Quest

Metalogix® Sensitive Content Manager 2.2

Installation Guide

© 2021 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

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.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Metalogix are trademarks and registered trademarks of Quest Software Inc. and its affiliates. 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.

Legend

CAUTION: An information icon indicates supporting information.

IMPORTANT, NOTE, TIP, MOBILE OR VIDEO: An information icon indicates supporting information.

Metalogix® Sensitive Content Manager
Updated July 2021
Version 2.2

Contents

Metalogix Sensitive Content Manager **4**

System Requirements **7**

Deployment Planning **9**

Pre-install Preparation **12**

Standalone SCM Installation **18**

Worksheet 18
Steps to setup the SCM Server 21
Steps to verify the standalone installation 32

Distributed SCM Installation **34**

Worksheet 35
Steps to setup the SCM Server 37
Steps to install a dedicated SCM Service server 51
Steps to verify the distributed installation 57

License Management **59**

Maintenance **68**

Upgrading SCM components 68
Repairing SCM components 78
Removing SCM components 81

Troubleshooting **85**

Appendix **92**

About Us **96**

Contacting Quest 96
Technical Support Resources 96

1

Metalogix Sensitive Content Manager

Metalogix Sensitive Content Manager (SCM) provides a reliable, accurate and flexible solution for detecting sensitive information such as Personally Identifiable Information (PII), Protected Health Information (PHI) and Payment Card Industry (PCI) within enterprise content management systems.

This guide contains instructions for installing SCM.

Integration with Metalogix ControlPoint and Microsoft SharePoint

SCM can leverage the existing security, compliance and administration capabilities of Metalogix ControlPoint to enforce policies using the full range of Microsoft SharePoint's permissions management, auditing and user activity reporting. With on-demand scanning, administrators can flag specific libraries, sites, or site collections for content discovery, or allow real-time content shield by analyzing files as they are created, modified, moved, or destroyed. The combination of SCM and Metalogix ControlPoint offers a powerful Data Loss Prevention (DLP) solution that uses customizable and intelligent scanning subsystems to identify, track, and secure documents. This ensures a more robust level of information governance inside increasingly complex enterprise environments.

NOTE: Metalogix SCM 2.2 can only be integrated with Metalogix ControlPoint 8.4 or higher which includes a compatible version of the SCM service.

Integration with Metalogix Essentials

Essentials and SCM together allow a customer to selectively migrate file-share content based on the sensitive nature of the content after analysis with SCM.

SCM Architecture

SCM uses a microservices architecture that is comprised of several services that can be deployed on a single server or distributed across several servers. These services work together to analyze documents using regular expressions and machine learning. The SCM components are described below:

SCM Databases

Each service has its own database which together form the SCM Databases and represent the central repository for the configuration, analysis results and operational metrics of the SCM.

Service Bus

SCM uses RabbitMQ as the service bus. It provides the intelligent message routing, event queuing and sequencing needed by SCM to analyze the files.

SCM Services (IIS)

- **Admin Portal** - The *SCMAdminPortal* service manages the SCM Administration Center.
- **Admin Services** - These are back-end services that feed information about other services to the SCM Administration Center.
  - *SCMAdminService* is used for license management, monitoring the system health and other administrative operations of SCM.
  - *SCMAdminService-Analytics*
  - *SCMAdminService-Notifications*
  - *SCMAdminService-Profiles*
  - *SCMAdminService-Scans*
  - *SCMAdminService-Subquestions*
- **File Upload Service** - When integrated with Metalogix ControlPoint, the *SCMFileUploadService* receives the requests to analyze one or more files. It stores these files and submits a request to the queue to analyze these files.
- **Profile Service** - A profile is a named collection of content search and analysis guidelines. Each profile is made up of sub-questions, weights and file thresholds. The *SCMProfileService* serves the profiles that are needed for content analysis.
- **Result Service** - When integrated with Metalogix ControlPoint, a REST API call requests the *SCMResultsService* to return the metrics and results of the files that were analyzed by the Analysis Service. Results are kept for a limited period of time.
- **Subquestion Service** - A sub-question is a search term used to identify a specific kind of sensitive content. The *SCMSubquestionService* serves the entire collection of sub-questions available for use within profiles.
- **Scan Service** - The process of analyzing files in a file-share and the generated report is called a *scan*. The *SCMScanService* allows you to submit, cancel or delete scans, and serves metadata about running scans and scan reports.
- **Analytics Service** - The *SCMAnalyticsService* collects and stores data about analysis throughput. Collected data supports the dashboard experience and is only kept for a limited period of time.
- **Notification Service** - The *SCMNotificationService* provides live-updates for scan progress, health and notifications within the SCM Administration Center.

SCM Services (Windows)

- **Document Routing Service** - When files are uploaded for analysis, they are stored in a specific *temporary folder* on the SCM Server. The *Metalogix SCM Document Routing Service* inspects each file from the folder to check whether these files are single files or complex files like compressed files or emails with attachments. Since only single files can be analyzed, this service submits complex files to the **Archive Extraction Service** to extract individual files for analysis. You can analyze the following file types: *Compressed files, Microsoft Office Files, Open Document Text, Portable Document Format, Rich Text Format,* and *Text Document*.
- **Archive Extraction Service** - When complex files are submitted for analysis, the *Metalogix SCM Extraction Service* extracts individual files from the file set.
- **Document Processing Service** - When single files are ready for analysis the *Metalogix SCM Document Processing Service* extracts the content from the files.
- **Analysis Service** - The *Metalogix SCM Analysis Service* analyzes the content in each file using regular expressions and machine learning technology. Sensitive files are permanently deleted from the *temporary folder* when the analysis is completed.
- **Crawler Service** - The *Metalogix SCM Crawler Service* inspects the contents of a file-share and the sub-folder hierarchy for supported files that are submitted for analysis.

2

System Requirements

The table below lists the minimum system requirements to install and use the SCM.

<table>
<tr><th>Component Type</th><th>Component</th></tr>
<tr><td>Hardware</td><td>
<table>
<tr><th>Type</th><th>SCM Server</th><th>SCM Node</th></tr>
<tr><td>CPU</td><td>8 CPU Cores</td><td>4 CPU Cores</td></tr>
<tr><td>RAM</td><td>32 GB RAM</td><td>12 - 16 GB RAM
(2 - 3 GB per core)</td></tr>
<tr><td>HDD free space</td><td>500 GB*</td><td>100 GB*</td></tr>
</table>
* The minimum space required is double the size of the physical RAM of the server where the temporary files are loaded.
</td></tr>
<tr><td>Operating System</td><td>Windows Server 2012, 2012 R2, 2016 or 2019</td></tr>
<tr><td>Database</td><td>SQL Server 2016 or greater.</td></tr>
<tr><td>Software components</td><td>• Microsoft .NET Framework 4.7.1 or later
• Microsoft .NET Core Hosting 3.1 (x64)
• Microsoft .NET Core Runtime 3.1
• Microsoft Visual C++ 2013 (x64) Redistributable
• Microsoft Visual C++ 2015 (x64) Redistributable
• Microsoft Visual C++ 2015-2019 (x64) Redistributable</td></tr>
<tr><td>Service Bus</td><td>RabbitMQ 3.8.17 with Erlang 24.0 (64-bit) recommended.</td></tr>
<tr><td>Browser</td><td>• Google Chrome (latest version recommended)
• Mozilla Firefox (latest version recommended)
• Microsoft Internet Explorer 11</td></tr>
</table>

3

Deployment Planning

The deployment topologies described below are based on simple estimates to provide some guidance on how to think about load sizing and analysis server distribution. Since processing efficiencies are heavily dependent on your analysis load and server configurations, some research and verification will be necessary to arrive at optimum server load configurations. It is recommended that you contact your Quest representative to assist you in this process.

In this topic:

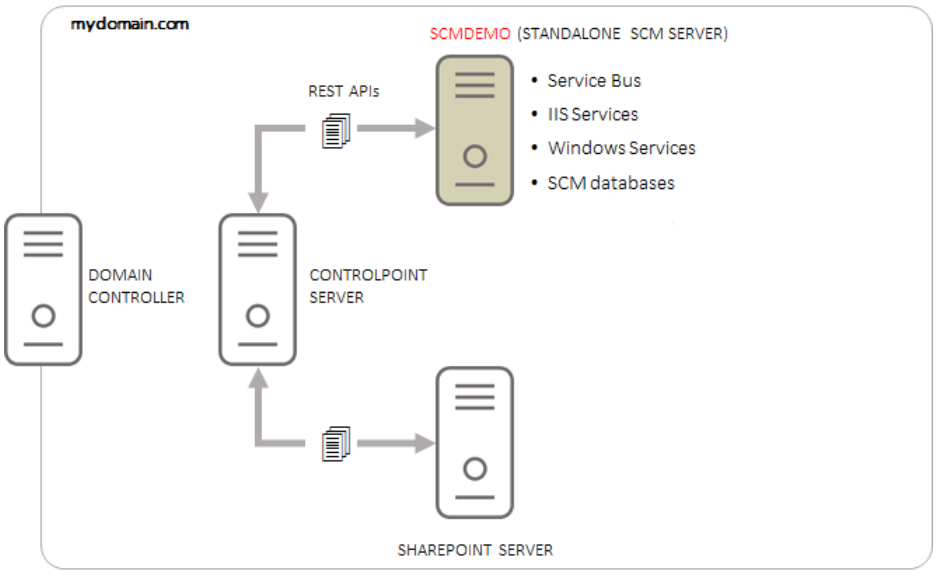
- Standalone SCM deployment topology
- Distributed SCM deployment topology

NOTE: Names of computers or servers used in subsequent topics are referenced from the illustrations below, to serve as conceptual and visual aids.

Standalone SCM deployment topology

This deployment topology assumes that you have several hundred megabytes of files (but less than a gigabyte) from a single Microsoft SharePoint or another file server, that needs analysis.

The suggested approach for this scenario would be to install the SCM databases, Service Bus, IIS and windows services on a single physical or virtual machine. This would be the stand-alone SCM server (SCMDEMO). You could then use Metalogix ControlPoint to submit files for analysis to the SCM server from the connected SharePoint or another file server.



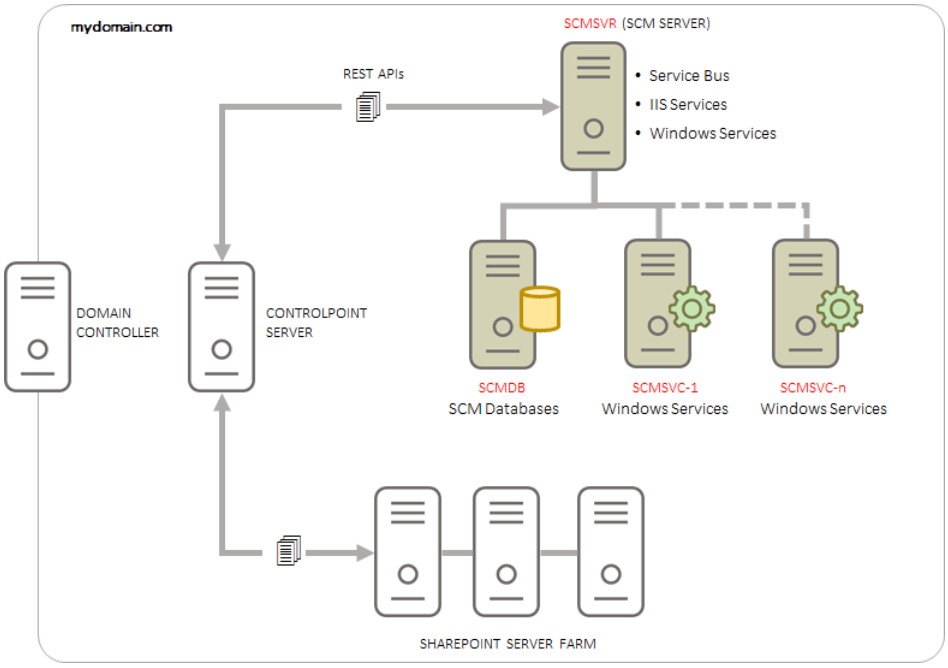
Distributed SCM deployment topology

This deployment topology assumes that you have several terabytes of files spread across a Microsoft SharePoint server farm, and about a gigabyte of these files need to be analyzed per day.

The suggested approach for this scenario would be to install the SCM databases on a dedicated server (SCMDB), the Service Bus, IIS and windows services on a separate server (SCMSVR), and additional Analysis services and/or Document Processing Services (*Metalogix SCM Analysis Service*) on multiple dedicated servers (SCMSVC-1 to SCMSVC-*n*).

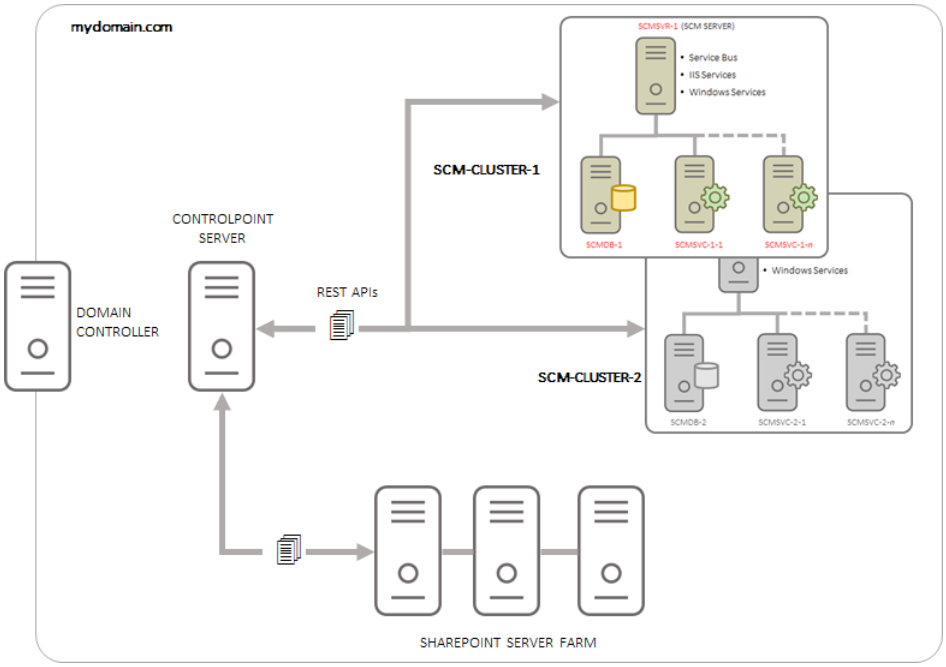
When the SCM Server is integrated with your Metalogix ControlPoint server that connects to your SharePoint farm, you can submit files for analysis. The files that are submitted through Metalogix ControlPoint can be efficiently distributed between the Analysis services on the dedicated servers including the Analysis service on SCMSVR. The distributed nature of the Analysis services ensures efficient processing of the contents of each file.

The number of dedicated servers that are deployed for scaling out the windows services is dependent on the number of files requiring analysis. You can deploy only when needed.



A primary SCM server, an SCM database server and one more service-only servers that are linked to the primary SCM server represents a logical group called a *cluster* as shown in the illustration above. You can deploy additional clusters to the same domain as shown in the next illustration. The scalability of the services architecture allows each cluster to be configured and scaled differently. Multiple clusters are best used when analysis of documents in one department must be segregated from another department within an organization for security reasons, or separate clusters are required for development, user-acceptance testing or other evaluation purposes.

NOTE: Multiple SCM clusters sharing a single SQL Server instance is not a supported deployment model. Each cluster must have its own SCM database instance.



Workload Planning

Planning the workload for document analysis presents significant challenges that arise from the type and size of the documents, the content to be analyzed and the volume of documents submitted for analysis. These factors may remain consistent from day to day, they may change over time or there could be sudden demands for higher than normal volumes of documents with large sizes and complex content.

The recommended approach to planning the workload is to start with a single SCM Server and submit an arbitrary set of up to 50,000 documents. Determine the total processor utilization across all cores (as indicated by the CPU percentage in Task Manager), and the time it takes for analyzing the documents from the analysis reports. If the CPU load is consistently above 90% and analysis reports indicate that most documents are being analyzed in about a second per document, and this pattern holds for a period then the workload is sufficient for a single SCM Server. These numbers are presented as a guidance and you can always increase or decrease the volume of documents being submitted to establish a performance benchmark that is acceptable to you.

The Documents Processing service and the Analysis service are impacted the most with heavy loads. If you expect volumes to either surge periodically or gradually increase over time, it is recommended that you add another server to the cluster with only the Documents Processing service and the Analysis service. Depending on the demands of your workload, adding service-only servers to a cluster could be a temporary or permanent solution.

For extreme levels of workload that require processing millions of documents per day, you can add more service-only servers or plan to add more clusters and distribute documents. The determination to scale out could be a heuristic process and will be unique to the needs of your organization, but the flexibility of the deployment makes it very easy to balance the workload on demand.

4

Pre-install Preparation

Before you begin installing SCM, your environment must be configured to ensure a successful installation of SCM.

NOTE:

- This release of SCM is not compatible with versions prior to 2.0. You must uninstall all SCM components and any distributed SCM Windows services before you install this version of SCM. See Steps to manually uninstall all SCM components for more information.
- If an integration with Metalogix ControlPoint is planned, the SCM Server must be in a domain that is in a full trust relationship with the domain in which ControlPoint is installed. Specifically, verify that the SCM Server is reachable from the ControlPoint Server.
- An empty file storage folder is required on the SCM server for a standalone deployment. An empty file storage *shared folder* must be created on the SCM Server for a distributed deployment. The designated file storage server must be protected with anti-virus software.
- The minimum space requirement for temporary file folders, SQL database drives and RabbitMQ server is approximately double the size of the physical RAM. For example, if you have 32GB of RAM then you must have 64GB of available space on the local drive. You can clear some unused files to recover the required space or select a suitable location on a larger drive.

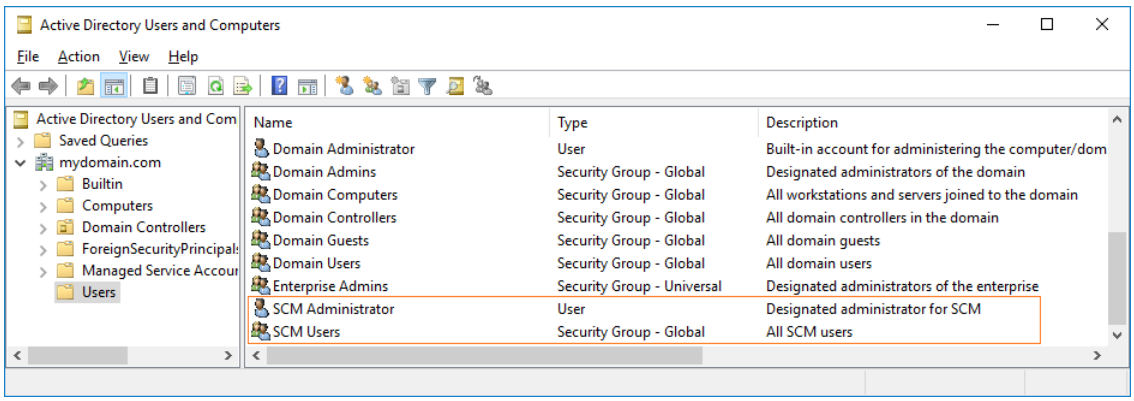
In this topic:

- Setting up users and groups in the Active Directory
- Steps to setup the SCM Administrator account
- Steps to grant additional privileges to the SCM Administrator
- About inbound rules for the service ports on the SCM Server
- Steps to download the installation media

Setting up users and groups in the Active Directory

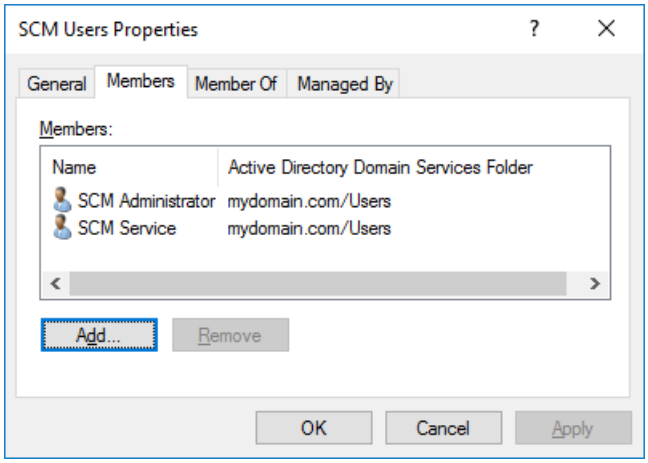
To manage SCM operations it is recommended that you create the following domain users and group in the Active Directory.

Object	Example	Description
Active Directory Group	SCM Users	The active directory (AD) group that contains all users that can log in to the SCM Administration Center.
Active Directory User	SCM Administrator (mydomain\scmadmin)	The designated administrator for SCM. This user is responsible for the installation and configuration of SCM components on one or more machines. This user account is also used to run the SCM Windows services on the primary SCM server or other dedicated service-only servers in a distributed deployment, and accessing enterprise file-share locations for scanning. In a stand-alone deployment, the *LocalSystem* user account can also be used to run the SCM Windows services.



Steps to add additional administrators

1. Open the Active Directory.
2. Expand the root domain and click **Users**.
3. Double-click **SCM Users** to open the *SCM Users Properties* window.



4. Click **Add** and then specify any existing Active Directory user who should be added.
5. Verify that the user appears in the *Members* list of the *SCM Users Properties* window.
6. Click **OK** to close the *SCM Users Properties* window.
7. The *SCM Users* group may be granted remote desktop access if needed. For more information see Steps to grant Remote Desktop Access.

Steps to setup the SCM Administrator account

The SCM Administrator must be granted the following memberships/privileges on the SCM Server in a standalone or distributed environment:

1. Must be a member of the local *Administrators* group.

   NOTE: The SCM Administrator must be a member of the local *Administrators* group on every computer where Sensitive Content Manager components are installed. For example, if dedicated servers are deployed for the SCM Databases and SCM Windows services, then the SCM Administrator must be a member of the local *Administrators* group on those servers as well.

2. Must be a member of the SCM Users group. Access to the SCM Administration Center is allowed for members of the SCM Users group.
3. Must be granted log in rights to the SCM database instances with *dbcreator* and *securityadmin* roles.
4. May be granted remote desktop access if needed. For more information see Steps to grant Remote Desktop Access.

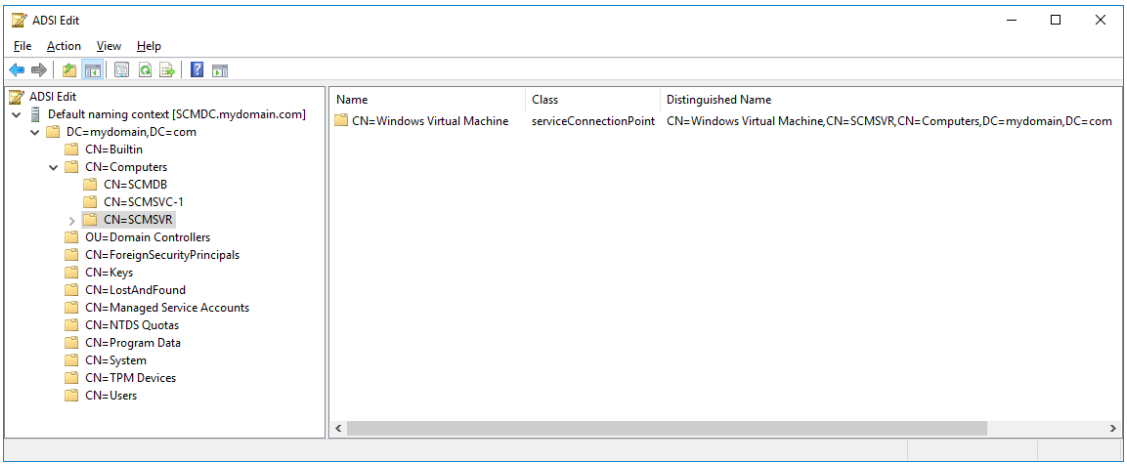
Steps to grant additional privileges to the SCM Administrator

NOTE:

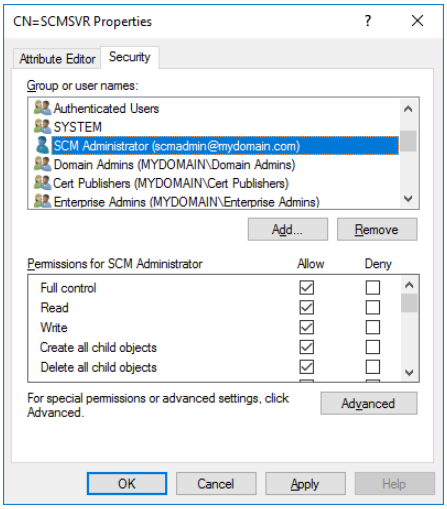
- These steps are optional for a standalone deployment when you choose the Local System account to run the windows services, access the co-located databases and work with file folders.
- These steps are required for a standalone or a distributed deployment when you choose a domain account like SCM Administrator to run the windows services on the primary SCM Server and the dedicated service-only servers, access a remote database server and work with files from a shared folder on the primary SCM server.

The SCM Administrator account must be setup with the following permissions:

1. Log in rights to the SCM database instances must be granted.
2. The *dbcreator* and *securityadmin* server roles, and the *db_owner* role for each database must be granted.
3. Read/Write access to a shared folder that must be created on the primary SCM Server. For details see Steps to grant read/write permissions to the shared folder.
4. Full access to the service connection point must be granted as described below
   a. Log in to your domain controller.
   b. Click **Start** > **Run**. Enter **ADSIEdit.msc** and click **OK** to start the *Active Directory Service Interfaces Editor*.
   c. From the *Console Tree*, expand the computers node and select the primary SCM Server (e.g., CN=SCMSVR). This step is necessary for the primary SCM server only.



   d. Right-click the SCM Server node and select **Properties** from the context menu.
   e. Select the *Security* tab and click **Add** and follow the steps to add a domain user designated to run the SCM Windows services (e.g., SCM Administrator)



f. In the *Permissions* window, select all the **Allow** check boxes.

g. Click **OK** to close the window.

About inbound rules for the service ports on the SCM Server

Service ports are required for the primary SCM Server if the Windows Firewall on the SCM Server is turned on in a distributed deployment. The ports allow services on dedicated servers to communicate with the primary SCM Server. The port numbers indicated here are defaults and you may choose your own port numbers that are unique and unused. The installer automatically creates the inbound rules based on the port numbers that you specify.

