

Quest® InTrust 11.4.2

## **Getting Started with InTrust**



**© 2020 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 Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

**Legend**

-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

InTrust Getting Started with InTrust

Updated - September 2020

Version - 11.4.2

# Contents

<b>First Steps</b> .....	<b>4</b>
Installing InTrust .....	4
Participation in the Quest Software Improvement Program .....	5
Collecting Events in Real Time .....	5
Introduction to Repositories .....	6
Common Tasks .....	6
Managing Collections .....	6
Availability of Collection Management Commands .....	8
Analyzing Collections .....	8
Exporting Collection Information .....	8
Advanced Analysis .....	9
Managing Repositories .....	9
Where to Keep Repositories .....	9
Setting Up Daily Cleanup .....	9
Gathering Windows Logs Other than Security, Application and System .....	10
Applications and Services Logs .....	10
Forwarded Events .....	10
Load Balancing .....	10
Example: Configuring Logon and User Session Auditing .....	12
Start Gathering .....	12
Put Auditing to a Test .....	12
View the Results in Repository Viewer .....	13
<b>Further Reading</b> .....	<b>14</b>
<b>About us</b> .....	<b>15</b>
Contacting Quest .....	15
Technical support resources .....	15

# First Steps

InTrust is an event-log management solution that provides for collection, correlation, archival, and reporting on the heterogeneous audit data from your enterprise-wide network. InTrust real-time alerting and notification capabilities allow you to stay aware of what is going on in your network and how your business-critical resources are functioning.

Although InTrust is a powerful and comprehensive framework for audit data, deployments can range widely in complexity. The following types of coverage are all possible:

- Basic everyday security auditing with a minimal set of components
- Archival of audit data in compressed repositories for regulations compliance
- Fast search and reporting tools that work with repository data
- Real-time monitoring for critical security events, with alert tracking and automated response actions
- Auditing of multiple platforms and custom logs with advanced reporting based on SQL Server Reporting Services
- Combinations of the above

This guide explains only the use of the basic InTrust deployment. More sophisticated features and workflows are described elsewhere in the InTrust documentation set—for example, in the [Deployment Guide](#).

## Installing InTrust

Before you begin installation, confirm that the system requirements are met (see [System Requirements](#)). Also note that the InTrust installer verifies this automatically.

If the computer where you are going to install InTrust is a SQL server, then make sure in advance that the installed version of SQL Server Native Client is no earlier than the version required by InTrust; version 11.0.6538.0 of the client is redistributed with InTrust.

To begin installation, use the Autorun application that comes with your InTrust distribution; click **InTrust Default Suite** on the **Install** tab to begin setup.

**i** | **NOTE:** If you need custom InTrust capabilities, consider the **InTrust Extended Suite** option, which is not covered in this set of topics. For details, see the [Deployment Guide](#).

Next, complete the remaining steps.

**!** | **CAUTION:** The default InTrust components require that ports 900 and 8340 be open for inbound traffic. The InTrust installer knows how to configure these ports automatically in Windows Firewall. In addition, IT Security Search and the InTrust repository API work with port 8341, which is not configured automatically. If you use the API or IT Security Search, make sure this port is open.

# Participation in the Quest Software Improvement Program

One of the setup steps prompts you to select the country where you are performing InTrust installation. This choice affects whether your participation in the Quest Software Improvement Program is enabled automatically. The Software Improvement Program involves Quest receiving anonymous usage statistics from the Quest software you install. No personal identifying data (such as account names) is included in this feedback. The purpose is to determine which features are most popular and find out how their use can be streamlined.

The following information is transmitted:

- Hardware configuration
- Which product features are used
- External IP addresses

Participation is voluntary. Although it is enabled automatically for some countries, you can change your choice at any time after InTrust setup is complete; for details, see the [Installing the First Server in InTrust Organization](#) topic in the [InTrust Deployment Guide](#).

## Collecting Events in Real Time

After you have installed the default components, run the InTrust Deployment Manager console by clicking its entry in the Start menu. This console manages gathering of audit data to InTrust repositories.

