します。

2. ページ上部の **フィールドとレイアウトのカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. チケットテンプレート セクションまで下にスクロールします。

   - 新しいチケットテンプレートをキューに追加するには、チケットテンプレート セクションで ＋ をクリックします。
   - 既存のチケットテンプレートを変更するには、チケットテンプレート セクションでチケットテンプレート名をクリックします。

   チケットテンプレートの詳細 ページが表示されます。
4. チケットテンプレートの詳細 ページで、以下の情報を入力します。

オプション	説明
名前	（ 必須 ）テンプレートの名称。
有効	テンプレートの使用が可能になったら、このチェックボックスにチェックします。このオプションは、

オプション	説明
	このテンプレートが完了する前にエンドユーザーに公開されないようにしたいときに便利です。
説明	テンプレートの簡単な説明。このチケットテンプレートのリンクをポイントすると、**ユーザーポータル**上にツールチップとしてこのテキストが表示されます。
プロセス専用	このチケットテンプレートをプロセステンプレートで使用できるようにするには、このチェックボックスにチェックします。これにより、チケットテンプレートの一部のオプションが無効になります。これは、そのオプションがこのコンテキストに該当しなくなるためです。例えば、**選択したユーザーにテンプレートを制限** オプションは、プロセスベースのチケットテンプレートには適用できません。これは、各プロセステンプレートのウィザードに、プロセステンプレートチケットにラベルを関連付けるためのオプションがあるためです。
選択したユーザーにテンプレートを制限	ラベルを使用している特定のユーザーのみがこのテンプレートを使用できるようにする場合、このチェックボックスをチェックします。次に、**関連ラベルの管理** をクリックして、表示された ラベルを選択 ダイアログボックスで、このチケットテンプレートへのアクセスを許可するユーザーに関連付けられたラベルを 1 つ以上選択します。完了したら、ダイアログボックスを閉じます。
デフォルト	このチケットテンプレートをキュー内のデフォルトテンプレートにする場合、このチェックボックスをチェックします。あるチケットテンプレートがキューのデフォルトテンプレートとして設定されている場合、チケットテンプレートを指定せずにそのキューでチケットを作成するたびに、デフォルトのテンプレートが適用されます。必要に応じて、テンプレートを切り替えられます。詳細については、「管理者コンソールのチケットページからのチケット作成」を参照してください。
ユーザーポータルに表示	エンドユーザー側で **ユーザーコンソール** の ヘルプが必要 ページにこのチケットテンプレートへのリンクを表示させる場合、このチェックボックスをチェックします。
レイアウト	ニーズに最適なレイアウトを選択します。 • **3 列のレイアウト**：テンプレートの各行に平均の高さのフィールドが含まれている場合は、このレイアウトを使用します。 • **2 列 + 右パネルのレイアウト**：このレイアウトは、テンプレートに同じ行の他のフィールドよりも高いフィールド（概要 や 解決 など）が 1 つ以上含まれている場合に使用します。他のフィールドが平均的な高さである 1 つの行に背の高いフィールドが 1 つあると、

オプション	説明
	同じ行の他のフィールドが下に押され、レイアウトにランダムなギャップが生じます。このオプションを選択すると、すべての背の高いフィールドを右パネルに配置して、垂直の表示領域を最適に活用できます。パネル間でフィールドを移動するには、フィールドをダブルクリックします。 必要に応じて、2 つのレイアウトを切り替えることができます。

5. チケットテンプレートに 1 つ以上のチケットフィールドを追加します。コンテンツを別々のセクションに分割するには、区切りフィールドを使用します。このフィールドには、データフィールドと同じオプションがあります。

   注: 追加できるチケットフィールドは、チケットテンプレートが属するキューに存在するもののみです。

   a. チケットフォームテンプレート セクションで、1 つ以上のフィールドを右の領域からドラッグします。
   b. フィールドを追加する際、このテンプレートの使用に最適なフィールド配置できます。関連フィールドをまとめて配置することも、テンプレート領域の端に近い場所にフィールドを配置して、必要に応じて間に空白スペースを作成することもできます。
   c. フィールドの幅は、1 列、2 列または 3 列に設定できます。フィールドの幅を変更するには、目的の幅になるまで をクリックします。
   d. フィールドを削除するには、 をクリックします。
   e. フィールドプロパティの上書きを設定したりフィールドが表示されるかどうかを決定する特定の条件を設定したりするには、 をクリックします。次に、表示されるダイアログボックスで、必要に応じて以下のオプションを設定します。

タブ	オプション	説明
上書き		このタブのオプションを使用して、このチケットテンプレートが属するキューですでに指定されているフィールドパラメータの上書きを設定します。
	ラベル	フィールド名。
	必須	フィールド値を指定する必要があるかどうかを示します。次のいずれかのオプションを選択します。 • **必須でありません** • **常に必須** • **閉じるときに必須** これらの値の詳細については、「カスタムチケットフィールドの定義」を参照してください。

タブ	オプション	説明
	権限	このフィールドにアクセスできるユーザーを指定します。次のいずれかのオプションを選択します。 • **読み取り専用** • **所有者のみ - ユーザーから非表示** • **所有者のみ - ユーザーに表示** • **ユーザー作成** • **ユーザー修正** これらの値の詳細については、「カスタムチケットフィールドの定義」を参照してください。
	デフォルト値	このフィールドのデフォルト値を設定します。 • 事前に定義された値にこのフィールドが関連付けられている場合、それらの値が一覧に表示されて選択できるようになります。例えば、チケットテンプレートに 所有者 フィールドを追加すると、キューに関連付けられているすべてのユーザーが一覧表示されます。 • テキストフィールドを選択した場合、必要に応じて目的の値を入力できます。
条件付きロジック		このタブのオプションを使用して、以前にチケットページで選択した値に基づいて特定のフィールドを表示または非表示にします。 例えば、プリンタの問題に関するチケットテンプレートがある場合、さまざまな種類のプリンタの問題に適用されるフィールドをセットとしていくつか表示できます。プリンタに用紙がないことをユーザーがチケット上に示すと、ユーザーが用紙の形式を指定できるフィールドのセットがページに表示されます。
	公開範囲	指定した条件を満たす場合、フィールドを表示するかどうかを指定します。

タブ	オプション	説明
	タイミング	条件式の結果に基づくフィールドでの動作を指定します。次のいずれかのオプションを選択します。 • **すべての条件が一致** • **いずれかの条件が一致**
	表示されている場合は必須	チケットに表示されたとき、エンドユーザーにこのフィールドに入力してほしい場合は、このオプションを選択します。
	条件	最大 5 つの条件を追加して、選択したフィールドの表示方法を制御します。それぞれの条件で、ページに表示されるフィールドの値が特定の値と一致しているかいないかを評価できます。選択できるのは、事前に定義された値が関連付けられているフィールド (通常はチケットページに複数値の一覧として表示されます) またはチェックボックスのみです。タイトルなどの単純なテキストフィールドは、選択できません。 例えば、プリンタの問題がインク、紙、または その他 と一致するかどうかを評価する条件を作成して、必要に応じて選択したフィールドを表示または非表示にできます。

完了したら、**更新** をクリックします。

ダイアログボックスが閉じます。

6. **変更の適用** をクリックします。

ヒント: **複製** をクリックして、このテンプレートのコピーを作成することもできます。

次に、チケットテンプレートをプレビューできます。詳細については、「チケットレイアウトのプレビュー」を参照してください。

チケットレイアウトのプレビュー

選択したチケットテンプレートの 新規チケット ページと チケットの詳細 ページにチケットを表示する方法の変更が完了したら、チケットページのレイアウトをプレビューできます。

いくつかのプレビューオプションを選択できます。チケットページの情報タイプは、ページ (ユーザーまたは所有者) にアクセスするユーザーに関連付けられた権限、およびアクションのタイプ (新しいチケット または チケットの詳細) に応じて異なります。例えば、チケット所有者は通常、チケットに関連するユーザーよりも多くの情報にアクセスできます。また、新規チケット ページでは、チケットの詳細 ページとは異なり、コメントの指定または添付ファイルのリンクようの追加制御があります。

注: チケットテンプレートをプレビューすると、チケットが作成されて保存されます。チケットのプレビュー中に作成した値は、デフォルトで保存されます。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。
    または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. **設定** パネルで **キュー** をクリックします。
    c. キューの詳細 ページを表示するには、次のいずれかを実行します。
    - キューの名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. ページ上部の **フィールドとレイアウトのカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
3. **キューのカスタマイズ** ページで、チケットテンプレート セクションまで下にスクロールして、プレビューするチケットテンプレートの名前をクリックします。

    チケットテンプレートの詳細 ページが表示されます。
4. チケットテンプレートの詳細 ページで、必要に応じてカスタマイズします。

    詳細については、「チケットテンプレートの設定」を参照してください。
5. ページ最下部の **保存してプレビュー** をクリックします。

    チケットの詳細 ページが表示されます。
6. チケットの詳細 ページの上部で、**プレビュー形式** をクリックし、必要に応じて次のいずれかのオプションを選択します。

オプション	説明
入力フォーム - ユーザー	新規チケット ページ、ユーザーとして
入力フォーム - 所有者	新規チケット ページ、チケット所有者として
編集フォーム - ユーザー	チケットの詳細 ページ、ユーザーとして
入力フォーム - 所有者	チケットの詳細 ページは、チケット所有者として

新規チケット ページが更新され、選択したチケットテンプレートと所有者の詳細に基づいてチケットページが表示されます。

親/子チケット関係の利用

任意のサービスデスクチケットを**親**チケットとして設定し、それに対して子チケットを割り当てることができます。

親/子関係を利用するためには、2通りの方法があります。

- **すべての子チケットがクローズされるまで、親をクローズすることを禁止する**: この方法では、親チケットをグローバルなToDoリストとして使用し、各子チケットをリスト上の個別のタスクとして使用します。すべてのタスクが完了し、子チケットがクローズされたら、親をクローズすることができます。
- **親チケットを閉じる時点ですべての子チケットを閉じる:** 同じ問題が複数のチケットで重複している場合は、この方法が有効です。例えば、サーバーがクラッシュし、その問題に関するチケットを複数のユーザーが提出したとします。サーバーが復旧したら、チケット所有者が親を閉じることで、同時にすべての子チケットを閉じることができます。

選択される戦略にかかわらず、子チケットは孤立させることができません。つまり、子チケットを閉じる前に、親チケットを閉じることができません。

注: 必要数のレベルの親/子チケット関係を作成できますが、親チケットを閉じることで子チケットを閉じることができるのは、1レベルの親/子だけです。

キューに対する親/子チケット関係の有効化

デフォルトでは親/子チケット関係が無効になっています。この機能を有効にするには、PARENT_INFO チケットフィールドが表示されるようにキューを設定します。キューが複数ある場合は、それぞれのキューで個別に親 / 子チケット関係を有効にします。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。
    d. キューの詳細 ページを表示するには、次のいずれかを実行します。
    - キューの名前をクリックします。
    - **アクションの選択 > 新規作成** を選択します。
2. ページ上部で、**フィールドとレイアウトのカスタマイズ** をクリックします。
3. チケットの関連フィールド セクションまで下にスクロールし、PARENT_INFO フィールドの **編集** ボタンを選択して、フィールドの設定に変更を加えます。 をクリックします。
4. Owners Only - Visible to Users（ 所有者のみ - ユーザーに表示 ） 権限設定の 1 つを選択します。
5. 行で **保存** をクリックします。
6. ページの一番下で **保存** をクリックします。

これらの変更を保存すると、チケット所有者と管理者（ デフォルト ）は、キュー内のどのチケットも子または親にできます。

親チケットが子チケットを閉じられるようにする

キューを設定して、親チケットが子チケットを閉じられるようにできます。この設定を行うと、親チケットを閉じた時点で、子チケットは自動的に閉じられます。

キューに対して親 / 子関係を有効にします。詳細については、「キューに対する親/子チケット関係の有効化」を参照してください。

1. サービスデスクの キューの詳細 ページに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    c. **設定** パネルで **キュー** をクリックします。

d. キューの詳細 ページを表示するには、次のいずれかを実行します。

- キューの名前をクリックします。
- **アクションの選択 > 新規作成** を選択します。

2. User Preferences（ユーザー基本設定）セクションで、Allow parent tickets to close child tickets（親チケットが子チケットを閉じることを許可）チェックボックスを選択します。
3. ページの一番下で **保存** をクリックします。

変更内容がキューに適用されます。親チケットを閉じると、子チケットは自動的に閉じられます。

チケットの子チケットの作成

子チケットは、他のチケットを親として持つサービスデスクチケットです。子チケットの作成は、チケットを編成し、関連するタスクを管理する場合に便利です。親 / 子チケット関係が有効になっている任意のキュー内の任意のチケットに対して子チケットを作成できます。

親 / 子チケット関係は、キューに対して有効になります。詳細については、「キューに対する親/子チケット関係の有効化」を参照してください。

1. サービスデスクの チケット リストに移動します。
   a. アプライアンス管理者コンソール（https://**appliance_hostname**/admin）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
   b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
2. 既存のチケットに対して子チケットを作成するには、次の手順を実行します。
   a. チケット（複数）リストで、チケットタイトルをクリックします。
   b. Ticket Detail（チケットの詳細）ページで、**アクションの選択 > 保存して子を作成** を選択します。

   注: このオプションは、親子関係がキューに対して有効である場合にのみ使用できます。

   c. 子チケットに必要な情報を指定し、**保存** をクリックします。
3. 新しいチケットの子を作成するには、次の手順を実行します。
   a. チケット（複数）リストで、**アクションの選択 > 新規作成** を選択します。
   b. Ticket Detail（チケットの詳細）ページで、親チケットに必要な情報を指定します。
   c. **アクションの選択 > 保存して子を作成** を選択します。

   注: このオプションは、親子関係がキューに対して有効である場合にのみ使用できます。

   d. 子チケットに必要な情報を指定し、**保存** をクリックします。

親チケットを使用して重複チケットを編成し、親チケットを有効にして子チケットをクローズできます。詳細については、以下を参照してください。

- 親チケットを使用した重複チケットの整理
- 親チケットが子チケットを閉じられるようにする

親チケットの指定と既存のチケットの子としての追加

チケットを親に指定して、チケット間に親/子関係を設定できます。親チケットを指定してから、既存のチケットを子として追加する必要があります。

キューに対して親 / 子関係を有効にします。詳細については、「キューに対する親/子チケット関係の有効化」を参照してください。

1. サービスデスクの チケットの詳細 ページに移動します。

a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。
c. チケットの詳細 ページを表示するには、次のいずれかを実行します。

- チケットの名前をクリックします。
- **新規作成 > キューからの新規チケット > キュー名** の順に選択します。

多数のキューがある場合は、検索ボックスを使用して特定のキューをすばやく検索します。

2. Related Ticket Information（ 関連するチケットの情報 ）セクションで、Parent Ticket（ 親チケット ）セクションが表示されることを確認します。表示されない場合は、キューに対して親/子関係が有効になっているかどうかを確認します。詳細については、「キューに対する親/子チケット関係の有効化」を参照してください。
3. Allow this ticket to be a parent（ このチケットが親になることを許可 ）チェックボックスをオンにして、このチケットを親にします。
4. **保存** をクリックします。
5. 既存のチケットを子チケットとして追加するには、次の手順を実行します。
   a. **子チケット** セクションで、**チケットの追加** をクリックします。
   b. コンマで区切って子チケット番号を入力するか、**追加するチケットを選択** ドロップダウンリストを使用して追加するチケットを検索します。
6. **保存** をクリックしてチケットへの変更を保存します。

ToDo リストとしての親チケットの使用

サービスデスクの親/子関係を利用すると、さまざまなユーザーが実行する必要のあるタスク（ 新しい社員を雇用する際に実施しなければならないタスクなど ）をグループ化できます。この方法によって、チケットをグループとして追跡できるようになります。

- 親/子関係を有効にします。詳細については、「キューに対する親/子チケット関係の有効化」を参照してください。
- チケットキューで、親が子チケットをクローズできることを確認します。詳細については、「親チケットが子チケットを閉じられるようにする」を参照してください。

ヒント: マルチフェーズタスクを定期的に繰り返すことが予想される場合は、そのタスクをプロセスチケットにすると効果的です。詳細については、「サービスデスクプロセスの使用」を参照してください。

1. 親として機能するチケットを作成します。詳細については、「親チケットの指定と既存のチケットの子としての追加」を参照してください。
2. 親チケットから、ToDo リスト上の必要なタスクごとに子チケットを追加します。
3. タスクが完了したら各子チケットを閉じます。
4. ダイアログが表示されたら、親チケットをクローズします。このダイアログは、最後の子タスクをクローズした時点で表示されます。

注: 親チケットの解決が空の場合、子チケットの解決が親の解決に追加されます。

親チケットを使用した重複チケットの整理

同じ問題に対して複数のチケットが提出されている場合、親チケットを使用して重複したチケットをグループとして整理し、管理することができます。

キューに対して親 / 子関係を有効にし、親が子チケットを閉じられるようにします。詳細については、以下を参照してください。

- キューに対する親/子チケット関係の有効化
- 親チケットが子チケットを閉じられるようにする

1. 重複したチケットのいずれかを親として指定します。詳細については、「親チケットの指定と既存のチケットの子としての追加」を参照してください。
2. 残りの重複チケットは子チケットに変更します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. **サービスデスク** をクリックして、チケット ページを表示します。
    c. 子チケットに変更するすべてのチケットを選択します。
    d. アクションの選択 メニューで、**親に追加** を選択します。

    注: **親に追加** は、単一のキューのチケットを表示しており、そのキューで親 / 子チケット関係が有効である場合にのみ表示されます。すべてのキュー ビューでは使用できません。詳細については、「キューに対する親/子チケット関係の有効化」を参照してください。

    選択したチケットは親の子チケットになります。
3. 問題が解決されたら、親チケットを閉じます。

    子チケットは自動的に閉じられます。

チケット承認者の使用

チケットを開閉する前に、特定のユーザーまたはグループによるチケットの承認を必須とすることができます。また、承認者として設定されたユーザーのみチケットを閉じることができるようにすることも可能です。キューが複数ある場合は、それぞれのキューの承認者設定を個別に定義できます。

チケット承認者のセットアップは、次のワークフローで構成されます。

- 承認者を指定するラベルを作成する。
- 上記のラベルにユーザー（ 承認者 ）を追加する。単一のキューに制限されないよう、キューにかかわらず「すべての」ユーザーのリストから承認者を選択します。
- この機能を要求するため、キューの APPROVAL_INFO チケットフィールドを設定する。

注: 承認者は、チケットの 承認 フィールドと 承認に関するメモ フィールドにのみアクセスできます。承認 フィールドで選択可能な値は次の通りです。

- 承認されました
- 拒否されました
- 追加の情報が必要です

注: Approval（ 承認 ）フィールドは、Required（ 必須 ）オプションの設定に応じて、チケットを開閉する前に設定する必要があります。承認に関するメモ フィールドはオプションです。承認者は、**サービスデスク > チケット** をクリックし、**特定基準で表示 > マイ承認** をクリックすることで、承認する必要があるすべてのチケットを確認できます。

チケット承認者の設定

キューでチケットを開閉する前に、特定のユーザーまたはグループによるチケットの承認を必須とすることができます。

1. ユーザー リストに移動します。
    a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
    b. 左のナビゲーションバーで **設定**、**ユーザー** の順にクリックします。
2. ユーザーの隣のチェックボックスをオンにします。
3. アクションの選択 メニューで、**ラベルの追加** を選択します。
4. ラベルの追加 ウィンドウでラベルの名前を入力し（「チケット承認者」など）、**ラベルの追加** をクリックします。

    ヒント: ラベル名にはバックスラッシュ（ \ ）を使用しないでください。ラベル名にバックスラッシュを使用する必要がある場合は、バックスラッシュをもう 1 つ追加して（ \\ ）エスケープします。
5. **サービスデスク** > **設定** > **キュー** の順にクリックして、サービスデスクキュー ページを表示します。
6. キューの名前をクリックして、キュー詳細 ページを表示します。
7. User Preferences（ ユーザー基本設定 ）セクションで Allow all users as approvers（ 承認者としてすべてのユーザーを許可 ）チェックボックスをオフにして、**保存** をクリックします。
8. チケットのデフォルト セクションで、**これらの値のカスタマイズ** をクリックして、キューのカスタマイズ ページを表示します。
9. チケットレイアウト セクションで、APPROVAL_INFO 行の **編集** ボタンをクリックします をクリックします。

    編集可能な APPROVAL_INFO 行が表示されます。
10. ラベル フィールドに、4で承認者向けに作成したラベルの名前を入力します。
11. 必須 フィールドで、**閉じるときに必須** を選択します。

    閉じるときに必須 または **常に必須** の選択により、このキューのすべてのチケットに対する承認要件が有効になります。これらの設定値のいずれかを選択すると、指定するオプションによっては、チケットに対して作業を行ったりクローズしたりするために、予め承認者を指定しておく必要があります。
12. その行で **保存** をクリックした後、ページの一番下にある **保存** をクリックします。

承認機能が有効になり、選択した承認オプションが、キューのチケットに対して適用されます。

Eメールによるチケットの承認

チケット承認が設定されると、指定されたチケット承認者は、Eメールメッセージを送信してチケットを承認、承認に関するメモを追加、または異なる承認者を指定することができます。

E メールによるチケットの変更の詳細については、Eメールによるチケットの作成と管理を参照してください。承認フィールドを変更するために使用されるフィールドのリストについては、Eメールを使用した、チケット承認フィールドの変更を参照してください。