- SCM Administration Center: 44300
- Admin Service: 44301
- Result Service: 44302
- File Upload Service: 44303
- Profile Service: 44304
- SubQuestion Service: 44305
- Scan Service: 44306
- Analytics Service: 44307
- Notification Service: 44308

Steps to download the installation media

1. From your browser, navigate to https://www.quest.com/products/metalogix-controlpoint/sensitive-content-manager.aspx

   or

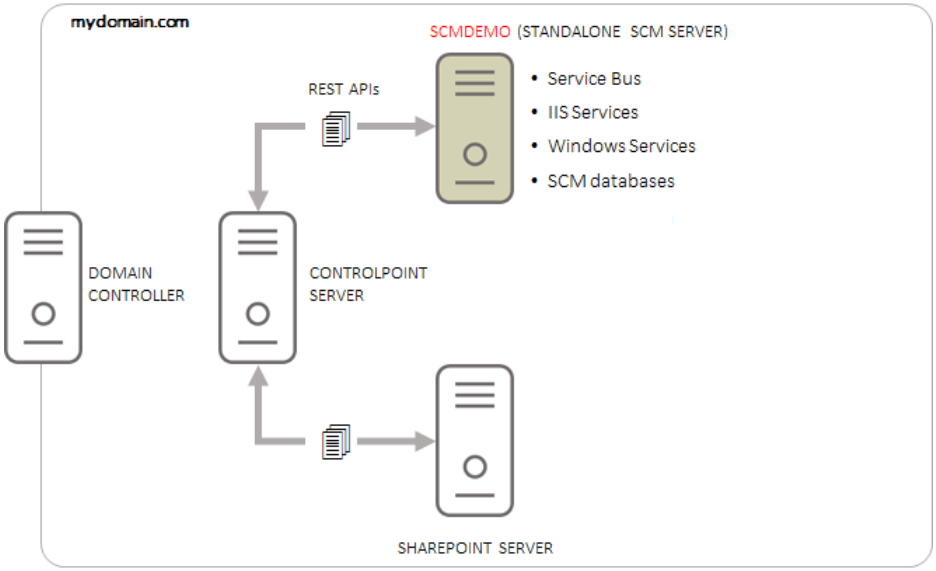
From your browser, navigate to the http://www.quest.com/trials page. Locate the product **Metalogix ControlPoint**. The Metalogix Sensitive Content Manager product is combined with the Metalogix ControlPoint product.

2. Click the **Download Free Trial** button.
3. Fill the *Download Your Free Trial* registration form and click **Download Trial**. The file download page opens.
4. Download the installation ZIP file and extract all the files on the machine on which you are planning to install the SCM components.
5. The trial license key is specified in the email that is sent to you.

5

Standalone SCM Installation

For this deployment topology, a single server is used to install all the components of the SCM as shown in the illustration below.



In this topic:

- Worksheet for this installation
- Steps to setup the SCM Server
- Steps to verify the standalone installation

Worksheet

The following information will be required through the installation process. Sample values are provided here as a guidance based on the illustration above.

Field	Description	Example
License Key	The license key that you received from Quest. If you don't have a license key, contact your Quest representative.	894K5-3M448-M544E-A594A-7K8Z7 (Sample only. This key is neither an active nor an expired license key)

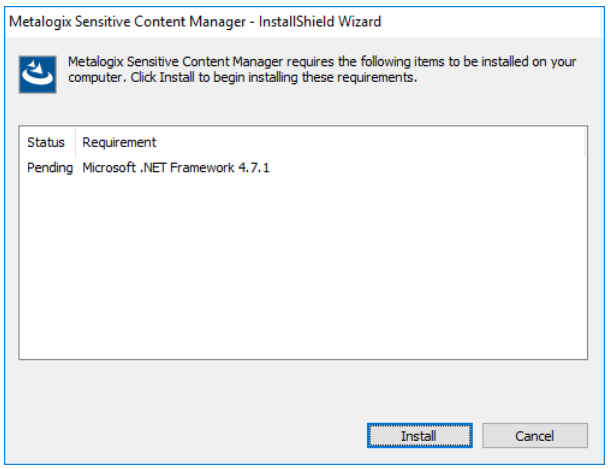
SCM Administrator	The domain user who will log into the SCM Administration Center	mydomain\scmadmin
SCM Server	The server where the SCM components will be installed.	SCMDEMO
SCM Database Server	The SQL server instance on which the SCM database will be installed.	SCMDEMO
Temporary Folder	Full path of the folder that will contain the files during analysis.	C:\ProgramData\Metalogix\Sensitive Content Manager\Storage **NOTE:** The root folder *ProgramData* is a Microsoft recommended folder to be used for application data that is not user specific. It is a hidden and shared folder for all users of the computer.
SSL Certificate friendly name	name of the self-signed certificate that secures all communication with the SCM web server.	scmdemo.mydomain.com
Host Name	The host name of the administration web site for the SCM. Specify a fully qualified domain name.	scmdemo.mydomain.com
Admin Portal Port	The port number for the SCM Administration Center. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44300
Admin Service Port	The port used by the Admin service to request various admin information. Specify a unique port number	44301

	between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	
Result Service Port	The port used for REST calls to request the results of the file analysis. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44302
File Upload Service Port	The port used for REST calls to submit files for analysis. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44303
Profile Service Port	The port used for REST calls to manage profiles. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44304
Subquestion Service Port	The port used for REST calls to manage search terms associated with the profiles. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44305
Scan Service Port	The port used for REST calls to submit, cancel or delete scans and get information about running scans and reports. Specify a unique port number between 1 and 65535. The port number	44306

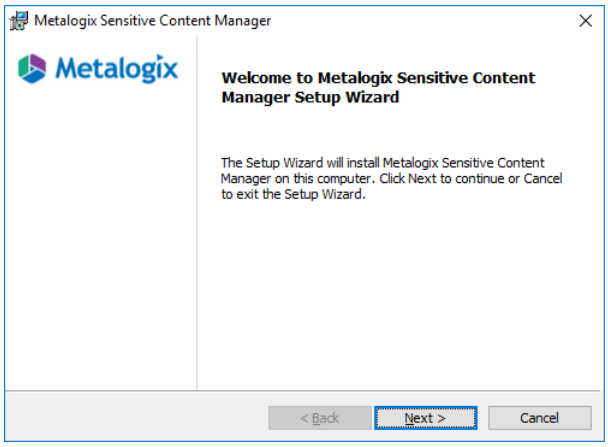
	cannot be a duplicate or a reserved port number.	
Notification Service Port	The port used for REST calls to send system notifications. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44307
Analytics Service Port	The port used for REST calls for analytics. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44308
RabbitMQ connection string	*Required* if a pre-configured instance of RabbitMQ and Erlang exists on another server.	Connection string as required. Contact your *Quest Technical Support Resources* for further assistance.

Steps to setup the SCM Server

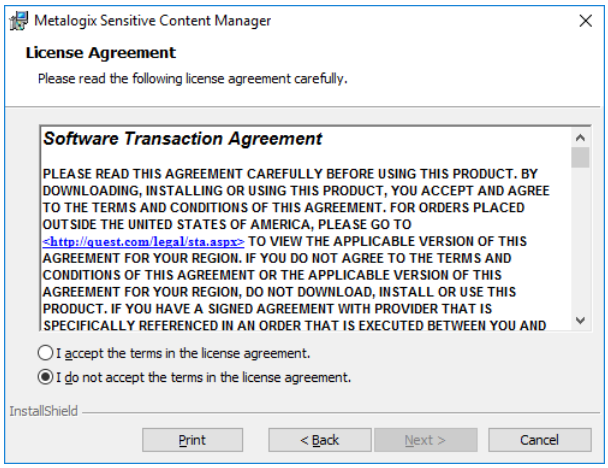
1. Log in to the SCM Server. For example, log in to SCMDEMO using the SCM Administrator credentials (mydomain\scmadmin).
2. Download and unzip the install media files to a local folder.
3. Click the windows installer file **Metalogix Sensitive Content Manager.exe**. The *Prerequisites* window opens if the installer determines that one or more prerequisites are required.



4. Click **Install**. When the prerequisites are installed, the *Welcome to Metalogix Sensitive Content Manager Setup Wizard* window opens. If the appropriate prerequisites are already installed, this is the first window that opens.

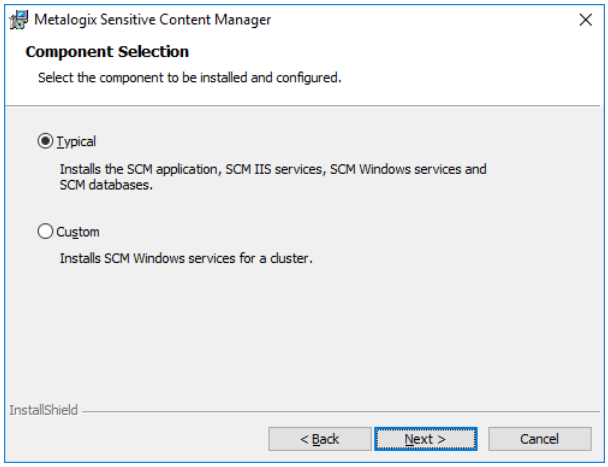


5. Click **Next**. The *License Agreement* window opens.

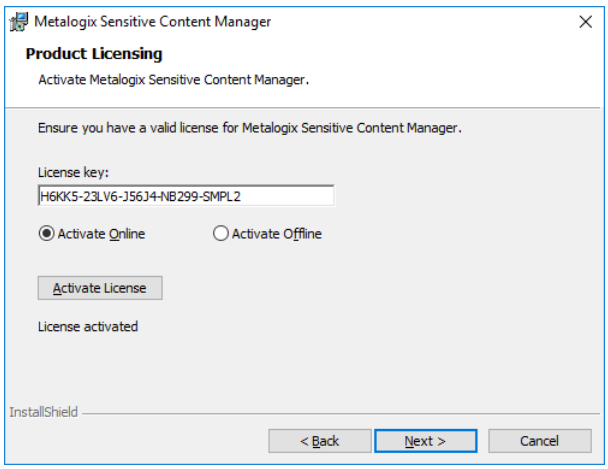


6. Click the check box **I accept the terms in the License Agreement** to activate the **Next** button. Click **Print** to print the License Agreement.

7. Click **Next**. The *Component Selection* window opens. Select **Typical** for a standalone installation.



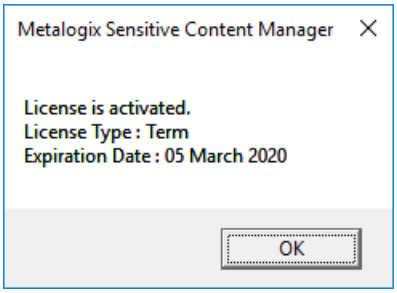
8. Click **Next**. The *Product Licensing* window opens. In the **License Key** field, enter your license key.



9. There are two options available to activate your license. The online activation steps are described here. See Steps to activate your license offline for more information about offline license activation.

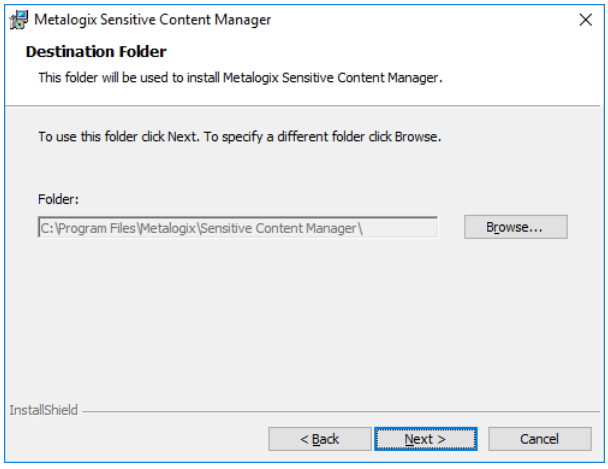
   a. Select **Activate Online**.

   b. Click **Activate License**. If the license activation is successful, a confirmation message opens.

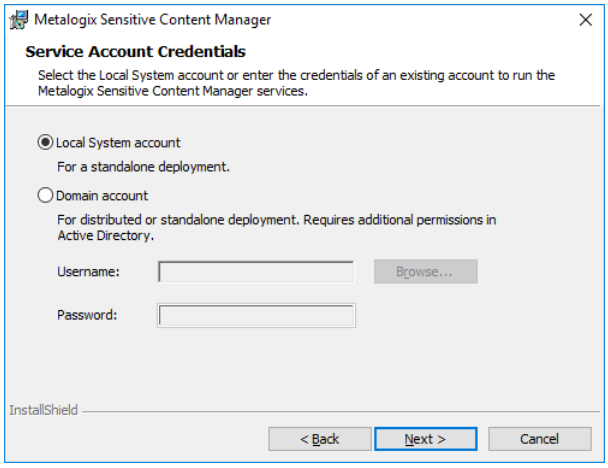


   c. Click **OK**. The status *License not activated* on the *Product Licensing* window changes to *License activated*. Verify your license details as they will differ from the license details shown here.

10. Click **Next**. The *Destination Folder* window opens. Click **Browse** to change the destination folder if necessary. If you change the destination folder ensure that the folder exists on this computer and there are no restrictions to reading or writing to the new folder.



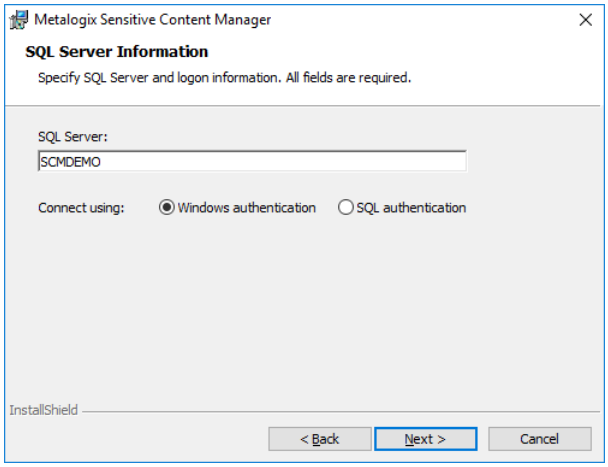
11. Click **Next**. The *Service Account Credentials* window opens.



12. Choose **Local System Account** or **Domain account**. If you choose **Domain account**, enter the credentials of a domain user that will be used to run the windows service.

> **NOTE:** The domain user must have read/write permissions to the Service Connection Point in the active directory. For more information see Steps to grant additional privileges to the SCM Administrator.

13. Click **Next**. The *SQL Server Information* window opens.



Enter the values as described below:

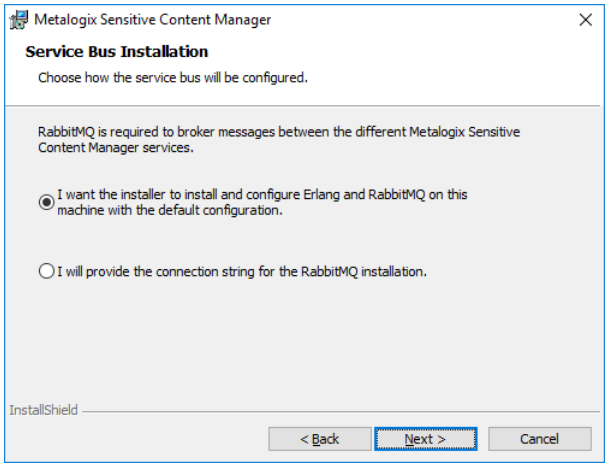
a. **SQL Server** - the name of the SQL Server instance where the SCM database will be installed. For a standalone deployment the SQL Server is the same as the SCM Server.

b. Connection options:

   i. **Windows authentication** - SQL Server validates the account name and password using the Windows principal token in the operating system. The user must have log in rights to the SQL Server instance with *security admin* and *dbcreator* roles assigned. This is the recommended authentication option.

   ii. **SQL authentication** - uses the user credentials stored in SQL Server that may not be based on Windows user accounts. The user must have log in rights to the SQL Server instance with *security admin* and *dbcreator* roles assigned.

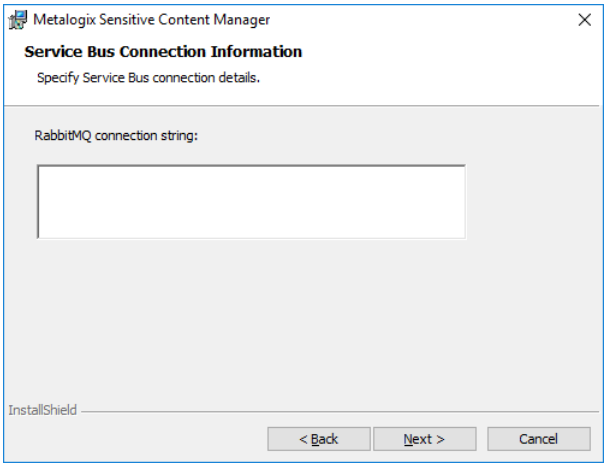
14. Click **Next**. The *Service Bus Installation* window opens. SCM uses RabbitMQ as the service bus.



Choose from one of the following options:

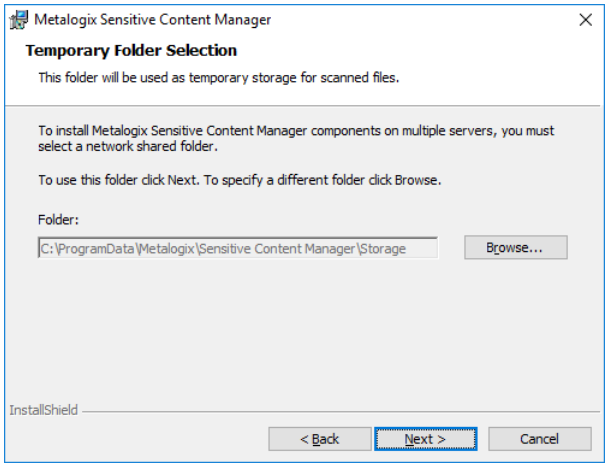
a. Select **I want the installer to install and configure Erlang and RabbitMQ on this machine with the default configuration** if you don't have an existing instance of the service bus. The installer will install the necessary files and dependencies at the end of the install process and create a certificate with the necessary credentials to operate RabbitMQ.

b. Select **I will provide the connection string for the RabbitMQ installation** if you already have a preinstalled instance that you have configured. When you click **Next** with this option selected, the *Service Bus Connection Information* window opens. Specify the RabbitMQ connection string.



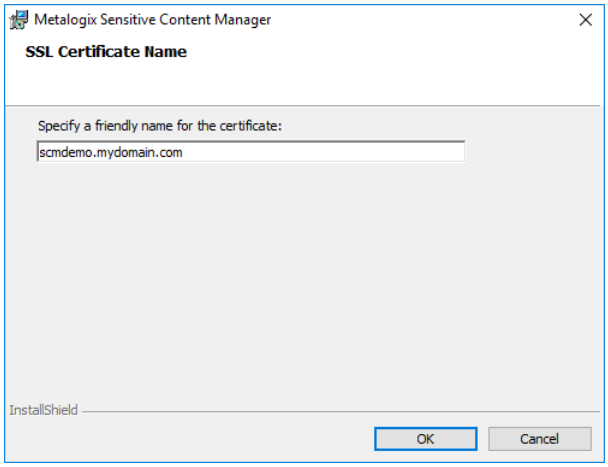
15. Click **Next**. The *Temporary Folder Selection* window opens. The default temporary folder is specified. You can use the same folder or click **Browse** to change to another local folder. If you change the temporary folder, ensure that the folder exists on this computer and there are no restriction to reading or writing to the new folder.

> **NOTE:** We recommend selecting a location on SSD or other fast access storage. The location will be heavily used and fast access storage can significantly improve file analysis

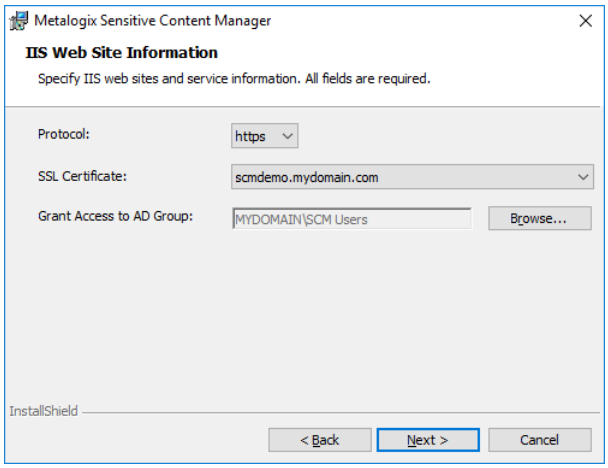


16. Click **Next**. The *IIS Web Site Information* window opens.

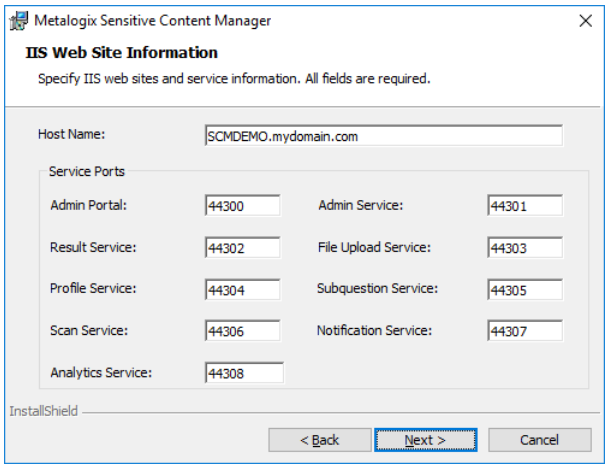
    a. Click the drop-down box for the **SSL Certificate** field and select **<Create Self Signed Certificate>** option. The SSL Certificate Name window opens. Enter a friendly name and click **OK**. The *IIS Web Site Information* window reopens with the specified SSL Certificate name.



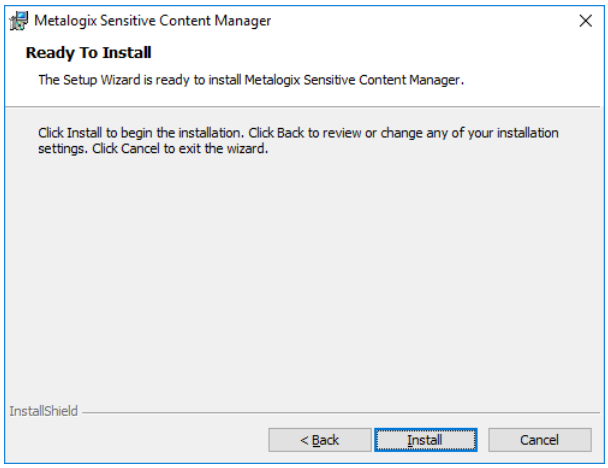
    b. For the **Security Group**, click **Browse** to open the *Select Group* window. Enter **SCM Users** in the **Enter the object name to select** field and click **Check Names**. When the **Domain Users** group is verified, click **OK** to add the group.



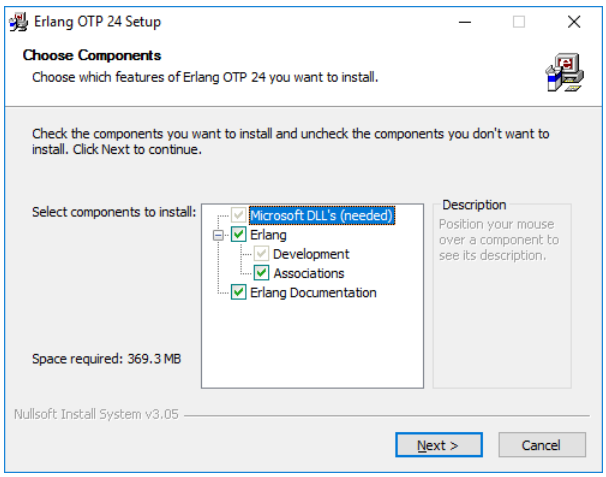
17. Click **Next**. The *IIS Web Site Information* window reopens with default port specifications for each IIS service. If you choose to change the default port numbers, ensure that the port numbers are within the range 1 to 65535 and they are unique and available for use.



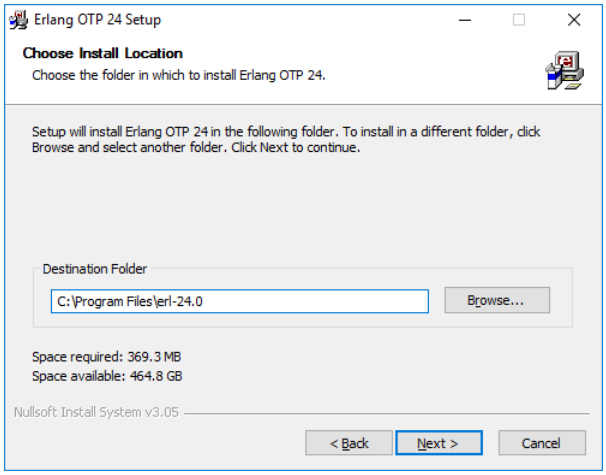
18. Click **Next**. The *Ready To Install* window opens.



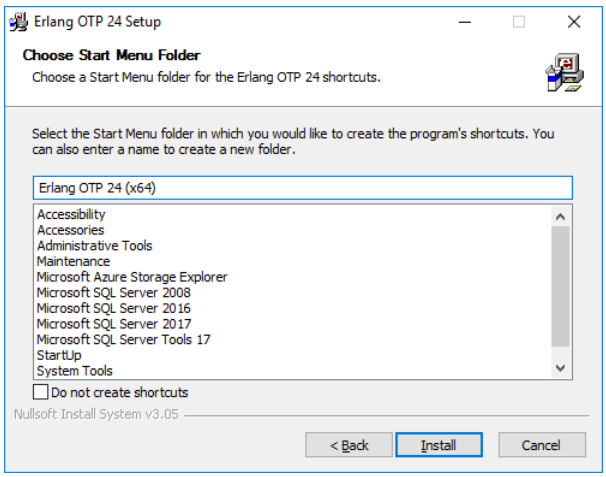
19. Click **Install**. The Erlang third-party component installer starts. You must allow additional Microsoft redistributable components to be installed if requested by the installer.



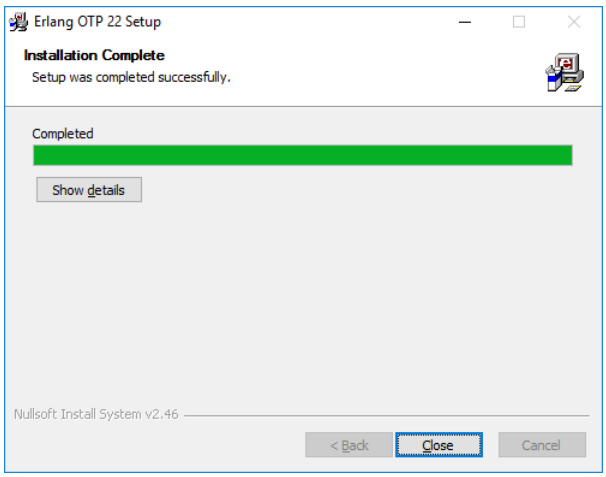
20. Keep the defaults as indicated and click **Next**. The *Choose Install Location* window opens. Click **Browse** to change the location if necessary.