In the console, you need to specify the computers you want to audit and specify what kinds of events you need. This is done by setting up collections. Collection settings include the computers to collect from, data sources (definitions of the types of events) and the repository to collect to. Simply put, the point of a collection is to “get this kind of data from these computers to this repository”.

For gathering to work, computers in collections need to have InTrust agents installed. You can install agents on specific computers by selecting them in the right pane while a collection is highlighted and clicking **Install Agents**. Alternatively, enable the **Install agents automatically** option while you are creating or editing a collection to automatically install them on all computers in the collection. If this option is off in a newly-created collection, no gathering occurs. Once you enable it, agents are installed and gathering begins.

**! CAUTION: If the Install agents automatically option is enabled for a collection, InTrust will try to keep the agents on all computers in the collection. If you uninstall an agent from a computer in such a collection, it will be reinstalled automatically.**

**In this situation, to stop gathering from a computer, you need to remove it from the collection.**

**If the Install agents automatically option is disabled, you need to install and uninstall agents manually using toolbar commands.**

When you run InTrust Deployment Manager, you are directed to the home view, where you are briefly introduced to the basics of real-time event collection workflow. This view explains collections (how InTrust organizes computers to collect from) and repositories (stores to collect data to), and it provides quick action links to help you get work done.

If you are starting InTrust Deployment Manager for the first time, take the opportunity to create a collection in the home view: either a Windows collection for gathering from Windows computers or a Syslog collection for capturing Syslog messages from devices and hosts.

# Introduction to Repositories

An InTrust repository is a store for audit data collected by InTrust. Its architecture is such that massive amounts of data can be stored efficiently in a compact way and indexed for fast browsing in InTrust Repository Viewer and streamlined access by IT Security Search.

This helps achieve security regulations compliance and provides a ready-made toolset for event analysis. For an in-depth description of InTrust repositories, see the [Understanding InTrust Repositories](#) topic.

For the purposes of this guide, however, it is sufficient to know the following about repositories:

- When you set up InTrust, a default repository is automatically created for you in the InTrust installation folder (by default, installation to Program Files is suggested). Note that the default repository is not recommended for real production use, but only for evaluation and training. When you are confident with the InTrust workflow, create your own repository on a server that has ample disk space and is ready for intensive disk writes.
- You can use the default repository for all your logon and user session auditing needs (unless further scaling is required).
- The folder where you create a repository should be available over the network.
- If necessary, you can have multiple repositories, specialized by the type of data they are supposed to contain, by their location, or by some other characteristic. However, try to keep a manageable number of repositories.
- The toolset described in this document works only with indexed repositories.

To manage repositories, use the **Storage** view in InTrust Deployment Manager.

## Common Tasks

The following topics describe how you can manage and adapt InTrust using the InTrust Deployment Manager console.

- [Managing Collections](#)
- [Analyzing Collections](#)
- [Managing Repositories](#)
- [Gathering Windows Logs Other than Security, Application and System](#)
- [Load Balancing](#)

## Managing Collections

You can add, delete and edit collections at any time. To work with collections, go to the **Collections** view of InTrust Deployment Manager.

To create a collection, right-click the **Collections** node and select **New Windows Collection** or **New Syslog Collection**. To edit or delete a collection, right-click it and use the corresponding command.

### ***To add computers to a collection***

Use any of the following ways:

- In the wizard that opens when you edit a collection, change the computer list on the Specify Computers step. For that, click the Add button under the computer list. You can supply the computers using a variety of methods:
  - Click **Computers** to supply individual computer names.
  - Click **Computer Names from Text File** to specify an existing computer list in a plain-text file. Note that this is only a one-off import action. InTrust does not track changes to the file or remember its location.
  - Click **Domains** to make InTrust enumerate the computers in the domains you select. InTrust will re-enumerate the computers periodically to keep the collection membership up to date.
  - Click **LDAP Query** to supply a detailed query that extracts computers from Active Directory. For convenience, the dialog box that opens provides the native Windows LDAP control to help you compose the query; click **New Query** to use the control. InTrust will rerun the query periodically to keep the collection membership up to date.
  - Click **All DCs in the domain** to include just the domain controllers. InTrust will re-enumerate them periodically to keep the collection membership up to date.
- Select the computers you need in the **Computers not in a collection** search folder in the navigation pane and click **Add to Collection** (in the toolbar or in the shortcut menu), and then select the collection you need.