SMTP Eメールサーバーの設定

SMTP Eメールサーバーを使用するようにサービスデスクを設定できます。

POP3 E メールサーバーを設定する手順については、Eメール設定の設定を参照してください。

アプライアンスへの E メールサーバの接続

サービスデスクが E メールサーバから E メールを受信できるように、E メールサーバをアプライアンスに接続できます。接続するためのプロセスは、各環境のEメール設定によって大きく左右されます。

Microsoft Exchange Serverを使用している場合は、トランスポートルールに関するマイクロソフトの文書参照してください。

1. Exchange Server Managerを開きます。
2. **オプション**：仮想SMTPサーバーを作成します。SMTPサーバーがある場合には不要です。
3. appliance_HelpDesk という仮想 SMTP コネクタを作成します。
4. **Administrative Groups** > **コネクタ** > **appliance_HelpDesk** を選択して、appliance_HelpDesk Properties（ appliance_HelpDesk プロパティ ）ページを表示します。
5. **一般設定** をクリックします。
6. **このコネクタの各アドレススペースへのルーティングにDNSを使用する** をクリックします。

   ローカルブリッジヘッド セクションが使用可能になります。
7. ローカルブリッジヘッド セクションを完了します。

サーバー	仮想サーバー
your_exchange_servername	デフォルトSMTP仮想サーバー

8. **アドレススペース** タブをクリックします。
9. **追加** をクリックし、アプライアンス SMTP サーバのアドレススペースを追加します。次の設定を使用します。
   - 「**タイプ**」: SMTP
   - 「**アドレス**」: 完全修飾された、アプライアンスサーバ名を入力します。構文はk1000.**mydomain**.comです。
   - 「**コスト**」: 他のコネクタの、1つ上のレベルを設定します。これにより、アプライアンスの E メールが最初にフィルタリングされ、アプライアンスの E メールが誤ってネットワーク伝送されるのを防ぐことができます。
10. コネクタのスコープ の下で、**組織全体** をクリックします。
11. **これらのドメインへのメッセージの中継を許可する** はオフのままにしておきます。
12. **OK** をクリックして保存し、appliance_HelpDesk Properties（ appliance_HelpDesk プロパティ ）ページを閉じます。

E メールサーバが、アプライアンスに接続されました。

内部および外部のSMTPサーバーの使用

環境のニーズに応じて、内部SMTPサーバーまたは外部SMTPサーバーを経由するようにEメールを設定できます。

アプライアンスには、内部 SMTP サーバが含まれています。アプライアンスが受信するほとんどの E メールトラフィックがサービスデスクスタッフとやり取りされる場合は、この内部サーバを使用すると良いでしょう。内部サーバーの設定については、内部SMTPサーバーの使用を参照してください。

すべての E メールが特定の外部 SMTP サーバを経由する必要がある場合は、このサーバを使用するように、アプライアンスに指示します。詳細については、「外部SMTPサーバーまたはセキュアなSMTPサーバーの使用」を参照してください。

内部SMTPサーバーの使用

アプライアンスのネットワーク設定を構成して、内部SMTP Eメールサーバーを使用するようにします。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **ネットワーク設定** をクリックして、ネットワーク設定 ページを表示します。
3. E メール設定 セクションで、**SMTP サーバーの有効化** チェックボックスをオフにします。この設定は、外部SMTPサーバーを参照します。
4. **保存** をクリックします。
5. 要求された場合は **はい** をクリックしてアプライアンスを再起動し、変更を適用します。

送信Eメールを処理するように内部SMTPサーバーが設定されます。キューに関する SMTP 設定の詳細については、POP3 Eメールアカウントの作成と設定を参照してください。

外部SMTPサーバーまたはセキュアなSMTPサーバーの使用

外部 SMTP サーバを使用するには、アプライアンスネットワーク設定で SMTP サーバのアカウントを設定し、さらに各サービスデスクキューに SMTP サーバのアカウントを設定する必要があります。

セキュアSMTP（ SSMTP ）を使用するには、各キューでSSL設定を選択します。Microsoftは、Exchange 365 サービスのアドレスからのエイリアスを許可していないため、これが必要です。

1. 外部ルーターとファイアウォールで、アプライアンスがポート 25 を使用し、E メールを送信できることを確認します。
2. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
3. **ネットワーク設定** をクリックして、ネットワーク設定 ページを表示します。
4. 外部 SMTP サーバーを使用するには、Email Configuration（ E メール設定 ）セクションで **SMTP サーバーの有効化** を選択し、SMTP サーバーオプションを指定します。

オプション	説明
サーバー	外部 SMTP サーバーのホスト名（ **smtp.gmail.com** など ）または IP アドレスを指定します。外部 SMTP サーバでは、匿名（ 認証なし ）のアウトバウンド E メール転送を許可する必要があります。ネットワークポリシーで、アプライアンスがSMTP サーバに直接問い合わせられることを確認します。また、メールサーバは、アプライアンスからのEメールのリレーを、認証なしで許可するように設定する必要があります。IP アドレスを指定する場合は、アドレスを括弧で囲みます。例えば、「[10.10.10.10]」と入力します。

オプション	説明
ポート	外部 SMTP サーバーに使用するポート番号を入力します。標準的な SMTP にはポート 25 を使用します。セキュアな SMTP にはポート 587 を使用します。
ログイン	外部 SMTP サーバーにアクセスするアカウントのユーザー名を入力します（「**your_account_name**@gmail.com」など）。
パスワードおよびパスワードの確認入力	指定したサーバーアカウントのパスワードを入力します。

5. SMTP 設定をテストします。
    a. **Test Connection**（テスト接続）をクリックします。
    b. 表示される 接続テスト SMTP ダイアログボックスに、新しく設定した SMTP サーバを使用してテスト E メールを送信する E メールアドレスを入力し、**テスト E メールを送信** をクリックします。

    接続テスト SMTP ダイアログボックスが更新され、テスト結果の E メール操作のステータスが表示されます。テストに失敗した場合は、設定を確認し、もう一度試してください。
6. **オプション**：各キューに別の SMTP または POP3 サーバーを設定するには サービスデスクキュー E メールの設定 ページに移動します。
    a. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**設定** をクリックします。
    b. **設定** パネルの E メール設定 セクションで、**サービスデスクキューの E メール設定** をクリックします。

    サービスデスクキュー E メール設定 ページが表示されます。
7. このキューに関連付けられた E メールに外部 SMTP サーバを使用する場合、送信 E メール設定 セクションの設定を使用してください。
    a. キュー固有の SMTP 設定の指定 チェックボックスをオンにします。
    b. 次のオプションを指定します。

オプション	説明
SMTPサーバ	外部 SMTP サーバーのホスト名（**smtp.gmail.com** など）または IP アドレスを指定します。外部 SMTP サーバでは、匿名（認証なし）のアウトバウンド E メール転送を許可する必要があります。ネットワークポリシーで、アプライアンスがSMTPサーバに直接問い合わせられることを確認します。また、メールサーバは、アプライアンスからのEメールのリレーを、認証なしで許可するように設定する必要があります。
SMTPポート	外部 SMTP サーバーに使用するポート番号を入力します。標準的な SMTP にはポート 25 を使用します。セキュアな SMTP にはポート 587 を使用します。
SMTP Username（SMTP ユーザー）	外部 SMTP サーバーにアクセスするアカウントのユーザー名を入力します（「**your_account_name**@gmail.com」など）。

オプション	説明
SMTP パスワード	指定したサーバーアカウントのパスワードを入力します。

8. **保存** をクリックします。

   アプライアンスが、指定した SMTP サーバーに E メールを転送するように設定されました。複数のキューがある場合、それぞれのキューについて前の手順を繰り返します。

ヒント: デフォルトでは、アプライアンスは、送信者の E メールアドレスがアプライアンス上のユーザーアカウントと一致する場合に限り、サービスデスクの E メールを許可します。この設定を変更するには、サービスデスクチケットキューの設定の 不明なユーザーからのEメールを許可 の設定を参照してください。

メンテナンスとトラブルシューティング

アプライアンスには、管理者がシステムの正常性を維持し、監視するために役立つ自動バックアップ機能、ログ、およびトラブルシューティングツールがあります。

アプライアンスのメンテナンス

アプライアンスのメンテナンスには、バックアップスケジュールの確立、システムの正常性の確認、およびアプライアンスソフトウェアへの更新の適用が含まれます。

設定の変更の追跡

履歴サブスクリプションが情報を保持するように設定されている場合、設定、資産、およびオブジェクトに加えられた変更の詳細を確認できます。

この情報には、変更を加えた日付および変更を加えたユーザーが含まれており、トラブルシューティングの際に役立ちます。詳細については、「履歴設定について」を参照してください。

アプライアンスバックアップについて

アプライアンスのバックアップとは、データロスなどの障害の発生時にアプライアンスを復元するために使用するファイルです。

アプライアンスのバックアップファイルには、次の 2 つのタイプがあります。

- **Base**（ベース）：ファイルシステムのバックアップです。ベースバックアップファイルは、通常は週に 1 回作成されます。
- **Differential**（差異）：最新のベースバックアップおよびデータベースファイルのバックアップ以降に変更されたベース（ファイルシステム）ファイルのバックアップです。差異バックアップは、入手可能な最新のベースバックアップを参照します。

ファイルを復元するには、差異バックアップファイルとベースバックアップファイルの一致するペアが必要です。バックアップファイルのペアは、同じアプライアンスのバージョン番号と日付を参照します。アプライアンスの復元に使用できるのは、ペアになっているバックアップファイルのみです。

注: バックアップは、アプライアンスの実行中に作成されます。アプライアンスは、バックアッププロセス中もオフラインになりません。ただし、アプライアンスのバックアップへの復元およびアプライアンスの出荷時設定へのリセットでは、引き続きアプライアンスをオフラインにする必要があります。

また、バックアッププロセスには 3 つのタイプがあります。

- **Scheduled daily backups**（スケジュール済み日ベースのバックアップ）：ほとんどの場合、日ベースのバックアップには差異バックアップファイルのみが含まれます。ベースバックアップが存在しない場合、または最新のベースバックアップが 7 日よりも古い場合は、日ベースのバックアップにベースバックアップファイルと差異バックアップファイルの両方が含まれます。このバックアップを完全バックアップと呼びます。デフォルトでは、日ベースのバックアップは 02:00:00 に実行されるようにスケジュールされてい

ますが、このスケジュールは変更できます。詳細については、「日ベースのバックアップスケジュールと保存されるバックアップ数の設定」を参照してください。

- **Scheduled monthly backups**（スケジュール済み月ベースのバックアップ）：月ベースのバックアップは、毎月の最終日に実行されます。このスケジュールを変更することはできません。このバックアップには、最新のベースバックアップと、ベースバックアップの後で収集された最新の差分バックアップファイルが含まれます。
- **Backups initiated using the Run Now command**（今すぐ実行 コマンドを使用して開始されるバックアップ）：バックアップ設定 ページで **今すぐ実行** をクリックすると、アプライアンスによって完全バックアップが生成されます。これにはベースバックアップファイルと差異バックアップファイルの両方が含まれます。

バックアップを無効化することができます。バックアップを無効化すると、既存のバックアップデータを削除するようにスケジュールされ、日ベースおよび月ベースのバックアップは無効になります。詳細については、「アプライアンスのバックアップの無効化または有効化」を参照してください。

ヒント: 更新のインストールまたはアプライアンスソフトウェアのアップグレード前には、必ずアプライアンスデータをバックアップしてください。

日ベースのバックアップスケジュールと保存されるバックアップ数の設定

日ベースのバックアップスケジュールと保存されるバックアップ数を設定できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
3. 保存 セクションで、各設定を次のように指定します。

オプション	説明
毎日	アプライアンスに保存する日ベースのバックアップ数。最大で7日分のバックアップを保存できます。
毎月	アプライアンスに保存する月ベースのバックアップの数。最大で2ヶ月分のバックアップを保存できます。月ベースのバックアップは、毎月の最終日に実行されます。このスケジュールを変更することはできません。

4. スケジュール セクションで、**日ベース**のバックアップを実行するスケジュールを指定します。

   時刻は 24 時間形式でリストされ、5 分間隔で選択できます。例えば、日ベースのバックアップを深夜 12 時の 5 分後にスケジュールするには、**0:05** を選択します。

   ヒント: 毎日のログメンテナンス中にバックアップログが入れ替わらないようにするために、日ベースのバックアップは深夜 12 時よりも後に実行されるようにスケジュールしてください。

5. **保存** をクリックします。

設定が適用されます。スケジュールした次のバックアップが実行される際に、アプライアンスで保存されているバックアップの数が 保存 セクションで指定した数を超える場合には、古いバックアップファイルが削除されます。

アプライアンスの手動バックアップ

アプライアンスは、いつでも手動でバックアップできます。さらに、アプライアンスの更新をインストールしたりアップグレードを実行したりする前には、手動でアプライアンスをバックアップすることをお勧めします。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
3. ページの下部で、**今すぐ実行** をクリックし、**はい** をクリックして確定します。

   システムによって完全バックアップが実行されます。これにはベースバックアップファイルと差異バックアップファイルの両方が含まれます。

バックアップが完了すると、ログ ページが表示されます。

別のアプライアンスに移行するためにアプライアンスをバックアップする場合は、古いアプライアンスの電源をオフにします。古いアプライアンスの電源がオンのままだと、同じ設定が新しいアプライアンスにアップロードされるときに、競合を引き起こす可能性があります。

管理者コンソールからのバックアップファイルのダウンロード

リカバリ性を向上させるために、**管理者コンソール**からバックアップファイルをダウンロードして、別の場所に保存することができます。

バックアップファイルにはFTP経由でもアクセスできます。詳細については、「FTP経由でのバックアップファイルへのアクセス」を参照してください。

注: ファイルを復元するには、差異バックアップファイルとベースバックアップファイルの一致するペアが必要です。バックアップファイルのペアは、同じアプライアンスのバージョン番号と日付を参照します。アプライアンスの復元に使用できるのは、ペアになっているバックアップファイルのみです。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
3. オンボードバックアップ セクションで、差異バックアップファイルとベースバックアップファイルの一致するペアをダウンロードします。
   a. バックアップファイルのペアに関連付けられている日付を選択します。

   差分ファイルのファイル名には incr があり、ベースファイルでは base を使用します。
   例：<date>_k1_incr_<version>.tgz および <date>_k1_base_<version>.tgz。

   各バックアップファイルには、SHA256 チェックサムも表示されます。このチェックサムは、バックアップ作成時に計算されます。ダウンロードしたバックアップファイルのチェックサムが、このページに表示されるチェックサムと一致しない場合は、転送が中断されたか（ データの破損 ）、ディスク上のデータが操作された可能性があります。

   b. 要求された場合は、各ファイルのダウンロード場所を選択します。

注: 保存されたバックアップファイルには、選択した日付の最新の自動バックアップ時間（デフォルトでは午前 2 時）のアプライアンスデータが反映されます。現在のアプライアンスの状態を反映したバックアップが必要な場合は、手動バックアップを実行できます。詳細については、「アプライアンスの手動バックアップ」を参照してください。

FTP経由でのバックアップファイルへのアクセス

アプライアンスバックアップファイルへのアクセスに FTP を使用できます。これは、別のサーバー上にプロセスを作成してバックアップにアクセスしたい場合や、バックアップファイルが 1 GB を超えているため管理者コンソールでアクセスするとブラウザがタイムアウトしてしまう場合に便利です。

1. セキュリティ設定でバックアップファイルへのFTPアクセスが有効になっているか、確認します。

   詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。

2. 次のいずれかを実行します。
   - **Windows デバイスでコマンドプロンプトを開き、C:\ プロンプトで「ftp k1000」と入力します。**
   - **FTPクライアントを使用して「ftp k1000」にアクセスします。**
3. ログイン資格情報を入力します。

   デフォルトの資格情報は次の通りです。

   ユーザー名：kbftp

   パスワード：getbxf

   注: FTP パスワードを変更するには、アプライアンスのセキュリティ設定の構成を参照してください。FTPユーザー名は変更できません。
4. コマンドプロンプトでバックアップファイルにアクセスするには、次のようにコマンドを入力します。

```
> type binary
> get k1_base.tg
> get k1_base.tgz
> get k1_incr.tgz
>close
>quit
```

アプライアンスのバックアップデータの削除について

アプライアンスのバックアップデータは、アプライアンスのバックアップを無効にすることによって削除できます。

バックアップの無効化は、アプライアンスが保存するデータの量を削減したい場合に役立ちます。例えば、仮想アプライアンスが、アプライアンスバックアップファイルを使用するのではなく仮想マシンのスナップショットを使用してアプライアンスデータをバックアップする場合、アプライアンスのバックアップを無効にして、仮想マシンのサイズを小さくすることができます。

重要: バックアップを無効にすると、障害が発生した場合に、管理者コンソールからアプライアンスの設定とデータを復元できなくなります。そのため、アプライアンスのバックアップの無効化は、仮想アプライアンスに対する仮想マシンのスナップショットなど、データをバックアップする別の方法を使用する場合のみにする必要があります。物理アプライアンスでは、バックアップを無効にすることは推奨されません。

アプライアンスのバックアップの無効化または有効化

デフォルトでは、アプライアンスのバックアップは有効になっています。必要に応じてアプライアンスのバックアップを無効化および有効化できます。

アプライアンスのバックアップを無効にすると、次にスケジュールされたバックアップ時に、既存のバックアップファイルが削除されるようにスケジュールされます。

重要: バックアップを無効にすると、障害が発生した場合に、管理者コンソールからアプライアンスの設定とデータを復元できなくなります。そのため、アプライアンスのバックアップの無効化は、仮想アプライアンスに対する仮想マシンのスナップショットなど、データをバックアップする別の方法を使用する場合のみにする必要があります。バックアップの無効化は、物理バージョンのアプライアンスにはお勧めできません。

1. **オプション**：障害が発生した場合にデータおよび設定を復元する能力を保持するには、バックアップを無効にする前に、管理者コンソールから最新のバックアップファイルをダウンロードして別の場所に保存します。詳細については、「管理者コンソールからのバックアップファイルのダウンロード」を参照してください。
2. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
3. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
4. Retention（ 保持 ）セクションで、**バックアップを無効にする** を選択します。
5. **保存** をクリックします。

   次のアクションが実行されます。
   - すべてのバックアップオプションが無効になります。
   - バックアップ保持設定は、日ベースのバックアップには 1 が、月ベースのバックアップには 0 が設定されます。
   - 既存のバックアップファイルは、次にスケジュールされたバックアップ時にアプライアンスから削除されるようにスケジュールされます。
6. アプライアンスのバックアップを有効にするには、**バックアップを無効にする** チェックボックスをオフにしてから **保存** をクリックします。
7. **オプション**：**今すぐ実行** をクリックしてシステムの完全バックアップを生成します。これにはベースバックアップファイルと差異バックアップファイルの両方が含まれます。

オフボードバックアップ転送の設定

アプライアンスのバックアップでは、データロスなどの障害が発生した場合にアプライアンスを復元できます。アプライアンスの OS またはデータベースに問題が発生し、アプライアンスのイメージを再作成するように求められた場合、イメージの再作成前に安全な場所にバックアップファイルをコピーしていないと、バックアップを復元できません。バックアップ設定 ページでは、外部の場所へのバックアップデータの転送を自動的に設定でき

ます。設定されている場合、アプライアンスでは、夜間バックアッププロセスが完了するたびに、バックアップファイルを外部の場所にコピーします。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
3. オフボードバックアップ転送の設定 セクションで、**オフボードバックアップ転送を無効にする** をオフにします。
4. **オフボードバックアップ転送プロトコル** をクリックし、バックアップファイルの転送に使用するプロトコルを**Samba**、**FTP**、または**Secure FTP** から選択します。

オプション	説明
オフボードバックアップ転送を無効にする	オフボードバックアップ転送を無効にするか有効にするかを指定します。オフボードバックアップ転送を有効にするには、このチェックボックスをオフにします。
オフボードバックアップ転送プロトコル	バックアップファイルの転送に使用するプロトコル：**Samba**、**FTP**、**セキュア FTP**、**Azure Blob Storage**、または **Amazon S3**。Azure Blob Storage または Amazon S3 を使用する場合は、ストレージアカウントを設定する必要があります。詳細については、MS Azure および Amazon のマニュアルを参照してください。 **重要: セキュア FTP（ SFTP ）、Azure Blob Storage、および Amazon S3 プロトコルは、整合性チェック機能を内蔵した安全な転送に対応するベストプラクティスの推奨です。FTP と Samba のオプションも利用できますが、これらのプロトコルに固有の脆弱性があり、データ転送が暗号化されないため、推奨されません。**
オフボードバックアップ転送サーバ	バックアップファイルのコピー先であるマシンのホスト名または IP アドレス。
パスまたは共有名	バックアップファイルのコピー先であるマシン上のディレクトリのパス。
ユーザー名	宛先マシンにアクセスするために使用するユーザーアカウントの名前。
ユーザーパスワード	ユーザー名に関連付けられたパスワード。

5. 提供されたアドレスおよび資格情報を使用して宛先マシンにアクセスできるかどうかを確認するには、**テスト** をクリックします。

   操作の成功を示すメッセージが表示されます。宛先サーバーへのアクセスに失敗した場合、このことがメッセージに示されます。設定を確認し、必要に応じて変更します。
6. **保存** をクリックします。

アプライアンスの復元

バックアップが有効であり、差異バックアップファイルとベースバックアップファイルの一致するペアがある場合は、バックアップファイルを使用してアプライアンスのデータを復元できます。また、アプライアンスはいつでも出荷時設定にリセットできます。