Erlang OTP 24 Setup
Choose Install Location
Choose the folder in which to install Erlang OTP 24.
Setup will install Erlang OTP 24 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Program Files\erl-24.0
Browse...
Space required: 369.3 MB
Space available: 464.8 GB
Nullsoft Install System v3.05
< Back
Next >
Cancel

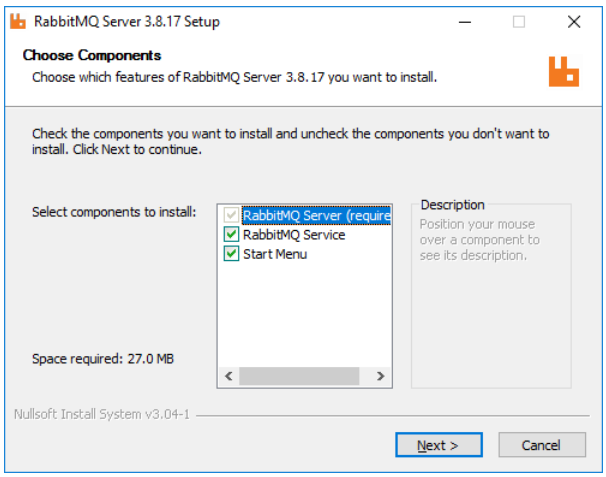
21. Click **Next**. The *Choose Start Menu Folder* window opens. Keep the defaults as indicated and select **Do not create shortcuts** to avoid shortcuts.



22. Click **Next**. The *Installation Complete* window opens when the installation is successful. You must allow additional Microsoft redistributable components to be installed if requested by the installer.

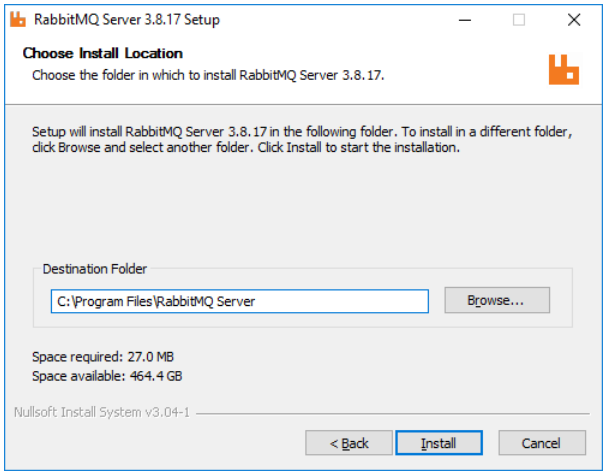


23. Click **Close**. The RabbitMQ installer starts. Keep the defaults as indicated.

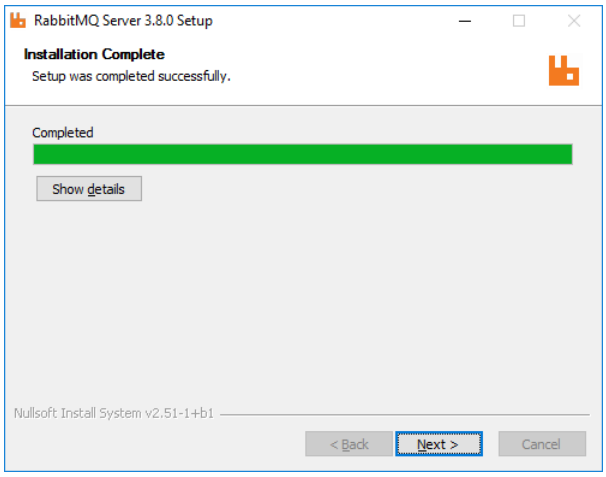


24. Click **Next**. The *Choose Install Location* window opens. Click **Browse** to change the location if necessary.

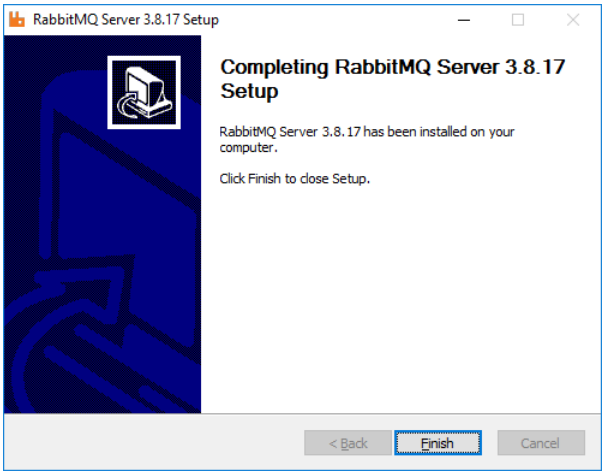
> **NOTE:** Only the *code* files for RabbitMQ are installed here. When you change the location, the *code* files will be installed in the new location.
>
> RabbitMQ *configuration and data* files are installed in the `%APPDATA%\RabbitMQ` folder. If the Metalogix Sensitive Content Manager temporary storage folder and the RabbitMQ *configuration and data* files are installed on the same drive then a heavy demand for resources could cause SCM to pause operations unexpectedly. To avoid this issue, you can manually move the RabbitMQ *configuration and data* files to an alternate drive after installation is complete. For detailed steps see Relocating the RabbitMQ installation directory.



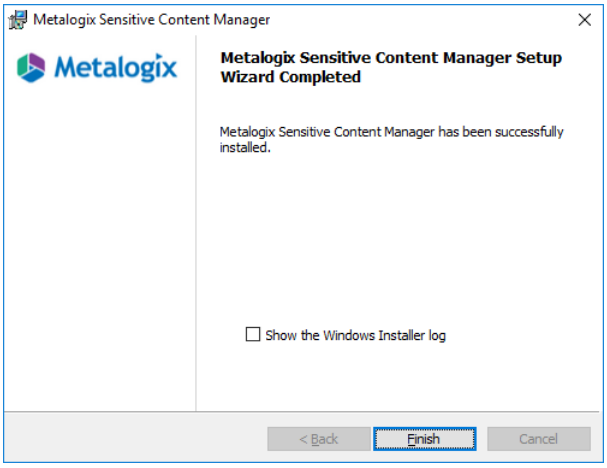
25. Click **Next**. The *Installation Complete* window opens when the installation is successful. Click Show Details to inspect the RabbitMQ installation locations.



26. Click **Next**. The confirmation window opens.



27. Click **Finish**. The rest of the SCM components and any prerequisites will be installed. If the installation is successful, the *SCM Setup Wizard Completed* window opens.

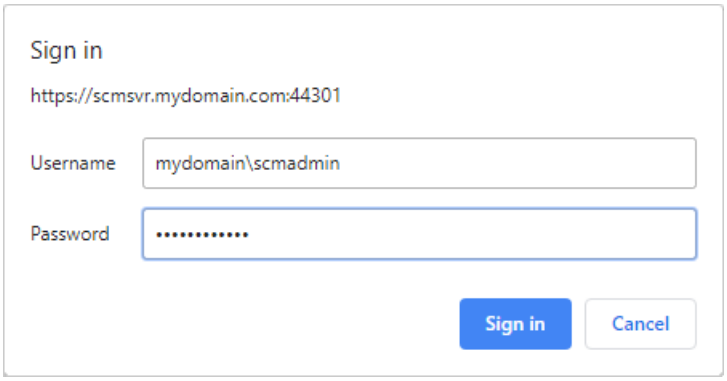


28. You can select the check box **Show the Windows Installer log** which opens the installation log file for reviewing or troubleshooting the installation. Click **Finish** to exit the wizard.

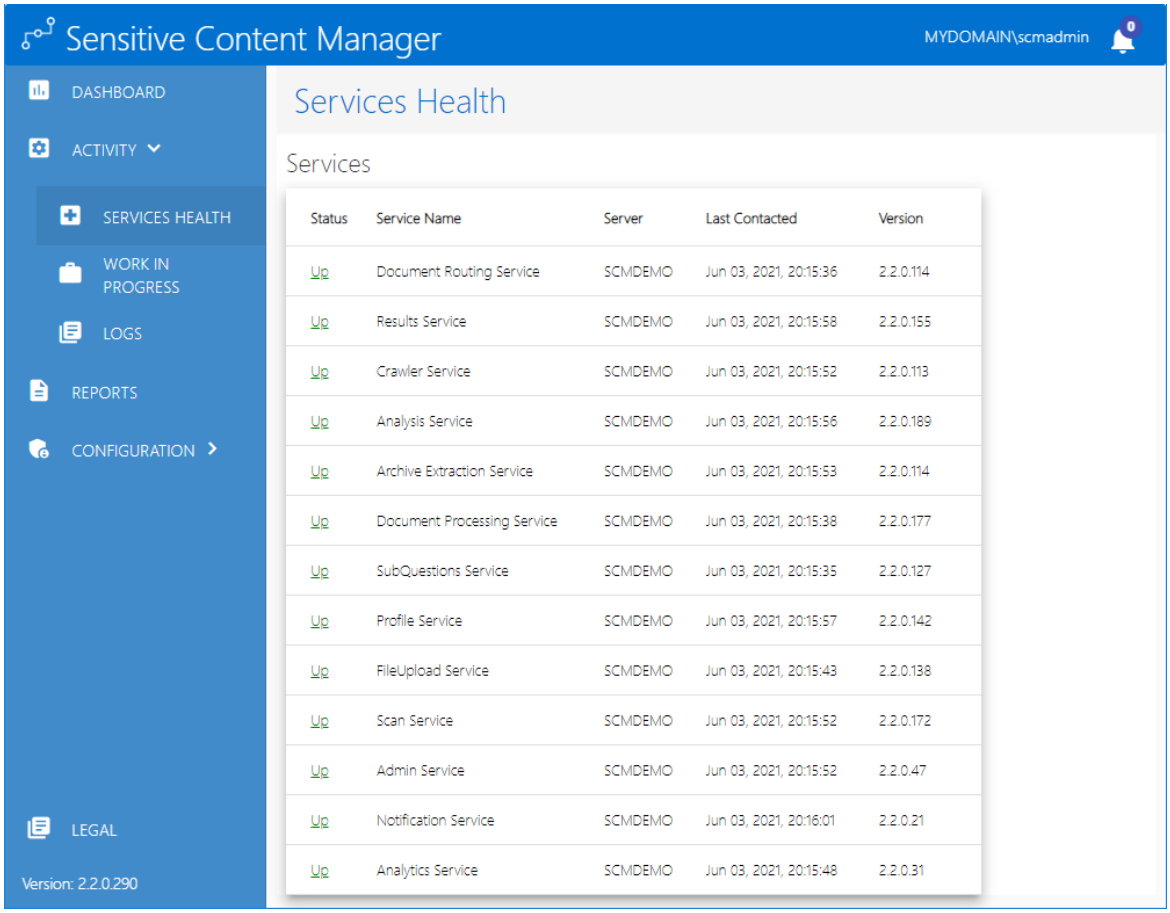
29. A shortcut is added to the desktop.

Steps to verify the standalone installation

1. Log in to the SCM Server (e.g., SCMDEMO)
2. Double-click the desktop shortcut to open the SCM Administration Center. You can also enter the URL directly in a browser. To get the URL for your own installation see Steps to get the URL for the SCM Administration Center.
3. In the *Sign in* dialog that opens, enter the credentials of the SCM Administrator.



4. Click **Sign In**. The *Dashboard* page opens.
5. From the navigation pane, expand **Activity** and then click **Services Health**.
   a. Verify that the software version at the bottom of the navigation pane is the expected upgrade version.
   b. Verify that all services indicate Status = Up.



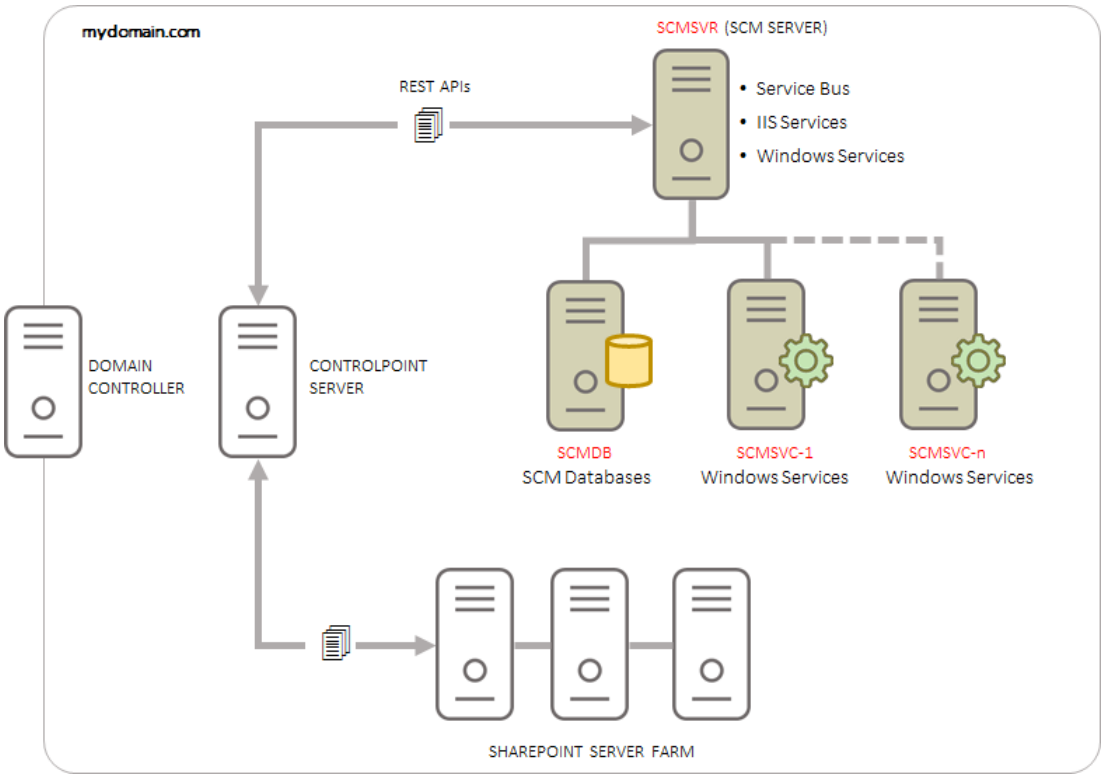
6. This completes the verification of the standalone SCM Server deployment.

6

Distributed SCM Installation

For this deployment topology, the SCM databases are installed on a dedicated server (**SCMDB**), and the rest of the components of the SCM are installed on a dedicated SCM server (**SCMSVR**) as shown in the illustration below.

Initially, the SCM Windows service that is installed on the SCMSVR analyzes documents that are submitted from Metalogix ControlPoint, file shares or other sources. As the analysis load increases, more servers can be deployed (**SCMSVC-1** to **SCMSVC-N**) to scale up the processing power of SCM in addition to the SCM Windows service that is installed on the SCMSVR.



In this topic:

- Worksheet for this installation
- Steps to setup the SCM Server
- Steps to install a dedicated Analysis server
- Steps to verify the distributed installation

Worksheet

The following information will be required through the installation process. Sample values are provided here as a guidance based on the illustration above.

Field	Description	Example
License Key	The license key that you received from Quest. If you don't have a license key, contact your Quest representative.	894K5-3M448-M544E-A594A-7K8Z7 (Sample only. This key is neither an active nor an expired license key)
SCM Administrator	The domain user who will log into the SCM Administration Center	mydomain\scmadmin
SCM Server	The server where the SCM Administration Center and related services are installed.	SCMSVR
SCM Databases Server	The SQL server instance on which the SCM databases will be installed.	SCMDB
SCM Windows service Server	The dedicated server where additional SCM Windows services will be installed.	SCMSVC-1
SCM Windows service account name	The account name that will be used to run the SCM Windows service on all servers.	mydomain\scmadmin. This is the username of the SCM Administrator.
Temporary Folder	Full path of the network shared folder that will contain the files during analysis. The shared folder must exist on the SCM server.	\\SCMSVR\Storage
Cluster Certificate name	Name of the cluster certificate used to locate and join an SCM cluster.	SCM-Cluster-Certificate.pfx
Host Name	The host name of the administration web site for the SCM.	scmsvr.mydomain.com

Admin Portal Port	The port used by the SCM Administration Center. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44300
Admin Service Port	The port used by the Admin service to request various admin information. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44301
Result Service Port	The port used for REST calls to request the results of the file analysis. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44302
File Upload Service Port	The port used for REST calls to submit files for analysis. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44303
Profile Service Port	The port used for REST calls to manage profiles. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44304
Subquestion Service Port	The port used for REST calls to manage search terms associated with the profiles. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44305

Scan Service Port	The port used for REST calls to submit, cancel or delete scans and get information about running scans and reports. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44306
Notification Service Port	The port used for REST calls to send system notifications. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44307
Analytics Service Port	The port used for REST calls for analytics. Specify a unique port number between 1 and 65535. The port number cannot be a duplicate or a reserved port number.	44308
RabbitMQ connection string	*Required* if a pre-configured instance of RabbitMQ and Erlang exists on another server.	Connection string as required. Contact your *Quest Technical Support Resources* for further assistance.

Steps to setup the SCM Server

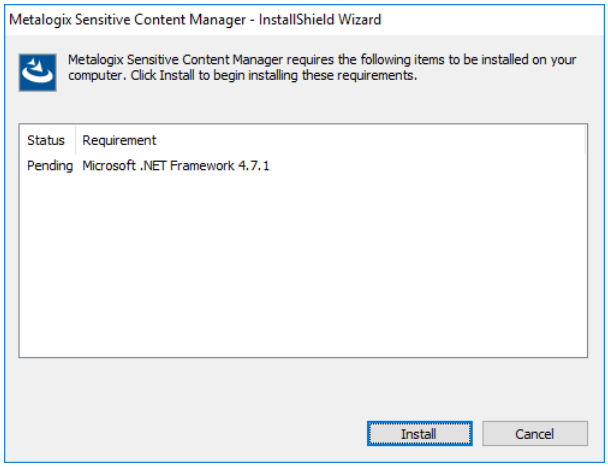
In this topic:

- Steps to install the SCM components on the SCM server
- Steps to grant read/write permissions to the temporary shared folder
- Steps to export the cluster certificate

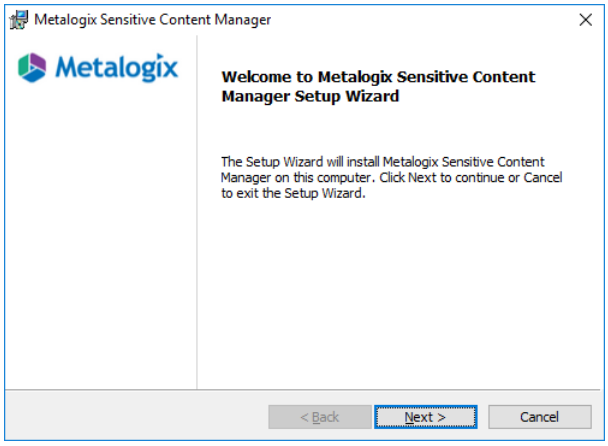
Steps to install the SCM components on the SCM server

The install steps described below assume that a SQL server machine that is designated to be configured as the SCM databases server (e.g., SCMDB) is available on the network and accessible by the domain user who will install the SCM Server.

1. Log in to the computer designated as the SCM Server. For example, log in to SCMSVR using the SCM Administrator credentials (mydomain\scmadmin).
2. Unzip the install media files to a suitable folder.
3. Click the windows installer file **Metalogix Sensitive Content Manager.exe**. The *SCM - Prerequisites* window opens. The prerequisites window will appear if the installer determines that one or more prerequisites are required.



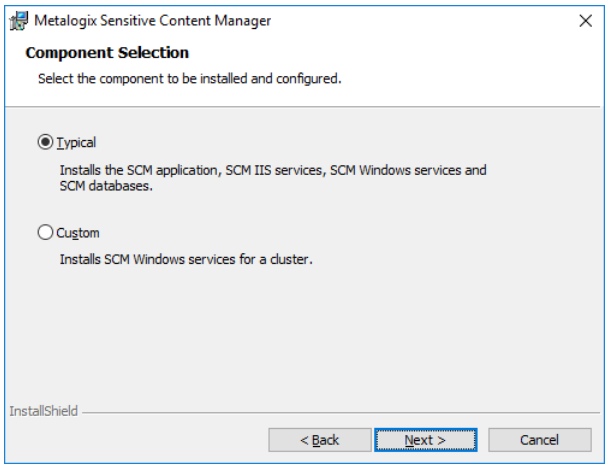
4. Click **Install**. When the prerequisites are installed, the *Welcome to Metalogix Sensitive Content Manager Setup Wizard* window opens. If the appropriate prerequisites are already installed, this is the first window that opens.



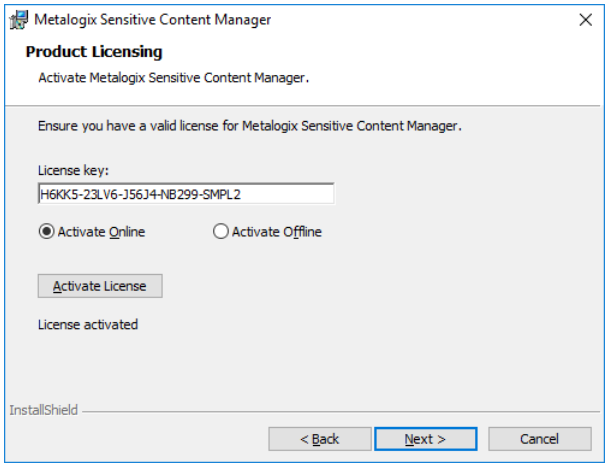
5. Click **Next**. The *License Agreement* window opens.

6. Click the check box **I accept the terms in the License Agreement** to activate the **Next** button. Click **Print** to print the License Agreement.

7. Click **Next**. The *Component Selection* window opens. Select **Typical** to install the components on the SCM Server.



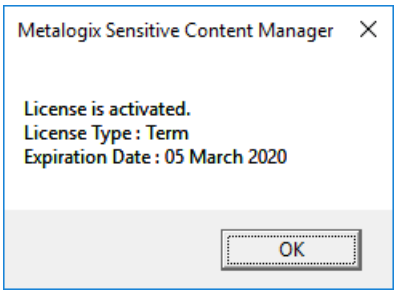
8. Click **Next**. The *Product Licensing* window opens. In the **License Key** field, enter your license key.



9. There are two options available to activate your license. The online activation steps are described here. See Steps to activate your license offline for more information.

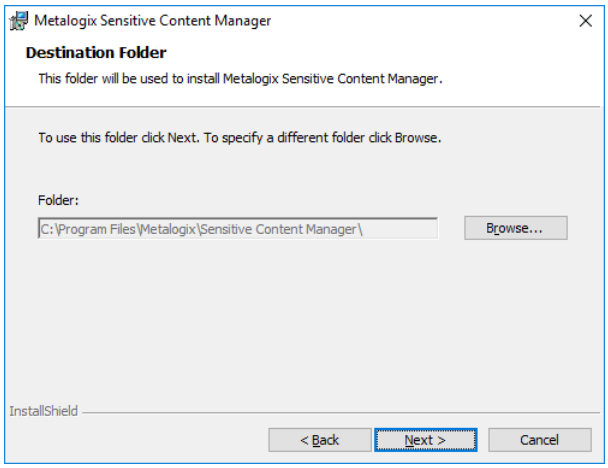
a. Select **Activate Online**.

b. Click **Activate License**. If the license activation is successful, a confirmation message opens.

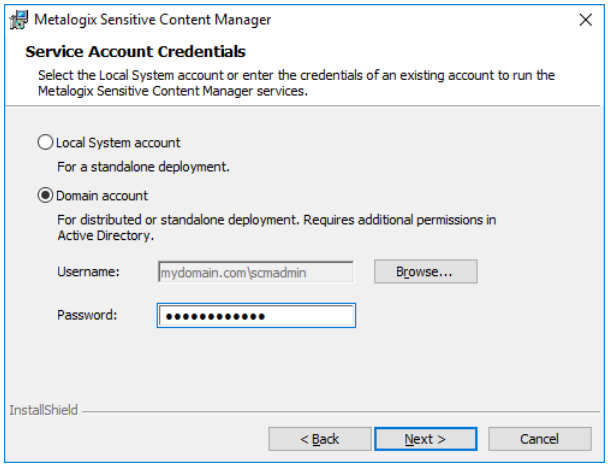


c. Click **OK**. The status *License not activated* on the *Product Licensing* window changes to *License activated*. Verify your license details as they will differ from the license details shown here.

10. Click **Next**. The *Destination Folder* window opens. Click **Browse** to change the destination folder. If you change the destination folder, ensure that the folder exists on this computer and there are no restrictions to reading or writing to the new folder.



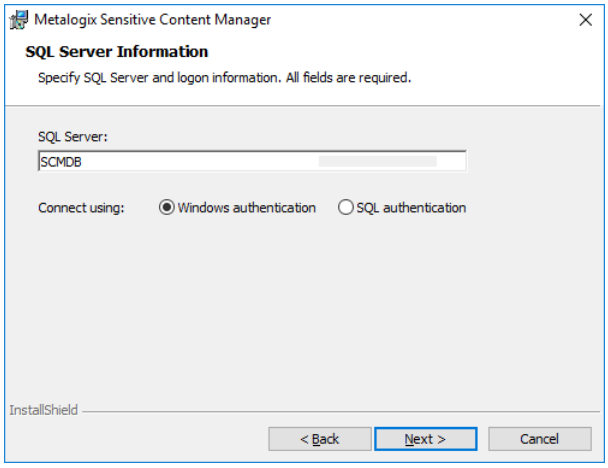
11. Click **Next**. The *Service Account Credentials* window opens.



12. Choose **Domain Account** and enter the credentials of the domain user.

NOTE: The domain user must have read/write permissions to the Service Connection Point in the active directory. For more information see Steps to grant additional privileges to the SCM Administrator.