### ***To delete computers from a collection***

1. Right-click the collection and select **Edit Collection**.
2. In the wizard that opens, go to the Specify Computers step.
3. In the list of computers, select the computers you do not need, and click **Remove** (in the toolbar or in the shortcut menu).

### ***To stop gathering from a computer without removing it from a collection***

This works only in collections where the **Install agents automatically** option is disabled. In such collections, use the **Install agent** and **Uninstall agent** commands (in the toolbar or in the shortcut menu) to manage gathering without affecting collection membership.

**i** **NOTE:** The **Install agent** command is not available for collections where the **Install agents automatically** option is enabled. The **Uninstall agent** command remains available, but its effect is temporary; an uninstalled agent is re-installed in a few hours.

In addition, the following management actions can be done in the wizard:

- Change the account used for connecting to the computers in the collection  
Set the credentials on the Specify Computers step.
- Change the list of logs that are gathered  
Select the data sources you need on the Data Sources and Repository step.

**i** **NOTE:** By default, InTrust gives you no indication of situations where a log that you selected is not available on an agent's computer. If you would prefer to know when this happens, select the **If any of the selected data sources cannot be found, consider this an error** option. Be aware that this will make InTrust Deployment Manager show the **Failed** status for computers where the logs are absent.

- Change the repository that events are gathered to  
Select the repository on the Data Sources and Repository step.

# Availability of Collection Management Commands

In some situations, you cannot perform a specific action (**Install agent**, **Uninstall agent** or **Remove**) on one or more computers in a collection, as explained below:

You cannot...	Possible reason
Install the agent	The <b>Install agents automatically</b> option is enabled for the collection. Manual installation is not needed.
Uninstall the agent	<ul style="list-style-type: none"><li>The <b>Install agents automatically</b> option is enabled for the collection. Manual agent removal makes no sense, because the agent would be automatically restored anyway.</li><li>The agent is not installed.</li></ul>
Remove a computer from a collection	<ul style="list-style-type: none"><li>The computer became a member of the collection dynamically instead of being added individually or through a computer list. For example, you cannot single out a computer for removal if it was added through an LDAP query. In this case, you need to edit the query to exclude it.</li><li>It is the last computer in the collection. Just delete the collection that contains this computer.</li></ul>

## Analyzing Collections

When a collection is selected, the right pane shows a table with information about the collection members. The table supports multi-level grouping of collection computers, so that you can organize the computers in tree-like views using any criteria. For example, you can group computers by status, then by domain, then by type.

To use multi-level grouping, drag table column names from the computer list to the area above the list. The computer list changes accordingly.

**i** **NOTE:** The difference between the “Not Installed” and “Failed” computer statuses is as follows:

- “Not Installed” means agent installation has never been tried for this computer.
- “Failed” means agent installation has been tried but failed

To hide the computers you are not interested in, you can use view filtering. To configure a view filter, use the controls underneath the table column names: click the operator icon to select the operator, and specify the value to filter by.

The same grouping and view filtering techniques are available in the views with search folder results.

## Exporting Collection Information

You can save information about the currently selected collection to a CSV file for comparison, bookkeeping or analysis. For that, click **Export list to CSV** in the toolbar above the collection view. Alternatively, right-click a collection in the left pane and select **Export List to CSV**. Note that the exported information is not necessarily the same as in the collection view; the specifics are as follows:

- No grouping or sorting from the collection view is applied to the CSV output.
- The set of exported table fields is always the same in the CSV output. The choice and order of fields in the collection view don't affect it.
- If the collection members are filtered, the same filter is applied to the CSV output.