アプライアンスを復元すると、アプライアンスに現在設定されているデータは破棄されます。Quest KACEでは、アプライアンスを復元する前に、残しておきたいあらゆるバックアップファイルまたはデータをオフロードすることをお勧めしています。また、アプライアンスの復元では、アプライアンスをオフラインにする必要があります。復元プロセス中は、**管理者コンソール**および**ユーザーコンソール**は使用できません。

注: ファイルを復元するには、差異バックアップファイルとベースバックアップファイルの一致するペアが必要です。バックアップファイルのペアは、同じアプライアンスのバージョン番号と日付を参照します。アプライアンスの復元に使用できるのは、ペアになっているバックアップファイルのみです。

最新のバックアップを使用したアプライアンスの復元

アプライアンスには、アプライアンスバックアップドライブ上にある最新のバックアップから設定を直接復元する組み込みの機能があります。

アプリケーションのバックアップが有効であり、差異バックアップファイルとベースバックアップファイルの一致するペアがあります。詳細については、「アプライアンスのバックアップの無効化または有効化」を参照してください。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
3. オンボードバックアップ セクションで、最も新しいバックアップファイルを選択します。
4. **バックアップからの復元** をクリックし、**はい** をクリックして確定します。

   アプライアンスが復元され、再起動します。復元プロセス中は、**管理者コンソール**および**ユーザーコンソール**は使用できません。ブラウザのウィンドウに進行状況が表示されます。

バックアップファイルのアプライアンスへのアップロード

アプライアンス以外の場所にバックアップファイルをコピーしてある場合は、**管理者コンソール**、FTP、またはクライアントドロップの場所プロセスを使用して、これらのファイルをアプライアンスに手動でアップロードできます。FTP およびクライアントドロップの場所によるアップロードは、バックアップファイルが 1 GB 超えるため**管理者コンソール**でアップロードするとブラウザがタイムアウトする場合に便利です。

バックアップファイルはアプライアンス以外の場所にコピーしてあります。

注: ファイルを復元するには、差異バックアップファイルとベースバックアップファイルの一致するペアが必要です。バックアップファイルのペアは、同じアプライアンスのバージョン番号と日付を参照します。アプライアンスの復元に使用できるのは、ペアになっているバックアップファイルのみです。

- 管理者コンソールを使用してファイルをアップロードするには、次の手順を実行します。

1. アプライアンスの コントロールパネル に移動します。
   - アプライアンスで組織コンポーネントが有効化されていない場合は、管理者コンソール（ http://**appliance_hostname**/admin ）にログインして、**設定** をクリックします。
   - アプライアンスで組織コンポーネントが有効化されている場合は、システム管理コンソール（ http://**appliance_hostname**/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから **システム** を選択して、**設定** をクリックします。
2. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
3. Uploads（ アップロード ）セクションの Differential（ 差異 ）の見出しの下で、**参照** または **ファイルの選択** をクリックし、アップロードする差異ファイルを指定します。

1.5 GB 以上のファイルをアップロードするには、FTP を使用する必要があります。詳細については、次の手順を参照してください。ファイルが FTP でアップロードされると、復元 セクションにダウンロードできると表示されます。

4. Uploads（ アップロード ）セクションの Base（ ベース ）の見出しの下で、**参照** または **ファイルの選択** をクリックし、アップロードするベースファイルを指定します。

注: ファイルを復元するには、差異バックアップファイルとベースバックアップファイルのペアをアップロードする必要があります。バックアップファイルのペアは、同じアプライアンスのバージョン番号と日付を参照します。アプライアンスの復元に使用できるのは、ペアになっているバックアップファイルのみです。

5. **ファイルのアップロード** をクリックします。

   アップロードしたファイルが バックアップ設定 ページの Backups（ バックアップ ）セクションに表示されます。

- FTP を使用してバックアップファイルをアプライアンスにアップロードするには、次の手順を実行します。
  1. セキュリティ設定でバックアップファイルへのFTPアクセスが有効になっているか、確認します。

  詳細については、「アプライアンスのセキュリティ設定の構成」を参照してください。

  2. 次のいずれかを実行します。
     - Windows デバイスでコマンドプロンプトを開き、C:\ プロンプトで「ftp k1000」と入力します。
     - FTPクライアントを使用して「ftp k1000」にアクセスします。
  3. FTP ログイン資格情報を入力します。

  デフォルトの資格情報は次の通りです。

  ユーザー名：kbftp
  パスワード：getbxf

  注: FTP パスワードを変更するには、アプライアンスのセキュリティ設定の構成を参照してください。FTPユーザー名は変更できません。

  アップロードしたファイルが バックアップ設定 ページの Backups（ バックアップ ）セクションに表示されます。

- クライアントドロップの場所の方法を使用してバックアップファイルをアップロードするには、アプライアンスのクライアントドロップの場所にバックアップファイルを置きます。

  クライアントドロップの場所に置かれたファイルは自動的にバックアップファイルとして識別され、5 分以内に バックアップ設定 ページで選択できるようになります。詳細については、「アプライアンスクライアントドロップの場所へのファイルのコピー」を参照してください。

アップロードしたバックアップファイルを使用して、アプライアンスを復元します。詳細については、「バックアップからのアプライアンスの復元」を参照してください。

バックアップからのアプライアンスの復元

必要に応じてアプライアンスをバックアップファイルから復元できます。

アプライアンス以外の場所からファイルを復元するには、差異バックアップファイルとベースバックアップファイルの一致するペアをアプライアンスにアップロードしておく必要があります。詳細については、「バックアップファイルのアプライアンスへのアップロード」を参照してください。

アプライアンスを新しいアプライアンスに移行する場合は、2 つのアプライアンスが同じバージョンである必要があります。同じでない場合、古いアプライアンスを新しいアプライアンスで実行されているバージョンにアップグレードする必要があります。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
3. オンボードバックアップ セクションで、復元したいファイルのペアを選択します。
4. バックアップファイルからネットワーク設定を無視し、復元オプション で新しい設定を指定する場合は、**ネットワーク設定のオーバーライド** を選択して、該当するオプションを指定します。

   このチェックボックスをオンにすると、このページに一連のオプションが表示されます。これらは、初期設定時に設定する必要があるアプライアンスネットワーク設定と同じです。詳細については、「アプライアンスのネットワーク設定の変更」を参照してください。
5. **バックアップからの復元** をクリックし、**はい** をクリックして確定します。

   アプライアンスが復元され、再起動します。復元プロセス中は、**管理者コンソール**および**ユーザーコンソール**は使用できません。ブラウザのウィンドウに進行状況が表示されます。

   このプロセスには最大 1 時間かかる可能性があり、アプライアンスはこの間使用できません。復元の時間は、バックアップファイルのサイズによって異なります。復元が完了すると、アプライアンスが再起動します。再起動後、アプライアンスは、バックアップファイルの作成時点と同じ状態になります。これには、同じ認証設定、ネットワーク設定などが含まれます。

   再起動時に IP 設定が行われていない場合は、IP 設定を適切に行うために、再起動を 1 回または 2 回試してください。この方法を使用しても設定が行われていない場合は、試しにコンソール ログイン netdiag/netdiag ユーティリティを使用して、IP アドレスを更新してください。

アプライアンスが復元され、再起動します。

出荷時設定へのアプライアンスの復元

アプライアンスには、出荷時設定に復元する組み込みの機能があります。これは、問題が発生した際にカスタム設定をすべて元に戻したいときに便利です。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **バックアップ設定** をクリックして、バックアップ設定 ページを表示します。
3. ページの下部で、**出荷時設定にリセット** をクリックし、**はい** をクリックして確定します。

   アプライアンスが復元され、再起動します。
4. 必要に応じてアプライアンスを再設定します。

   詳細については、「アプライアンスの設定」を参照してください。

アプライアンスソフトウェアの更新

アプライアンスソフトウェア更新を確認してインストールできます。アプライアンスを更新した場合、サービスデスクや資産のカスタマイズなど、カスタム設定は保持されます。

アプライアンス通知更新の確認および適用

アプライアンスは、アプライアンスソフトウェアの更新が公開されているかどうかを確認するために、Quest のサーバに毎日チェックインします。これらの更新は通知更新と呼ばれます。

適用可能な更新プログラムがある場合は、次回管理者アカウント権限でログインしたときに、ホーム ページに警告が表示されます。

ヒント: 更新のインストールまたはアプライアンスソフトウェアのアップグレード前には、必ずアプライアンスデータをバックアップしてください。手順については、アプライアンスバックアップについてを参照してください。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。
3. サーバー セクションで、**更新の確認** をクリックして ログ ページを表示します。

   確認の結果がログに表示されます。
4. 更新が使用可能な場合は、データベースとファイルをバックアップしてください。

   詳細については、「アプライアンスバックアップについて」を参照してください。
5. **更新** をクリックします。

更新が適用されます。**管理者コンソール**は、アップデートが完了するまで利用できません。ブラウザウィンドウと**管理者コンソール**に進捗が表示されます。

手動による更新ファイルのアプライアンスへのアップロード

Questで更新ファイルが公開されている場合、手動でアプライアンスにアップロードできます。

アプライアンスを手動で更新する前に更新ファイルのリリースノートを読んで、ご使用のアプライアンスがサーババージョンの最小要件を満たしているか確認してください。アプライアンスが最小要件を満たしていない場合には、アプライアンスソフトウェアを更新する前に最小バージョンへアップグレードする必要があります。詳細については、「アプライアンスバージョン、モデル、およびライセンス情報の表示」を参照してください。

1. データベースとファイルをバックアップします。詳細については、「アプライアンスバックアップについて」を参照してください。
2. k1000_upgrade_server_**XXXX**.kbin ファイルをダウンロードして、ローカルで保存します。
3. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
4. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。
5. 手動によるアップデート セクションで次の操作を実行します。
   a. **参照** または **ファイルを選択** をクリックして、アップデートファイルを見つけます。
   b. **アップデート** をクリックし、**はい** をクリックして確認します。

更新が適用されます。**管理者コンソール**は、アップデートが完了するまで利用できません。ブラウザウィンドウと**管理者コンソール**に進捗が表示されます。

更新の検証

更新の適用後、更新ログを参照して、更新が正常に完了したことを確認できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **ログ** をクリックして、ログ ページを表示します。
3. ログ ドロップダウンリストから、**更新** を選択します。
4. ログでエラーメッセージと警告を確認します。
5. ページの右上隅にある **サポートが必要な場合** をクリックし、ヘルプ パネルの下部にある **バージョン情報** をクリックして、現在のバージョンを確認します。詳細については、「アプライアンスバージョン、モデル、およびライセンス情報の表示」を参照してください。

アプライアンスライセンスキーの更新

ライセンス機能を拡張した場合、または組織コンポーネントなどの追加コンポーネントを購入した場合に、アプライアンスのライセンスキーが必要になることがあります。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。
3. License Information（ ライセンス情報 ） セクションで、ライセンスキーを入力します。
4. **更新** をクリックします。

アプライアンスの再起動またはシャットダウン

トラブルシューティングやメンテナンスタスクの実行時には、アプライアンスの再起動やシャットダウンが必要になることがあります。

また、アプライアンスの電源を切る前にもシャットダウンが必要です。

ヒント: 物理アプライアンスを任意のときにシャットダウンするには、電源ボタンを1回素早く押します。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。
3. アプライアンスの管理 セクションで、次のいずれかを実行します。
   - **再起動 をクリックします。アプライアンスが再起動します。**
   - **データベースを再起動してチェックする をクリックします。アプライアンスが再起動し、データベースが検証されます。**
   - **シャットダウン をクリックします。アプライアンスがシャットダウンされ、アプライアンスハードウェアの電源を安全に切れるようになります。**

KACEからのOVAL定義の更新

OVAL（ Open Vulnerability Assessment Language ）テストの定義はスケジュールに従って自動的に更新されますが、アプライアンスの更新 ページから最新のファイルを手動で取得することもできます。

OVAL 定義の詳細については、デバイスとアプライアンスのセキュリティの維持を参照してください。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、アプライアンスの更新 ページを表示します。
3. OVALカタログ セクションで **更新の確認** をクリックし、**はい** をクリックします。

日次実行出力の理解

アプライアンスの **日次実行出力** は、ディスクステータス、ネットワークインターフェイスステータス、アプライアンスの稼働時間平均など、アプライアンスのステータス情報を示すレポートです。

このレポートは毎日、午前 2:00 に E メールでシステム管理者に自動的に送信されます。システム管理者の E メールアドレスを変更するには、組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定または組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。

ディスクステータス

毎日システム管理者にEメールで自動的に送信される日次実行出力レポートには、ディスクステータス 表があります。

ファイルシステム	サイズ	使用中	使用可能	容量	マウント場所
/dev/twed0s1a	38G	3.6G	32G	10%	/
devfs	1.0K	1.0K	0B	100%	/dev
fdescfs	1.0K	1.0K	0B	100%	/dev
procfs	4.0K	4.0K	0B	100%	/proc

Disk status（ **ディスクステータス** ） **表には次の列が表示されます。**

列の見出し	説明
ファイルシステム	ファイルシステムの名前。
サイズ	指定したファイルシステムに割り当てられているディスクスペースの容量。
使用中	指定したファイルシステムによって使用中のディスクスペースの容量。
使用可能	指定したファイルシステムに使用可能なディスクスペースの空き容量。

列の見出し	説明
容量	指定したファイルシステムに使用可能なディスクスペースの割合。
マウント場所	指定したファイルシステムが置かれているディスクパーティション。

アプライアンスのネットワークインターフェイスのステータス

毎日システム管理者に E メールで自動的に送信される日次実行出力レポートには、ネットワークインタフェースステータス 表があります。

Ierrs/Oerrs がゼロであることを確認します。その他の値はネットワークエラーを示します。

エラーが続く場合は、**Questサポート**（https://support.quest.com/contact-support）にお問い合わせください。

```
Network interface status:
Name    Mtu Network       Address              Ipkts Ierrs    Opkts Oerrs  Coll
em0    1500 <Link#1>      00:0c:29:83:85:63 30383751     0 29509710     0     0
em0    1500 192.168.200.0 MyK1              30379356     - 29509310     -     -
plip0  1500 <Link#2>                            0     0        0     0     0
lo0   16384 <Link#3>                       392328     0   392328     0     0
lo0   16384 fe80:3::1     fe80:3::1             0     -        0     -     -
lo0   16384 localhost     ::1                 216     -      216     -     -
lo0   16384 your-net      localhost          392112     -   392112     -     -
```

アプライアンスの稼働時間と負荷平均

毎日システム管理者に E メールで自動的に送信される日次実行出力レポートは、アプライアンスの稼働時間と読み込み平均を示します。

負荷平均は、レポートが実行されたときのアプライアンスの負荷によって異なります。

以下の内容は、前回に電源がオフになってからアプライアンスが稼働していた時間を示しています。この例では、アプライアンスにログオンしているユーザーはいません。

Local system status:
2:01AM up 7 days, 4:12, 0 users, load averages: 0.05, 0.20, 0.15

Eメールシステムの正常性

毎日システム管理者に E メールで自動的に送信される日次実行出力レポートは、E メールシステムの正常性を示します。

次に示すメッセージは、Eメールシステムの正常性に関する標準的なFreeBSDのメッセージです。

キュー内にEメールメッセージはありません。キュー内にメッセージがある場合は、SMTP設定の検証を参照してください。

Mail in local queue:
/var/spool/mqueue is empty
    Total requests: 0
Mail in submit queue:
/var/spool/clientmqueue is empty
    Total requests: 0
Security check:
  (output mailed separately)
Checking for rejected mail hosts:
Checking for denied zone transfers (AXFR and IXFR):
tar: Removing leading /' from member names

SMTP設定の検証

キュー内にEメールメッセージがある場合は、SMTP設定を検証します。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. **ネットワーク設定** をクリックして、ネットワーク設定 ページを表示します。

アプライアンスのバックアップステータス

毎日システム管理者に E メールで自動的に送信される日次実行出力レポートは、アプライアンスのバックアップステータスを示します。

次に示すアプライアンス固有のメッセージは、バックアップが正常に完了して、FTPを通じて使用可能な/kbackupディスク上に保存されていることを示します。

詳細については、「FTP経由でのバックアップファイルへのアクセス」を参照してください。

[2015/06/21 02:01:24 -0700] Backup: Complete.

RAIDドライブのステータス

物理 KACE SMA の場合、RAID ドライブのステータスがサーバーログに表示されます。このステータスは、物理 KACE SMA に関してのみ表示されます。

次のログメッセージは、RAIDドライブが正しく機能していることを示しています。

Logical Drive 0 (RAID 5) Information
RAID Array Status: Logical Drive 0 is not rebuilding: status is Optimal.
ステータス: Online.Spun Up

RAID ドライブのパフォーマンスが低下している場合、または適切に再構築されない場合は、**Questサポート**（ https://support.quest.com/contact-support ）にお問い合わせください。

アプライアンスのトラブルシューティング

アプライアンスには、システムの正常性を監視し、問題を解決するために役立つツール、ログ、およびレポートが含まれています。

トラブルシューティングツールの使用

トラブルシューティングツールを使用して、問題を特定し、解決できます。

ネットワーク上のデバイスのステータス確認

ネットワーク上のデバイスのステータスを確認するには、pingトラブルシューティングユーティリティを使用します。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**サポート** をクリックして、サポート ページを表示します。
3. トラブルシューティングツール セクションで、**診断ユーティリティの実行** をクリックして、診断ユーティリティ ページを表示します。
4. テキストボックスにデバイスのIPアドレスを入力します。
5. ドロップダウンリストの **ping** を選択します。
6. **今すぐ実行** をクリックします。

   結果が表示されます。
7. 他のユーティリティを使用するには、ドロップダウンリストから選択して、**今すぐ実行** をクリックします。

デバイスの問題の識別

デバイスの問題 リストを使用して、管理対象デバイスのいずれかにエージェントへの接続の問題があるかどうか、またはその他の問題があるかどうかを確認します。

アプライアンスは、KACE エージェントを使用して、組織内のエージェント管理対象デバイスから情報を収集します。デバイスのエージェントへの接続で問題が発生した場合、またはその環境に関連するその他の問題が発生した場合、アプライアンスはそのデバイスのインベントリ情報を取得できません。

デバイスの問題 リストページには、次のいずれかの問題が原因でインベントリに情報が表示されないエージェント管理デバイスが表示されます。

- WMI（ Windows Management Instrumentation ）の破損です。
- デスクトップのヒープが枯渇状態です。

  ヒント: ほとんどの場合、この問題はデバイスを再起動するだけで解決できます。
- amp.conf への書き込みに失敗しました。

これらの問題の詳細については、「https://support.quest.com/kace-systems-management-appliance/kb」を参照してください。

1. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。
2. **設定 > サポート** の順に選択して、サポート ページを表示します。
3. トラブルシューティングツール セクションで、**デバイスの問題** をクリックして、デバイスの問題 ページを表示します。
4. デバイスの問題 の不良デバイスのリストを確認し、必要に応じてこれらの問題を解決するための手順を実行します。

Quest KACE サポートへの tether を有効にする

Questサポートポータルにアクセスして、アプライアンスへのtetherを要求し、Quest KACEテクニカルサポートが問題をトラブルシューティングできるようにすることができます。

Questサポート（https://support.quest.com/contact-support）に連絡して tether キーを取得します。

セキュリティを確保するために、サポートチームがアプライアンスへのリモートアクセスを有効にすることを承認した後で、アプライアンスへのリモートアクセスを有効にします。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（https://appliance_hostname/admin）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（https://appliance_hostname/system）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. アプライアンスの コントロールパネル で **セキュリティ設定** をクリックして、セキュリティ設定 ページを表示します。
3. **SSH の有効化** チェックボックスがオンになっていることを確認します。
4. **保存してサービスを再起動** をクリックします。
5. 左側のナビゲーションバーで、**サポート** をクリックして、サポート ページを表示します。
6. トラブルシューティングツール セクションで、**tether キーの入力** をクリックして、Support Tether キー ページを表示します。
7. Support Tether キー ページで、テキストフィールドに問題の説明を入力し、次のいずれかの手順を実行します。
   - **tether キーを自動的に取得してテクニカルサポートにメッセージを送信するには、tether を有効にする をクリックします。**

     このプロセスが失敗した場合は、**tether を有効にする** を選択し、指示に従って tether キーを入力します。**保存** をクリックします。
   - **テクニカルサポートから提供される tether キーを使用するには、すでに tether キーを保持しているをクリックし、tether を有効にする を選択して、指示に従って tether キーを入力します。保存 をクリックします。**

アプライアンスの問題のトラブルシューティング

アプライアンスサーバログは、管理者と **Questサポート**がエラーを検出して解決する際に役立ちます。

ログには過去7日分のアクティビティが記録され、毎日コピーされて圧縮されます。圧縮されたログは、作成後7日間を超えると削除されます。

ログメンテナンスのチェックは毎日実行されるため、管理ログのメンテナンスを行うための追加作業は特に必要ありません。

アプライアンスログの表示

アプライアンスログは、**管理者コンソール**で確認できます。アプライアンスログには、アプライアンスプロセスに関連する情報と、システムで発生したエラーに関連する情報が記載されます。

Quest KACE と使用率の詳細データが共有されるようにアプライアンスが設定されている場合は、アプライアンスとエージェントの例外やエラーが毎日 Quest にレポートされます。詳細については、以下を参照してください。

- 組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定
- 組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**ログ** をクリックして、ログ ページを表示します。
3. ログ ドロップダウンリストでログを選択します。