13. Click **Next**. The *SQL Server Information* window opens.



Enter the values as described below

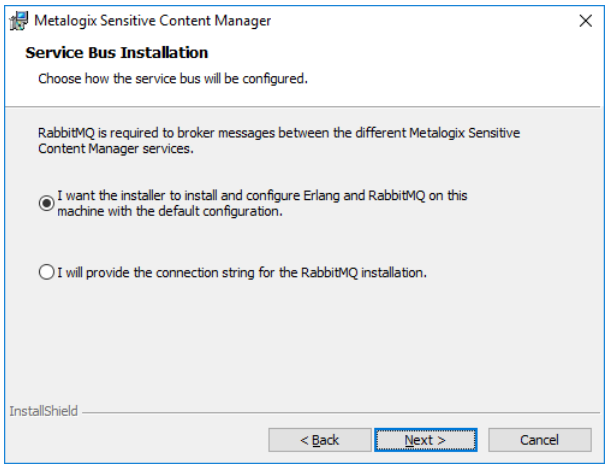
a. **SQL Server** - the name of the SQL Server instance where the SCM database will be installed.

b. Connection options:

   i. **Windows authentication** - SQL Server validates the account name and password using the Windows principal token in the operating system. The user must have log in rights to the SQL Server instance with *security admin* and *dbcreator* roles assigned. This is the recommended authentication option.

   ii. **SQL authentication** - uses the user credentials stored in SQL Server that may not be based on Windows user accounts. The user must have log in rights to the SQL Server instance with *security admin* and *dbcreator* roles assigned.

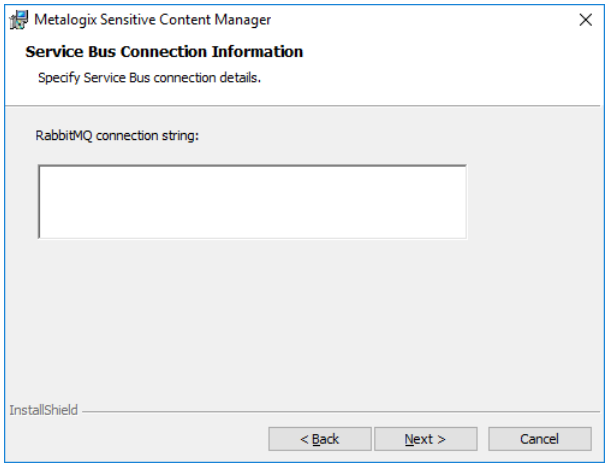
14. Click **Next**. The *Service Bus Installation* window opens. Metalogix SCM uses RabbitMQ as the service bus.



Choose from one of the following options:

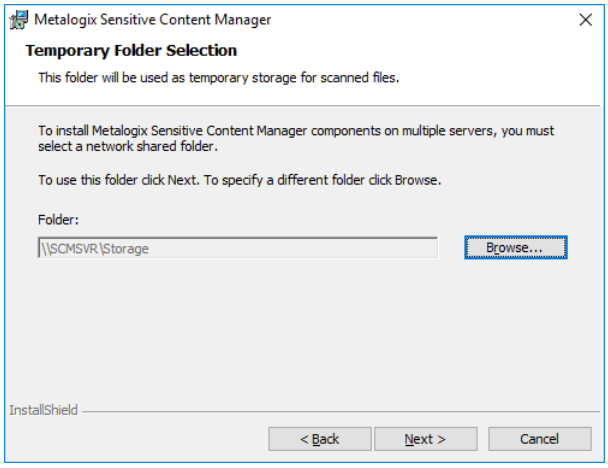
a. Select **I want the installer to install and configure Erlang and RabbitMQ on this machine with the default configuration** if you don't have an existing instance of the service bus. The installer will install the necessary files and dependencies at the end of the install process and create a certificate with the necessary credentials to operate RabbitMQ.

b. Select **I will provide the connection string for the RabbitMQ installation** if you already have a preinstalled instance that you have configured. When you click **Next** with this option selected, the *Service Bus Connection Information* window opens. Specify the RabbitMQ connection string.



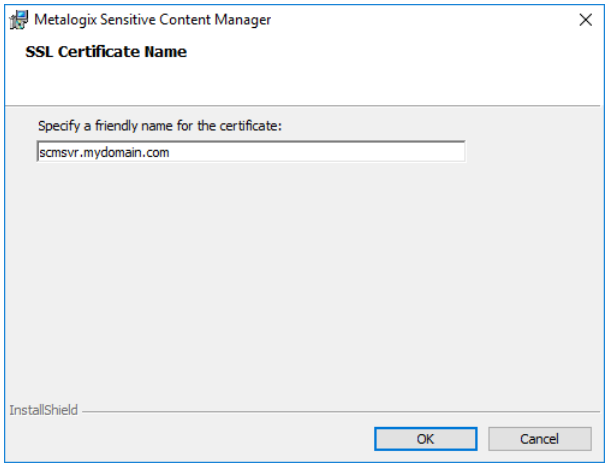
15. Click **Next**. The *Temporary Folder Selection* window opens. A default temporary storage folder is specified. Click **Browse** to change to a network shared folder which exists on this computer and there are no restriction to reading or writing to the new folder.

> **NOTE:** We recommend selecting a location on SSD or other fast access storage. The location will be heavily used, and fast access storage can significantly improve file analysis times.

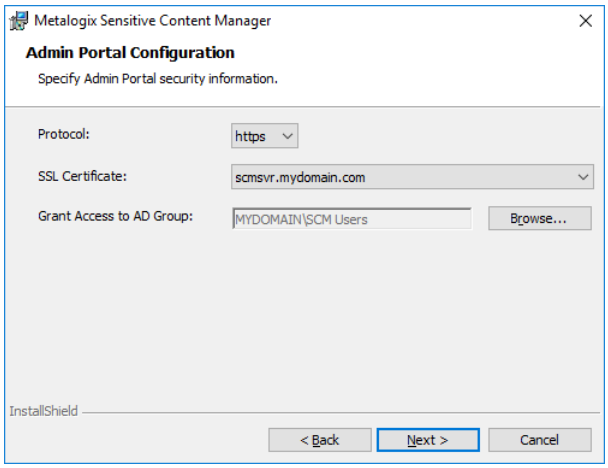


16. Click **Next**. The *IIS Web Site Information* window opens.

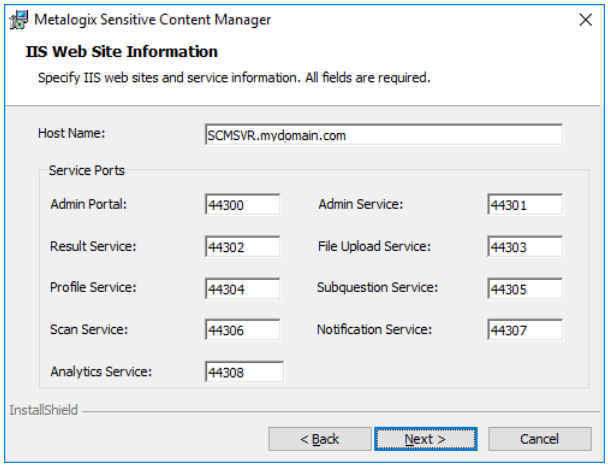
a. Click the drop-down box for the **SSL Certificate** field and select **<Create Self Signed Certificate>** option. The SSL Certificate Name window opens. Enter a friendly name and click **OK**. The *IIS Web Site Information* window reopens with the specified SSL Certificate name.



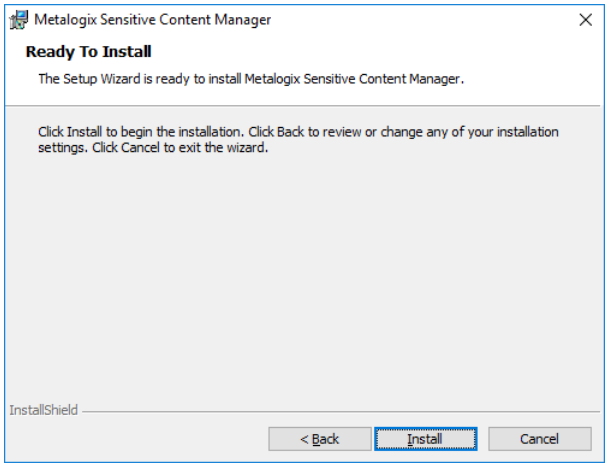
b. For the **Security Group**, click **Browse** to open the *Select Group* window. Enter **SCM Users** in the **Enter the object name to select** field and click **Check Names**. When the **Domain Users** group is verified, click **OK** to add the group.



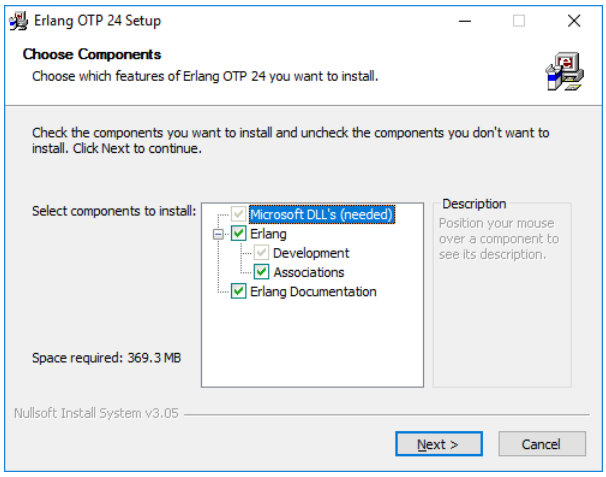
17. Click **Next**. The *IIS Web Site Information* window reopens with default port specifications for each IIS service. If you choose to change the default port numbers, ensure that the port numbers are within the range 1 to 65535 and they are unique and available for use.



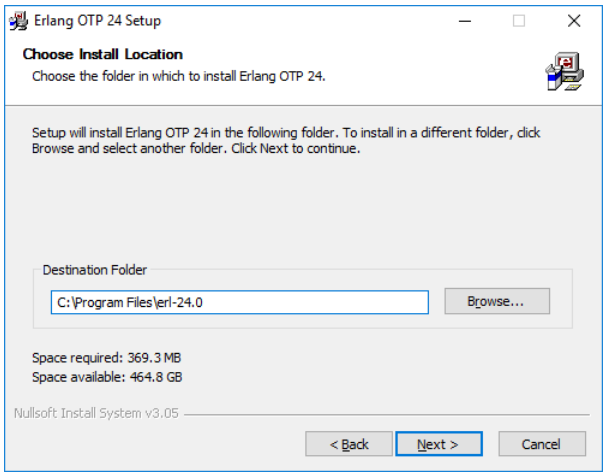
18. Click **Next**. The *Ready To Install* window opens.



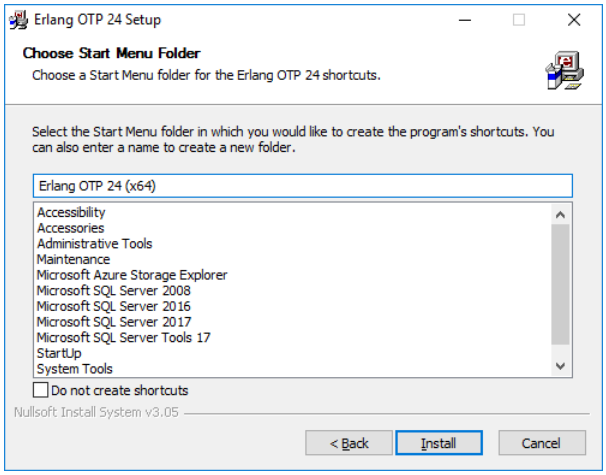
19. Click **Install**. The Erlang third-party component installer starts. You must allow additional Microsoft redistributable components to be installed if requested by the installer.



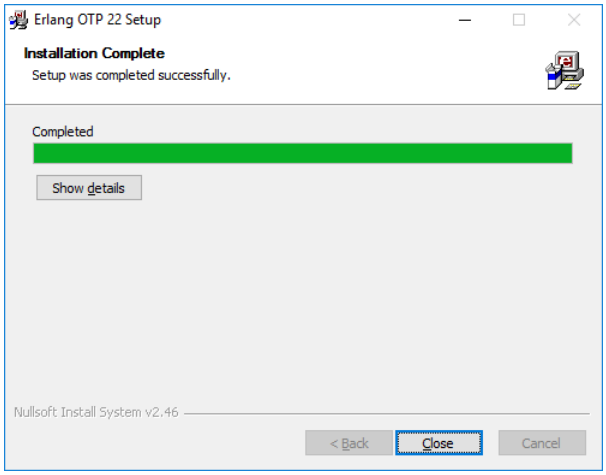
20. Keep the defaults as indicated and click **Next**. The *Choose Install Location* window opens. Click **Browse** to change the location if necessary.



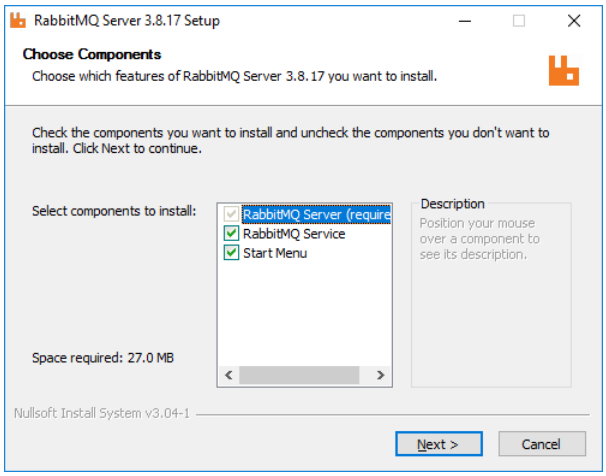
21. Click **Next**. The *Choose Start Menu Folder* window opens. Keep the defaults as indicated and select **Do not create shortcuts** to avoid shortcut creation. You must allow additional Microsoft redistributable components to be installed if requested by the installer.



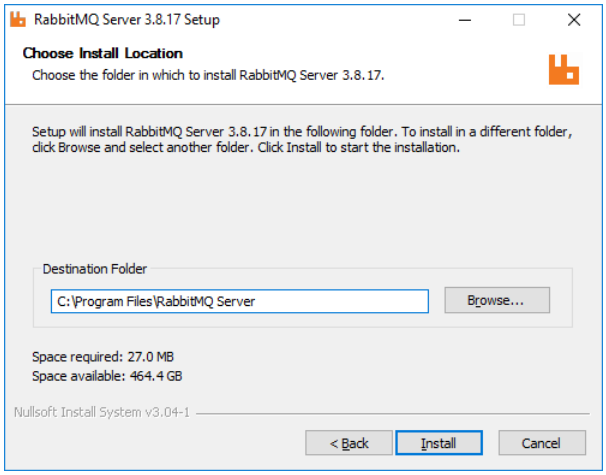
22. Click **Next**. The *Installation Complete* window opens when the installation is successful.



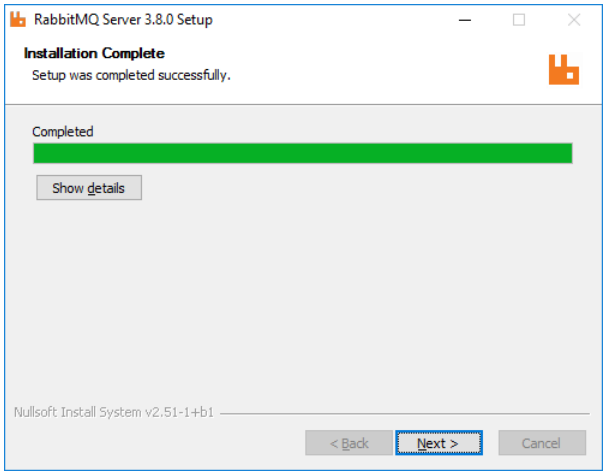
23. Click **Close**. The RabbitMQ installer starts.



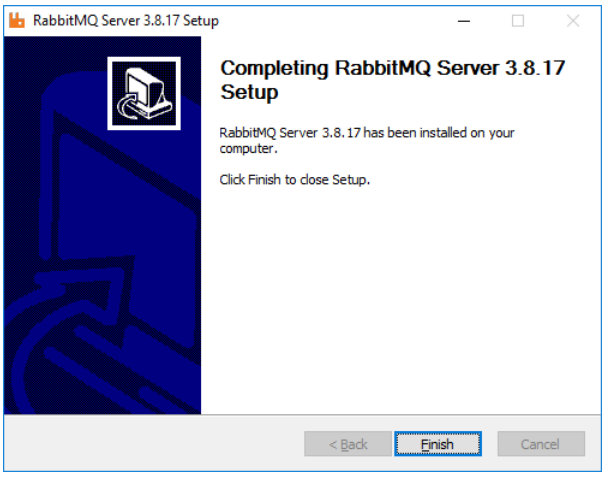
24. Keep the defaults as indicated click **Next**. The *Choose Install Location* window opens. Click **Browse** to change the location if necessary.



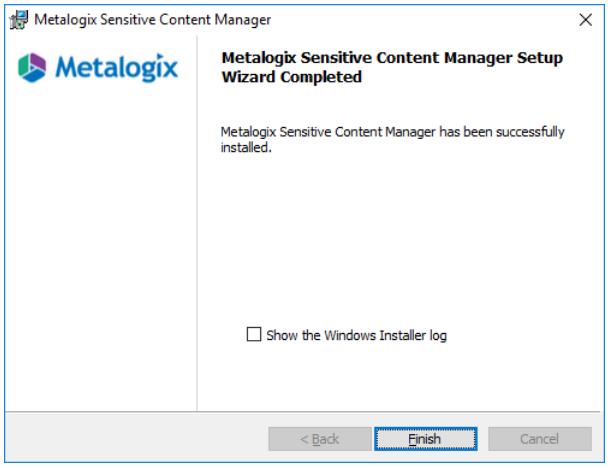
25. Click **Next**. The *Installation Complete* window opens when the installation is successful. Click Show details to inspect the RabbitMQ installation locations.



26. Click **Next**. The confirmation window opens.



27. Click **Install**. The rest of the SCM components and any prerequisites will be installed. If the installation is successful, the *SCM Setup Wizard Completed* window opens.



28. You can select the check box **Show the Windows Installer log** which opens the installation log file for reviewing or troubleshooting the installation. Click **Finish** to exit the wizard.

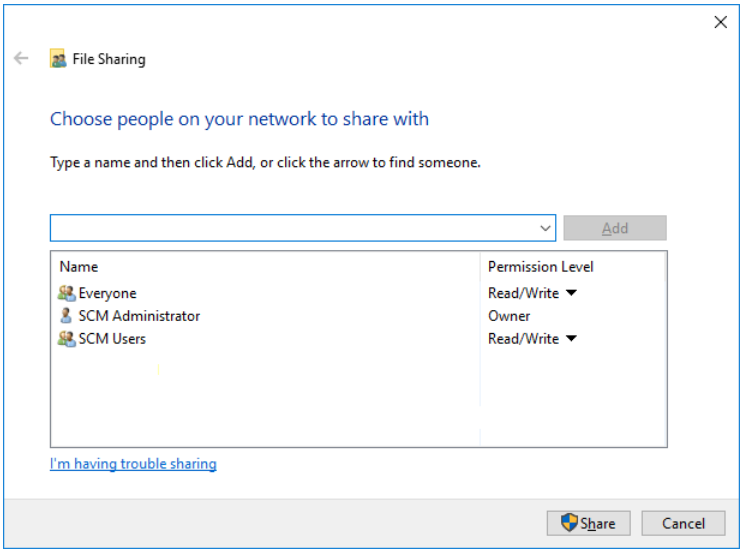
29. A shortcut is added to the desktop.

Steps to grant read/write permissions to the temporary shared folder

Read/Write permission is granted to the SCM Windows service account so that files that are submitted for analysis to the shared folder can be accessed and disposed by the SCM Windows service on the same server or from dedicated servers.

> **NOTE:** If the account used to run the SCM Windows service is the same as the account used to install the SCM Server, then the account is automatically added to the folder with the **Owner** permission level when the folder is created. the permission level does not need to be changed.

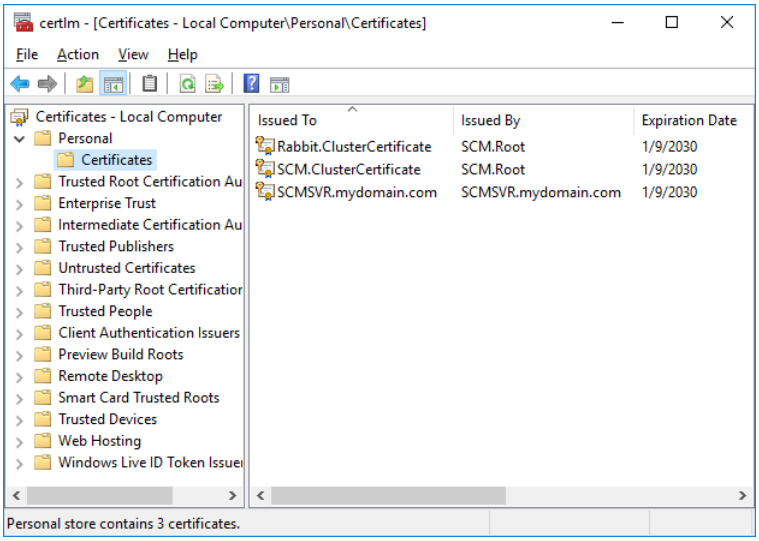
1. Log in to the SCM Server (SCMSVR).
2. Locate the shared folder. For example, C:\Storage.
3. Right-click on the folder and select **Properties**. The *SCM Temporary Storage Properties* window opens.
4. Click the **Sharing** tab.
5. Click **Share**. The *File Sharing* window opens.
6. Enter the user name that will be used to run the SCM Windows service. Click **Add**.
7. Change the *Permission Level* of the added user to **Read/Write**.



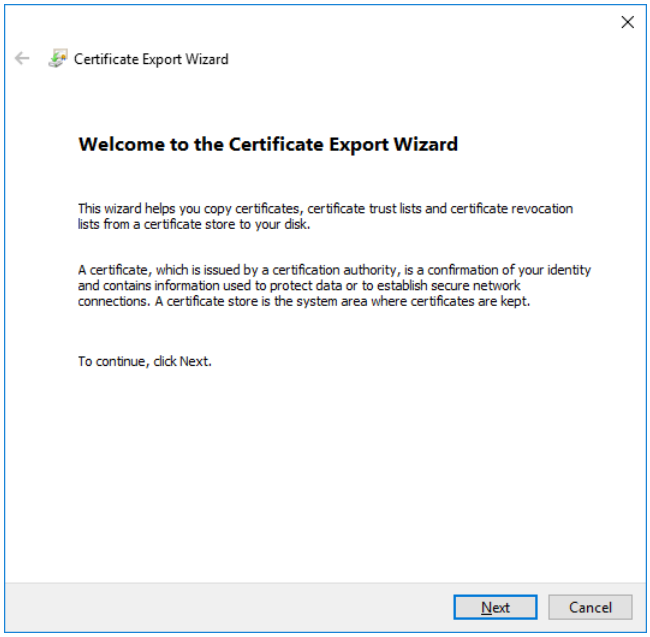
8. Click **Share**.
9. Click **Done** to close the *File Sharing* window.
10. Click **OK** to close the *SCM Temporary Storage Properties* window.

Steps to export the cluster certificate

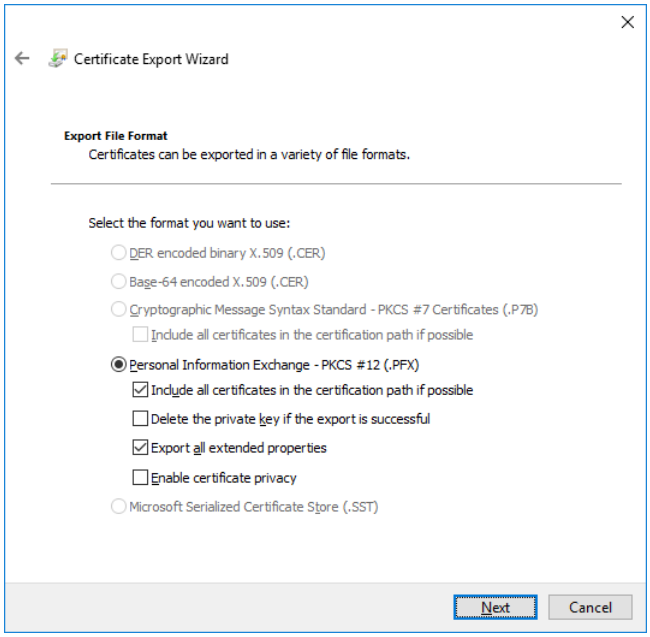
1. In the SCM Server, right-click **Start** > **Run**. Enter **certlm.msc** and click **OK**.
2. If the *User Account Control* window opens, click **Yes**. Then the *Certificate Manager* window opens.
3. From the *Certificates* hierarchy, expand the **Personal** node and click **Certificates**.
4. From the list of certificates that are displayed in the right-hand pane, right-click **SCM.ClusterCertificate**.



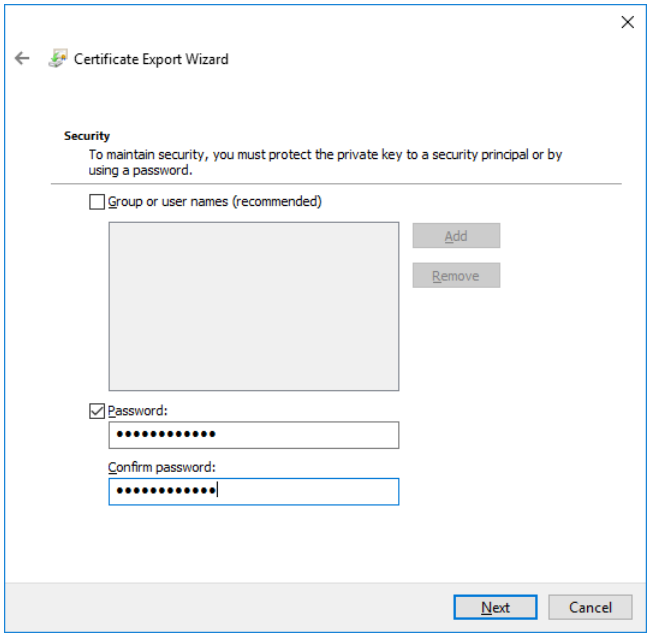
5. From the context-menu that appears, select **All Tasks** > **Export**. The *Certificate Export Wizard* starts.



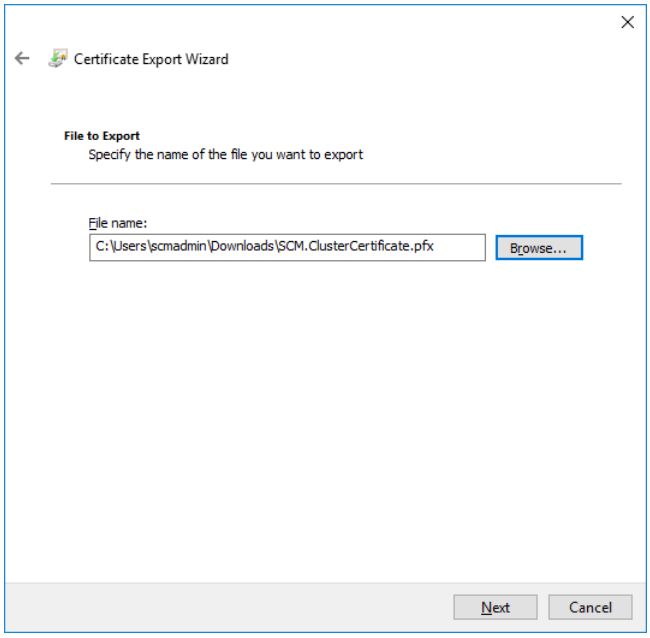
6. Click **Next**. Select **Yes, export the private key**.
7. Click **Next**. Verify the settings on the *Export File Format* step as shown.