The data fields in CSV are made independent of the collection view by design. This way the data layout stays the same and is easier to handle with the tools you use for working with CSV.

## Advanced Analysis

If you need to troubleshoot your collections or examine your real-time gathering workflow in the greatest possible detail, you can use the **RealTimeCollectionStatus.ps1** script, which outputs raw information about your collections to a CSV file. For details, see [Tracking Real-Time Event Collection State](#).

## Managing Repositories

You can add, delete and edit repositories at any time. To work with repositories, go to the **Storage** view of InTrust Deployment Manager.

In this view, the left-hand pane lists the available repositories, and the right-hand pane shows the properties of the selected repository.

To create and delete repositories, use the **New** and **Delete** buttons. To edit the properties of a repository, select it and click the **Edit** link for the group of settings you want.

**i** **IMPORTANT:** The defining property of a repository is the path to the network share that contains the collected data. When you specify the path, use a UNC name. This makes the repository available to client applications in the network, such as Repository Viewer and IT Security Search. It will also make it easier to integrate the repository into an extended InTrust deployment if you decide to perform it.

You can also create a repository when you create a new collection or edit an existing collection (see [Managing Collections](#)), on the Data Sources and Repository step of the wizard.

## Where to Keep Repositories

Repositories should not be located on the InTrust server. Admittedly, the default repository is automatically created on the server, but this is only a fallback choice. For day-to-day real-time event collection purposes, create repositories in network shares on separate computers to which client applications, such as Repository Viewer and IT Security Search, have fast network connections.

## Setting Up Daily Cleanup

You can configure a repository to keep only recent data and automatically discard data that is too old. For that, edit the **Daily Cleanup** settings in the repository properties in the **Storage** view. Specify how old data can get before it is considered too old and at what time daily cleanup should start.

# Gathering Windows Logs Other than Security, Application and System

## Applications and Services Logs

To gather a third-party Windows event log that is available in the Applications and Services Logs subtree in Windows Event Viewer, you need to create a data source for it. This is done in the wizard used for creating and editing collections, on the Data Sources and Repository step.

Proceed to that step, and then do the following:

1. Click **Add**. The New Data Source dialog box opens.
2. Specify a meaningful name for the new data source. Optionally, provide a description.
3. In the text box below, specify the exact log name.

**i** **NOTE:** If you don't know the name, look it up in Event Viewer, as follows:

1. Run Event Viewer on a computer where the log is available, and locate the log you need.
  2. Open the properties of the log. The name is in the **Full Name** text box.
4. Click **OK** to save the new data source, and select the check box next to it in the data source list.
  5. Complete the wizard.

## Forwarded Events

One of the available Windows log types is Forwarded Events. If subscription-based logging of these events is enabled, InTrust can collect them just like other events. It is possible to configure the gathering using the procedure above; the exact log name in step 3 is **ForwardedEvents** in this case.

However, due to the limitations of this forwarding technology, data in the forwarded events is mostly meaningless. You can gather it to a repository, but you cannot search in it or build reports on it. Therefore, collecting this data is not recommended. Instead, use InTrust to gather the original events from the sender computers.

## Load Balancing

The metrics and suggestions in this section are based on tests performed by quality control.

InTrust agents send events to InTrust servers in batches. By default, the event submission rates are as follows:

- On Windows servers, including domain controllers, a batch file is sent every minute.
- On workstations, a batch file is sent every seven minutes.

There are two primary limits to consider when estimating if an InTrust server can cope with its load. On the one hand, an InTrust server can gather from no more than 10,000 computers (servers or workstations) at a time. On the other hand, an InTrust server should not receive more than 60,000 events per second in a steady stream. The rate of events from a computer depends very much on the number of data sources that are processed on that computer.

For example, a collection of about 3000 computers with 5 data sources each, 4 events per second per data source, produces a combined stream of 60,000 events per second. This is a load that a 16-core InTrust server with SSD storage and 16GB of memory should handle without problems.