ログタイプ	ログ名	説明
ハードウェア	ディスクステータス	物理アプライアンスディスクアレイのステータス（仮想アプライアンスには使用できません）。
サーバー	K1000ログ	アプライアンス上で発生したエラー。
	アクセス	HTTPサーバーのアクセス情報。
	サーバーエラー	アプライアンスサーバープロセスに関するエラーやサーバー警告。
	状態	アプライアンスが一定期間に処理している接続の数。
	更新	アプライアンスに適用される、アプライアンスのパッチまたはアップグレードの詳細。
	レポートログ	実行されたレポートの詳細。
	レポートエラー	実行されたレポートに関連するエラー。
	Konductorログ	Konductor関連の口グ。Konductorは、アプライアンスと管理対象デバイスの間の通信を調整してシステムのスムーズな実行を維持する内部アプライアンスコンポーネントです。Konductorが実行しているタスクの数は、進行中のタスク数 ウィジェットに表示されます。さらに、タスクスループット情報が、アプライアンスの 一般設定 ページ（組織コンポーネントが有効なアプライアンスの場合）ま

ログタイプ	ログ名	説明
		たは 通信設定 ページ (組織コンポーネントが有効になっていないアプライアンスの場合) に表示されます。詳細については、以下を参照してください。 • 組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定 • エージェント通信とログ設定の定義
	パッチダウンロードのログ	アプライアンスにダウンロードされたパッチに関する情報。
	Dell アップデートログ	アプライアンスにダウンロードされた Dell ハードウェアアップデートに関する情報。
	バックアップログ	日ベースおよび月ベースのアプライアンスバックアップの詳細。
	復元ログをバックアップする	アプライアンスのバックアップからの情報の復元に関する詳細。
	検出ログ	検出プロセスに関連する情報。
	プロビジョニングログ	KACE エージェントのプロビジョニングに関する情報。
	エージェント不要ログ	アプライアンスへのエージェント不要デバイス接続に関する情報。
	Monitoring Log (監視ログ)	監視対象サーバおよびそれらのアプライアンスへの接続に関連する情報。
	ソフトウェアインベントリ	ソフトウェアカタログインベントリ処理に関連する情報。
	Software Inventory Errors (ソフトウェアインベントリエラー)	アプライアンスソフトウェアカタログインベントリ処理に関連する処理エラー。
	資産のインポートログ	資産のインポートに関する情報。
	Dell 保証ログ	Dell 保証アップデートに関連する情報。

ログタイプ	ログ名	説明
	ユーザー認証ログ	ユーザー認証に関連する情報。ログの各エントリには、次の情報が含まれています。 • ログインを試行するユーザーアカウントの名前。 • ログイン試行の発信元デバイスの IP アドレス。 • ユーザーがログインを試行するコンソール：userui（**ユーザーコンソール**）、systemui（**システム管理コンソール**）、adminui（**管理者コンソール**）、またはリンク先アプライアンス。 • ユーザが認証される組織の名前。 • 使用する認証のタイプ：ローカル認証、シングルサインオン、systemui ローカル認証、または LDAP。 • ログイン試行の結果：success または failed 例： [2018-04-26 07:27:06 -0700] AUTH [info] admin - 10.1.243.172 - adminui - Default - systemui Local Authentication - success
メール	**Service Desk Incoming Mail Log（サービスデスク受信メールログ）**	Exim サーバー（メール転送エージェント）がサービスデスクキューの E メールを処理する際に発生した問題に関連する情報。例えば、無効な E メールアドレスや、サービスデスクのライセンスの問題などです。
	Service Desk Incoming Mail Error Log（サービスデスク受信メールエラーログ）	受信 E メールメッセージが処理されたときに発生した PHP エラー。
	Service Desk Outgoing Mail Log（サービスデスク送信メールログ）	メールデーモンが送信 E メールメッセージを送信する際に発生したエラー。例えば、無効な E メールアドレスなどです。
	Service Desk Outgoing Mail Error Log（サービスデスク送信メールエラーログ）	送信 E メール通知が処理されたときに発生した PHP エラー。

ログタイプ	ログ名	説明
	KMailServices ログ	KMailServices プロセスに関連する情報。
EXIM	**Exim メインログ**	各メッセージの到着終了配信に関連する情報。
	Exim 拒否ログ	拒否されたメッセージに関連する情報。
デバイス	**クライアントアクセス**	KACE エージェントアクセスログ。
	クライアントエラー	KACE エージェント例外ログ。
	エージェントのメッセージプロトコルサーバー	サーバーに関連するエージェントメッセージプロトコルログエントリ。
	エージェントのメッセージプロトコルサーバーエラー	サーバーに関連するエージェントのメッセージプロトコルログエラー。
	エージェントのメッセージプロトコルキュー	サーバーに関連するエージェントメッセージングプロトコルログエントリ。
	エージェントメッセージプロトコルキューエラー	キューに関連するエージェントのメッセージプロトコルログエラー。

システムで組織コンポーネントが有効になっている場合は、保持されている毎日のログの数を変更できます。この設定は、アプライアンスの 一般設定 の ログの保持 セクションに表示されます。詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。

アプライアンスのアクティビティログのダウンロード

アプライアンスのアクティビティログは、**管理者コンソール**からダウンロードできます。これらのログは、トラブルシューティング時に役立ちます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**サポート** をクリックして、サポート ページを表示します。
3. **アプライアンスのアクティビティログの取得** をクリックします。

   ログは k1000_logs.tgz ファイルとしてダウンロードされます。

デバッグで使用するログの詳細については、以下を参照してください。

- プロビジョニングスケジュールの管理
- KACE エージェントのトラブルシューティングとデバッグ
- アプライアンスログの表示

システムで組織コンポーネントが有効になっている場合は、保持されている毎日のログの数を変更できます。この設定は、アプライアンスの 一般設定 の ログの保持 セクションに表示されます。詳細については、「組織コンポーネントが有効になっている場合のアプライアンス一般設定項目の設定」を参照してください。

日次実行出力の表示

日次実行出力は、ディスクステータス、ネットワークインターフェイスステータス、稼働時間と読み込み平均、メールシステムの正常性、およびデータベースのステータスなどのアプライアンス情報を示すレポートです。このレポート使用して、システムのステータスを確認し、解決が必要な問題を特定します。

このレポートは毎日実行され、Eメールで管理者に送信されます。日次実行出力の理解およびセキュリティの実行出力を参照してください。

KACE エージェントのトラブルシューティングとデバッグ

エージェント関連の問題をトラブルシューティングするには、エージェントのデバッグ機能を使用します。

デバイスがインベントリに表示されない場合は、**エージェントのデバッグトレース** オプションが 通信設定 ページで有効になっていることを確認します。詳細については、「エージェント通信と口グ設定の定義」を参照してください。

その他のサポートについては、**Questサポート**ウェブサイト（ https://support.quest.com/contact-support ）にアクセスしてください。このWebサイトには、サポート技術情報が含まれており、トラブルシューティングに役立てることができます。

エージェントのプロビジョニングを妨げる Windows のセキュリティに関する問題の解決

Windows のセキュリティ設定によって、アプライアンスによる Windows デバイスへのエージェントのプロビジョニングが妨げられる場合は、コマンドプロンプトを使用して設定を変更できます。

プロビジョニングを許可するには、ファイアウォールを開いてセキュリティ設定を行う必要があります。

1. デバイスでコマンドプロンプトを開きます。
2. ファイアウォールを開いてセキュリティ設定を行います。

   reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v ForceGuest /t REG_DWORD /d 0 /f

   reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f

   reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v FdenyTSConnections /t REG_DWORD /d 0 /f

   netsh.exe firewall set service type=FILEANDPRINT mode=ENABLE scope=ALL

   netsh.exe firewall set service type=REMOTEADMIN mode=ENABLE scope=ALL

Eメール通信のテストとトラブルシューティング

いくつかの手順を実行して、サービスデスクのEメール通信が正しく機能していることを確認できます。送信Eメールと受信Eメールをテストして、Eメールシステムの設定を確認できます。さらに、Telnetを使用してEメールをテストできます。エラー情報を提供するためにログファイルを利用できます。

テストとトラブルシューティング情報では、「Eメール設定の設定」で説明するように、POP3 E メールサーバを使用してアプライアンスと通信していることを前提としています。

送信Eメールのテスト

送信Eメールをテストして、システムの設定を確認できます。

1. アプライアンスの コントロールパネル に移動します。
   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**
2. 左側のナビゲーションバーで、**サポート** をクリックして、サポート ページを表示します。
3. トラブルシューティングツール セクションで、**診断ユーティリティの実行** をクリックして、診断ユーティリティ ページを表示します。
4. テスト ドロップダウンリストで、**email sending** を選択します。
5. テキストボックスに、有効なEメールアドレスを入力します。
6. **今すぐ実行** をクリックして、E メールのパスの口グを表示します。
7. エラーについて口グファイルを確認します。
   - **エラーがレポートされない場合、送信Eメールは正常に送信されています。**
   - **エラーの場合には、以下の手順を実行します。**
     - メールとスパムフィルタを確認します。
     - アプライアンスのネットワーク設定を確認します。独自のSMTPサーバーを使用している場合、アプライアンスは、そのSMTPサーバー経由でEメールを中継します。多くのSMTPサーバーでは、これを行うには特定の権限が必要となります。使用可能なサーバーのリストに、アプライアンスのIPアドレスを追加します。
     - ルーター設定を確認します。アプライアンスが、SMTPポート（ 25 ）を使用できることを確認します。
     - ファイアウォール設定を確認します。アプライアンスが、SMTPポート（ 25 ）を使用できることを確認します。
     - 問題を解決できない場合は、**Questサポート**（ https://support.quest.com/contact-support ）にお問い合わせください。

受信Eメールのテスト

受信Eメールをテストして、システムの設定を確認できます。

1. SMTPサーバーに口グオンし、アプライアンスのサポートEメールアドレスにEメールメッセージを送信して、サービスデスクチケットを作成します。
2. サービスデスクの チケット（ 複数 ）ページに移動します。

a. アプライアンス管理者コンソール（ https://**appliance_hostname**/admin ）にログインします。または、管理ヘッダーに組織メニューを表示 オプションがアプライアンスの 一般設定 で有効になっている場合は、ページの右上隅で、ログイン情報の横にあるドロップダウンリストから組織を選択します。

b. 左側のナビゲーションバーで、**サービスデスク** をクリックして、**チケット** をクリックします。

3. チケットが表示されていることを確認します。

   アプライアンスの有効なアカウントからEメールを送信すると、チケットが自動的に作成されます。

Telnetを使用した受信Eメールのテスト

Telnet を使用すると、アプライアンスの SMTP サーバと通信して、テスト E メールを送信できます。

1. 次のコマンドを入力します：

   >telnet **k1000.mydomain**.com 25
   >EHLO **mydomain**.com
   >MAIL FROM:<admin@**mydomain**.com>
   >RCPT TO:<servicedesk@k1000.**mydomain**.com
   >DATA
   >Test data here
   >QUIT
   .

   これらのコマンドは通信を開始し、メッセージの送信元をサーバーに伝え、メッセージの宛先をサーバーに伝え、データを送信する準備をし、Telnetを終了します。

2. サービスデスクの E メールボックスで、admin@**mydomain**.com からの E メールが届いていることを確認します。

アプライアンスログにアクセスしてMicrosoft Exchange Serverサーバーエラーを表示する

Exchange Server でロギングが有効になっている場合、アプライアンスのログファイルで Microsoft Exchange Server エラーに関する情報を確認できます。

1. Microsoft Exchange Serverで、SMTPサーバーのプロパティ ウィンドウを開きます。
2. 一般タブで、Enable Logging（ ログ記録を有効にする ）チェックボックスがオンになっていることを確認します。このチェックボックスがオフの場合は、オンにしてからテストEメールをアプライアンスに送信します。
3. アプライアンスの コントロールパネル に移動します。

   - **アプライアンスで組織コンポーネントが有効化されていない場合は、アプライアンス管理者コンソール（ https://appliance_hostname/admin ）にログインして、設定 > コントロールパネル を選択します。**
   - **アプライアンスで組織コンポーネントが有効化されている場合は、アプライアンスシステム管理コンソール（ https://appliance_hostname/system ）にログインします。または、ページの右上隅にあるドロップダウンリストから システム を選択して、設定 > コントロールパネル を選択します。**

4. 左側のナビゲーションバーで、**ログ** をクリックして、ログ ページを表示します。
5. ログ ドロップダウンリストからログを選択します。
6. 問題について、exim_mainlog_*ファイルおよびexim_paniclog_*ファイルを調べます。

   次のような問題があります。

   - エラーと失敗した手順。
   - 完全に解決されていないホスト名と他の変数。

7. ランナウェイEximプロセスなど、Eximの他の問題について、Debug_*ログを調べます。

次に示すその他のログにより、問題のヒントが示されることもあります。

- khelpdeskmailhandler_output
- khelpdeskmailnotifier_error
- khelpdeskmailnotifier_output

8. C:\windows\system32\ologFiles*SMTPにある Microsoft Exchange SMTP サービスログで、問題を調べます。

Eメールエラーのトラブルシューティング

一部の典型的なEメールエラーには、解決策があります。

Eメールエラー	解決策
550 不明なユーザー	• アドレスが正しいことを確認します。 • アドレスが、サービスデスクによって使用されるアドレスと一致していることを確認します。 • 外部SMTPサーバーを無効化し、ネットワーク設定からアドレスを削除します。再起動してアドレスを復元します。もう一度再起動します。
451エラー - 送信者を確認できません	DNS設定を確認します。

診断コンソールの 2 要素認証について

診断コンソールの 2 要素認証（2FA）を使用すると、アプライアンスのバックエンドへのアクセスを制御できます。アプライアンスへの SSH アクセスを有効にしてテザリングを作成すると、**Questサポート**チームはアプライアンスのルートパスワードとアクセストークンを使用して、アプライアンスのバックエンドにログインできます。トークンは 初期セットアップウィザード で提供されます。トークンは、アプライアンスのシステムコンソールの 診断コンソールの 2 要素認証 ページを使用して表示および再生成できます。各トークンを使用できるのは 1 回限りです。トークンが**Questサポート**の連絡先に提供されて初めて、コンソールのテザリングを使用してアプライアンスにログインできます。

このページに移動するには、アプライアンスシステムコンソールにログインします。左側のナビゲーションバーの 設定 で、**サポート** をクリックし、サポート ページの トラブルシューティングツール で、**診断コンソールの 2 要素認証** をクリックします。

初期セットアップ時にアプライアンスで提供されるセキュリティキーとオフライントークンは、アプライアンスマシン上ではない安全な場所に記録、保管してください。この情報は、サポートへの入力が必要になる場合があります。

以前のバージョンからアップグレードした後、診断コンソールの 2 要素認証が無効になっていることを示すメッセージが表示されます。それを拡張セキュリティに対して有効にする場合は、メッセージの指示に従って有効にします。

- シークレットキーを交換して、オフライントークンを再生成するには、**シークレットキーの置き換え** をクリックします
- オフライントークンを再生成するには、**オフライントークンの再生成** をクリックします。

付録

データベーステーブル名

データベーステーブル名は、レポートおよび他のデータベースクエリで使用できます。

次の表に、現在のデータベーステーブル名およびアプライアンスの 6.3 バージョンと 6.4 バージョンとの間で変更されたテーブル名を示します。

- 組織レベル (ORG1) のデータベーステーブル
- システムレベル (KBSYS) のデータベーステーブル

組織レベル (ORG1) のデータベーステーブル

次の表に、組織レベル (ORG1) のデータベーステーブル名を示します。SQLクエリを使用するカスタムレポートを作成する際に、これらのテーブル名を参照します。詳細については、「SQLクエリを使用したレポートの作成」を参照してください。

ORG1データベーステーブルおよびコンポーネント

テーブル	コンポーネント
ADVISORY	サービスデスク：サポート技術情報
ADVISORY_LABEL_JT	サービスデスク：サポート技術情報
ADVISORY_RATINGS	サービスデスク：サポート技術情報
AGENTLESS_TASK_LOG	アプライアンス管理: 検出
ASSET	資産管理
ASSET_ASSOCIATION	資産管理
ASSET_CATALOG_ASSOCIATION	資産管理
ASSET_CLASS	資産管理：資産サブタイプ
ASSET_DATA_1	資産管理：資産のインポート
ASSET_DATA_2	資産管理：資産のインポート
ASSET_DATA_3	資産管理：資産のインポート
ASSET_DATA_4	資産管理：資産のインポート
ASSET_DATA_5	資産管理：資産のインポート
ASSET_DATA_6	資産管理：資産のインポート

テーブル	コンポーネント
ASSET_DATA_7	資産管理：資産のインポート
ASSET_FIELD_DEFINITION	設定：資産履歴
ASSET_FILTER	資産管理：ラベル作成
ASSET_HIERARCHY	資産管理
ASSET_HISTORY	設定：資産履歴
ASSET_TYPE	資産管理：資産タイプ
AUTHENTICATION	アプライアンス管理
CLIENTDIST_LABEL_JT	アプライアンス管理: KACE エージェント
CLIENT_DISTRIBUTION	アプライアンス管理: KACE エージェント
CREDENTIAL	設定：資格情報
CUSTOM_FIELD_DEFINITION	アプライアンス管理
CUSTOM_VIEW	アプライアンス管理: サービスデスク設定
DASHBOARD	ダッシュボード
DASHBOARD_CACHE	ダッシュボード
DELL_ASSET	セキュリティ: Dellアップデート
DELL_INVENTORY	セキュリティ: Dellアップデート
DELL_INVENTORY_APPLICATION_DEVICE_JT	セキュリティ: Dellアップデート
DELL_INVENTORY_DEVICE_JT	セキュリティ: Dellアップデート
DELL_INVENTORY_LOG	セキュリティ: Dellアップデート
DELL_MACHINE_PKG_UPDATE_STATUS	セキュリティ: Dellアップデート
DELL_MACHINE_STATUS	セキュリティ: Dellアップデート
DELL_PKG_LABEL_JT	セキュリティ: Dellアップデート
DELL_PKG_STATUS	セキュリティ: Dellアップデート
DELL_PKG_UPDATE_HISTORY	セキュリティ: Dellアップデート

テーブル	コンポーネント
DELL_SCHEDULE	セキュリティ: Dellアップデート
DELL_SCHEDULE_LABEL_JT	セキュリティ: Dellアップデート
DELL_SCHEDULE_MACHINE_STATUS	セキュリティ: Dellアップデート
DELL_SCHEDULE_OS_JT	セキュリティ: Dellアップデート
DELL_SCHEDULE_UPDATE_LABEL_JT	セキュリティ: Dellアップデート
DELL_WARRANTY	セキュリティ: Dellアップデート
DEVICE_DETAIL_FIELD	インベントリ：デバイス
DEVICE_DETAIL_GROUP	インベントリ：デバイス
DEVICE_DETAIL_GROUP_ASSET_CLASS_JT	インベントリ：デバイス
DEVICE_DETAIL_SECTION	インベントリ：デバイス
DEVICE_DETAIL_SECTION_ASSET_CLASS_JT	インベントリ：デバイス
DEVP_PROFILE_APPLIED	スクリプト作成：Mac プロファイル
DEVP_PROFILE_APPLIED_MACHINE	スクリプト作成：Mac プロファイル
DEVP_PROFILE_APPLIED_PAYLOAD	スクリプト作成：Mac プロファイル
DEVP_PROFILE_APPLIED_PAYLOAD_ATTRIBUTE	スクリプト作成：Mac プロファイル
FILTER	ラベル
FS	ファイル同期
FS_LABEL_JT	ファイル同期
FS_MACHINE_JT	ファイル同期
GLOBAL_OPTIONS	アプライアンス管理
GRID_COLUMNS_OVERRIDES	アプライアンス管理
HD_ANNOUNCEMENT	サービスデスク：告知
HD_ANNOUNCEMENT_LABEL_JT	サービスデスク：告知
HD_ARCHIVE_ATTACHMENT	サービスデスク：チケットアーカイブ

テーブル	コンポーネント
HD_ARCHIVE_TICKET	サービスデスク：チケットアーカイブ
HD_ARCHIVE_TICKET_CHANGE	サービスデスク：チケットアーカイブ
HD_ARCHIVE_TICKET_CHANGE_FIELD	サービスデスク：チケットアーカイブ
HD_ARCHIVE_WORK	サービスデスク：チケットアーカイブ
HD_ATTACHMENT	サービスデスク：チケット（複数）
HD_CATEGORY	サービスデスク：チケット（複数）
HD_CUSTOM_FIELDS	サービスデスク：チケット（複数）
HD_EMAIL_EVENT	サービスデスク：チケット（複数）
HD_FIELD	サービスデスク：チケット（複数）
HD_HOME_PAGE_WIDGET	サービスデスク：ユーザーコンソールのホームページ
HD_IMPACT	サービスデスク：チケット（複数）
HD_LINK	サービスデスク：ユーザーコンソールのホームページ
HD_MAILTEMPLATE	サービスデスク：チケット（複数）
HD_PRIORITY	サービスデスク：チケット（複数）
HD_QUEUE	サービスデスク：キュー（複数）
HD_QUEUE_APPROVER_LABEL_JT	サービスデスク：キュー（複数）
HD_QUEUE_OWNER_LABEL_JT	サービスデスク：キュー（複数）
HD_QUEUE_SUBMITTER_LABEL_JT	サービスデスク：キュー
HD_SERVICE	サービスデスク：チケット（複数）
HD_SERVICE_TICKET	サービスデスク：チケット（複数）
HD_SERVICE_USER_LABEL_JT	サービスデスク：チケット（複数）
HD_SLA_BUSINESS_HOURS	サービスデスク：サービスレベル契約
HD_SLA_HOLIDAYS	サービスデスク：サービスレベル契約
HD_STATUS	サービスデスク：チケット（複数）