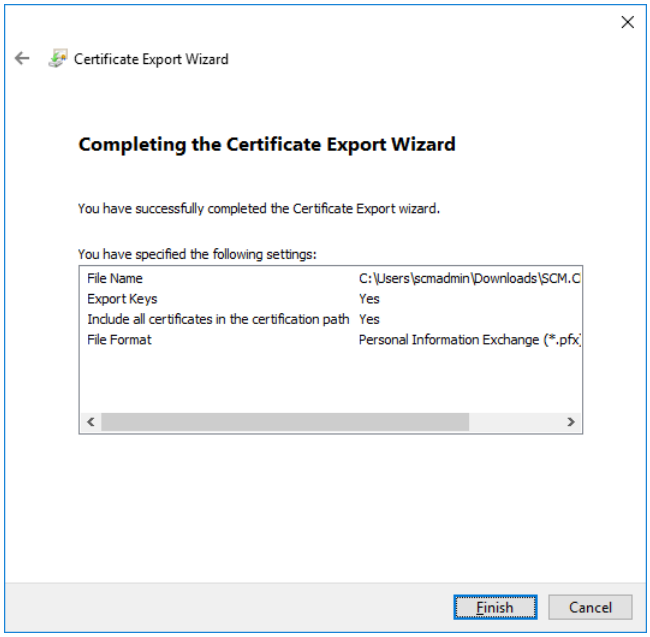
8. Click **Next**. Select **Password** and then enter a password and confirm the password. Remember this password for future use.



9. Click **Next**. Click **Browse** and select a local folder on the SCM Server where the certificate file will be exported.



10. Click **Next**. Verify the settings and click **Finish** to export the certificate. Click **OK** in the confirmation dialog and close the *Certificate Manager* window.



IMPORTANT: Copy this certificate to a local folder on each server that will host a dedicated service so that the service can identify and join the same cluster during installation of the service.

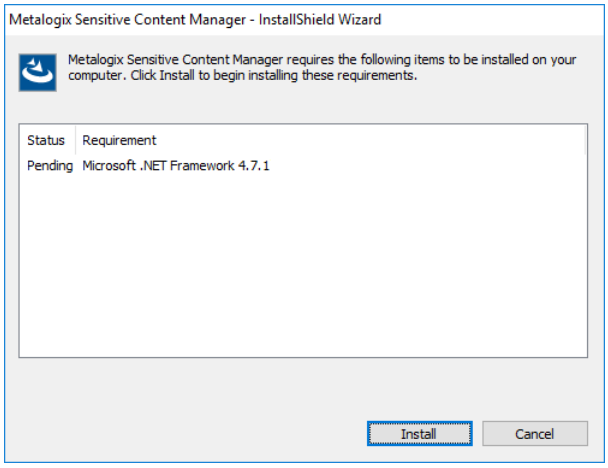
Steps to install a dedicated SCM Service server

Before you start installing the SCM Windows services on a dedicated server verify the following prerequisites:

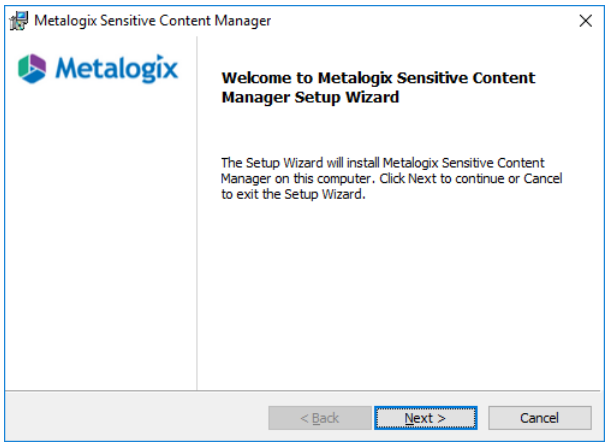
- The cluster certificate has been copied to the dedicated server. The installer will help you install the certificate.
- The temporary folder on the SCM Server has been shared and the SCM Windows service account that will be used to run the SCM services on this server has been granted read/write permission to the shared folder.
- The SCM Windows service account is a member of the local Administrators group.

Steps to install the SCM Windows services

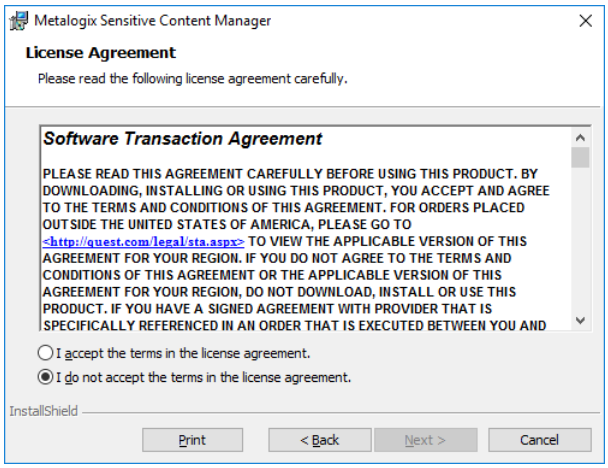
1. Log in to the SCM service server using the credentials of the SCM Windows service account. For example, log in to SCMSVC-1 using mydomain\scmadmin.
2. Download and unzip the install media files to a suitable folder.
3. Click the windows installer file **Metalogix Sensitive Content Manager.exe**. The *SCM - Prerequisites* window opens. The prerequisites window will appear if the installer determines that one or more prerequisites are required.



4. Click **Install**. When the prerequisites are installed, the *Welcome to SCM Setup Wizard* window opens. If the appropriate prerequisites are already installed, this is the first window that opens.

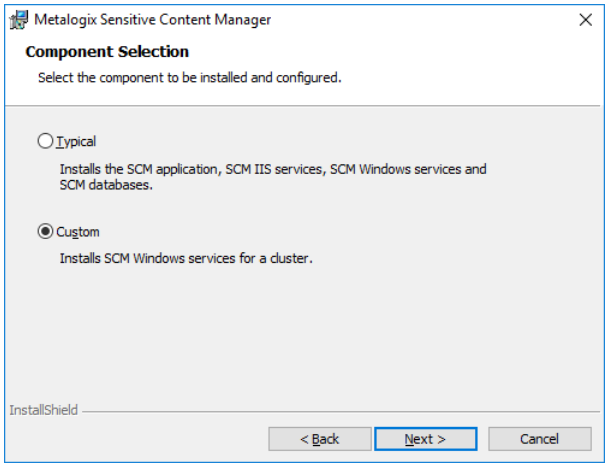


5. Click **Next**. The *License Agreement* window opens.

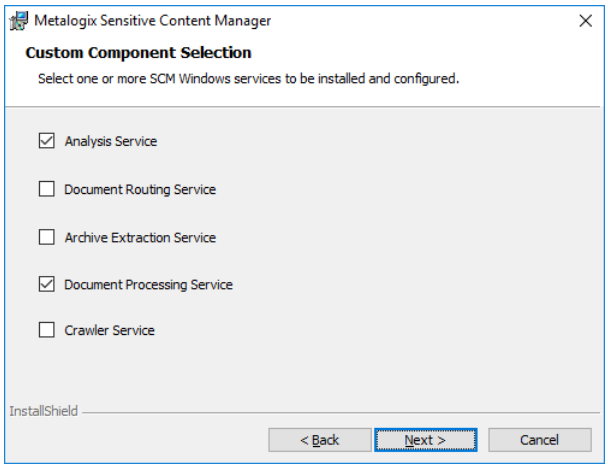


6. Click the check box **I accept the terms in the License Agreement** to activate the **Next** button. Click **Print** to print the License Agreement.

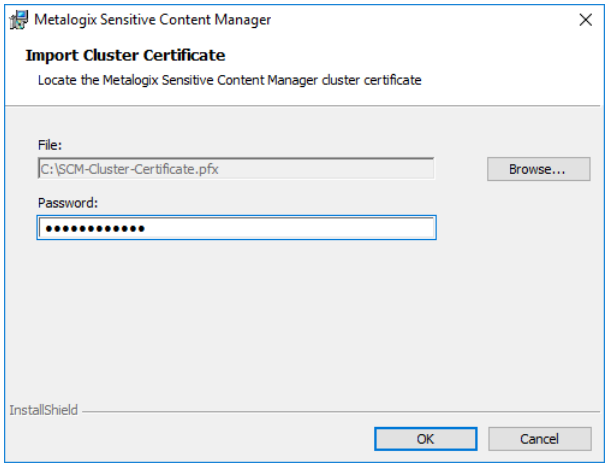
7. Click **Next**. The *SCM Components Selection* window opens. Select **Custom**.



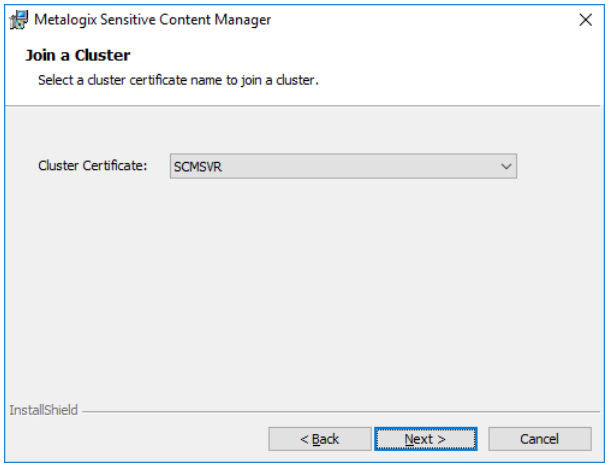
8. Click **Next**. The *Custom Component Selection* window opens. Select **Analysis Service** and **Document Processing Service**. These are typical high-load services, but you can choose more services if required.



9. Click **Next**. The *Import Cluster Certificate* window opens. Click **Browse** and locate the cluster certificate that was copied from the primary SCM Server. Then enter the password associated with the certificate.

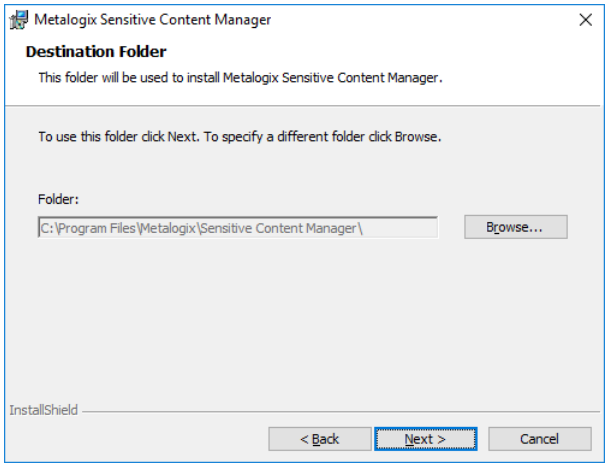


10. Click **OK**. The J*oin a Cluster* window opens.

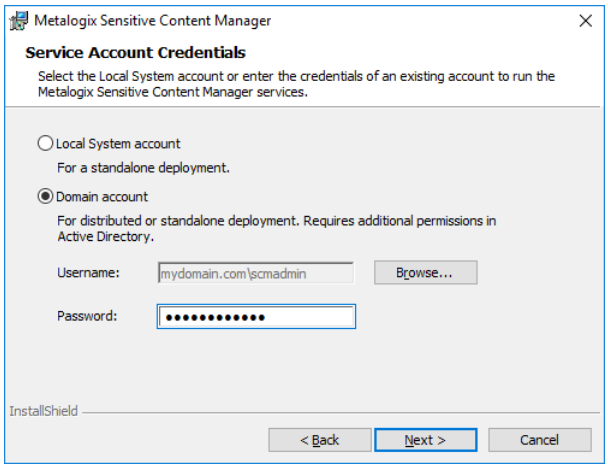


Verify the cluster name displayed. The cluster bears the name of the SCM server. If the name is incorrect, click drop-down and re-import the correct cluster certificate. The SCM Windows services will be linked to this cluster. There could be multiple deployments of SCM clusters in the same domain for development, user-acceptance testing or others. Ensure that the SCM cluster you select is a part of your installation.

11. Click **Next**. The *Destination Folder* window opens. Click **Browse** to change the destination folder if necessary. If you change the destination folder, ensure that the folder exists on this computer and there are no restrictions to reading or writing to the new folder.

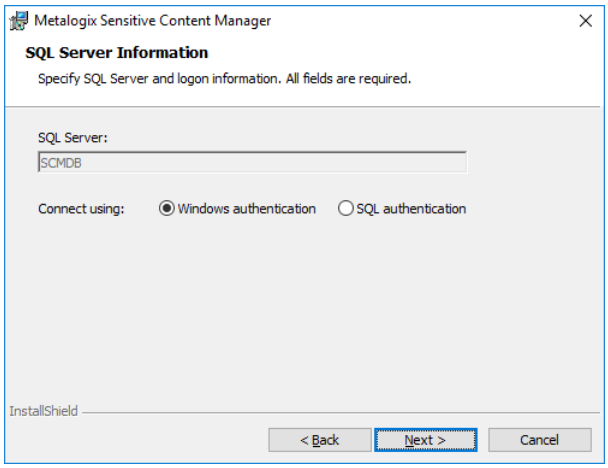


12. Click **Next**. The *Service Account Credentials* window opens.

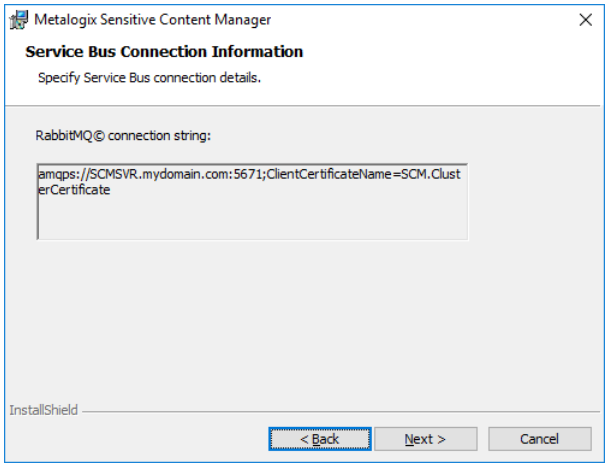


Choose **Domain account** and enter the valid credentials of the SCM Service user that will be used to run the windows service.

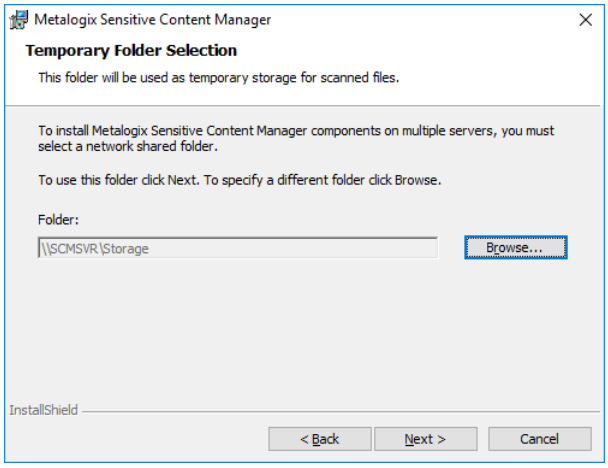
13. Click **Next**. The *SQL Server Information* page opens. Verify that the SQL Server information is correct.



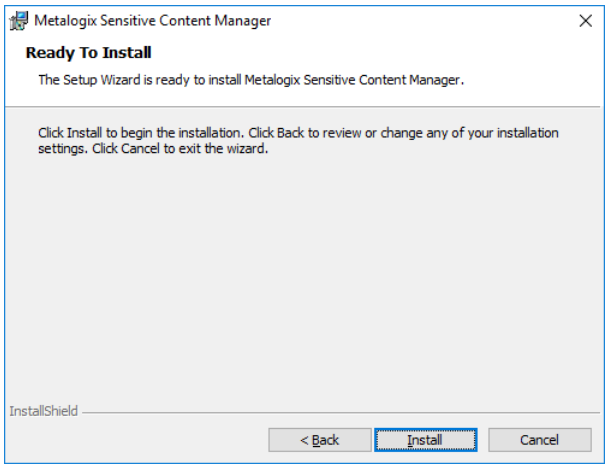
14. Click **Next**. The Service Bus Connection Information window opens. Verify that the connection string indicates the appropriate cluster certificate.



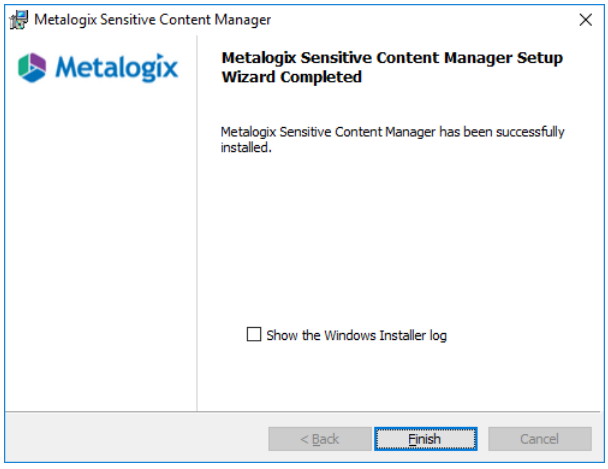
15. Click **Next**. The *Temporary Folder Selection* window opens. You must change the default folder to use a shared folder. Click **Browse** and locate a suitable shared folder with *Read/Write* permissions. For example, \\SCMSVR\Storage. Ensure that the folder is shared with SCM Service users in the same cluster but is *not shared* with other users in other SCM clusters.



16. Click **Next**. The *Ready To Install* window opens.



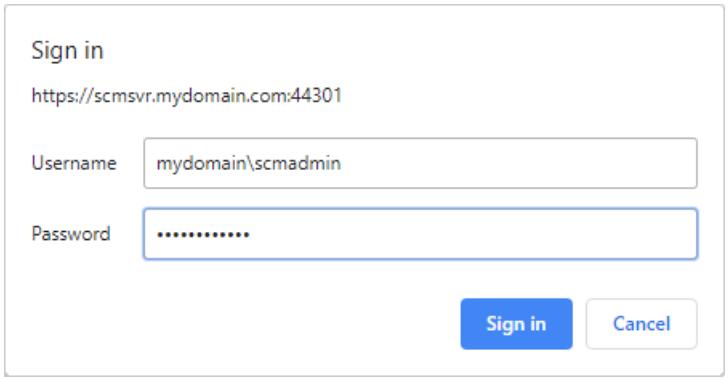
17. Click **Install**. If the installation is successful, the *SCM Setup Wizard Completed* window opens.



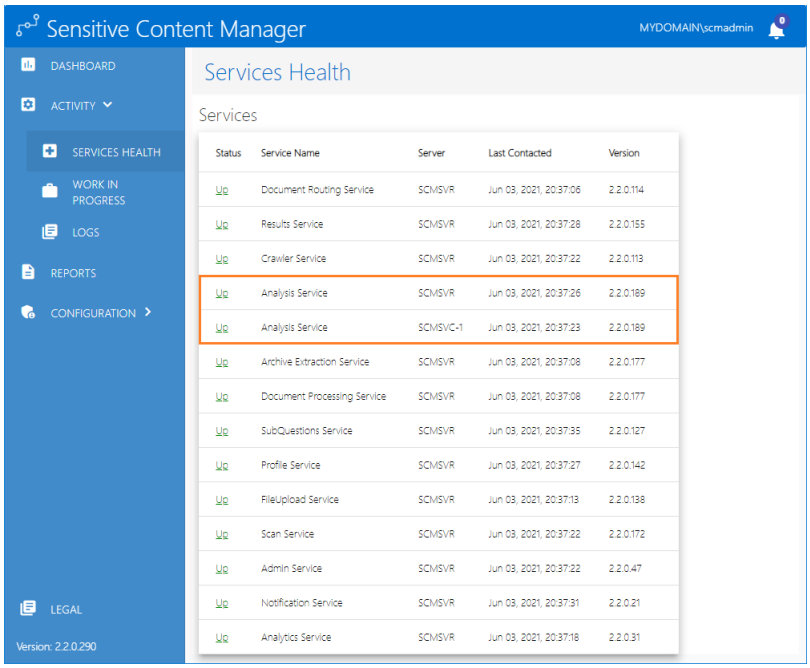
18. Click **Finish** to exit the wizard.

Steps to verify the distributed installation

1. Log in to the SCM Server (e.g., SCMSVR)
2. Double-click the desktop shortcut to open the SCM Administration Center. You can also enter the URL directly in a browser. To get the URL for your own installation see Steps to get the URL for the SCM Administration Center.
3. In the *Sign in* dialog that opens, enter the credentials of the SCM Administrator.



4. Click **Sign In**. The *Dashboard* page opens.
5. From the navigation pane, expand **Activity** and then click **Services Health**.
   a. Verify that the software version at the bottom of the navigation pane is the expected upgrade version.
   b. Verify that all services indicate Status = Up.
   c. Verify that each service version on the dedicated servers matches the same service version on the SCM Server.



6. This completes the verification of the distributed SCM deployment.

TIP: By default, RabbitMQ installs the configuration and data files in **%APPDATA%\RabbitMQ**. Metalogix Sensitive Content Manager configures RabbitMQ to work with at least two times the amount of available memory in the operating system. If Metalogix Sensitive Content Manager and RabbitMQ are both installed on the same server, memory constraints may cause unpredictable behavior. To address this issue, you can move the Rabbit configuration and data files to a secondary drive. For detailed steps see Relocating the RabbitMQ installation directory.

7

License Management

The *License Information* page of the SCM Administration Center allows you to register your product and view your license details. When you download and install a trial version of SCM Server you get a free 30-day trial license. For more information about getting a trial version, see Steps to download the install media. If you would like to purchase a license, contact Quest to get your license key and follow the instructions presented here.

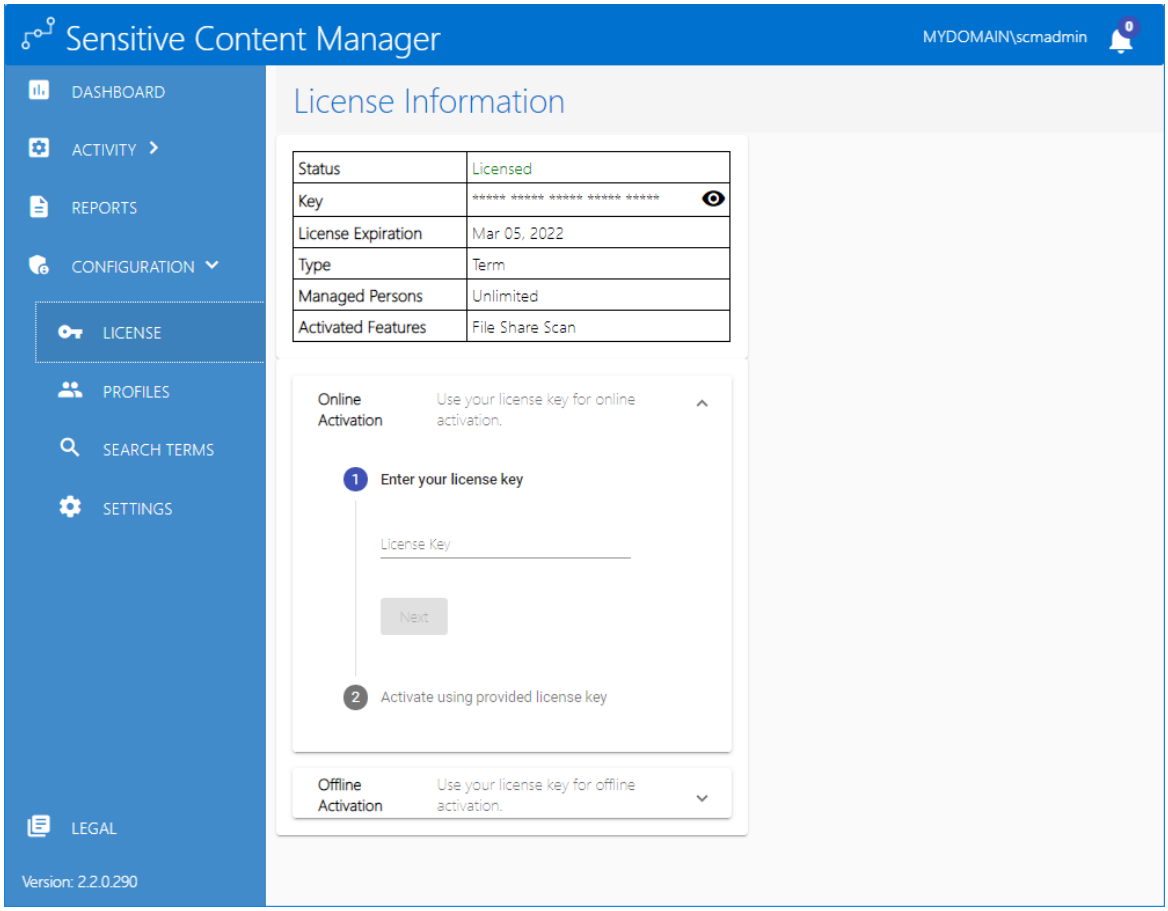
NOTE: You must reactivate your license after an upgrade to ensure new license-linked features are synchronized with your license.