Tips on avoiding excessive workload on a server:

- Keep track of how many computers there are per InTrust server.
- Add InTrust servers if necessary.
- Assign different servers to different collections.
- Distribute the computers among your collections evenly.

**! CAUTION:** When adding an InTrust server to your existing organization, you should run InTrust setup under an account that can manage the InTrust configuration. The account used for installing the first InTrust server automatically has these privileges. To add InTrust organization administrators, in InTrust Deployment Manager click Manage | Configure Access. Of course, to add organization administrators, you must be an organization administrator yourself.

# Example: Configuring Logon and User Session Auditing

InTrust lets you gather two types of data related to users logging on and off computers:

1. Native Windows Security log events  
These events provide basic logon and logoff information, but contain no indication of the user's presence in the system at any particular time. They only capture the act of logging on and off, and their reliability is limited.
2. User session events enabled by InTrust  
These advanced events contain enough information to help you track not only logons and logoffs, but also when users are actively using computers. For example, they indicate the exact times and durations of terminal sessions connected to domain controllers. User session events are logged locally on computers that have the InTrust agent installed and are processed by collections where the "InTrust User Session Tracking" data source is enabled.

For logon and user session tracking to be complete, make sure both the "Windows Security Log" and "InTrust User Session Tracking" data sources are enabled in your collections. For details about enabling data sources, see [Managing Collections](#).

## Start Gathering

For the purposes of this topic, configure logon event gathering only from domain controllers. Take the following steps:

1. Right-click **Collections** and select **New Collection**.
2. On the General Properties step, give the collection a name indicating that it contains domain controllers.
3. Proceed to the Specify Computers step of the wizard, and add your domain controllers to the list. Make sure the **Install agents automatically** option is selected.
4. On the Data Sources and Repository step, make sure the "Windows Security Log" and "InTrust User Session Tracking" data sources are enabled.
5. Complete the steps.

After this, agents are installed on the domain controllers, and gathering starts automatically.

If you want to watch other computers in addition to or instead of domain controllers (for example, Exchange or file servers), create a new collection and add all the computers you need to it. Configure the gathering options for this collection likewise.

## Put Auditing to a Test

To confirm that auditing is working as intended, deliberately perform some of the activity you are watching for on the computers you are watching. Do any of the following:

- Log on to the computers included in the collection and log off
- Lock and unlock the computers
- Set a low screensaver timeout to cause the screensaver to start
- Switch the user

Next, check that your actions have been captured in the repository.

## View the Results in Repository Viewer

The InTrust Repository Viewer application lets you explore and analyze the contents of InTrust repositories. To browse the repository you have been collecting to, run Repository Viewer from the Start menu, and click **File | Open Repository**.

In the dialog box that opens, select the **Production repository** option, and proceed to specify the repository you have been working with.

**i** | **NOTE:** A *production repository* is a repository that is available in InTrust Deployment Manager or InTrust Manager. For details about production and idle repositories, see [Repository Connections](#).

The left pane of the Repository Viewer console shows:

- A navigation tree that organizes events by domain and log type
- A collection of predefined search folders with preconfigured popular filters for quick event analysis

You can select any of the search folder nodes or any of the repository hierarchy nodes, and view the events they contain by clicking the **Go** button. For the purposes of this document, the following predefined searches are useful:

- Searches in the **Logons** subfolders of the topmost search folders
- Searches in the **User sessions** subfolders of the topmost search folders

Select one of these searches and click **Go**. If events about your activity are displayed in the right pane, then auditing has been set up correctly.

For detailed Repository Viewer documentation, see [Searching in Repositories with Repository Viewer](#).

# Further Reading

This guide dealt with the default InTrust configuration. If you are interested in other InTrust capabilities and alternative workflows, or if you need in-depth information about the topics covered here, go to the [InTrust online documentation library](#).

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](http://www.quest.com).

## Contacting Quest

For sales or other inquiries, visit [www.quest.com/contact](http://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 enables 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