テーブル	コンポーネント
HD_TICKET	サービスデスク：チケット（複数）
HD_TICKET_CHANGE	サービスデスク：チケット（複数）
HD_TICKET_CHANGE_FIELD	サービスデスク：チケット（複数）
HD_TICKET_FILTER	サービスデスク：チケット（複数）
HD_TICKET_RELATED	サービスデスク：チケット（複数）
HD_TICKET_RULE	サービスデスク：チケット（複数）
HD_WORK	サービスデスク：チケット（複数）
IM_CRON	アプライアンス管理
KBOT	スクリプト
KBOT_CRON_SCHEDULE	スクリプト
KBOT_DEPENDENCY	スクリプト
KBOT_EVENT_SCHEDULE	スクリプト
KBOT_FORM	スクリプト
KBOT_FORM_DATA	スクリプト
KBOT_LABEL_JT	スクリプト
KBOT_LOG	スクリプト
KBOT_LOG_DETAIL	スクリプト
KBOT_LOG_LATEST	スクリプト
KBOT_OS_FAMILY_JT	スクリプト
KBOT_OS_JT	スクリプト
KBOT_RUN	スクリプト
KBOT_RUN_MACHINE	スクリプト
KBOT_RUN_TOKEN	スクリプト
KBOT_SHELL_SCRIPT	スクリプト

テーブル	コンポーネント
KBOT_UPLOAD	スクリプト
KBOT_VERIFY	スクリプト
KBOT_VERIFY_STEPS	スクリプト
KMON_ALERT	監視
KMON_CONDITION	監視
KMON_CONFIG	監視
KMON_CONFIG_DEFAULT	監視
KMON_CONFIG_DETAIL	監視
KMON_CONFIG_DEVICE_JT	監視
KMON_INSTALL_LEP_DEVICE_JT	監視：Log Enablement Packages
KMON_LEP	監視：Log Enablement Package
KMON_LEP_INSTALL	監視：Log Enablement Package
KMON_LOG_CONFIG	監視
KMON_MAINT_CONFIG	監視
KMON_MONITORED_DEVICE	監視
LABEL	ラベル
LABEL_LABEL_JT	ラベル
LDAP_FILTER	ラベル：LDAP
LDAP_IMPORT_USER	ラベル：LDAP
MACHINE	インベントリ：デバイス
MACHINE_ACTIONS	インベントリ：デバイス
MACHINE_BITLOCKER_VOLUME	インベントリ：デバイス
MACHINE_CHROMEOS_DETAILS	インベントリ：デバイス
MACHINE_CUSTOM_INVENTORY	インベントリ：デバイス

テーブル	コンポーネント
MACHINE_DAILY_UPTIME	インベントリ：デバイス
MACHINE_DCM_AMT_SETTINGS	インベントリ：デバイス
MACHINE_DCM_BATTERY	インベントリ：デバイス
MACHINE_DCM_DESKTOP_MONITOR	インベントリ：デバイス
MACHINE_DCM_FLAT_PANEL	インベントリ：デバイス
MACHINE_DCM_LOG_ENTRY	インベントリ：デバイス
MACHINE_DCM_PHYSICAL_MEMORY	インベントリ：デバイス
MACHINE_DCM_PROCESSOR	インベントリ：デバイス
MACHINE_DCM_VPRO_SETTINGS	インベントリ：デバイス
MACHINE_DDPE	インベントリ：デバイス
MACHINE_DDPE_VOLUME	インベントリ：デバイス
MACHINE_DISKS	インベントリ：デバイス
MACHINE_DRIVE_ENCRYPTION_SUMMARY	インベントリ：デバイス
MACHINE_FIELD_DEFINITION	インベントリ：デバイス
MACHINE_FILEVAULT_VOLUME	インベントリ：デバイス
MACHINE_INTEL_AMT	インベントリ：デバイス
MACHINE_LABEL_JT	インベントリ：デバイス
MACHINE_LOCATION	インベントリ：デバイス
MACHINE_MOBILE	インベントリ：デバイス
MACHINE_NICS	インベントリ：デバイス
MACHINE_NTSERVICE_JT	インベントリ：デバイス
MACHINE_PROCESS_JT	インベントリ：デバイス
MACHINE_REPLITEM	インベントリ：デバイス
MACHINE_SNMP_DATA	インベントリ：デバイス

テーブル	コンポーネント
MACHINE_SOFTWARE_JT	インベントリ：デバイス
MACHINE_STARTUPPROGRAM_JT	インベントリ：デバイス
MACHINE_TPM	インベントリ：デバイス
MESSAGE	配布：警告
MESSAGE_LABEL_JT	配布：警告
MI	配布：管理対象インストール
MI_ATTEMPT	配布：管理対象インストール
MI_LABEL_JT	配布：管理対象インストール
NODE	インベントリ：検出
NODE_LABEL_JT	インベントリ：検出
NODE_PORTS	インベントリ：検出
NODE_SNMP_IF	インベントリ：検出
NODE_SNMP_SYSTEM	インベントリ：検出
NOTIFICATION	レポート作成：通知
NOTIFICATION_USER_JT	レポート作成：通知
NTSERVICE	インベントリ：サービス
NTSERVICE_LABEL_JT	インベントリ：サービス
OBJECT_FIELD_DEFINITION	設定：履歴
OBJECT_HISTORY	設定：履歴
OBJECT_HISTORY_CONFIGURATION	設定：履歴
OPERATING_SYSTEMS	インベントリ：デバイス
OVAL_STATUS	セキュリティ: OVAL
PATCH_FILTER	セキュリティ: パッチ管理
PATCH_LABEL_JT	セキュリティ: パッチ管理

テーブル	コンポーネント
PATCH_MACHINE_REMEDIATION_STATUS	セキュリティ: パッチ管理
PATCH_MACHINE_STATUS	セキュリティ: パッチ管理
PATCH_PATCH_COUNT	セキュリティ: パッチ管理
PATCH_SCHEDULE	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_DEPLOY_LABEL_JT	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_DETECT_LABEL_JT	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_LABEL_JT	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_MACHINE_STATUS	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_OS_JT	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_ROLLBACK_LABEL_JT	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_RUN	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_RUN_COUNTS	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_RUN_LOG	セキュリティ: パッチスケジュール
PATCH_SCHEDULE_RUN_MACHINE	セキュリティ: パッチスケジュール
PATCH_SETTINGS	セキュリティ: サブスクリプション
PATCH_STATUS	セキュリティ: パッチ管理
PORTAL	サービスデスク：**ユーザーコンソール**
PORTAL_LABEL_JT	サービスデスク：**ユーザーコンソール**
PROCESS	インベントリ：プロセス（複数）
PROCESS_LABEL_JT	インベントリ：プロセス
PROVISION_CONFIG	設定：エージェントのプロビジョニング
PROVISION_NODE	設定：エージェントのプロビジョニング
REMOTE_CHROMEOS_HOST	設定：エージェント不要のプロビジョニング
REMOTE_DMM_HOST	設定：エージェント不要：Dell Mobility Manager

テーブル	コンポーネント
REMOTE_HOST	設定：エージェント不要のプロビジョニング
REMOTE_HOST_KUID	設定：エージェント不要のプロビジョニング
REMOTE_SHELL_HOST	設定：エージェント不要のプロビジョニング
REMOTE_SNMP_HOST	設定：エージェント不要のプロビジョニング
REMOTE_WSMAN_HOST	設定：エージェント不要のプロビジョニング
REPLICATION_LANGUAGE	配布：レプリケーション
REPLICATION_PLATFORM	配布：レプリケーション
REPLICATION_SCHEDULE	配布：レプリケーション
REPLICATION_SHARE	配布：レプリケーション
REPORT_FIELD	レポート作成
REPORT_FIELD_GROUP	レポート作成
REPORT_JOIN	レポート作成
REPORT_OBJECT	レポート作成
REPORT_OBJECT_JOIN	レポート作成
REPORT_SCHEDULE	レポート作成
SAM_CATALOG_FILTER	インベントリ：ソフトウェアカタログ
SAM_CATALOG_LABEL_JT	インベントリ：ソフトウェアカタログ
SAM_COMPLIANCE_DETAIL	資産管理：ライセンスコンプライアンス
SAM_COMPLIANCE_SUMMARY	資産管理：ライセンスコンプライアンス
SAM_COUNT	インベントリ：ソフトウェアカタログ
SAM_MACHINE_JT	インベントリ：ソフトウェアカタログ
SAM_MACHINE_TERMINATED_APPS	インベントリ：ソフトウェアカタログ
SAM_METER	インベントリ：ソフトウェアカタログ
SAM_METER_DATA	インベントリ：ソフトウェアカタログ

テーブル	コンポーネント
SAM_METER_TITLED_APPLICATION	インベントリ：ソフトウェアカタログ
SAM_NOT_ALLOWED	インベントリ：ソフトウェアカタログ
SAVED_SEARCH	アプライアンス管理
SCAN_FILTER	インベントリ：検出
SCAN_SETTINGS	インベントリ：検出
SCAP_BENCHMARK	セキュリティ: SCAP
SCAP_GROUP	セキュリティ: SCAP
SCAP_PROFILE	セキュリティ: SCAP
SCAP_RESULT	セキュリティ: SCAP
SCAP_RESULT_RULE	セキュリティ: SCAP
SCAP_RESULT_SCORE	セキュリティ: SCAP
SCAP_RULE	セキュリティ: SCAP
SCAP_RULE_IDENT	セキュリティ: SCAP
SETTINGS	設定
SETTINGS_HISTORY	設定：履歴
SETTINGS_HISTORY_CONFIGURATION	設定：履歴
SETTINGS_HISTORY_FIELD_DEFINITION	設定：履歴
SMARTY_REPORT	レポート作成
SNMP_INVENTORY_OIDS	インベントリ：SNMP
SNMP_INVENTORY_SETTINGS	インベントリ：SNMP
SNMP_INVENTORY_SETTINGS_JT	インベントリ：SNMP
SNOOZE_ALERT	パッチスケジュール
SOFTWARE	インベントリ：ソフトウェア
SOFTWARE_LABEL_JT	インベントリ：ソフトウェア

テーブル	コンポーネント
SOFTWARE_OS_JT	インベントリ：ソフトウェア
STARTUPPROGRAM	インベントリ：スタートアッププログラム
STARTUPPROGRAM_LABEL_JT	インベントリ：スタートアッププログラム
THROTTLE	アプライアンス管理
ユーザー	設定：ユーザー
USERIMPORT_SCHEDULE	設定：ユーザー認証
USER_AUTO_REFRESH	設定：ユーザー
USER_HISTORY	設定：ユーザー
USER_KEYS	設定：ユーザー
USER_LABEL_JT	設定：ユーザー
USER_ROLE	設定：ユーザー
USER_ROLE_PERMISSION_VALUE	設定：ユーザー

システムレベル（KBSYS）のデータベーステーブル

次の表に、システムレベル（KBSYS）のデータベーステーブル名を示します。SQLクエリを使用するカスタムレポートを作成する際に、これらのテーブル名を参照します。詳細については、「SQLクエリを使用したレポートの作成」を参照してください。

KBSYSデータベーステーブルおよびコンポーネント

テーブル	コンポーネント
ACCESS_STATS	アプライアンス管理（ページビューを追跡するために使用）
AGENTLESS_TASK	インベントリ
APPLE_MODEL	インベントリ：デバイス
AUTHENTICATION	設定：ユーザー
CLIENT_CRASH	アプライアンス管理
COUNTRYCODE_MAPPING	インベントリ：デバイス（Dell製デバイス用に使用）
CREDENTIAL_CONSUMER	設定：資格情報
DASHBOARD	ダッシュボード

テーブル	コンポーネント
DASHBOARD_BASE_WIDGETS	ダッシュボード
DASHBOARD_CACHE	ダッシュボード
DASHBOARD_CUSTOM_WIDGETS	ダッシュボード
DASHBOARD_DATASOURCES	ダッシュボード
DASHBOARD_WIDGET_TYPES	ダッシュボード
DELL_CATALOG	セキュリティ: Dellアップデート
DELL_CRITICALITY	セキュリティ: Dellアップデート
DELL_ERROR_CODE	セキュリティ: Dellアップデート
DELL_PKG	セキュリティ: Dellアップデート
DELL_PKG_DEVICE	セキュリティ: Dellアップデート
DELL_PKG_DEVICE_DEPENDENCY	セキュリティ: Dellアップデート
DELL_PKG_DEVICE_PCI	セキュリティ: Dellアップデート
DELL_PKG_DEVICE_PNP	セキュリティ: Dellアップデート
DELL_PKG_DEVICE_VERSION	セキュリティ: Dellアップデート
DELL_PKG_OS	セキュリティ: Dellアップデート
DELL_PKG_OS_LANG	セキュリティ: Dellアップデート
DELL_PKG_SYSTEM	セキュリティ: Dellアップデート
DELL_RESOURCE	セキュリティ: Dellアップデート
DELL_SUPPORTED_MODELS	セキュリティ: Dellアップデート
DELL_UPDATE_STATUS	セキュリティ: Dellアップデート
GLOBAL_OPTIONS	アプライアンス管理
GRID_COLUMNS_BASE	アプライアンス管理
GRID_COLUMNS_OVERRIDES	アプライアンス管理
HD_EMAIL_EXCLUSION	サービスデスク：E メールの除外リスト

テーブル	コンポーネント
HISTORY_FIELD_VALUE_LABEL_MAP	設定：履歴
IM_CRON	アプライアンス管理（スケジュールされたプロセス用に使用）
INVENTORY	インベントリ
INVENTORY_FAILURES	インベントリ
KBOT_GRAMMAR	スクリプト
KBOT_GRAMMAR_ATTRIBUTE	スクリプト
KBOT_UPLOAD_TOKENS	スクリプト
KBOX	スクリプト
KBOX_VERSION	スクリプト
KONDUCTOR_TASK	アプライアンス管理
KUID_MACHINE	アプライアンス管理
KUID_ORGANIZATION	アプライアンス管理
LICENSE_MODE	アプライアンス管理
LINKED_APPLIANCE	設定：アプライアンスリンク
LINKED_USER_TOKEN	設定：アプライアンスリンク
LOCALE_BROWSER	アプライアンス管理
LOCALE_COLLATION_RULES	アプライアンス管理
LOCALE_SERVER	アプライアンス管理
LOCALE_TIME_FORMAT	アプライアンス管理
MSI_ERROR_CODES	配布
NETWORK_SETTINGS	アプライアンス管理
ORGANIZATION	組織
ORGANIZATION_FILTER	組織：フィルタ
ORGANIZATION_FILTER_CRITERIA	組織：フィルタ

テーブル	コンポーネント
ORGANIZATION_FILTER_CRITERIA_LDAP	組織：フィルタ
ORG_ROLE	組織：役割
ORG_ROLE_PERMISSION_VALUE	組織：役割
OS_FAMILY	インベントリ：デバイス
OVAL_DEFINITION	セキュリティ: OVAL
OVAL_UPDATE_STATUS	セキュリティ: OVAL
PATCH_ATTRIBUTE	セキュリティ: パッチ管理
PATCH_CATALOG_RUN_STATUS	セキュリティ: パッチ管理
PATCH_CATALOG_UPDATE_STATUS	セキュリティ: パッチ管理
PATCH_ERROR_CODE	セキュリティ: パッチ管理
PATCH_LANGUAGE	セキュリティ: パッチ管理
PATCH_OS	セキュリティ: パッチ管理
PATCH_PACKAGE	セキュリティ: パッチ管理
PATCH_PAYLOAD_DOWNLOAD_STATUS	セキュリティ: パッチ管理
PATCH_PRODUCT	セキュリティ: パッチ管理
PATCH_PRODUCT_JT	セキュリティ: パッチ管理
PATCH_PRODUCT_OS_JT	セキュリティ: パッチ管理
PATCH_PRODUCT_TITLED_APPLICATION_JT	セキュリティ: パッチ管理
PATCH_PRODUCT_TITLED_SUITE_JT	セキュリティ: パッチ管理
PATCH_RESOURCE	セキュリティ: パッチ管理
PATCH_SUPERCEDES_JT	セキュリティ: パッチ管理
PERMISSION_DEFINITION	設定：役割
PORT_SERVICES	インベントリ：検出
PROVISIONING_ERRORS	設定：プロビジョニング

テーブル	コンポーネント
REPORT_FIELD	レポート作成
REPORT_FIELD_GROUP	レポート作成
REPORT_JOIN	レポート作成
REPORT_OBJECT	レポート作成
REPORT_OBJECT_JOIN	レポート作成
REPORT_SCHEDULE	レポート作成
RESOURCE_EXPORTED	設定：リソース
RESOURCE_QUEUE	設定：リソース
SAM_APPLICATION	ソフトウェアカタログ
SAM_HARDWARE	ソフトウェアカタログ
SAM_LINUX_APPLICATION	ソフトウェアカタログ
SAM_MUI_CACHE_DATA	ソフトウェアカタログ
SAM_PUBLISHER	ソフトウェアカタログ
SAM_SOFTWARE_TAG	ソフトウェアカタログ
SAM_TITLE_REQUEST	ソフトウェアカタログ
SAM_VIEW_ALL_SOFTWARE	ソフトウェアカタログ
SAM_VIEW_DISCOVERED_APPLICATIONS	ソフトウェアカタログ
SAM_VIEW_DISCOVERED_SOFTWARE	ソフトウェアカタログ
SAM_VIEW_DISCOVERED_SUITES	ソフトウェアカタログ
SAM_VIEW_INVENTORY_ADD_REMOVE_PROGRAMS	ソフトウェアカタログ
SAM_VIEW_INVENTORY_MOBILE_APPS	ソフトウェアカタログ
SAM_VIEW_MACHINE_DISCOVERED_SOFTWARE	ソフトウェアカタログ
SAM_VIEW_TITLED_SOFTWARE	ソフトウェアカタログ

テーブル	コンポーネント
SERVER_CRASH	アプライアンス管理（内部エラーを追跡するために使用）
SERVICE_LEVEL_MAPPING	インベントリ：デバイス（Dell製デバイス用に使用）
SETTINGS	設定
SETTINGS_HISTORY	設定：履歴
SETTINGS_HISTORY_CONFIGURATION	設定：履歴
SETTINGS_HISTORY_FIELD_DEFINITION	設定：履歴
SHAPING_METADATA	インベントリ：API
SMARTY_REPORT	レポート作成
SMMP_CONNECTION	検出
SMMP_CONNECTION_PLUGIN_JT	検出
SMMP_MSG_Q	検出
SMMP_NIC	検出
SMMP_PLUGIN	検出
SOFTWARE_INVENTORY	インベントリ
SOFTWARE_INVENTORY_FAILURES	インベントリ
SSL_CERT	設定：セキュリティ設定
SSL_CSR	設定：セキュリティ設定
SSL_PRIVATEKEY	設定：セキュリティ設定
SYSTEM_DEFINED_ROLES	組織：役割
TIME_SETTINGS	設定：日付と時刻の設定
ユーザー	設定：認証
USER_AUTH	設定：認証
USER_AUTO_REFRESH	設定：認証

スクリプトのタスクセクションへの手順の追加

スクリプト作成コンポーネントでスクリプトに手順を追加できます。

次の表では、スクリプトのタスクセクションに追加可能な手順について詳しく説明します。タスクセクションは、タスクを追加すると スクリプトの詳細 ページに表示されます。詳細については、「スクリプトの追加と編集」を参照してください。

列見出し「V」、「OS」、「R」、「ORS」、および「ORF」は、対応するタスクセクションで次の特定の手順が使用可能かどうかを示しています。「検証」、「成功時」、「修復」、「修復の成功時」、および「修復の失敗時」。

- Windowsデバイス用の手順
- Mac OS Xデバイス用の手順
- Red Hat Enterprise Linuxデバイス用の手順

Windowsデバイス用の手順

注: レジストリパスを指定するときに使用する構文については、Windows レジストリパスの指定を参照してください。

Windowsデバイスで使用されるスクリプトへの手順の追加

手順	説明	V	OS	R	ORS	ORF
常に失敗する		X		X		
カスタムDLL関数を呼び出す	「%{path}\%{file}」から関数「%{procName}」を呼び出します。	X	X	X		
カスタムDLLオブジェクトを作成する	「%{path}\%{file}」からオブジェクト「%{className}」を作成します。	X	X	X		
メッセージウィンドウを作成する	「%{name}」という名前のメッセージウィンドウを作成し、タイトル「%{title}」、メッセージ「%{message}」、およびタイムアウト「%{timeout}」	X	X	X	X	X

手順	説明	V	OS	R	ORS	ORF
	（秒）を設定します。					
レジストリキーを削除する	レジストリから「%{key}」を削除します。詳細については、「Windows レジストリパスの指定」を参照してください。		X	X		
レジストリ値を削除する	レジストリから「%{key}!%{name}」を削除します。詳細については、「Windows レジストリパスの指定」を参照してください。		X	X		
メッセージウィンドウを破棄する	「%{name}」という名前のメッセージウィンドウを破棄します。	X	X	X	X	X
アプリケーションパッケージをインストールする	引数「%{install_cmd}」を指定して「%{name}」をインストールします。		X	X		

手順	説明	V	OS	R	ORS	ORF
	注: この手順では、インベントリ > ソフトウェアページにある機能を使用して、既にアップロードされているアプリケーションパッケージのリストからパッケージを選択する必要があります。詳細については、「ソフトウェアページインベントリ内のアプリケーションの追加と削除」を参照してください。					
プロセスを停止する	プロセス「%{name}」を停止します。	X	X	X	X	X