In this topic

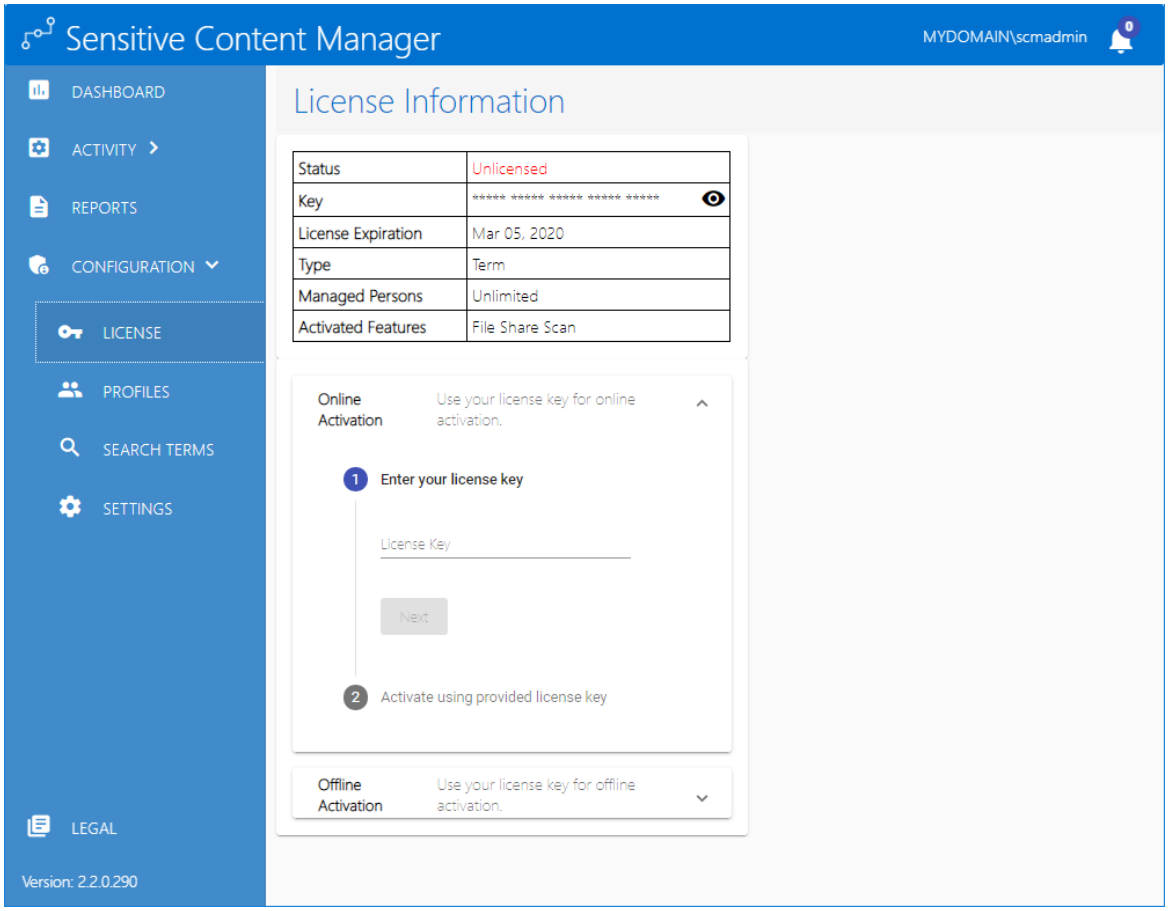
- Steps to view the license information
- About the trial License
- Steps to activate your license online from the SCM Administration Center
- Steps to activate your license offline from the SCM Administration Center
- Steps to activate your license offline from the SCM Wizard

Steps to view the license information

1. From the navigation panel on the left, expand **Configuration** and then click **License**. The *License Information* page opens.



2. If the license has expired, the *License Information* page will indicate the details of the expired license.



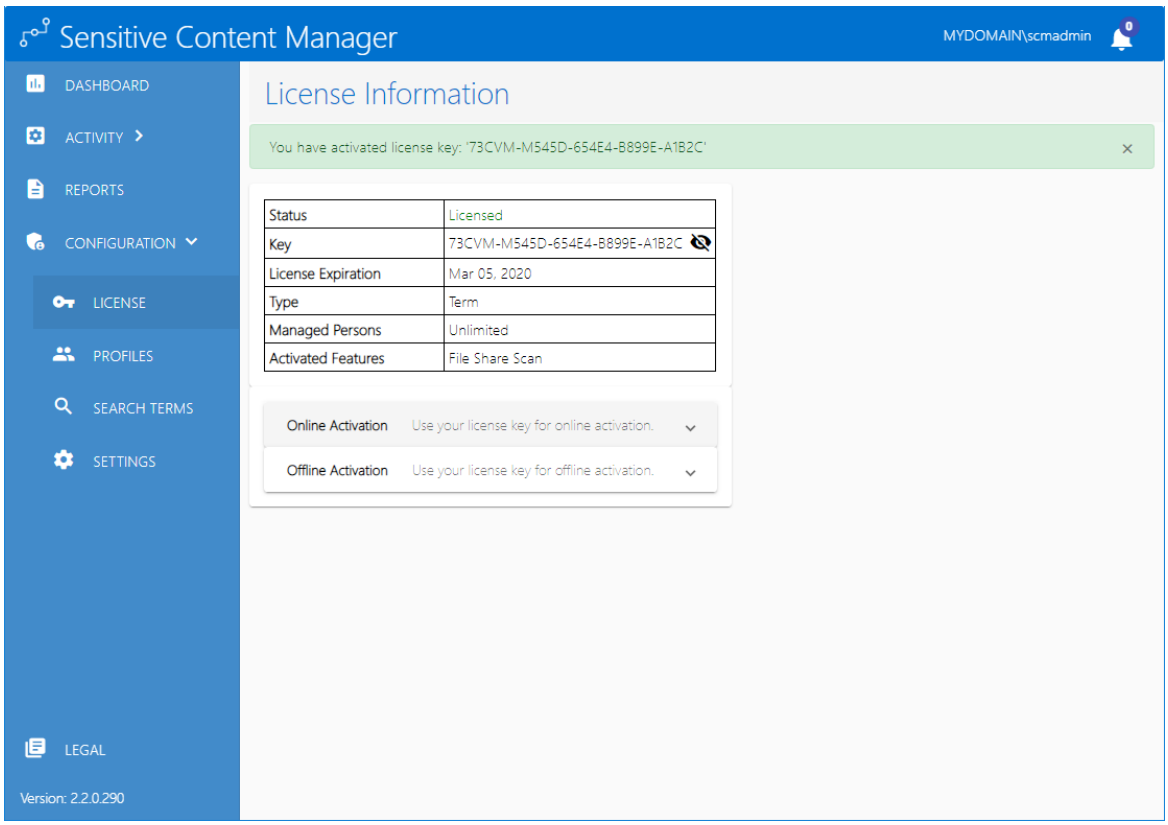
3. Contact your Quest sales representative to renew your license.

About the trial License

- When you register and download a trial version of the SCM, the trial license key is specified in the email that is sent to you.
- When you activate the trial license, the *License Information* page opens.
- The **Type** field indicates *Trial*.
- It is valid for 30 days (date of license issue + 29 days) and you can try all the features that are available.
- The Analysis service and the File Upload service will stop functioning after 30 days.

Steps to activate your license from the SCM Administration Center

1. Log in in to the SCM Administration Center.
2. From the navigation panel expand **Configuration** and then click **License**. The *License Information* page opens.
3. Enter your license key in the **License Key** field.
4. Click **Next**. The **Activate using provided license key** step is activated**.**
5. Click **Activate Online**. If the **License Key** is valid, the confirmation message appears and the **Status** changes to **Licensed**.



6. Click **Finish**. Refresh the page to update the license status and access the licensed features.

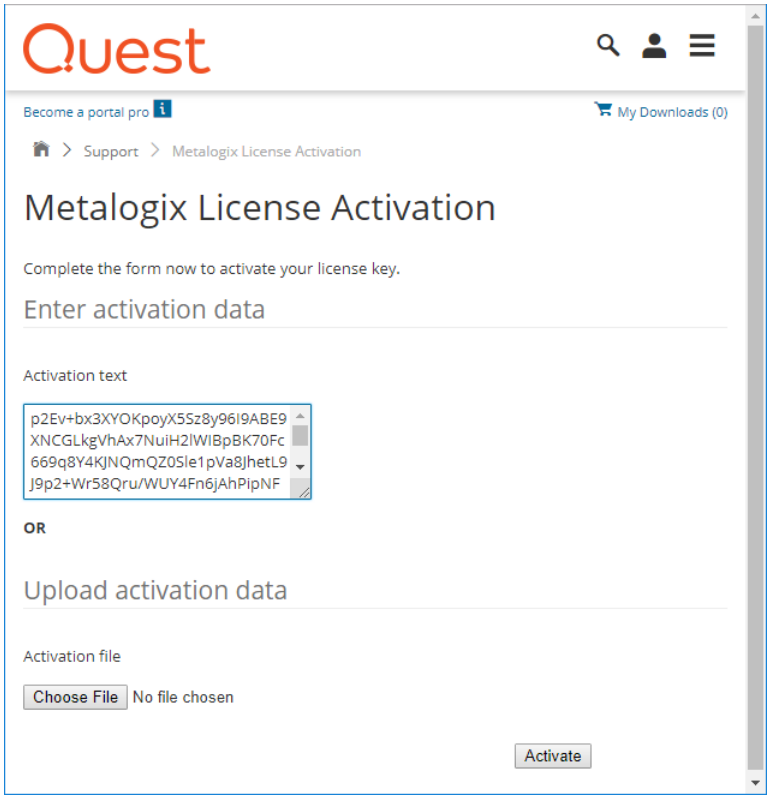
Steps to activate your license offline from the SCM Administration Center

This option lets you activate your license from another computer with a working internet connection.

1. Log in to the SCM Administration Center and click **License** from the navigation panel. The License Information page opens.
2. Expand the **Offline Activation** section.
3. **Step 1: Enter your license key**
   a. In the **License Key** field, enter your license key and click **Next**.
4. **Step 2: Get Activation Data**
   a. Click **Get Activation Data**.
   b. When the data is available, the next step is activated.
5. **Step 3: Copy/Save activation data**
   a. Select from the two options described below:

   Option 1: Click **Save Activation Data to Clipboard**. The activation data is saved to memory. Use this option if you plan to follow through with the subsequent steps immediately.

   Option 2: Click **Save Activation Data to File**. The Windows File dialog opens. Use this option if you plan to activate the license from a different computer. Specify a file name for the activation data file and click **Save** to save the file to a location of your choice.
6. **Step 4: Submit Activation Data**
   a. Using your alternate internet connection navigate to https://support.quest.com/offline-activation.
   b. In the previous step, if you opted to click **Save Activation Data to Clipboard**, place your cursor in the **Activation text** field and click **Ctrl-V** to paste the activation data.
   c. In the previous step, if you opted to click **Save Activation Data to File**, click **Choose File** and locate the saved activation data file.

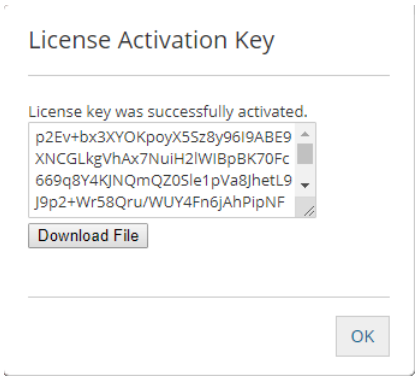


d. Click **Activate**. The *License Activation Key* dialog opens.

e. Copy the encrypted activation key to memory by selecting the activation key and using Ctrl-C

or

Click **Download File** which will download the **LicenseActivationResponse.dat** file to your computer. If you downloaded the file to a location that is on another computer, make sure you copy the file to the computer where you are installing the SCM software.



f. Return to the *License Information* page in the SCM Administration Center.

7. **Step 5: Apply Activation Response**

a. Click **Ctrl + V** to paste the activation response if you copied the activation response to clipboard.

or

b. Click **Choose File**. The Windows file dialog opens.

c. Locate the activation key file that you saved if you followed step 6b and click **Open**. The file name opens next to the **Choose File** button.

d. Click **Complete Activation** to complete the activation process.

8. **Step 6: Activation Complete**

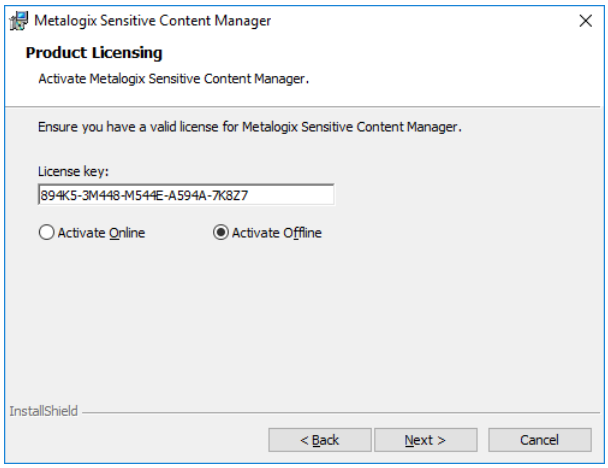
a. Click Finished to acknowledge the license activation.

b. Log out and log in again to access all the licensed features.

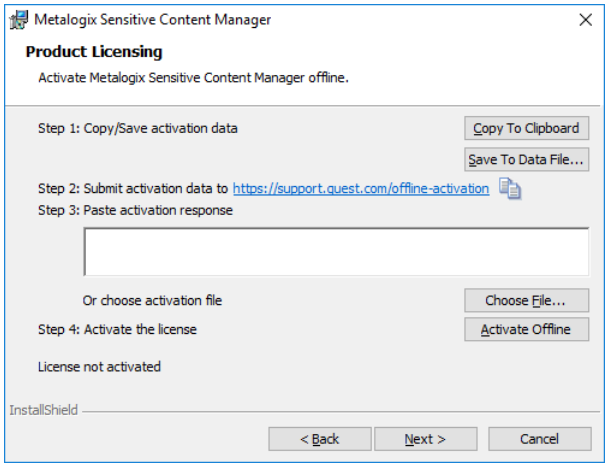
Steps to activate your license offline

This option lets you use an alternate internet connection to access the required activation data from the Quest offline activation web site.

1. Select **Activate Offline**.



2. Click **Next**. The *Product Licensing* window for offline activation opens.



3. **Step 1: Copy/Save activation data**

a. Select from the two options described below:

Option 1: Click **Copy To Clipboard**. The activation data is saved to memory. Use this option if you plan to follow through with the subsequent steps immediately.

Option 2: Click **Save To Data File...** The Windows File dialog opens. Use this option if you plan to activate the license later.

b. Specify a file name for the activation data file.

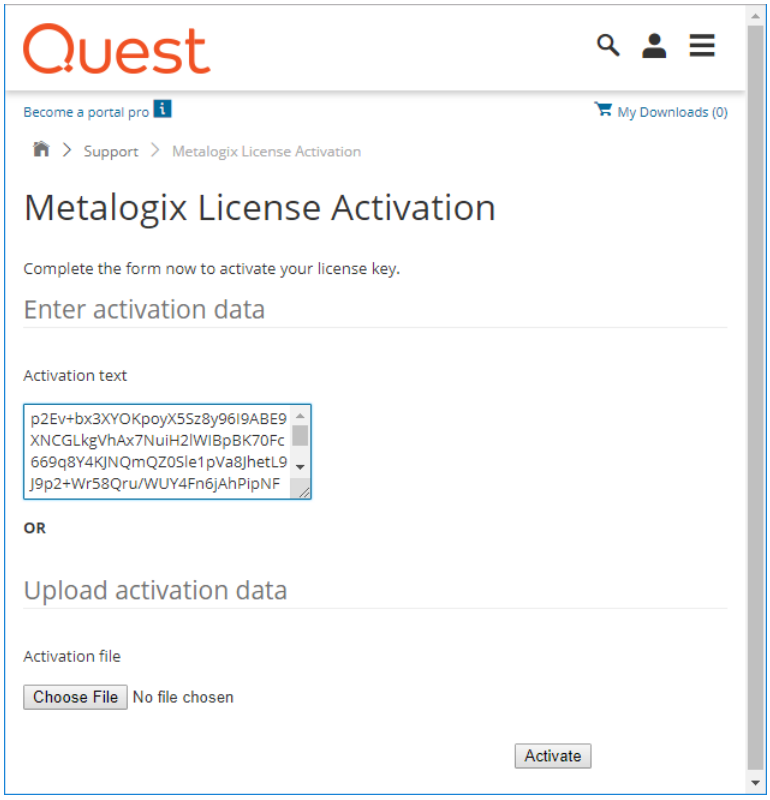
c. Click Save to save the file to a location of your choice.

4. **Step 2: Submit activation data**

a. Using your alternate internet connection navigate to https://support.quest.com/offline-activation.

b. If you opted to click **Copy to Clipboard**, place your cursor in the **Activation text** field and click **Ctrl-V** to paste the activation data.

c. If you opted to click **Save to Data File**, click **Choose File** and locate the saved activation data file.

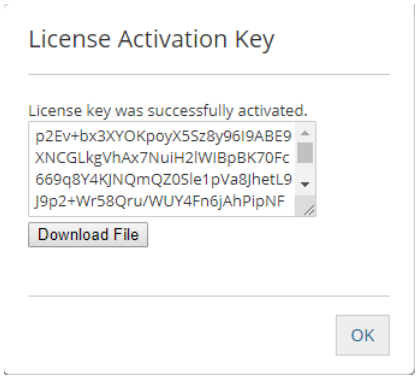


d. Click **Activate**. The *License Activation Key* dialog opens.

e. Copy the encrypted activation key to memory by selecting the activation key and using Ctrl-C

or

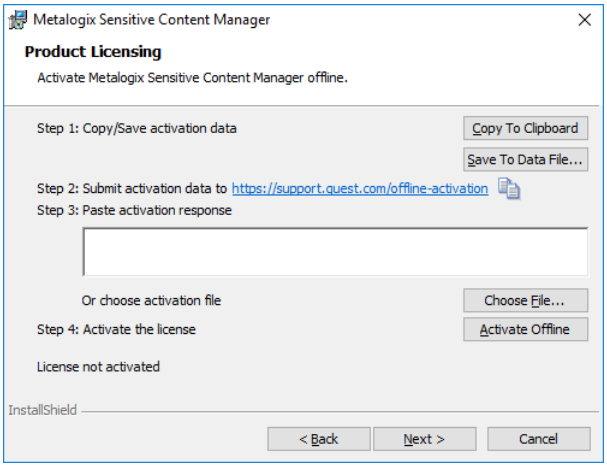
Click **Download File** which will download the **LicenseActivationResponse.dat** file to your computer. If you downloaded the file to a location that is on another computer, make sure you copy the file to the computer where you are installing the SCM software.



f. Click **OK**. The *Product Licensing* window for offline activation reopens.

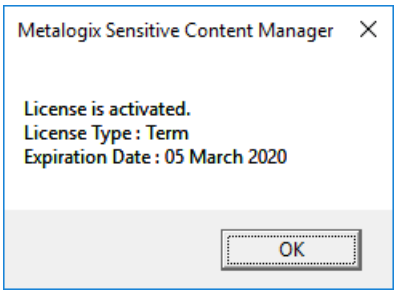
5. **Step 3: Paste Activation Response**

a. Paste the copied activation key in the activation response text field or click **Choose File** to locate and select the **LicenseActivationResponse.dat** file.



6. **Step 4: Activate the license**

a. Click **Activate Offline**. If the license activation is successful, a confirmation message opens.



b. Click **OK**. The status *License not activated* on the Product Licensing window will change to *License activated*. The license details may not be the same as shown here.

8

Maintenance

Maintaining your deployment ensures compatibility with integrated applications like Metalogix ControlPoint and business continuity.

In this topic:

- Upgrading SCM components
- Repairing SCM components
- Removing SCM components

Upgrading SCM components

IMPORTANT: This release of SCM is not compatible with versions prior to 2.0. You must uninstall all SCM components and any distributed SCM Windows services before you install this version of SCM. See Steps to manually uninstall all SCM components for more information.

NOTE: You must re-activate your license after an upgrade to ensure new license-linked features are synchronized with your license.

In this topic:

- Preparing for the upgrade
- Upgrading SCM components
- Verifying your upgrade

Preparing for the upgrade

The **ScanDetail** table in the **SCMScanService** database can accumulate a large volume of data over time, which impacts report generation, and must be indexed. To check for the number of records in the table, run the following script in your SCM database:

```
select count(*) from SCMScanService.dbo.ScanDetail;
```

If this table contains less than 100,000 records, no further action is necessary and you can proceed with the upgrade. If this table contains more than 100,000 rows of data, you must prepare your

SCM server to allow the installer to index the **ScanDetail** table. Two separate configuration settings are required as described below:

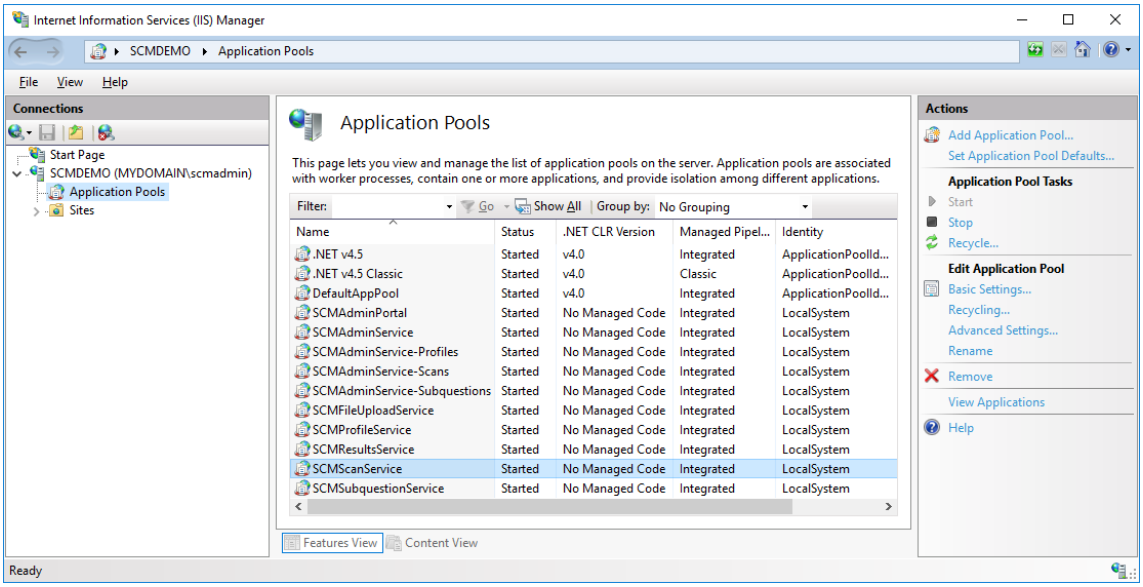
Set the timeout in the appsettings.json file

1. Open the `C:\Program Files\Metalogix\Sensitive Content Manager\Scans\appsettings.json` file with a text editor.
2. Add the timeout setting as indicated below and save the changes.

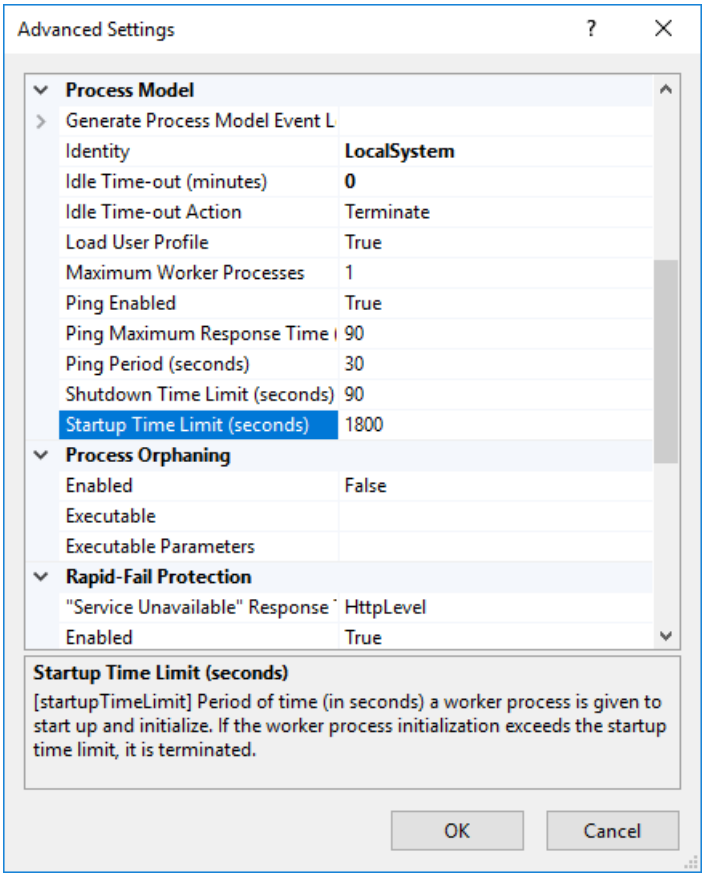
```
{
 ...
 ...
 "AllowedHosts": "*",
 "ScmDatabaseCommandTimeout": 1800
}
```

Modify the start-up time in IIS for the Scan Service

1. Log in to the SCM server. Open **IIS Manager** from Control Panel > System and Security > Administrative Tools > Internet Information Services (IIS) Manager.
2. Expand the server tree in the *Connections* pane and click **Application Pools**.



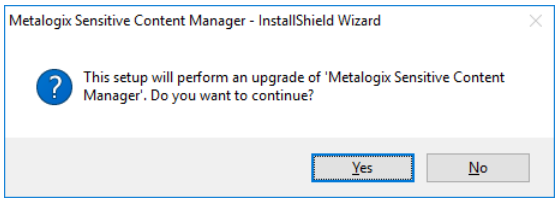
3. Select **SCMScanService** from the *Application Pools* workspace and then click **Advanced Settings** in the *Actions* pane.
4. In the *Advanced Settings* window expand the **Process Model** section.
5. Set **Startup Time Limit (seconds)** to **1800**



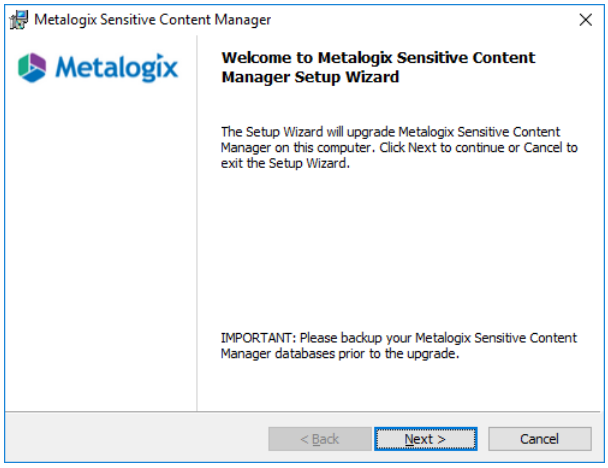
6. Click **OK** to save the setting and then close the IIS Manager.
7. Restart your SCM server.