手順	説明	V	OS	R	ORS	ORF
プログラムを起動する	パラメータ「%{parms}」を付けて「%{path}\%{program}」を起動します。	X	X	X	X	X
レジストリ値をログに記録する	「%{key}!%{name}」をログに記録します。			X		
ファイル情報をログに記録する	「%{path}\%{file}」の「%{attrib}」をログに記録します。			X	X	X
メッセージをログに記録する	「%{message}」のログを「%{type}」に記録します。			X		
サービスを再開する	サービス「%{name}」を再開します。			X		
バッチファイルを実行する	パラメータ「%{parms}」を指定してバッチファイル「%{_fake_name}」を実行します。	X	X	X		

手順	説明	V	OS	R	ORS	ORF
	注: この手順で、バッチファイルをアップロードする必要はありません。表示された領域にスクリプトを貼り付けることにより、バッチファイルを作成します。					
レジストリキーを設定する	「%{key}」を設定します。	X	X			
レジストリ値を設定する	「%{key}!%{name}」を「%{newValue}」に設定します。	X	X			
サービスを開始する	サービス「%{name}」を再開します。			X		
サービスを停止する	サービス「%{name}」を停止します。			X		
ファイルを解凍する	「%{target}」に「%{path}\%{file}」を解凍します。	X		X	X	X
メッセージウィンドウテキストを更新する	「%{name}」という名前のメッセージウィンドウのテキストを	X		X	X	X

手順	説明	V	OS	R	ORS	ORF
	「%{text}」に設定します。					
ポリシーとジョブスケジュールを更新する	アプライアンスからポリシーとジョブスケジュールを更新します。	X				
ファイルをアップロードする	サーバーに「%{path}\%{file}」をアップロードします。		X	X		
ディレクトリが存在することを確認する	ディレクトリ「%{path}」が存在することを確認します。	X				
ファイルが存在することを確認する	ファイル「%{path}\%{file}」が存在することを確認します。	X				
ファイルのバージョンが正確に次の値であることを確認する	ファイル「%{path}\%{file}」のバージョンが「%{expectedValue}」であることを確認します。	X				
ファイルのバージョンが次の値よりも大きいことを確認する	ファイル「%{path}\%{file}」のバージョンが「%{expectedValue}」よりも上位であることを確認します。	X				
ファイルのバージョンが次の値以上であることを確認する	ファイル「%{path}\%{file}」のバージョンが「%{expectedValue}」以上であることを確認します。	X				

手順	説明	V	OS	R	ORS	ORF
ファイルのバージョンが次の値よりも小さいことを確認する	ファイル「%{path}\%{file}」のバージョンが「%{expectedValue}」よりも下位であることを確認します。	X				
ファイルのバージョンが次の値以下であることを確認する	ファイル「%{path}\%{file}」のバージョンが「%{expectedValue}」以下であることを確認します。	X				
ファイルのバージョンが次の値でないことを確認する	ファイル「%{path}\%{file}」のバージョンが「%{expectedValue}」でないことを確認します。	X				
ファイルがその後修正されたことを確認する	ファイル「%{path}\%{file}」が「%{expectedValue}」から変更されたことを確認します。	X				
プロセスが動作していないことを確認する	プロセス「%{name}」が動作していないことを確認します。	X				
プロセスが動作していることを確認する	プロセス「%{name}」が動作していることを確認します。	X				
製品のバージョンが正確に次の値であることを確認する	製品「%{path}\%{file}」のバージョンが「%{expectedValue}」であることを確認します。	X				

手順	説明	V	OS	R	ORS	ORF
製品のバージョンが次の値よりも大きいことを確認する	製品「%{path}\%{file}」のバージョンが「%{expectedValue}」よりも上位であることを確認します。	X				
製品のバージョンが次の値以上であることを確認する	製品「%{path}\%{file}」のバージョンが「%{expected-Value}」以上であることを確認します。	X				
製品のバージョンが次の値よりも小さいことを確認する	製品「%{path}\%{file}」のバージョンが「%{expectedValue}」よりも下位であることを確認します。	X				
製品のバージョンが次の値以下であることを確認する	製品「%{path}\%{file}」のバージョンが「%{expectedValue}」以下であることを確認します。	X				
製品のバージョンが次の値でないことを確認する	製品「%{path}\%{file}」のバージョンが「%{expectedValue}」でないことを確認します。	X				
注: レジストリパスを指定するときに使用する構文については、Windows レジストリパスの指定を参照してください。						
レジストリキーが存在しないことを確認する	「%{key}」が存在しないことを確認します。	X				

手順	説明	V	OS	R	ORS	ORF
レジストリキーが存在することを確認する	「%{key}」が存在することを確認します。	X				
レジストリキーのサブキー数が正確に次の値であることを確認する	「%{key}」のサブキー数が正確に「%{expectedValue}」個であることを確認します。	X				
レジストリキーのサブキー数が次の値よりも大きいことを確認する	「%{key}」のサブキー数が「%{expectedValue}」個よりも多いことを確認します。	X				
レジストリキーのサブキー数が次の値以上であることを確認する	「%{key}」のサブキー数が「%{expectedValue}」個以上であることを確認します。	X				
レジストリキーのサブキー数が次の値よりも小さいことを確認する	「%{key}」のサブキー数が「%{expectedValue}」個よりも少ないことを確認します。	X				
レジストリキーのサブキー数が次の値以下であることを確認する	「%{key}」のサブキー数が「%{expectedValue}」個以下であることを確認します。	X				
レジストリキーのサブキー数が次の値でないことを確認する	「%{key}」のサブキー数が正確には「%{expectedValue}」個でないことを確認します。	X				
レジストリキーの値数が正確に次の値であることを確認する	「%{key}」の値数が正確に「%{expectedValue}」個であることを確認します。	X				

手順	説明	V	OS	R	ORS	ORF
レジストリキーの値数が次の値よりも大きいことを確認する	「%{key}」の値数が「%{expectedValue}」個よりも多いことを確認します。	X				
レジストリキーの値数が次の値以上であることを確認する	「%{key}」の値数が「%{expectedValue}」個以上であることを確認します。	X				
レジストリキーの値数が次の値よりも小さいことを確認する	「%{key}」の値数が「%{expectedValue}」個よりも少ないことを確認します。	X				
レジストリキーの値数が次の値以下であることを確認する	「%{key}」の値数が「%{expectedValue}」個以下であることを確認します。	X				
レジストリキーの値数が次の値でないことを確認する	「%{key}」の値数が正確には「%{expectedValue}」個でないことを確認します。	X				
レジストリパターンが一致しないことを確認する	「%{key}!%{name}=%{expectedValue}」が一致しないことを確認します。	X				
レジストリパターンが一致することを確認する	「%{key}!%{name}=%{expectedValue}」が一致することを確認します。	X				
レジストリ値が存在しないことを確認する	「%{key}!%{name}」が存在しないことを確認します。	X				

手順	説明	V	OS	R	ORS	ORF
レジストリ値が存在することを確認する	「%{key}!%{name}」が存在することを確認します。	X				
レジストリ値が正確に次の値であることを確認する	「%{key}!%{name}」が「%{expectedValue}」と等しいことを確認します。	X				
レジストリ値が次の値よりも大きいことを確認する	「%{key}!%{name}」が「%{expectedValue}」よりも大きいことを確認します。	X				
レジストリ値が次の値以上であることを確認する	「%{key}!%{name}」が「%{expectedValue}」以上であることを確認します。	X				
レジストリ値が次の値よりも小さいことを確認する	「%{key}!%{name}」が「%{expectedValue}」よりも小さいことを確認します。	X				
レジストリ値が次の値以下であることを確認する	「%{key}!%{name}」が「%{expectedValue}」以下であることを確認します。	X				
レジストリ値が次の値でないことを確認する	「%{key}!%{name}」が「%{expectedValue}」と等しくないことを確認します。	X				
サービスが存在することを確認する	サービス「%{name}」が存在することを確認します。	X				

手順	説明	V	OS	R	ORS	ORF
サービスが動作していることを確認する	サービス「%{name}」が動作していることを確認します。	X				

Windows レジストリパスの指定

Windows レジストリパスを指定するときは、ベースキーを使用し、レジストリを置くデバイスのオペレーティングシステムおよびハードウェアが 32 ビットと 64 ビットのどちらであるかを指定します。

ベースキー	短縮名
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_USER	HKCU
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_PERFORMANCE_DATA	HKPD
HKEY_PERFORMANCE_TEXT	HKPT
HKEY_PERFORMANCE_NLSTEXT	HKPN
HKEY_CURRENT_CONFIG	HKCC
HKEY_DYN_DATA	HKDD

例えば、32 ビットと 64 ビットのそれぞれの Windows デバイスの HKEY_LOCAL_MACHINE へのパスは、次のように指定します。

- HKLM\Software\32BitProgramA\installDate
- HKLM64\Software\64BitProgramB\installDate

Mac OS Xデバイス用の手順

Mac OS Xデバイスで使用されるスクリプトへの手順の追加

手順	説明	V	OS	R	ORS	ORF
常に失敗する		X		X		
メッセージウィンドウを作成する	「%{name}」という名前のメッセージウィンドウを作成し、タイトル「%{title}」、メッセージ「%{message}」、およびタイムアウト「%{timeout}」	X	X	X	X	X

手順	説明	V	OS	R	ORS	ORF
	（秒）を設定します。					
メッセージウィンドウを破棄する	「%{name}」という名前のメッセージウィンドウを破棄します。	X	X	X	X	X
プロセスを停止する	プロセス「%{name}」を停止します。	X	X	X	X	X
プログラムを起動する	パラメータ「%{parms}」を付けて「%{path}\%{program}」を起動します。	X	X	X	X	X
PLIST値をログに記録する	「%{key}!%{name};」をログに記録します。			X		
メッセージをログに記録する	「%{message}」のログを「%{type}」に記録します。			X		
ファイルシステムを検索する	「%{drives}」上の「%{startingDirectory}」で「%{name}」を検索して「%{action}」します。	X				
ファイルを解凍する	「%{target}」に「%{path}\%{file}」を解凍します。	X		X	X	X
メッセージウィンドウテキストを更新する	「%{name}」という名前のメッセージウィンドウのテキストを「%{text}」に設定します。	X		X	X	X

手順	説明	V	OS	R	ORS	ORF
ポリシーとジョブスケジュールを更新する	アプライアンスからポリシーとジョブスケジュールを更新します。	X				
ファイルをアップロードする	サーバーに「%{path}\%{file}」をアップロードします。		X	X		
ディレクトリが存在することを確認する	ディレクトリ「%{path}」が存在することを確認します。	X				
ファイルが存在することを確認する	ファイル「%{path}\%{file}」が存在することを確認します。	X				
ファイルがその後修正されたことを確認する	ファイル「%{path}\%{file}」が「%{expectedValue}」から変更されたことを確認します。	X				
プロセスが動作していないことを確認する	プロセス「%{name}」が動作していないことを確認します。	X				
プロセスが動作していることを確認する	プロセス「%{name}」が動作していることを確認します。	X				
PLIST値が次の値と等しいことを確認する		X				
PLIST値が存在することを確認する	「%{key}」が存在することを確認します。	X				

手順	説明	V	OS	R	ORS	ORF
PLIST値が次の値よりも大きいことを確認する		X				
PLIST値が次の値よりも小さいことを確認する		X				
環境変数が次の値に等しいことを確認する		X				
環境変数が存在することを確認する		X				
環境変数が次の値よりも大きいことを確認する		X				
環境変数が次の値よりも小さいことを確認する		X				
regexに一致するファイルが1つ以上存在することを確認する		X				
regexに一致するファイル名の数が次の値よりも多いことを確認する		X				
regexに一致するファイル名の数が次の値よりも少ないことを確認する		X				
regexに一致するファイル名の数を確認する		X				

手順	説明	V	OS	R	ORS	ORF
ファイル情報が次の値と等しいことを確認する		X				
ファイル情報が次の値よりも大きいことを確認する		X				
ファイル情報が次の値よりも小さいことを確認する		X				

Red Hat Enterprise Linuxデバイス用の手順

RHEL用のスクリプトへの手順の追加

手順	説明	V	OS	R	ORS	ORF
常に失敗する		X		X		
プロセスを停止する	プロセス「%{name}」を停止します。	X	X	X	X	X
プログラムを起動する	パラメータ「%{parms}」を付けて「%{path}\%{program}」を起動します。	X	X	X	X	X
メッセージをログに記録する	「%{message}」のログを「%{type}」に記録します。			X		
ファイルシステムを検索する	「%{drives}」上の「%{startingDirectory}」で「%{name}」を検索して「%{action}」します。	X				
ファイルを解凍する	「%{target}」に「%{path}\	X		X	X	X

手順	説明	V	OS	R	ORS	ORF
	%{file}」を解凍します。					
ポリシーとジョブスケジュールを更新する	アプライアンスからポリシーとジョブスケジュールを更新します。	X				
ファイルをアップロードする	サーバーに「%{path}\%{file}」をアップロードします。		X	X		
ディレクトリが存在することを確認する	ディレクトリ「%{path}」が存在することを確認します。	X				
ファイルが存在することを確認する	ファイル「%{path}\%{file}」が存在することを確認します。	X				
ファイルがその後修正されたことを確認する	ファイル「%{path}\%{file}」が「%{expectedValue}」から変更されたことを確認します。	X				
プロセスが動作していないことを確認する	プロセス「%{name}」が動作していないことを確認します。	X				
プロセスが動作していることを確認する	プロセス「%{name}」が動作していることを確認します。	X				
環境変数が次の値よりも小さいことを確認する		X				
regexに一致するファイル		X				

手順	説明	V	OS	R	ORS	ORF
が1つ以上存在することを確認する						
regexに一致するファイル名の数が次の値よりも多いことを確認する		X				
regexに一致するファイル名の数が次の値よりも少ないことを確認する		X				
regexに一致するファイル名の数を確認する		X				
ファイル情報が次の値と等しいことを確認する		X				
ファイル情報が次の値よりも大きいことを確認する		X				
ファイル情報が次の値よりも小さいことを確認する		X				

LDAP 変数

アプライアンスでは、LDAP ラベルおよびデータベースクエリで使用する変数がサポートされます。

デバイス変数またはマシン変数

デバイス変数またはマシン変数を LDAP ラベルおよびクエリで使用すると、デバイスを名前、説明、およびその他の LDAP 基準で自動的にグループ化できます。LDAP ラベル処理中に、アプライアンスはすべての KBOX_ 定義変数をそれぞれの実行時値に置き換えます。次の表に、サポートされるデバイス変数またはマシン変数と、それぞれの MACHINE データベーステーブルの列および LDAP 属性へのマッピングを示します。

デバイス変数またはマシン変数とマッピング

アプライアンス変数	アプライアンス MACHINE データベーステーブルの列	LDAP 属性のマッピング
KBOX_COMPUTER_NAME	名前	cn | name
KBOX_COMPUTER_DESCRIPTION	SYSTEM_DESCRIPTION	説明
KBOX_COMPUTER_MAC	MAC	macAddress
KBOX_COMPUTER_IP	IP	ipHostNumber
KBOX_USER	USER_NAME	
KBOX_USER_DOMAIN	USER_DOMAIN	
KBOX_DOMAINUSER	ユーザー	
KBOX_CUSTOM_INVENTORY_*	CUSTOM_INVENTORY	

KBOX_CUSTOM_INVENTORY_* 変数は、カスタムインベントリ値を確認するために使用できます。*はカスタムインベントリルールの表示名に置き換えられます。許可される文字は、「a〜z」、「0〜9」、「.」、「-」で、その他すべての文字はアンダースコア (_) に置き換えられます。

ユーザー変数

ユーザー変数を LDAP ラベルおよびクエリで使用すると、ユーザーをドメイン、場所、予算コード、およびその他の LDAP 基準で自動的にグループ化できます。LDAP ラベル処理中に、アプライアンスはすべての KBOX_ 定義変数をそれぞれの実行時値に置き換えます。次の表に、サポートされるユーザー変数と、それぞれの USER データベーステーブルの列および LDAP 属性へのマッピングを示します。

ユーザー変数とマッピング

アプライアンス変数	アプライアンス USER データベーステーブルの列	LDAP 属性のマッピング
KBOX_USER_NAME	USER_NAME	samAccountName
KBOX_FULL_NAME	FULL_NAME	cn | name
KBOX_EMAIL	EMAIL	mail
KBOX_DOMAIN	DOMAIN	
KBOX_BUDGET_CODE	BUDGET_CODE	
KBOX_LOCATION	LOCATION	1
KBOX_WORK_PHONE	WORK_PHONE	telephoneNumber
KBOX_HOME_PHONE	HOME_PHONE	homePhone

アプライアンス変数	アプライアンス USER データベーステーブルの列	LDAP 属性のマッピング
KBOX_MOBILE_PHONE	MOBILE_PHONE	mobile
KBOX_PAGER_PHONE	PAGER_PHONE	ポケットベル
KBOX_CUSTOM_1	CUSTOM_1	
KBOX_CUSTOM_2	CUSTOM_2	
KBOX_CUSTOM_3	CUSTOM_3	
KBOX_CUSTOM_4	CUSTOM_4	
KBOX_ROLE_ID	ROLE_ID	
KBOX_API_ENABLED	API_ENABLED	• 値なし：KACE GO アプリケーションへのユーザーアクセスを無効にします
KBOX_AMS_ID	AMS_ID	値なし。この変数は使用されません。
KBOX_LOCALE_BROWSER_ID	LOCALE_BROWSER_ID	
KBOX_HD_DEFAULT_QUEUE_ID	HD_DEFAULT_QUEUE_ID	
KBOX_LDAP_UID	LDAP_UID	objectGUID

用語集

A

使用可能な使用ポリシー

ユーザーが**管理者コンソール**、**コマンドラインコンソール**、または**ユーザーコンソール**にログインする際に表示されるステートメントまたはポリシー。詳細については、「使用可能な使用ポリシーの有効化または無効化」を参照してください。

カタログへの追加の要求

カタログ登録要求は、ソフトウェアカタログに含まれていないアプリケーション（カタログ未登録）をパブリックのソフトウェアカタログに追加するよう要求するために送信できるフォームです。Questがカタログ登録要求を受け取ると、その要求が評価され、アプリケーションを公開ソフトウェアカタログに含めるべきかどうかが決定されます。さらに、カタログ登録要求が送信されると、アプリケーションが自動的にアプライアンス上のローカル版のソフトウェアカタログに追加されます。詳細については、「ソフトウェアカタログへのアプリケーションの追加」を参照してください。

管理者コンソール

管理者コンソール は、アプライアンスを制御するために使用する Web ベースインターフェイスです。**管理者コンソール** にアクセスするには、http://<appliance_hostname>/admin に移動します。<appliance_hostname> はアプライアンスのホスト名です。組織コンポーネントが有効になっている場合は、http://<appliance_hostname>/system から、**管理者コンソール** のシステムレベル設定にアクセスできます。**管理者コンソール** で URL の完全パスを表示すると、データベースの検索やリンクの共有に便利です。完全パスを表示するには、ログインで使用する URL に、「ui」を追加します。例：http://<appliance_hostname>/admin。

エージェント

KACE エージェントは、デバイスにインストールして、アプライアンス経由でのデバイス管理を可能にするアプリケーションです。管理対象デバイスにインストールされたエージェントは、エージェントメッセージプロトコルを通じてアプライアンスと通信します。エージェントは、管理対象デバイスからのインベントリ情報の収集や、管理対象デバイスへのソフトウェアの配布などのスケジュール済みタスクを実行します。プリンタや、エージェントによるサポート対象以外のオペレーティングシステムを搭載したデバイスなど、エージェントソフトウェアをインストールできないデバイスでは、エージェント不要の管理も使用可能です。詳細については、「KACE エージェントのプロビジョニング」を参照してください。

エージェント不要の管理

エージェント不要デバイス管理は、デバイスに KACE エージェントソフトウェアを展開および保守する必要なく、デバイスを管理する方法です。エージェント不要管理では、SSH、SNMP、およびその他の方法を使用して、プリンタ、ネットワークデバイス、およびストレージデバイスなどのエージェントをインストールできないデバイスに接続し、アプライアンス **管理者コンソール** にインベントリをレポートします。これは、オペレーティングシステムのバージョンおよび配布が KACE エージェントのサポート対象ではない場合や、エージェントをインストールするよりもエージェント不要管理が望ましい場合に有用です。詳細については、「エージェント不要デバイスの管理」を参照してください。

アラート

ブロードキャストアラートは、エージェント管理対象デバイスで表示される、アプライアンスからブロードキャストできるポップアップなどのメッセージです。警告は、緊急情報を送信する必要がある場合、またはデバイス上でアクションやスクリプトを実行する際に前もってユーザーに通知する必要がある場合に便利です。詳細については、「管理対象デバイスへの警告のブロードキャスト」を参照してください。

警告の監視は、サポートされているサーバデバイスで生成され、アプライアンスに送信されるメッセージです。このメッセージにより、デバイスのイベントおよびシステムログにレポートされるエラーおよび問題に関してスタッフに注意喚起を行います。詳細については、「サーバーの監視」を参照してください。

代替のダウンロード場所

代替のダウンロード場所には、特定のアプリケーションをインストールするために必要なすべてのファイルが格納されている任意のネットワーク上の場所を指定できます。UNCアドレスやDFSソースなどの代替のダウンロード場所からパッケージを配布できます。CIFSとSMBのプロトコル、SAMBAサーバー、およびファイルサーバーアプライアンスがサポートされています。代替のダウンロード場所は、管理対象インストールを作成する際に指定します。詳細については、「管理対象インストールの使用」を参照してください。

AppDeploy Live

詳細については、「ITNinja」を参照してください。

app

詳細については、「KACE GO」を参照してください。

アプライアンスリンク

アプライアンスをリンクすることで、**管理者コンソール**の右上隅にあるドロップダウンリストから1つのアプライアンスにログインしたり、各アプライアンスに個別にログインすることなく、リンクされたすべてのアプライアンスにアクセスしたりできます。管理対象のすべてのQuest Kシリーズアプライアンスをリンクできます。詳細については、「Quest KACEアプライアンスのリンク」を参照してください。