Steps to upgrade the SCM components

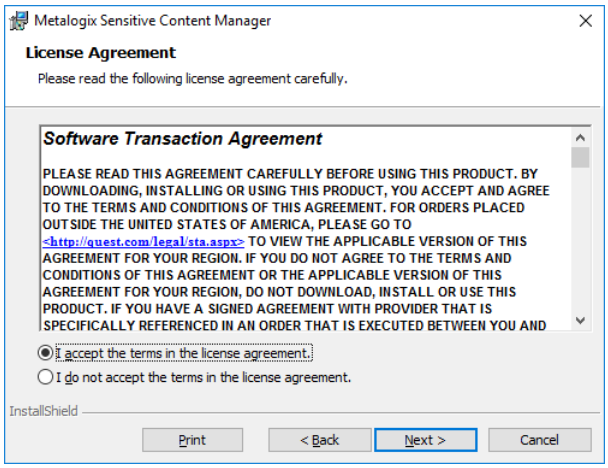
1. Log in to the SCM Server.
2. Download and unzip the install media files to a suitable folder.
3. Click the windows installer file **Metalogix Sensitive Content Manager.exe**. Click **OK** in the *User Account Control* window if it opens and then click **Yes** in the confirmation dialog that opens.



4. Click **Yes** to proceed. The *Welcome to SCM Setup Wizard* opens.



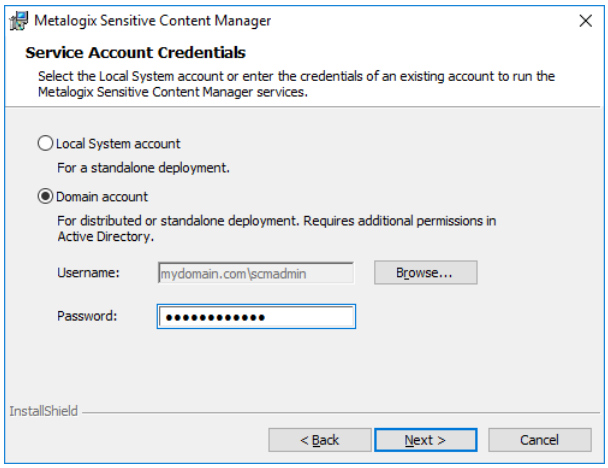
5. Click **Next**. The *License Agreement* window opens.



6. Click the check box **I accept the terms in the license agreement** to activate the **Next** button. Click **Print** to print the License Agreement.

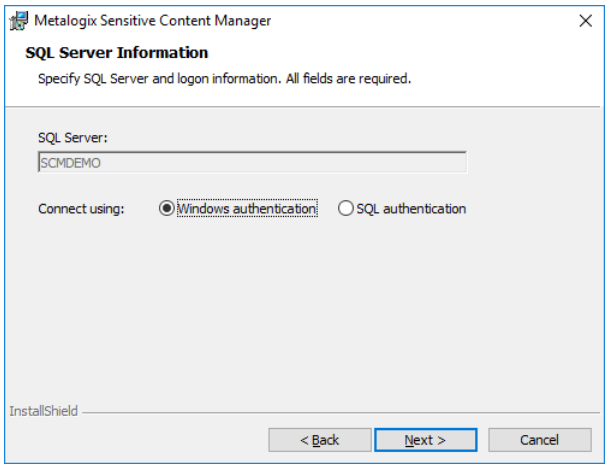
7. If your license is not active or it has expired, the *Product Licensing* window opens. Enter your license key and click **Activate License**. Then click **OK** to close the confirmation window. See License Management for alternate licensing options,

8. Click **Next**. The *Service Account Credentials* window opens.

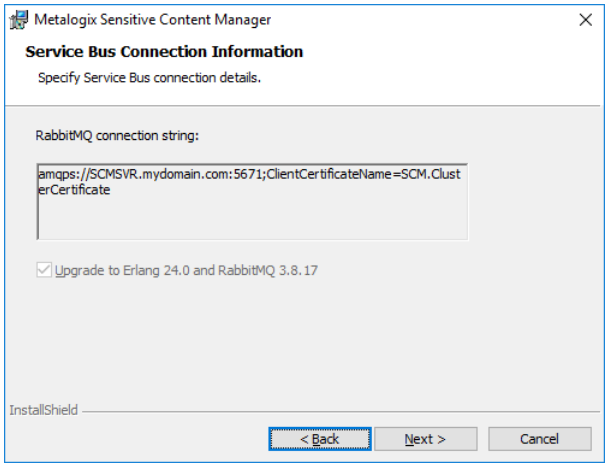


9. Choose the **Local System Account** or **Domain account** based on the account that is used to run the SCM Windows service. If you choose **Domain account** verify the username and enter the credentials of the domain user that runs the service.

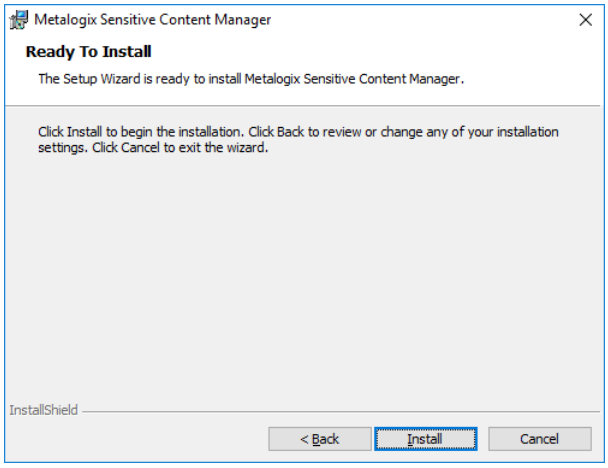
10. Click **Next**. The *SQL Server Information* window opens. For a standalone environment, the SQL Server name would be the same as the SCM server name. Verify the information in the window.



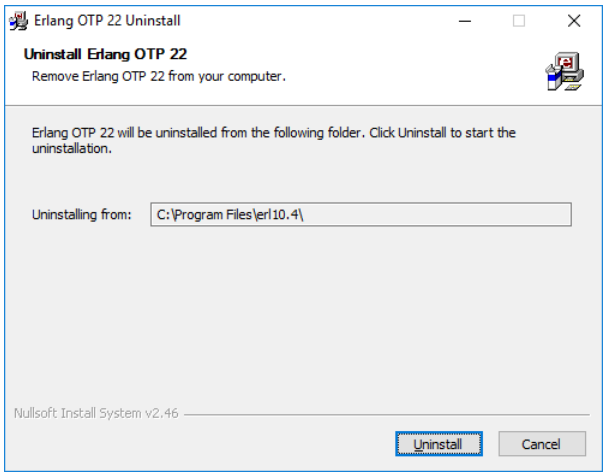
11. Click **Next**. The Service Bus Connection Information window opens and displays the RabbitMQ connection string. The check box **Upgrade to Erland 24.0 and RabbitMQ 3.8.17** is pre-selected (for information purpose only) to upgrade the the third-party components.



12. Click **Next**. The *Ready To Install* window opens.

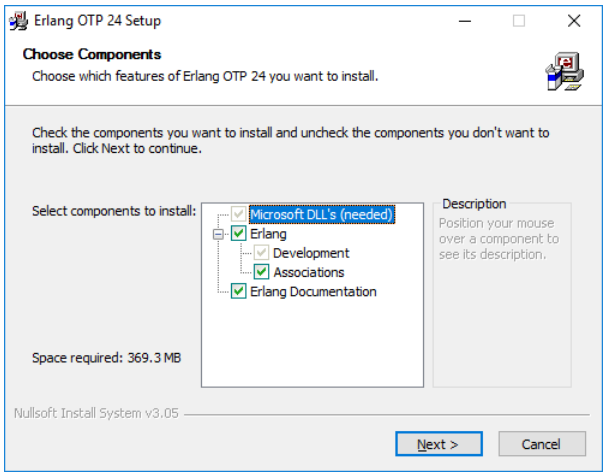


13. Click **Install**. The *Uninstall Erlang OTP 22* window opens.

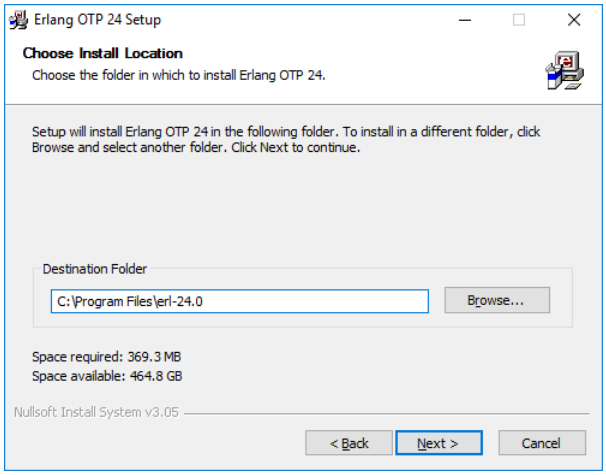


14. Click **Uninstall** to run the removal program. Click **Close** in the *Uninstallation Complete* window that opens when the olde version is successfully removed.

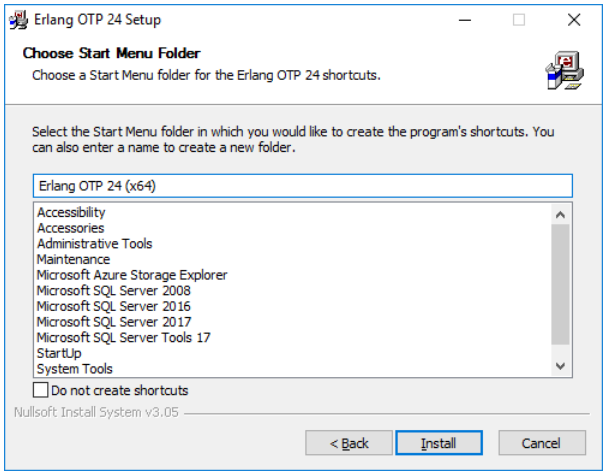
15. The *Erlang OTP 24 Setup* window opens.



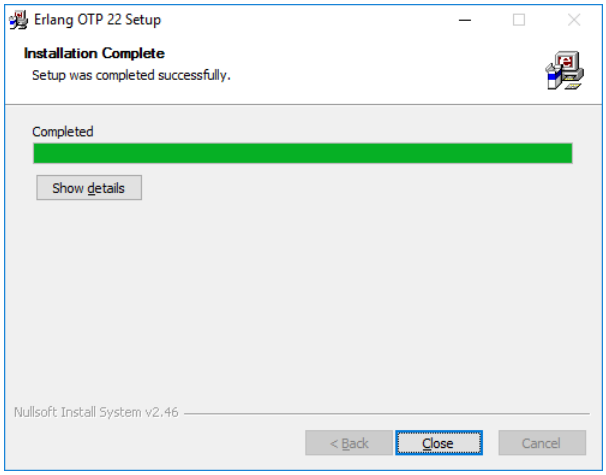
16. Keep the defaults as indicated and click **Next**. The *Choose Install Location* window opens. Click **Browse** to change the location if necessary.



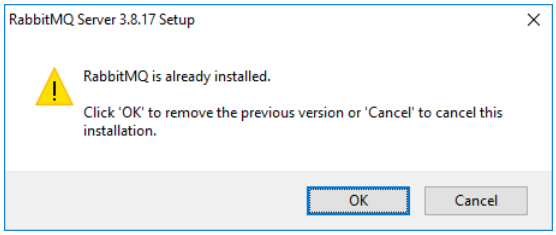
17. Click **Next**. The *Choose Start Menu Folder* window opens. Keep the defaults as indicated and select **Do not create shortcuts** to avoid shortcut creation. You must allow additional Microsoft redistributable components to be installed if requested by the installer.



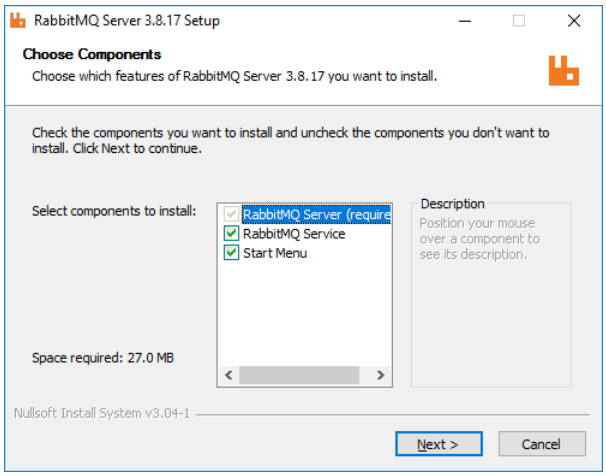
18. Click **Next**. The *Installation Complete* window opens when the installation is successful.



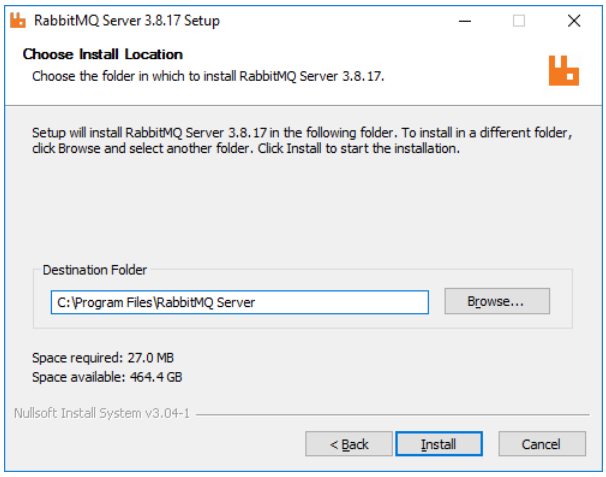
19. Click **Close.** If you have an older version of RabbitMQ the upgrade confirmation dialog opens.



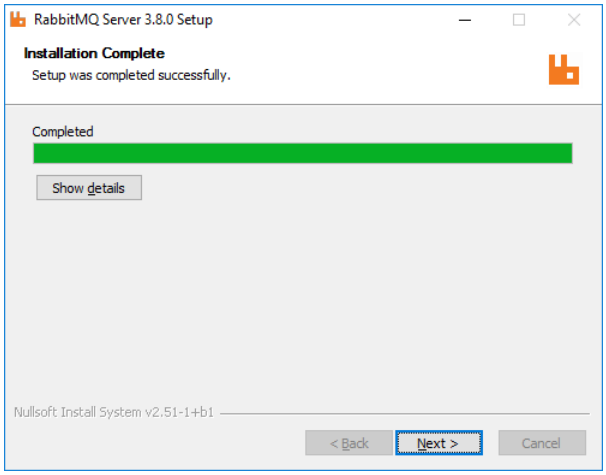
20. Click **OK**. The RabbitMQ upgrade installer starts. Keep the defaults as indicated.



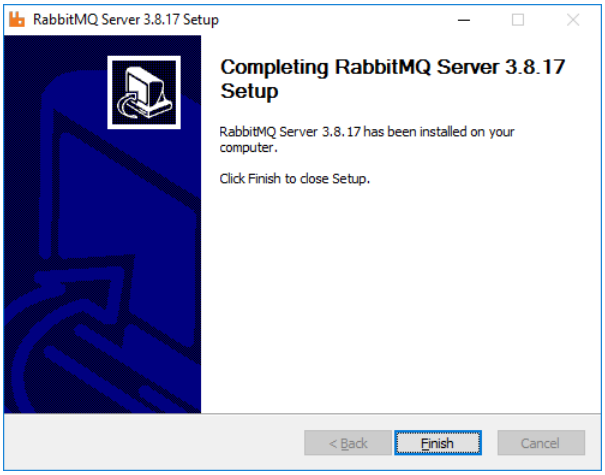
21. Click **Next**. The *Choose Install Location* window opens. Click **Browse** to change the location if necessary.



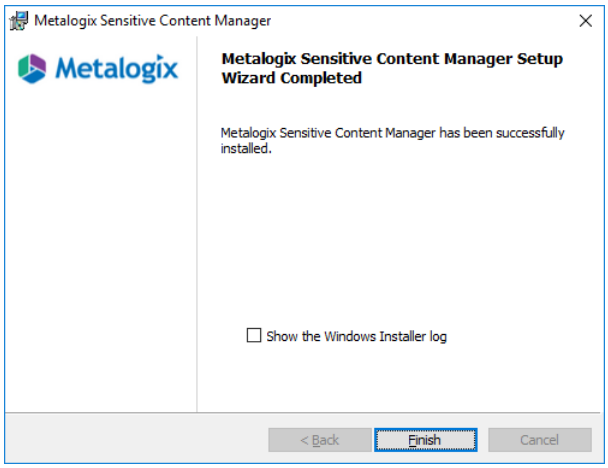
22. Click **Next**. The *Installation Complete* window opens when the installation is successful. Click Show details to inspect the RabbitMQ installation locations.



23. Click **Next**. The confirmation window opens.



24. Click **Finish** and allow to upgrade to complete. When the installation completes successfully, the *SCM Setup Wizard Completed* window opens.



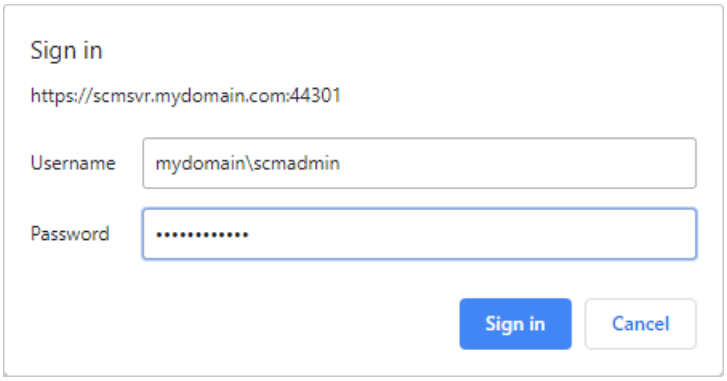
25. Select the **Show the Windows Installer log** inspect the log file if necessary. Click **Finish** to exit the wizard.

NOTE: If you are upgrading a distributed environment, you must upgrade all other servers in the cluster that are used to host dedicated services to ensure all component versions are

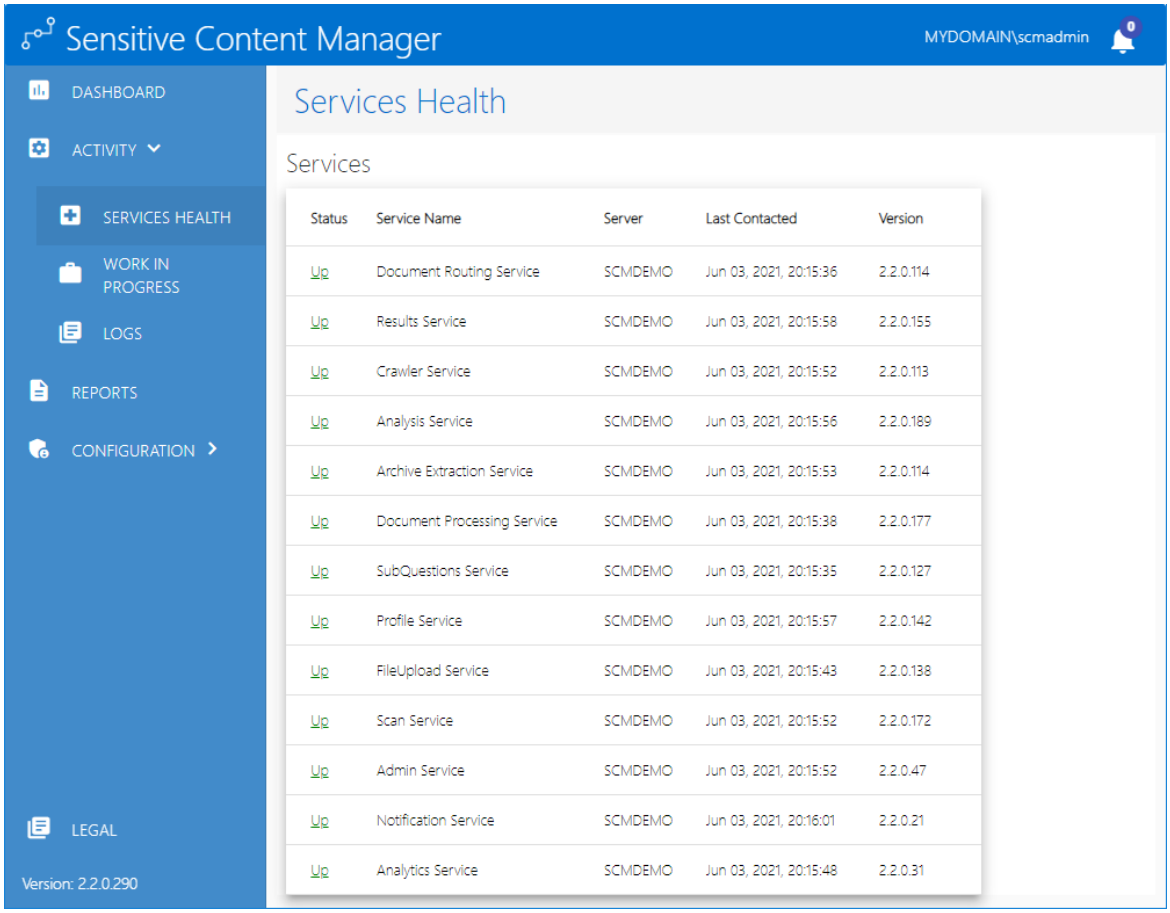
the same. Working with mismatched component versions is not recommended.

Verifying your upgrade

1. Log in to the SCM Sever as an SCM Administrator.
2. Open a supported browser such as Chrome, on the SCM Server.
3. Enter the Admin URL. For example, enter https://scmsvr.mydomain.com:44300
4. In the *Sign in* dialog that opens, enter the credentials of the SCM Administrator.



5. Click **Sign In**. The *Dashboard* page opens.
6. From the navigation pane, expand **Activity** and then click **Services Health**.
   a. Verify that the software version at the bottom of the navigation pane is the expected upgrade version.
   b. Verify that all services indicate Status = Up.
   c. For a distributed environment, you must also verify that each service version on the dedicated servers matches the same service version on the SCM Server.



7. This completes the upgrade verification.

Repairing SCM components

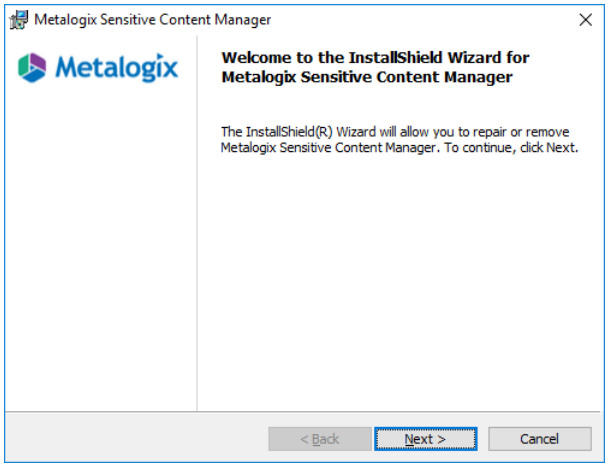
When troubleshooting fails to address problems with unresponsive SCM components, follow the steps below to repair the SCM components in your deployment.

Steps to repair SCM components

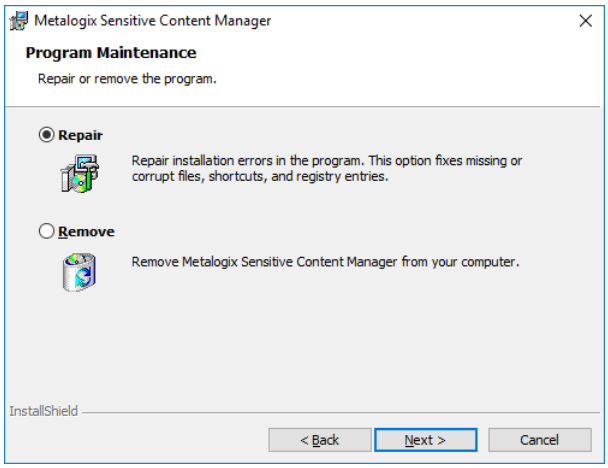
1. Log in to the primary SCM Server. For example, log in to SCMSVR using the SCM Administrator credentials (mydomain\scmadmin).
2. Unzip the install media files to a suitable folder.

> **NOTE:** You must use the same version of the install media that was used in your deployment.

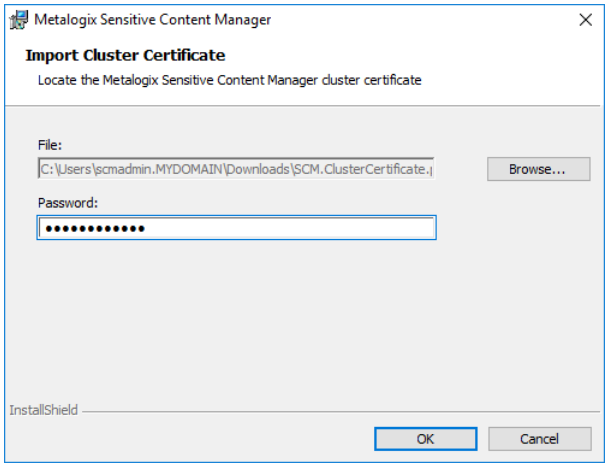
3. Click the windows installer file **Metalogix Sensitive Content Manager.exe**. The *Welcome to SCM Setup Wizard* opens.



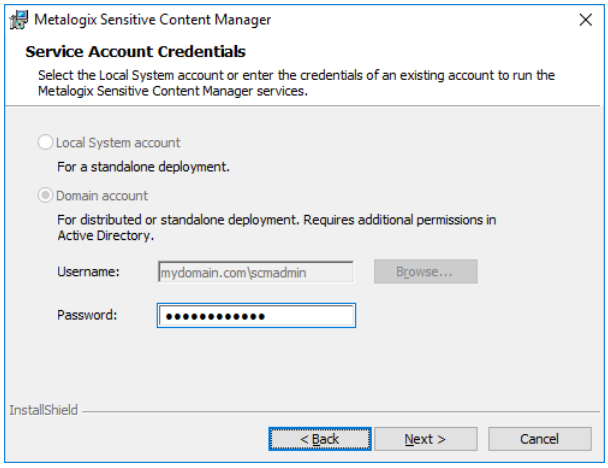
4. Click **Next**. The *Program Maintenance* window opens. Select **Repair**.



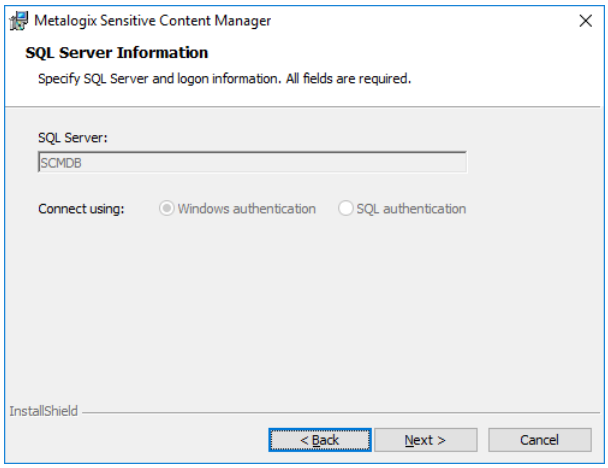
5. If the cluster certificate or license is invalid, you will be prompted to provide the file path or license key respectively. Click **OK** to import the cluster certificate. Otherwise Click **Next**.P



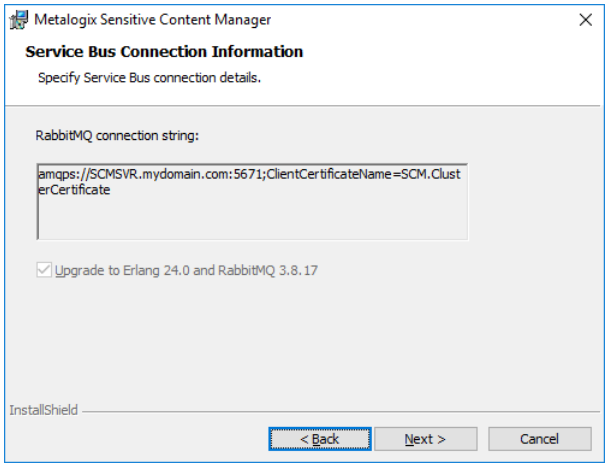
6. The *Service Account Credentials* window opens. Enter the password if the server uses the **Domain account** setting.



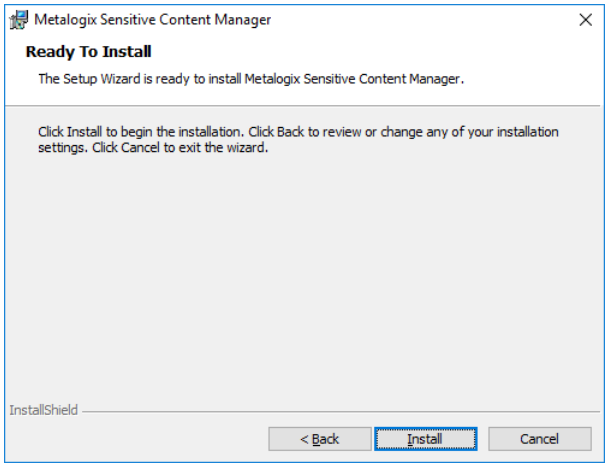
7. Click **Next**. The *SQL Server Information* window opens. Verify the information in the window.



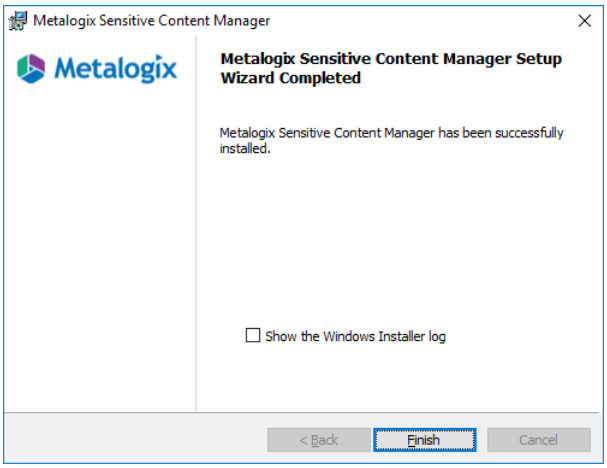
8. Click **Next.** The *Service Bus Connection Information* window opens. verify the information shown in the RabbitMQ connection string field.



9. Click **Next**. The Ready to Install window opens.



10. Click **Install**. Each SCM component is removed and re-installed. If the installation is successful, the *SCM Setup Wizard Completed* window opens.



11. Click **Finish** to exit the wizard.

Removing SCM components

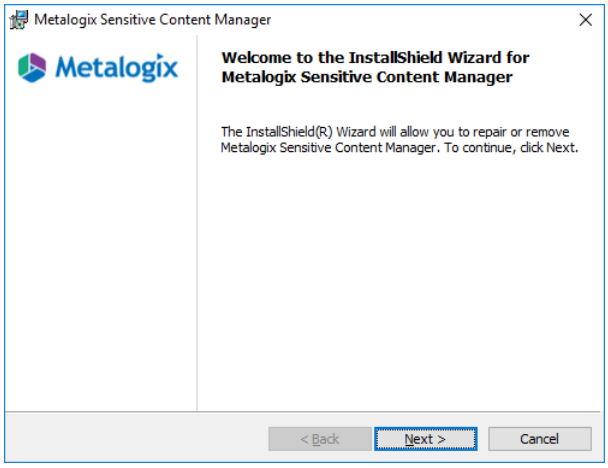
This topic describes two methods to uninstall SCM components.

Steps to uninstall SCM components with the SCM windows installer

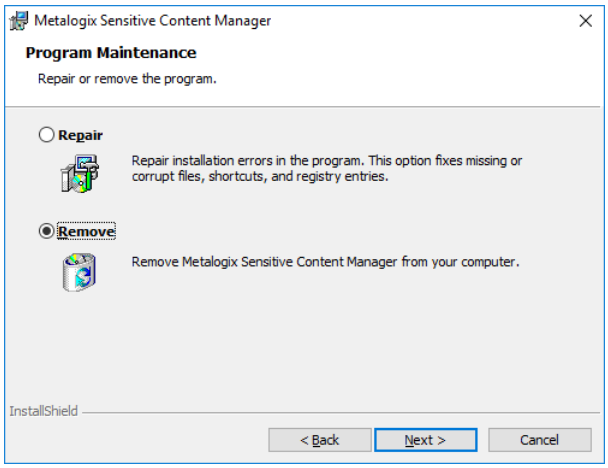
Steps to manually uninstall all SCM components

Steps to uninstall SCM components with the SCM windows installer

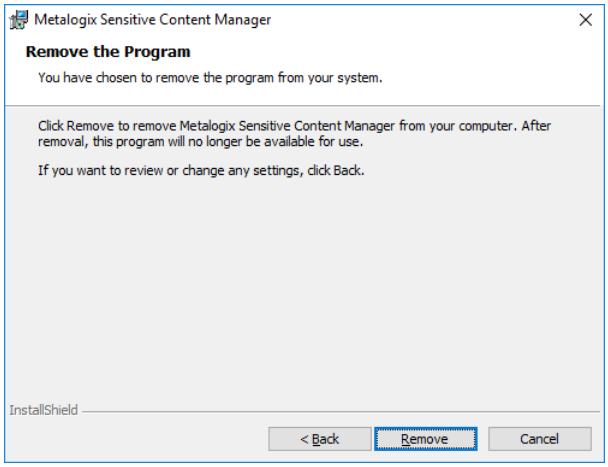
1. Log in to the computer designated as the SCM Server.
2. Unzip the install media files to a suitable folder.
3. Click the windows installer file **Metalogix Sensitive Content Manager.exe**. If the *User Account Control* window opens, click **Yes** and the *Welcome to SCM Setup Wizard* opens.



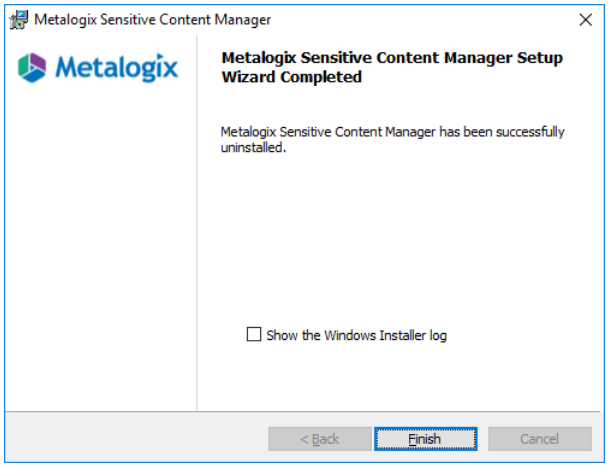
4. Click **Next**. The *Program Maintenance* window opens. Select **Remove**.



5. Click **Next**. The *Remove the Program* window opens.



6. Click **Remove**. If the removal is successful, the *SCM Setup Wizard Completed* window opens.



7. Click **Finish** to exit the wizard.

NOTES:

1. Third party components like Erlang and RabbitMQ must be manually uninstalled.
2. The SCM databases cannot be removed with the SCM windows installer. To remove the SCM databases you could delete the databases using Microsoft SQL Server tools.
3. In a standalone deployment, all SCM components except the SCM databases and certificates are removed.
4. In a distributed deployment:
   a. Only the components from the computer are removed where the SCM windows installer is being used. For example, if the removal steps are followed on the SCM Server only the SCM components installed on the SCM Server are removed. If dedicated servers are used for other services, then these components must be removed separately from each of those servers.
   b. The shared folder is not removed. This folder must be deleted manually to ensure that sensitive files are disposed carefully.

Steps to manually uninstall all SCM components

NOTE: Take a backup of the SCM databases if you plan to remove components.

For a standalone SCM installation

1. Navigate to *Control Panel* > *All Control Panel Items* > *Programs and Features*.
2. Uninstall *SCM*.
3. Remove all SCM IIS application pools and sites.
4. Stop and remove the SCM Windows services.
5. Delete the temporary file storage folder.

6. Delete the installation folder.
7. Restart the computer.

For a distributed SCM installation

1. Log in to the SCM Server and navigate to *Control Panel* > *All Control Panel Items* > *Programs and Features*.
   a. Uninstall *SCM*.
   b. Remove all SCM IIS application pools and sites.
   c. Stop and remove the SCM Windows services.
   d. Delete the shared temporary file storage folder.
   e. Delete the installation folder.
   f. Restart the computer.
2. Log in to each server that has an instance of the SCM Windows service
   a. Navigate to *Control Panel* > *All Control Panel Items* > *Programs and Features*.
   b. Uninstall *SCM*.
   c. Stop and remove the SCM Windows service.
   d. Restart the computer.

9

Troubleshooting

The first step in solving an installation issue is to trace the source of the issue through the **installer.log** file which is created during each install attempt in the same folder where your installation file is located. The troubleshooting messages listed below will help you identify some of the most common issues during the install process and are grouped into installation categories:

- License activation messages
- Destination and Temporary Folder messages
- Windows Service Account messages
- Database messages
- IIS messages
- Service Bus messages

License activation messages

Error Message	Resolution
License key <*LicenseKey*> has expired. Please contact your Quest sales representative.	Contact Quest support.
License key <*LicenseKey*> is invalid. Please contact your Quest sales representative.	Contact Quest support.
Please activate your license.	Click **Activate License** for online activation or click **Activate Offline** for offline activation. If the license activation is successful, a confirmation message opens.
The license key <*LicenseKey*> does not match the currently activated license key <*activatedLicenseKey*>. Please activate your license again.	Try reactivating the old license, and then activate the new license.
An error occurred while copying the activation string to the clipboard.	Try again. If the error persists, contact Quest support.

An error occurred while saving the file.	The folder may be read only or may not exist. Try saving to a different folder. If the error persists, contact Quest support.
An error occurred while reading the file.	The file may be corrupted. Try generating the file again by attempting an offline activation. If the error persists, contact Quest support.

Destination and Temporary Folder messages

Error Message	**Resolution**
The folder <*folderpath*> is invalid or does not exist.	The destination or temporary folder that was specified should exist. If you choose to keep the default settings, then the folder will be created by the installer.
The folder <*folderpath*> is read only.	Remove the read restriction on the destination or temporary folder.
An error occurred while creating the destination folder.	Ensure that the destination folder exists, and the account used for installing the product or service has permissions to create the destination folder.
An error occurred while validating the destination folder.	Ensure that the destination folder exists, and the account used for installing the product or service has permissions to write to the destination folder.
An error occurred while selecting the destination folder.	Ensure that the destination folder exists.
The folder must be a local folder.	The destination folder for installing the product or service cannot be a shared folder.
An error occurred while ensuring user <*serviceIdentityUserName*> permission on <*targetPath*>.	Ensure that the temporary folder exists, and the account used for installing the product or service has read/write permissions on the temporary folder.
An error occurred while validating the temporary storage folder.	Ensure that the temporary folder exists, and the account used for installing the product or service has read/write permissions on the temporary folder.

An error occurred while selecting the temporary storage folder.	Ensure that the temporary folder exists.
The folder <*folderpath*> must be a shared folder.	If a service instance is installed on a dedicated server for scalability, the temporary folder selected must be a shared folder.
Insufficient disk space detected for temporary folder <folderPath>. Select a folder on a larger drive or a dedicated UNC location.	The expected space requirement is approximately double the size of the physical RAM. For example, if you have 32GB of RAM then you must have 64GB of available space on the local drive. You can clear some unused files to recover the required space or select a folder on a larger drive or select a dedicated UNC location.

Windows Service Account messages

Error Message	**Resolution**
An error occurred while validating the user's credentials.	Please check the windows log in credentials of the user that will run the Windows service or re-enter the correct credentials.
The specified account does not exist, or the user's credentials are invalid.	Check the windows log in credentials of the user that will run the windows service, or re-enter the correct credentials. if the user is a domain user, please verify the user account in the domain active directory.
Access to the Service Connection Point is denied	Ensure that the domain user or LocalSystem account that is used to run the windows service has been added to the Service Connection Point of the SCM Server in the active directory and *all* permissions have been granted. For more information see Steps to grant permissions to the SCM Service account for the Service Connection Point.
Unable to reach the SCM services	1. Log in to the dedicated service server. Open a command window with Start > Run > cmd. At the command prompt run the command **ping** <*SCM Server IP Address*> and ensure that you get the responses to verify that SCM Server is reachable.

	2. Log in to the SCM Server and verify that the ports are open. For more information see Steps to configure the inbound rules for the service ports on the SCM Server. 3. In the SCM Server open the *Internet Information Services (IIS) Manager* and verify that the *Application Pools* and *Sites* related to SCM are running.
An error occurred while checking for existing Service Connection Point.	Ensure that the domain user or LocalSystem account that is used to run the windows service has been added to the Service Connection Point of the SCM Server in the active directory and *all* permissions have been granted. For more information see Steps to grant permissions to the SCM Service account for the Service Connection Point
A Service Connection Point already exists for '*<computerName>*' but the Local System account ('*<SCM_MACHINE_FRIENDLY_DOMAINNAME}\\{computerName>*$') may not have write permissions.	Ensure that the domain user or LocalSystem account that is used to run the windows service has been added to the Service Connection Point of the SCM Server in the active directory and *all* permissions have been granted. For more information see Steps to grant permissions to the SCM Service account for the Service Connection Point.

Database messages

Error Message	**Resolution**
Unable to connect to the SQL Server *<sqlServerName>* using service account *<serviceIdentityUserName>*.	Verify that the SQL Server is accessible to the logged in user. If a firewall is active, ensure that an inbound port rule on the SCM Server is created for port 1433.
The specified account does not have the required permissions on SQL Server.	Verify that the user exists in the SQL Server with appropriate log in rights. This is usually the case with orphaned users.
The installation account *<sqlUserName>* must have the 'dbcreator' and 'securityadmin' roles assigned in *<sqlServerName>*.	The logged in user who is installing the SCM components must be granted the 'dbcreator' and 'securityadmin' roles in the SQL Server.

The service account <*serviceIdentityUserName*> must have the 'db_owner' role assigned in <*sqlServerName*> for database(s): <*missingDbOwnerDatabaseNames*>.	The SCM Service user account on a distributed node must be granted the 'db_owner' roles in the SQL Server. The SQL Server must be accessible to the SCM Service user. If a firewall is active, ensure that an inbound port rule on the SCM Server is created for port 1433.
Insufficient disk space detected on the SQL Server database drive.	The expected space requirement is approximately double the size of the physical RAM. For example, if you have 32GB of RAM then you must have 64GB of available space on the SQL Server database drive. You can clear some unused files to recover the required space or move your database default drive to a disk drive with the required disk space.
The ScanDetail table contains a large volume of data that impacts report generation. Configure additional settings to prepare for the upgrade as described in the SCM Installation Guide.	Additional configuration that is required is described in the topic Preparing for the upgrade.

IIS messages

Error Message	**Resolution**
Please enter a port number between 1 and 65535.	Specify a port number that is within the bounds indicated.
Port number is already in use.	Specify a different port number that is within the bounds indicated.
An error occurred while validating the IIS web site information.	This is a generic error. If the error persists, contact your IT resource or contact Quest support.
An error occurred while creating the self-signed certificate <*friendlyName*>.	Try creating another self-signed certificate. For the SCM Server, ensure that the self-signed certificates are kept in: • Trusted Root Certification Authorities store, and • Personal or Web certificate store

	If you have a Verisign, Thawte or another commercial certificate then they do not need to be placed in the Trusted Root Certification Authorities store.
An error occurred while binding certificates.	Verify that the certificate is in the correct folder or regenerate the certificate as it may be corrupted and try again or contact Quest support.
Security group <*groupName*> does not exist. or An error occurred while verifying security group <*groupName*>.	Verify that a valid security group exists in the domain active directory.
The computer must be joined to a domain.	The computer should be added to the domain. Start > Run > sysdm.cpl to open the System properties window. Add your computer to the domain from there.

Service Bus messages

Error Message	**Resolution**
Unable to connect to the RabbitMQ.	Check that RabbitMQ is accessible. Verify that the Rabbit.ClusterCertificate (if applicable) is in the certificate store. Verify that the connection string is valid. If the connection uses *amqp* then port 5672 must be open, or if connection uses *amqps (secured)* then port 5671 must be open.
RabbitMQ is already installed. Click 'OK' to remove the previous version or 'Cancel' to cancel this installation	A mismatch between the installed version of RabbitMQ and the required version was detected. Click **OK** to allow the installer to uninstall and install the required version of RabbitMQ.
An error occurred while validating the service bus connection string.	This is an unexpected error from the service bus. Check that RabbitMQ is accessible. Verify that the *Rabbit.ClusterCertificate* is in the certificate store. Verify that the connection string is valid. If the connection uses *amqp* then port 5672 must be open, or if connection

	uses *amqps (secured)* then port 5671 must be open or contact Quest support.
Insufficient disk space detected on the Rabbit drive.	The expected space requirement is approximately double the size of the physical RAM. For example, if you have 32GB of RAM then you must have 64GB of available space on the SQL Server database drive. You can clear some unused files to recover the required space.

10

Appendix

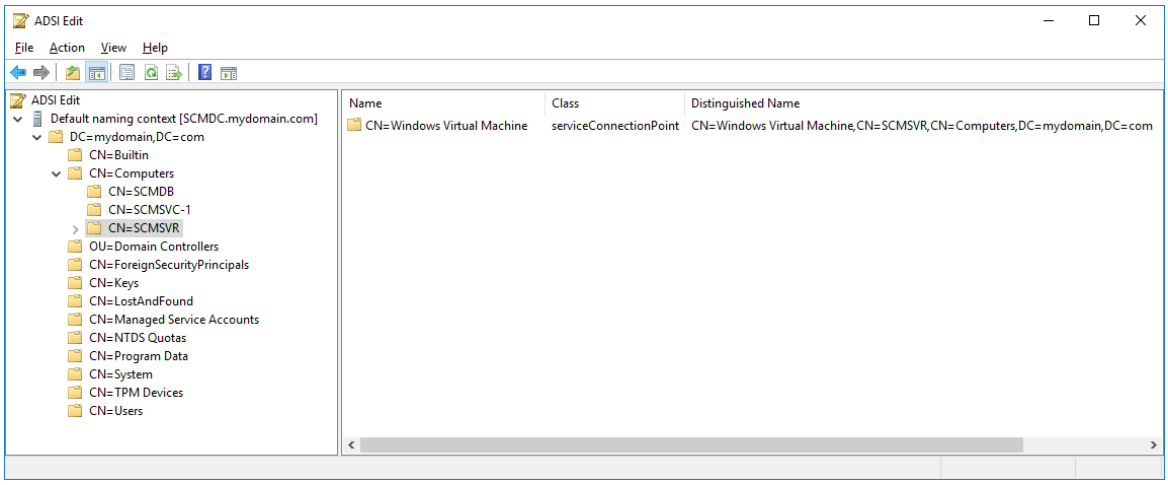
In this chapter:

- Steps to grant permissions to the SCM Service account for the Service Connection Point
- Steps to grant Remote Desktop Access
- Steps to get the URL for the SCM Administration Center
- Relocating the RabbitMQ installation directory

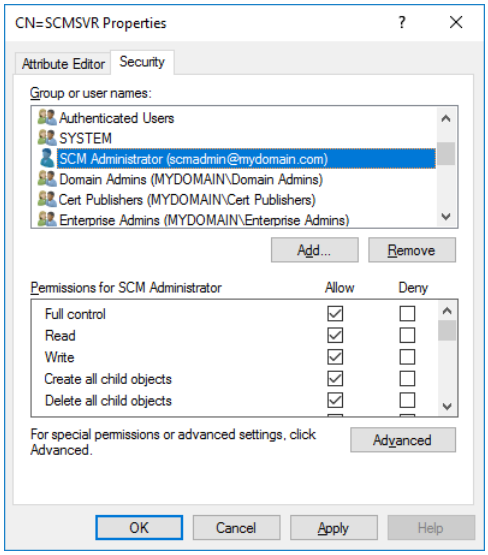
Steps to grant permissions to the SCM Service account for the Service Connection Point

Contact your domain administrator to help with these steps if needed.

1. Log in to your domain controller
2. Click **Start** > **Run**. Enter **ADSIEdit.msc** and click **OK** to start the *Active Directory Service Interfaces Editor*.
3. From the *Console Tree*, expand the computers node and select the SCM Server (e.g., CN=SCMSVR).



4. Right-click the **CN=Sensitive Content Manager** node and select **Properties** from the context menu.
5. Select the *Security* tab.
6. Click **Add** and follow the steps to add a domain user (eg. SCM Administrator)



7. In the *Permissions* window, select all the **Allow** check boxes.
8. Click **OK** to close the window.

Steps to grant Remote Desktop Access

Follow the steps below to grant the required privilege to log on through Remote Desktop Services:

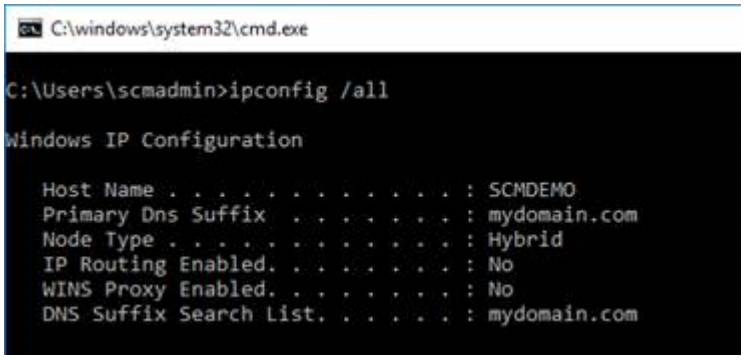
1. Log in to the computer with the local administrator credentials.
2. *Start* > *Run* > *secpol.msc*
3. From the *Security Settings* pane, open *Local Policies* > *User Rights Assignment*.
4. From the right-hand pane, double-click on **Allow log on through Remote Desktop Services** to open the properties window.
5. Select the *Local Security Settings* tab and click **Add User or Group...**
6. Add the **SCM Administrator** and the **SCM Users** group.
7. Click **OK** to save the changes and exit.

Steps to get the URL for the SCM Administration Center

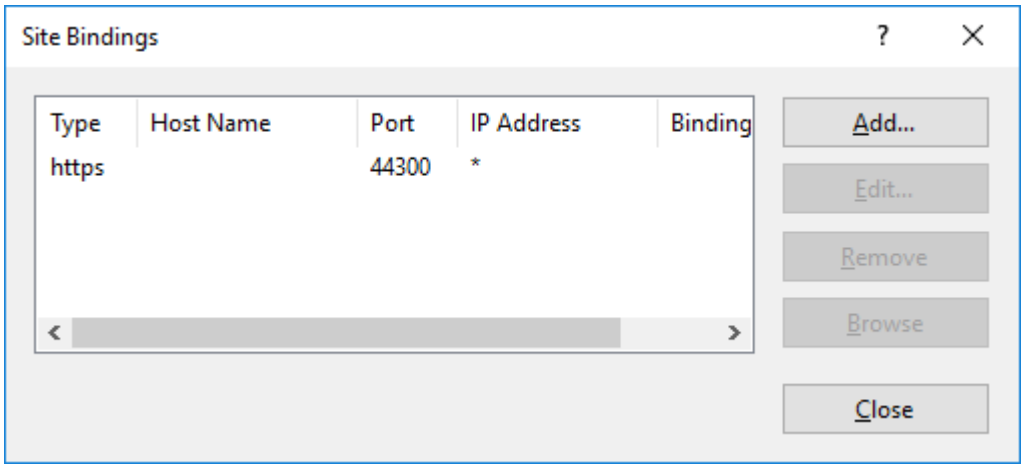
1. Right-click the desktop shortcut and select **Properties**.
2. Click the **Shortcut** tab and note the value of the **Target** field.

or

1. Log in to the SCM Server and open the **Command** console.
2. Run the command `ipconfig /all`



3. Get the FQDN of the server from the windows command prompt. This will give you **[Hostname]**.**[Primary Dns Suffix]**. For example, `SCMDEMO.mydomain.com`
4. To get the protocol and port open **IIS Manager**
   a. Expand the server node.
   b. Expand the **Sites** node and select **SCMAdminPortal**
   c. From the *Actions* pane click **Bindings**. This will gives you [protocol] and [port]. For example, the protocol is https and the port binding is 44300.



You can put all this information together and get **[protocol]**:// **[Hostname]**.**[Primary Dns Suffix]**: **[Port]**. For example, `https://SCMDEMO.mydomain.com:44300`

Relocating the RabbitMQ installation directory

To move the Rabbit configuration and data files to a secondary drive (for example, **E:\RabbitMQ**)

1. Run the following commands to stop and remove the service
   - `rabbitmq-service.bat stop`
   - `rabbitmq-service.bat remove`
2. Physically move all the existing RabbitMQ files from **%APDATA%\RabbitMQ** to the new location **E:\RabbitMQ**
3. Use a text editor to update the **rabbitmq.conf** file located in the **E:\RabbitMQ** folder with the new certificate location path
   - `ssl_options.cacertfile = E:\\RabbitMQ\\CertificatePemFiles\\cabundle.pem`

- `ssl_options.certfile   = E:\\RabbitMQ\\CertificatePemFiles\\rabbit.pem`
- `ssl_options.keyfile    = E:\\RabbitMQ\\CertificatePemFiles\\key.pem`

4. Run the following commands to install and start the RabbitMQ service and point them to the new location.

   - `SET RABBITMQ_BASE=E:\RabbitMQ`
   - `rabbitmq-service.bat install`
   - `rabbitmq-service.bat start`

11

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal allows you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product