アプライアンス/仮想アプライアンス

アプライアンスは、物理的またはハードウェアベースのアプライアンスとして、および仮想アプライアンスとして使用できます。仮想アプライアンスは、VMware インフラストラクチャを使用します。物理アプライアンスと仮想アプライアンスのどちらでも、同じシステム管理機能が利用できます。詳細については、「アプライアンスコンポーネントについて」を参照してください。

アプリケーション制御

アプリケーション制御を使用すると、アプリケーションを「不許可」としてマーク付けして、エージェント管理対象の Windows デバイスおよび Mac デバイスでの実行をブロックしたり、禁止したりできます。これは、環境内で特定のアプリケーションの実行を制限する場合に役立ちます。詳細については、「アプリケーション制御ラベルのデバイスへの適用」を参照してください。

資産管理

アプライアンスインベントリプロセスを通じて収集されたデータのフレームワーク上に構築される、複合的なライセンスコンプライアンスのレポートをサポートします。資産管理を使用すると、管理対象デバイスに関する追加データ（購入日、サポート契約、資産タグなど）の追跡も可能になります。詳細については、「資産管理コンポーネントについて」を参照してください。

資産管理コンポーネントで使用される資産、資産タイプ、および資産サブタイプ

資産管理コンポーネントで使用される資産および資産タイプには、デバイス、アプリケーション、プリンタ、ライセンス、部門、場所、およびベンダーなどの物理的なアイテムおよび論理的なアイテムがあります。資産管理コンポーネントを使用すると、資産間の関係の構築、インベントリデータの追跡、変更レコードの表示、資産に対する変更のレポート作成ができるようになります。資産は資産タイプに基づきます。必要に応じて、デフォルトの資産タイプの変更、カスタムの資産タイプの作成、および資産情報のインポートを行うことができます。詳細については、「資産タイプについて」を参照してください。資産サブタイプは、カスタム資産タイプを含め任意の資産タイプに追加可能な資産のサブカテゴリです。これにより、資産のサブタイプを識別し、管理できます。サブタイプには、コンピュータやプリンタやルーターといったデバイス資産や、アプライアンスインベントリの Windows や Mac や Linux のシステムで動作するソフトウェア資産などがあります。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。

アプライアンスライセンスの上限の計算に含まれる資産

アプライアンスライセンス契約に従い、指定された数のデバイスを管理できます。これらのデバイスは資産として分類されますが、この資産は、資産管理コンポーネントで使用される資産とは異なります。ライセンスの上限の計算に含まれる資産とは、1）アプライアンスのインベントリに追加されているが管理対象コンピュータまたは監視対象サーバの定義には適合しないデバイスで、かつ 2）WSAPI またはモバイル管理を使用してインベントリに手動で追加されていないデバイスを指します。例えば、プリンタ、プロジェクタ、ネットワーク製品、ストレージデバイスなどは資産に該当します。

注: 資産管理コンポーネントを使用して作成、管理している資産は、ライセンスの上限の計算に含まれません。

詳細については、「製品ライセンス情報の表示」を参照してください。

AUP

詳細については、「使用可能な使用ポリシー」を参照してください。

自動ラベル

自動的に適用されるラベル（Smart Labelなど）。詳細については、「アイテムのグループを管理するためのラベルのセットアップおよび使用」を参照してください。

B

ブロック

詳細については、「アプリケーション制御」を参照してください。

ベンチマーク

SCAPベンチマークは、特定の運用環境でデバイスの脆弱性を評価するための一連のルールを含む、セキュリティ設定チェックリストです。NIST（National Institute of Standards and Technology）が管理するNational Checklist Repositoryには、特定のIT製品とIT製品のカテゴリに関するさまざまなセキュリティ設定チェックリストが格納されています。詳細については、「ベンチマークについて」を参照してください。

C

カタログ登録済みのアプリケーション

カタログ登録済みのアプリケーションは、公式のソフトウェアカタログデータベースに登録されている実行可能ファイルです。これには、アプライアンスインベントリに表示されるアプリケーション（検出されたアプリケーション）と、アプライアンスインベントリに表示されないアプリケーション（未検出のアプリケーション）の両方が含まれます。詳細については、「カタログ登録済みのアプリケーションについて」を参照してください。

カタログ登録要求

詳細については、「カタログへの追加の要求」を参照してください。

カテゴリ

詳細については、「ソフトウェアカテゴリ」を参照してください。

変更管理

管理者コンソールで、スクリプト、レポート、資産、および設定などのアイテムに対する変更を追跡する機能。詳細については、「履歴設定の定義」を参照してください。

Charlie Root

アプライアンスからの通信に使用する E メールアドレス。

注: 通知および日次レポートは、デフォルトのアドレスである Charlie Root（root@<appliance_hostname>）から送信されます。このアドレスを変更することはできません。

クラシックメータリング

クラシックメータリングは、バージョン 5.5 より前のアプライアンスで提供されていたメータリングシステムです。5.4 以下のバージョンからバージョン 5.5 にアップグレードした場合でも、アップグレード前にメータリングを有効にしていた場合は、引き続き、アプライアンス 5.5 リリースでクラシックメータリングにアクセスすることができます。ただし、クラシックメータリングよりも詳細な情報を提供するソフトウェアカタログのメータリングシステムが、クラシックメータリングに代わって6.0リリースで導入されました。クラシックメータリングは、バージョン6.0以降では使用できなくなりました。詳細については、「メータリング」を参照してください。

クラシックレポート

アプライアンスバージョン 5.2 以前で使用できるレポート作成機能。クラシックレポートは、バージョン 5.5以降では使用できなくなりました。

クライアントドロップの場所

クライアントドロップの場所とは、アプリケーションインストーラやアプライアンスバックアップファイルなどの大規模ファイルをアプライアンスにアップロードするために使用されるファイル共有です。クライアントドロップの場所へのファイルのアップロードは、大規模ファイルではブラウザがタイムアウトする可能性がある、**管理者コンソール**でデフォルトの HTTP メカニズムを使用してファイルをアップロードする方法の代わりになります。詳細については、「アプライアンスクライアントドロップの場所へのファイルのコピー」を参照してください。

クライアント数

詳細については、「デバイス」を参照してください。

コマンドラインコンソール

コマンドラインコンソール は、アプライアンスへのターミナルウィンドウインターフェイスです。これは主に、**管理者コンソール**にアクセスできない場合にアプライアンスの設定とポリシーの適用を行うためのインターフェイスです。詳細については、「アプライアンスの電源投入と管理者コンソールへのログイン」を参照してください。

コンピューター

コンピュータは、アプライアンスで管理可能なデバイスのカテゴリです。例えば、コンピューターには、クライアントコンピューター、サーバー、ノートPC、タブレット、およびスマートフォンが含まれます。アプライアンスライセンス契約に従い、指定された数のコンピュータを管理できます。詳細については、「管理対象コンピューター」を参照してください。

資格情報管理

資格情報管理を使用して、管理対象コンピューターやサーバーなどの他のシステムへのログインに必要なユーザー名とパスワードや、Google または SNMP 認証に必要な情報を整理できます。これにより、資格情報および認証情報の入力と管理のプロセスが簡素化されます。詳細については、「資格情報の管理」を参照してください。

D

データの保持

メータリング、デバイス管理時間、カタログ未登録のアプリケーション、およびバックアップのデータをアプライアンスに保存するためのオプション。管理者レベルまたは組織固有の一般設定項目の設定および日ベースのバックアップスケジュールと保存されるバックアップ数の設定を参照してください。

データ共有

Quest KACEとアプライアンスの情報を共有するためのオプション。詳細については、「データ共有の基本設定の構成」を参照してください。

Dell Command | Monitor

Dell Command | Monitor は、Dell Command Suite の監視ツールです。アプライアンスなどのリモート管理アプリケーションが、管理情報や監視ステータスにアクセスして、エンタープライズクライアントシステムの状態を変更できるようにします。管理対象デバイスで Dell Command | Monitor が検出されると、アプライアンスは WMI（Windows Management Instrumentation）インターフェイスを使用して、詳細なハードウェアインベントリおよび正常性状態を収集します。詳細については、「Dell Command | Monitor について」を参照してください。

デバイスのアクション

デバイス リストから管理対象デバイスに対してコマンドを実行できる機能。デバイスアクションの設定の詳細については、組織コンポーネントが無効になっている場合のアプライアンス一般設定項目の設定を参照してください。

デバイス

デバイスとは、アプライアンスによって管理されるマシン、つまりエンドポイントです。製品ライセンス契約に従い、管理対象コンピュータ、資産、および監視対象サーバに分類された、指定された数のデバイスを管理できます。管理対象デバイスは、ソフトウェア、ハードウェア、ネットワーク情報などのデータをアプライアンスにレポートします。詳細については、「製品ライセンス情報の表示」を参照してください。

検出されたアプリケーション

検出されたアプリケーションはアプライアンスインベントリ内で実行可能で、ソフトウェアカタログに定義されたアプリケーションと一致します。検出されたアプリケーションおよびスイートに対して、メータリングの有効化や「不許可」としてのマーク付けを行ったり、ライセンス情報の追加を行うことができます。また、検出されたソフトウェアのリストをCSV形式でエクスポートすることもできます。検出されたソフトウェアのリスト、カタログ未登録のリスト、およびローカルカタログ登録済みのリストはエクスポートできますが、ソフトウェアカタログ全体のエクスポートはできません。

未検出のアプリケーションも参照してください。詳細については、「検出されたアプリケーション」を参照してください。

検出

検出は、ネットワークに接続されているデバイスを識別し、これらのデバイスに関する情報を取得するプロセスです。検出可能なデバイスには、ノートPC、デスクトップ、サーバー、モバイルデバイス、仮想デバイス、プリンタ、ネットワークデバイス、ワイヤレスアクセスポイント、ルーター、スイッチなどがあります。これらのデバイスは、デバイス上に KACE エージェントがインストールされていなくてもスキャンして識別できます。検出スキャンはオンデマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。詳細については、「デバイス検出とデバイス管理について」を参照してください。

E

Eメール通知

詳細については、「アラート」を参照してください。

F

組織およびリンク先アプライアンスの高速切り替え

高速切り替えを有効にすると、各組織に個別にログインせずに、**管理者コンソール**の右上隅にあるドロップダウンリストを使用して、組織間の切り替えを行えるようになります。また、各アプライアンスに個別にログインせずに、リンクされているKシリーズアプライアンス間の切り替えを行えるようになります。詳細については、「組織およびリンク先アプライアンスの高速切り替えの有効化」を参照してください。

ファイル同期

ファイル同期を使用すると、ファイルを管理対象デバイスに配布できます。ただし、管理対象インストールとは異なり、ファイル同期ではファイルがインストールされません。ファイルが単に配布されるだけです。ファイル同期は、管理対象デバイスに任意のタイプのファイルをコピーする場合に使用してください。詳細については、「ファイル同期の作成および使用」を参照してください。

フィルタ

ラベルおよび組織フィルタを参照してください。

I

インベントリ

インベントリには、ネットワーク上の管理対象デバイスのデバイス、アプリケーション、プロセス、スタートアッププログラム、およびサービスに関する情報が含まれます。インベントリは、管理対象デバイスにインストールされている KACE エージェントによって収集され、インベントリ API を使用してアップロードされるか、エージェント不要デバイスへの接続を通じて取得されます。個々の管理対象デバイスの詳細データを参照することも、すべての管理対象デバイスから収集された集計データを参照することもできます。また、インベントリ情報はレポートに使用することもできれば、アップグレード、トラブルシューティング、購入、ポリシーなどについて決定を下す際に使用することもできます。詳細については、「KACE エージェントのプロビジョニング」を参照してください。

IPスキャン

詳細については、「検出」を参照してください。

ITNinja

Quest KACEがスポンサーとなっているITNinja.com（以前のAppDeploy.com）は、ITに焦点を絞った製品不問のコミュニティウェブサイトです。このサイトは、IT プロフェッショナルが、システム管理に関連する情報を共有したり、質問したりする主要なインターネットサイトになっています。このWebサイトでは、質疑応答セクションとブログプラットフォームを提供しています。匿名の使用率データをITNinjaと共有することを選択すると、ITNinjaフィードが**管理者コンソール**の ソフトウェア、管理対象インストール、および ファイル同期 などの詳細ページに表示されます。フィードは ソフトウェアカタログ の詳細ページでは利用できません。詳細については、「ITNinjaフィードの有効化」を参照してください。

Questは、Windows信頼性およびパフォーマンスモニタ（PerfMon）テンプレートの基本セットおよびWindows以外のオープンソースのPerlスクリプトをITNinjaで公開しています。そのため、ユーザーはサーバー監視機能を拡張し、システムおよびアプリケーションのパフォーマンス問題を特定できます。これらの管理対象外のテンプレートとスクリプトはダウンロードできるため、ユーザーは最初から作成する必要はありません。

K

KACE GO

KACE GOは、管理者がスマートフォンやタブレットを使用して、サービスデスクチケット、インベントリ情報、警告の監視、およびアプリケーション展開機能にアクセスするためのアプリケーションです。このアプリケーションにより、管理者以外のユーザーもサービスデスクチケットの送信、提出されたチケットのステータスの表示、およびモバイルデバイスからのサポート技術情報記事の閲覧を行うことができるようになります。iOSデバイスの場合はApple App Storeから、Androidデバイスの場合はGoogle Playストアからそれぞれ KACE GOをダウンロードできます。詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。

KACE SDA シリーズアプライアンス

K2000シリーズには、オペレーティングシステム（OS）の導入を完全に自動化するように設計されたシステム導入アプライアンスが含まれています。KACE SDA シリーズの詳細については、Quest のウェブサイト（https://quest.com/products/kace-systems-deployment-appliance/）を参照してください。

アプライアンスシリーズアプライアンス

アプライアンスシリーズには、システムの管理、アプリケーションの導入、資産管理などのシステム管理タスクを完全に自動化するように設計されたシステム管理アプライアンスが含まれています。アプライアンスシリーズの詳細については、Quest の Web サイト（https://quest.com/products/kace-systems-management-appliance/）を参照してください。

サポート技術情報

Quest では、アプライアンスについての記事を掲載したサポート技術情報を https://support.quest.com/kace-systems-management-appliance/kb にご用意しています。サポート技術情報記事は、管理者が経験した実際の問題に対する解決策が継続的に追加され、更新されています。

Konductor

Konductor は、アプライアンスと管理対象デバイスの間の通信を調整してシステムのスムーズな実行を維持する内部アプライアンスコンポーネントです。Konductorが実行しているタスクの数は、進行中のタスク数 ウィジェットに表示されます。加えて、タスクスループット情報が ー般設定（組織コンポーネントが有効なアプライアンスの場合）または エージェント設定（組織コンポーネントが有効になっていないアプライアンスの場合）に表示されます。

詳細については、以下を参照してください。

- ダッシュボードのウィジェットについて
- システムレベルおよび管理者レベルの一般設定項目の設定

KScript

オフラインKScriptおよびオンラインKScriptを参照してください。

L

ラベル

ラベルは、デバイスなどのアイテムをグループとして管理できるよう、整理および分類するためのコンテナです。例えば、オペレーティングシステムが同じデバイスや地理的に同じ場所にあるデバイスを、ラベルを使用して識別することができます。その後、そのラベルが割り当てられているすべてのデバイス上で、ソフトウェアの配布やパッチの導入などのアクションを開始できます。ラベルは、特定のアイテムに手動で割り当てることもできれば、SQLやLDAPクエリなどの基準に関連するアイテムに自動で割り当てることもできます。詳細については、「アイテムのグループを管理するためのラベルのセットアップおよび使用」を参照してください。

ラベルグループ

ラベルグループを使用してラベルを整理すると、ラベルをグループとして管理できます。ラベルグループに含まれるラベルは、互いにタイプを共有しています。ラベルグループに複数のラベルを含めることができるだけではなく、ラベルに対して複数のラベルグループを関連付けることもできます。詳細については、「ラベルグループの追加、表示、または編集」を参照してください。

LDAPブラウザ

LDAP ブラウザを使用すると、Active Directory サーバーなどの LDAP サーバー上にあるデータを参照および検索できます。詳細については、「LDAPブラウザの使用」を参照してください。

LDAPラベル

LDAP（Lightweight Directory Access Protocol）ラベルは、Active Directoryサーバーや LDAPサーバーと通信するラベルです。LDAPラベルを使用すると、LDAPやActive Directoryのクエリまたは検索フィルタに基

づいてデバイスレコードとユーザーレコードに自動でラベル付けできます。LDAPラベルは、検索条件に合致するデバイスに適用されます。詳細については、「LDAPラベルの管理」を参照してください。

リンク

詳細については、「アプライアンスリンク」を参照してください。

各国語コンポーネント

コマンドラインコンソール、**管理者コンソール**、および **ユーザーコンソール** で使用する言語の選択を可能にする、アプライアンスのコンポーネント。詳細については、「ロケール設定の構成」を参照してください。

ローカルカタログ登録済みのアプリケーション

公式版のソフトウェアカタログになく、アプライアンス上のローカル版のカタログに追加されたアプリケーションは、ローカルカタログ登録済みのアプリケーションと呼ばれます。ローカルカタログ登録済みのアプリケーションには、メータリング、「不許可」としてのマーク付け、およびライセンス資産との関連付けを行うことができます。詳細については、「ローカルカタログ登録済みのアプリケーションについて」を参照してください。

Log Enablement Package

Log Enablement Package（LEP）を導入すると、サーバーに対してパフォーマンスしきい値および Exchange や Internet Information Services（IIS）などのアプリケーションを監視できます。Log Enablement Packages リストページでは、QuestがWindows信頼性およびパフォーマンスモニタ（PerfMon）テンプレートの基本セット、およびWindows以外のオープンソースのPerlスクリプトを公開しています。そのため、ユーザーは監視機能を拡張し、システムおよびアプリケーションのパフォーマンス問題を特定できます。アプライアンスでの監視はこれらの追加のテンプレートおよびスクリプトがなくても機能しますが、パフォーマンスしきい値監視を実行する場合はテンプレートおよびスクリプトから作成されたプロファイルが役立ちます。詳細については、「Log Enablement Package を使用したアプリケーションおよびしきい値監視の設定」を参照してください。

ログ

詳細については、「スクリプトログの検索」を参照してください。

M

マシン

詳細については、「デバイス」を参照してください。

Mac プロファイル

Mac プロファイルは、ユーザーレベルおよびシステムレベルのポリシーを Mac デバイスで設定するために使用するファイルです。アプライアンスを使用して、Mac OS X を実行するエージェント管理対象デバイスに Mac プロファイルを配布できます。「Mac プロファイルの管理」を参照してください。

管理対象コンピューター

製品ライセンス契約に従い、管理対象コンピュータに分類された、指定された数のデバイスを管理できます。管理対象コンピュータとはアプライアンスインベントリに含まれるデバイスで、1）Windows、Mac、Linux、またはUNIXオペレーティングシステムが搭載され、2）PCまたはサーバーとして分類され、かつ3）WSAPIまたはモバイルデバイスの管理機能を使用してインベントリに手動で追加されていないデバイスを指します。詳細については、「製品ライセンス情報の表示」を参照してください。

管理対象インストール

管理対象インストール（MI）は、アプライアンス管理対象デバイスにアプリケーションを展開する、または管理対象デバイスからアプリケーションを削除するためののプライマリメカニズムです。各管理対象インストールでは、インストールまたは削除される特定のアプリケーションのタイトルおよびバージョンの情報（インストールコマンド、インストールファイル、ターゲットデバイス（ラベル別）など）が記述されます。管理対象インストールは、管理対象デバイスがアプライアンスにインベントリデータをアップロードするのと同時に常に実行されます。このように、アプライアンスは、インストールが実際に必要かどうかを、インストールを実行する前に確認します。インストールパッケージは、サイレントモードまたはユーザーとの対話モードで実行されるよう設定できます。管理対象インストールには、インストール用、アンインストール用、コマンドライン用のパラメータを含めることができます。詳細については、「管理対象インストールの使用」を参照してください。

手動ラベル

詳細については、「ラベル」を参照してください。

メータリング

ソフトウェアメータリングにより、管理対象のWindowsデバイスおよびMacデバイス上での、アプリケーションのインストール状況および使用状況に関する情報を収集することができます。これには、Bingトラベルなどの Windowsストアのアプリケーションが含まれます。Linuxなど他のオペレーティングシステムにインストールされたアプリケーションに対しては、メータリングを使用できません。メータリングは、ソフトウェアカタログで「検出済み」および「未検出」と表示されているアプリケーション、およびローカルカタログに登録されているアプリケーションに対して有効にすることができます。オペレーティングシステムソフトウェア、サポートされないオペレーティングシステム（Linuxなど）にインストールされたアプリケーション、またはソフトウェアカタログ内で「カタログ未登録」としてリストされているアプリケーションに対しては、メータリングを有効にできません。詳細については、「ソフトウェアメータリングについて」を参照してください。

MIA

「未同期（Missing in action）」のこと。アプライアンスによる管理対象だがスケジュールどおりにインベントリ設定されていないデバイスを、MIAデバイスと呼びます。詳細については、「MIAデバイスの管理」を参照してください。

モバイルデバイスによるアクセス

モバイルデバイスによるアクセスでは、KACE GO を使用してアプライアンスと対話できるようになります。

KACE GOは、管理者がスマートフォンやタブレットを使用して、サービスデスクチケット、インベントリ情報、およびアプリケーション導入機能にアクセスするためのアプリケーションです。このアプリケーションにより、管理者以外のユーザーもサービスデスクチケットの送信、提出されたチケットのステータスの表示、およびモバイルデバイスからのサポート技術情報記事の閲覧を行うことができるようになります。iOSデバイスの場合はApple App Storeから、Androidデバイスの場合はGoogle PlayストアからそれぞれKACE GOをダウンロードできます。

詳細については、「モバイルデバイスによるアクセスの設定」を参照してください。

管理対象サーバー

製品ライセンス契約に従い、管理対象サーバに分類された、指定された数のデバイスを管理できます。監視対象サーバーとは、1）管理対象コンピューターの要件を満たし、かつ2）監視が有効なサーバーを指します。アプライアンスライセンスで 5 台のサーバを監視できます。最大200台のサーバーを監視可能にするには、監視モジュールのライセンスを取得する必要があります。製品ライセンス情報の表示およびデバイスの監視の管理を参照してください。

MSIインストーラーテンプレート

このテンプレートを使用すると、MSIベースのインストーラーを実行するための基本的なコマンドライン引数を設定するためのスクリプトを作成できます。コマンドラインオプションについては、Microsoft の MSI コマンドラインのマニュアル（http://msdn.microsoft.com）を参照してください。詳細については、「「MSIインストーラー」スクリプトの追加」を参照してください。

N

ノード

詳細については、「デバイス」を参照してください。

コンピューター以外のデバイス

コンピューター以外のデバイスとは、プリンタ、ルーター、ネットワーク製品など、コンピューターの定義に適合しない資産です。管理者は、資産サブタイプを作成して、特定のコンピューター以外のデバイスに関する情報を追跡できます。詳細については、「資産サブタイプ、カスタムフィールド、およびデバイス詳細基本設定について」を参照してください。

不許可のアプリケーション

不許可のアプリケーションとは、ソフトウェアカタログ ページで「不許可」としてマーク付けされたアプリケーションです。WindowsおよびMacのアプリケーションでは、検出済み、未検出、またはローカルカタログ登録済みアプリケーションのいずれかに分類されている場合のみ、「不許可」としてマーク付けできます。カタログ未登録のアプリケーションは、ソフトウェアカタログに追加されない限り、「不許可」としてマーク付けすることはできません。「不許可」としてマーク付けされているアプリケーションは、

アプリケーション制御対応のラベルがデバイスに適用されている場合、管理対象デバイスで実行されないようにすることが可能です。詳細については、「アプリケーション制御の使用」を参照してください。

未検出のアプリケーション

インベントリ内に存在せず、Quest KACE ソフトウェアカタログに存在するアプリケーションは、未検出のアプリケーションと呼ばれます。未検出のアプリケーションに対してメータリングを有効化し、「不許可」としてマーク付けを行い、ライセンス情報の追加を行うことができます。ただし、ローカルのアプライアンスインベントリで検出されなかったアプリケーションであるため、未検出のソフトウェアのリストを CSV 形式でエクスポートすることはできません。検出されたアプリケーションも参照してください。詳細については、「未検出のアプリケーション」を参照してください。

通知

通知は、デバイス、スキャン結果、および資産が指定された条件を満たす場合に、アプライアンスから管理者宛てに送信されるEメールメッセージです。例えば、デバイスがディスク領域の制限に近づいたときに管理者に通知する場合は、ディスク使用量に基づき警告をセットアップできます。通知は、デバイスが指定された条件を満たす場合に送信されます。

アプライアンスは、指定された頻度で実行される通知スケジュールに従って、インベントリと条件を照合します。アイテムが基準を満たした場合、指定された受信者にEメールが送信されます。

選択した条件に基づいて、スケジュールされた間隔でEメールで送信されるメッセージ。詳細については、「通知のスケジュール」を参照してください。

O

オフラインKScript

ターゲットデバイスのクロックに基づいて、スケジュールされた時間に実行されるスクリプト。オフライン KScript は、デバイスの起動時やユーザーのログイン時など、ターゲットデバイスがアプライアンスに接続されていないときでも実行できます。スクリプトは、スクリプト作成テンプレートを使用して作成できます。詳細については、「スクリプトの追加と編集」を参照してください。

オンラインKScript

ターゲットデバイスがアプライアンスに接続されている場合にのみ実行されるスクリプト。オンライン KScriptは、アプライアンスのクロックに基づいて、スケジュールされた時間に実行されます。これらのスクリプトは、スクリプト作成テンプレートを使用して作成できます。詳細については、「スクリプトの追加と編集」を参照してください。

オンラインシェルスクリプト

ターゲットデバイスがアプライアンスに接続されている場合にのみ、アプライアンスのクロックに基づいて、スケジュールされた時間に実行されるスクリプト。オンラインシェルスクリプトは、ターゲットデバイスのオペレーティングシステムによってサポートされている簡単なテキストベースのスクリプト（ Bash、Perl、バッチなど ）を使用して作成します。バッチファイルはWindowsでサポートされていますが、同様にさまざまなシェルスクリプト形式がターゲットデバイスの各オペレーティングシステムによってサポートされています。詳細については、「スクリプトの追加と編集」を参照してください。

組織コンポーネント

アプライアンス内で組織を作成し、管理するためのアプライアンスコンポーネント。これにより、個々の組織にデバイスを割り当て、組織ごとに管理者およびユーザーのアクセスを制御するユーザーの役割を作成できるようになります。例えば、ある組織のデバイスに対してのみ管理者による表示とアクションの実行を許可し、他の組織に属するデバイスについては許可しない、というような設定が行えます。

詳細については、「組織の作成と管理」を参照してください。

組織フィルタ

組織フィルタは、ラベルに似ていますが、固有の用途も持っています。組織フィルタでは、デバイスがインベントリ設定されると、デバイスが自動的に組織に割り当てられます。

組織フィルタには2つのタイプがあります。

- **データフィルタ**: 検索条件に基づいて、デバイスを自動的に組織に割り当てます。デバイスがインベントリ設定されるときに、デバイスが条件を満たしている場合は、デバイスが組織に割り当てられます。この

フィルタは、デバイスが指定された条件と一致する場合に自動的に組織にデバイスを割り当てるという点で、Smart Labelに似ています。

- **LDAPフィルタ**: LDAPまたはActive Directoryとの対話に基づいて、デバイスを自動的に組織に割り当てます。デバイスがインベントリ設定されると、クエリがLDAPサーバーに対して実行されます。デバイスが条件を満たすと、組織に自動的に割り当てられます。

  組織フィルタの管理を参照してください。

組織

組織は、単一のアプライアンスで動作するのアプライアンスの論理インスタンスです。アプライアンス上で組織コンポーネントが有効になっている場合は組織を作成できます。各組織には専用のデータベースが用意されます。また、各組織のインベントリとその他のコンポーネントは別々に管理します。詳細については、「組織の作成と管理」を参照してください。

OVAL

OVAL（Open Vulnerability and Assessment Language）は、Windowsデバイス上のセキュリティの脆弱性および設定の問題を検出するための、国際的に認定された標準です。OVALセキュリティチェックは、コンプライアンスに準拠していない資産を判別し、セキュリティポリシーをカスタマイズして、ルールの施行、テストのスケジュールによる自動実行、結果に基づくレポートの作成を行えます。

OVALはCVE（Common Vulnerabilities and Exposures）リストと互換性があります。CVEコンテンツは、国際的な情報セキュリティコミュニティからのエキスパートで構成されるCVE Editorial Boardによって決定されます。コミュニティフォーラムで審議されたセキュリティの脆弱性に関する新しい情報は、リストに追加可能かを確認するためにCVEイニシアチブに送信されます。CVE、MITRE Corporation、または OVAL Board の詳細については、http://cve.mitre.orgを参照してください。

脆弱性と危険性について一般的な言葉で説明できることにより、他のCVE互換のデータベースおよびツールとセキュリティデータを共有することがさらに容易になります。

詳細については、「OVALテストと定義の理解」を参照してください。

P

パッチ適用

パッチ適用は、Microsoft、Apple、およびその他のサードパーティベンダー（アドビなど）から提供される、セキュリティ関連のパッチやその他の重要なパッチを展開するメカニズムです。これには、アプリケーションと同様にオペレーティングシステムのパッチが含まれます。本番稼働環境でパッチを展開する際に、パッチを適用するオペレーティングシステムを選択し、ラベルを使用してスケジュールを定義できます。詳細については、「パッチ管理について」を参照してください。

プロビジョニングスケジュール

プロビジョニングスケジュールは、エージェントソフトウェアを使用して管理する対象のデバイスに、KACE エージェントをインストールする方法と、インストールする時間を指定します。詳細については、「プロビジョニングスケジュールの管理」を参照してください。

プロビジョニング

管理対象デバイスに KACE エージェントをインストールするプロセス。詳細については、「KACE エージェントのプロビジョニング」を参照してください。

R

レプリケーション共有

レプリケーション共有は、配布対象ファイルのコピーを保持するデバイスであり、管理対象デバイスが複数の地理的な場所に展開されている場合に特に有用です。例えば、レプリケーション共有を使用すると、ロサンゼルスにあるアプライアンスからニューヨークにあるデバイスにファイルをダウンロードしなくても、ニューヨークの同じオフィスにある別のデバイスからファイルをダウンロードできます。レプリケーション共有は、すべてのデジタル資産の完全なレプリケーションであり、アプライアンスによって自動的に管理されます。ラベルでレプリケーション共有を指定していると、そのラベルに含まれるデバイスは、常にレプリケーション共有にアクセスしてファイルを取得します。詳細については、「レプリケーション共有の使用」を参照してください。

レポート作成

ハードウェア、ソフトウェア、およびライセンスコンプライアンスに関する情報をデバイスごとに収集する機能。標準レポートを実行することもできますし、ステップバイステップのレポートウィザードを使用

してカスタムレポートを作成することもできます。また、レポートのスケジュール実行とEメールによる配信も可能です。詳しい知識のあるユーザーであれば、ODBC（Open DataBase Connectivity）に準拠した任意のレポート作成エンジンを使用して、アプライアンスデータベースに対するレポートを作成することもできます。詳細については、「レポートの使用と通知のスケジュール」を参照してください。

リソース

組織およびアプライアンス間でインポートやエクスポートが行えるアイテム（スクリプト、レポート、管理対象インストール、ソフトウェアなど）。詳細については、「アプライアンスリソースのインポートとエクスポート」を参照してください。

役割

ユーザーアカウントと組織に関連する権限。詳細については、以下を参照してください。

- システムレベルユーザーアカウントの管理
- 組織ユーザーアカウントの管理
- 組織の役割とユーザーの役割の管理
- 監視固有の役割の作成と割り当て

S

SAM

SAMは、Software Asset Management（ソフトウェア資産管理）の略で、インベントリのアプリケーションを管理する手段です。詳細については、「ソフトウェアカタログインベントリの管理」を参照してください。

SAMBA共有

アプライアンスに組み込まれているファイル共有システム。詳細については、「システムレベルでのファイル共有の有効化」を参照してください。

SCAP

SCAP（Secure Content Automation Protocol）は、Windowsデバイス上で、ソフトウェアの脆弱性の列挙、セキュリティ関連の設定および製品名の監視、システムの検査による脆弱性の検出と検出されたセキュリティ問題のインパクトの評価（スコア付け）を行う、一連のオープンスタンダードです。SCAPはNational Institute of Standards and Technology（NIST）によって管理されており、US OMB（米国行政管理予算局）などの政府系機関によってSCAPの使用が義務付けられています。

SCAPでは、基準ベースの脆弱性管理データリポジトリである米国政府のNational Vulnerability Database（NVD）を利用します。NVDには、セキュリティチェックリスト、セキュリティ関連ソフトウェアの脆弱性、構成ミス、製品名、およびインパクトメトリックのデータベースが含まれます。SCAP および NVD の詳細については、NIST のウェブサイト（http://scap.nist.gov/index.html および http://nvd.nist.gov/）を参照してください。

詳細については、「SCAPについて」を参照してください。

スクリプト作成

管理対象デバイスに対する一連のアクションを作成して実行する機能。スクリプトは、アプリケーションのインストールや削除から、管理対象デバイスの設定（ファイアウォール設定など）の確認と変更にいたるまで、さまざまなタスクを実行するように設計できます。スクリプトは、定義するラベルおよびスケジュールに基づいて展開し、実行できます。また、管理対象インストールの中心的な役割を果たすインベントリプロセスとは無関係に動作します。詳細については、「スクリプトの追加と編集」を参照してください。

スクリプト

オフラインKScript、オンラインKScript、およびオンラインシェルスクリプトを参照してください。

サーバー監視

アプライアンスでは、インベントリ内のサーバに対する基本的なパフォーマンス監視を実行するモジュールを提供しています。この監視機能は、サーバークラスのオペレーティングシステムを対象とし、各オペレーティングシステムのパフォーマンス警告の基準を定義するデフォルトの監視プロファイルを提供します。同様の基準または別の基準を使用して、代替のイベントログまたはOSレベルログを参照する別のカスタムプロファイルを定義できます。

サービスデスク

サービスデスクはエンドユーザーのトラブルチケット追跡システム（アプライアンス **ユーザーコンソール** の一部）のデフォルト名です。サービスデスクを利用すると、エンドユーザーが E メールを使用して、または **ユーザーコンソール**（http://<appliance_hostname>/user）を介してトラブルチケットを送信できます。ここで、<appliance_hostname> はアプライアンスのホスト名です。ヘルプデスクチームは、E メール、**管理者コンソール**、http://<appliance_hostname>/admin、または KACE GO アプリケーションを使用してこれらのチケットを管理します。必要に応じて、チケットに関連付けられたカテゴリやフィールドをカスタマイズできます。詳細については、「サービスデスクについて」を参照してください。

Questとの共有

Questとアプライアンスの情報を共有するためのオプション。詳細については、「データ共有の基本設定の構成」を参照してください。

シングルサインオン：アプライアンス

詳細については、「アプライアンスリンク」を参照してください。

シングルサインオン：管理者コンソールおよび ユーザーコンソール

シングルサインオンを使用すると、ドメインにログオンしているユーザーが、アプライアンスのログインページに資格情報を再入力する必要なく、アプライアンス **管理者コンソール** と **ユーザーコンソール** にアクセスできるようになります。詳細については、「シングルサインオン（SSO）について」を参照してください。

Smart Label

Smart Labelは、指定した基準に基づいて自動的に適用および除去されるラベルです。例えば、特定のオフィス（この例ではSan Franciscoのオフィス）にあるノートPCを追跡するには、まず「San Francisco Office」というラベルを作成します。次に、このオフィスにあるデバイスのIPアドレス範囲（サブネット）に基づいてSmart Labelを作成します。このIPアドレス範囲内にあるデバイスがインベントリに設定されるたびに、「San Francisco」というSmart Labelが自動的に適用されます。デバイスがIPアドレス範囲外になり、再度インベントリに設定されると、ラベルは自動的に削除されます。

Smart Labelは、アプライアンスがデバイスインベントリを処理するときに、管理対象デバイスに対して適用または削除されます。そのため、デバイスでメータリングを有効化するSmart Labelを作成しても、Smart Labelがデバイスに対して適用されるまでに時間がかかることがあります。また、デバイスがメータリング情報をレポートするまでにも時間がかかる場合があります。デバイスがインベントリ設定され、Smart Labelが適用された後にのみ、Smart Labelの基準に一致するデバイスでメータリングが有効化されます。

詳細については、「Smart Labelの管理」を参照してください。

ソフトウェアカタログ

ソフトウェアカタログは、57,000超のWindowsとMacのアプリケーションおよびソフトウェアスイートに関する標準化された情報を格納しているデータベースです。カタログの情報には、各アプリケーションまたはスイートの名前、バージョン、発行元、カテゴリ、およびアプリケーションまたはスイートを実行するオペレーティングシステムが含まれます。詳細については、「ソフトウェアカタログインベントリの管理」を参照してください。

ソフトウェアカテゴリ

ソフトウェアカテゴリは、ソフトウェアドライバまたはセキュリティアプリケーションなど特定のグループに属するソフトウェアを分類します。ソフトウェア ページにリストされたアプリケーションについては、カテゴリは手動で割り当てられます。ソフトウェアカタログ ページにリストされたアプリケーションについては、ソフトウェアカテゴリはアプリケーションに自動的に割り当てられます。詳細については、「ソフトウェア脅威レベルとカテゴリの使用」を参照してください。

T

tether

Questサポートへの接続。Questの担当者は、tetherを利用してトラブルシューティング時にユーザーのシステムに接続します。詳細については、「Quest KACE サポートへの tether を有効にする」を参照してください。

タスクスループット

アプライアンスでのタスクの読み込み。詳細については、「Konductor」を参照してください。

サードパーティのアプリケーション

サードパーティによって作成され、Quest KACE製品での使用をライセンスされたアプリケーション。

脅威レベル

脅威レベルを使用して、アイテムの相対的な安全性、およびそのアイテムがインストールされているデバイスの数を示すことができます。この情報は、追跡のみを目的としています。アプライアンスが、脅威レベルに基づきポリシーを強制することはありません。詳細については、「ソフトウェア脅威レベルとカテゴリの使用」を参照してください。

U

カタログ未登録のアプリケーション

カタログ未登録のアプリケーションは、インベントリには存在するが、ソフトウェアカタログには表示されない実行可能ファイルです。ソフトウェアカタログ ページでは、「カタログ未登録」としてリストされたアプリケーションを表示できます。ただし、カタログ未登録のアプリケーションのメータリングの有効化、「不許可」としてのマーク付け、およびライセンス情報の追加を行うことはできません。カタログ未登録のアプリケーションに対してメータリング、「不許可」としてのマーク付け、またはライセンス情報との関連付けを行うには、カタログ未登録のアプリケーションをローカルまたはパブリックのソフトウェアカタログに追加する必要があります。詳細については、「カタログ未登録のアプリケーション」を参照してください。

ユーザーコンソール

ユーザーコンソールは、ソフトウェア、スクリプトなどのダウンロード可能なアイテムをセルフサービス方式で使用できるようにするウェブベースのインターフェイスです。このインタフェースから、サポート技術情報記事にアクセスしたり、サービスデスクのサポートチケットを提出してヘルプを要求したり問題をレポートしたりすることもできます。**ユーザーコンソール** にアクセスするには、http://<appliance_hostname>/user に移動します。<appliance_hostname> はアプライアンスのホスト名です。詳細については、「サービスデスクについて」を参照してください。

ユーザーダウンロード

ユーザーダウンロードは、**ユーザーコンソール**を通じてユーザーに配布される、プリンタドライバなどのアプリケーションが含まれるソフトウェアインストールパッケージです。詳細については、「ユーザーダウンロードの管理」を参照してください。

V

仮想アプライアンス

詳細については、「アプライアンス/仮想アプライアンス」を参照してください。

脆弱性テスト

脆弱性テストは、Open Vulnerability Assessment Language（OVAL）の一連のテストを使用して、既知の脆弱性を発見するためにWindowsデバイスをスキャンするプロセス、およびスキャンをスケジュールするプロセスです。脆弱性テストは、パッチ適用およびその他のセキュリティ強化に役立つ補足機能であり、これらの手段が既知の問題に対応しているかどうかを確認できます。詳細については、「OVALセキュリティチェックについて」を参照してください。

W

Wake On LAN

Wake On LAN を使用すると、KACE エージェントのインストールの有無にかかわらず、アプライアンスからリモートでデバイスの電源を投入できます。詳細については、「Wake On LANの使用」を参照してください。

当社について

Quest は、複雑化する IT 環境において、新しいテクノロジの利点を現実のものにするソフトウェアソリューションを生み出しています。データベースとシステム管理から Active Directory と Office 365 の管理、サイバーセキュリティの回復力まで、Quest はお客様の次の IT の課題を今すぐ解決できるように支援します。世界中で、130,000 社以上の企業と Fortune 500 企業の 95% が、次の企業イニシアチブのプロアクティブな管理と監視を実施し、複雑なマイクロソフトの課題に対応する次のソリューションを見つけ、次の脅威に先んじるために、Quest を頼りにしています。Quest Software。今「次」に備える。詳細に関しては、「www.quest.com」を参照してください。

テクニカルサポートのリソース

Quest の有効なメンテナンス契約をお持ちのお客様、および試用版をお持ちのお客様は、テクニカルサポートをご利用いただけます。Quest サポート ポータルは、https://support.quest.com からアクセスできます。

サポートポータルは、問題を迅速に自身で解決するのに使用できるセルフヘルプツールを提供しており、毎日24時間アクセスできます。このサイトでは、以下の操作を実行できます。

- サービスリクエストの送信と管理
- サポート技術情報記事の表示
- 製品情報への登録
- ソフトウェアと技術文書のダウンロード
- 説明ビデオの再生
- コミュニティの討論への参加
- サポートエンジニアとのオンラインチャット
- 製品のサポートサービスの表示

法的情報

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

特許

Quest Software の先進技術は、当社の誇りです。この製品には特許および出願中の特許が適用される場合があります。この製品に該当する特許の最新情報については、当社の Web サイト https://www.quest.com/legal をご覧ください。

Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

凡例

注意: **注意アイコンは、指示に従わなかった場合に、ハードウェアの損傷やデータ損失につながる可能性があることを示します。**

重要、注、ヒント、モバイル、またはビデオ: 情報アイコンは、補足情報を表しています。

KACE システム管理アプライアンス管理者ガイド

更新日 - 2022年9月

ソフトウェアバージョン - 13.0

索引

数値

Default

A

C

D

E

F

G

I

K

L

あ

い

う

え

お

か

き

く

こ

さ

し

す

せ

そ

た

ち

て

と

ね

は

ふ

へ

ほ

ま

め

も

ゆ

よ

ら

り

る

れ

ろ

わ

ん