

Quest® InTrust 11.4.2

Understanding InTrust Repositories



© 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 Understanding InTrust Repositories

Updated - September 2020

Version - 11.4.2

Contents

Introduction to InTrust Repositories	4
Repository Types	5
File-Based Repositories	5
Centera-Based Repositories	5
Centera Clusters	6
Centera Nodes and Their Roles	6
Centera Security Model	6
Centera Retention Policy	6
Centera Access	7
Repository Structure Integrity	7
Repository Connections	8
Creating and Editing Repositories	9
Centera Connection and Security Settings	10
Centera Retention Policy	10
Repository Indexing Configuration	11
Cloning Repositories	12
Repository Tools	13
Converting EVT Files to Repository Format (Evt2Repository.exe)	13
Removing Repositories (ITRepositoryRemover.exe)	15
Restoring Events in Native Format (ITEventExtractor.exe)	15
Restoring Centera-Specific References (ServiceFolderRestorer.exe)	17
About us	18
Contacting Quest	18
Technical support resources	18

Introduction to InTrust Repositories

The repository is the primary type of audit data store in InTrust. The other type is the audit database. Repositories are intended for long-term archiving of data in a compressed format. You can do the following with an InTrust repository:

- View its contents in InTrust Repository Viewer
- Generate reports from the contents in Repository Viewer
- Use it as the source of data for an import job
- Use it as the source or the target for a consolidation job
- Clear unnecessary data from it using repository cleanup jobs

Repository Types

There are two types of repositories in InTrust: file-based and Centera-based.

- File-based repositories are specially organized structures of folders and compressed files.
- Centera-based repositories use EMC Centera™ devices for storage.

File-Based Repositories

File-based repositories can store large amounts of data (because it is compressed), and they have a hierarchical structure, which ensures fast access and easy data selection and retrieval.

Repositories of this type differ from arbitrary file system hierarchies in that they contain files with very long paths and need specialized tools for handling. This means that some generic file and folder operations may not work with file-based repositories. For example, it is not recommended that you copy a repository to another location as you would a regular folder or share. For information about copying and backing up repositories, see the [Cloning Repositories](#) topic in this document.

Centera-Based Repositories

Centera is a powerful networked storage solution that integrates hardware and software components. Audit data is one of the types of data that Centera is designed for. Event records must remain unchanged once they are created, they need to be retained as long as compliance regulations specify, and they should always be readily available.

To successfully set up Centera-based repositories, an InTrust administrator should at least be familiar with the basic concepts described below, which have a direct bearing on interoperability between InTrust and Centera. For additional information, refer to the Centera documentation.

Centera offers the following advantages over file-based repositories:

- Data integrity—data is guaranteed to remain unmodified
- Data protection—due to flexible retention policies, only expired data is cleared
- Data safety—Centera provides failover capabilities ensuring that no data is lost; this is achieved through redundancy
- High scalability
- Streamlined performance
- Reliability
- Additional application-level security

Centera Clusters

A cluster is the largest physical unit of a Centera storage. Clusters are made up of cubes. Cubes contain between 4 and 32 nodes, which are the smallest physical elements.

Failover facilities are cluster-wide, meaning that you ensure failover for the entire cluster rather than specific nodes.

Centera Nodes and Their Roles

A node is a physical device that can be represented by a network identity and can act as an interface between the network environment outside the Centera cluster and the data stored in the cluster.

Whether the node can provide this interface depends on the role it is assigned. The following roles are available for Centera nodes:

- Access role
- Storage role

Nodes with the access role are gateways to the data stored in Centera. These nodes have IP addresses on the network and are responsible for authentication. If you successfully connect to one such node, you have access to the entire cluster. However, to connect faster, you can specify several available nodes with the access role.

Applications such as InTrust use these nodes to access the storage facilities. The properties of a Centera-based InTrust repository include the IP address of the Centera node with the access role that provides data access.

Centera Security Model

Centera is designed for access by applications, not by security principals. For this reason, security is configured on a per-application basis and does not involve any accounts in the environment.

Centera authorization is also built around this model. Centera provides application profiles that determine which data is made available to specific applications.

The Centera cluster must have an application profile for InTrust before any jobs can use the Centera-based repository. The properties of a Centera-based InTrust repository include settings for all supported authentication methods.

For more information, see the [Creating and Editing Repositories](#) topic.

Centera Retention Policy

Centera associates retention periods with the data it stores, based on the properties of the data. A retention period is the period after which the data can be deleted by an application that works with it.

Retention models differ depending on the Centera edition: Basic, Compliance Edition Plus, and Governance Edition. For more information, refer to the Centera documentation.

The properties of a Centera-based InTrust repository include retention period settings. For more information, see the [Creating and Editing Repositories](#) topic.

Differences from File-Based Repositories

Working with Centera-based repositories is essentially the same as working with file-based repositories. You can select the type—file-based or Centera-based—when you create a repository. Further settings depend on the repository type you select.

Although there are differences in repository properties, the auditing workflow is uniform for both types. Whichever type of repository you create, you can use it in any job that involves repositories. You cannot convert one repository type to another. However, you can use InTrust consolidation jobs to relocate data.

From the user perspective, the difference is that Centera-based repositories cannot be viewed in InTrust Repository Viewer. Instead, use the Legacy Repository Viewer MMC snap-in shipped with InTrust.

Centera Access

A Centera-based repository is a split structure that has two parts:

- Actual Centera node
- Service folder, which is a network share with InTrust-generated data for data referencing

The service folder does not contain actual audit data, but redirects InTrust to the Centera node and helps perform read and write operations. This service data cannot be located in the Centera node, because this contradicts Centera's data immutability requirement.

Therefore, connecting to a Centera-based repository is different from connecting to a file system-based repository. To access Centera, InTrust must have access to both of the locations.

Repository Structure Integrity

Although a Centera-based repository is made up of two parts, it should be considered a single unit. The service folder must always reference data in the same Centera cluster; otherwise, the data will become unavailable.

For example, the properties of a Centera-based repository must always specify access nodes that belong to the same cluster. Supplying the IP address of a node in a different cluster will not prevent gathering, but will result in data unavailability.

In addition, if the IP addresses of your Centera nodes with the access role are changed, edit the properties of your Centera-based repositories accordingly.

Repository Connections

Connections to production repositories normally occur through an InTrust server, unlike connections to idle repositories. The distinction between these two kinds of repository is as follows:

- A *production repository* is managed by an InTrust server and is available in InTrust Manager.
- An *idle repository* is not attached to any InTrust server. For example, it can be a backup copy of a production repository or a store for historical data.

For successful connections to production repositories, make sure all InTrust servers in the organization have the agent communication port (900 by default) and InTrust Server management port (8340 by default) open for inbound traffic.

Creating and Editing Repositories

Make sure that the file server where you create a new repository share has fast and reliable connections to InTrust Server.

To create a file-based repository in InTrust Deployment Manager

1. Start creating a collection or editing an existing collection.
2. On the Data Sources and Repository step of the wizard, create your repository.

To create a file-based repository in InTrust Manager

1. Expand the **Configuration | Data Stores** node.
2. Right-click **Repositories** and select **New Repository** to start the New Repository Wizard.
3. On the Repository Type step of the wizard, select **File-based storage**.
4. Complete the remaining steps.

To create a Centera-based repository (only in InTrust Manager)

1. Expand the **Configuration | Data Stores** node.
2. Right-click **Repositories** and select **New Repository** to start the New Repository Wizard.
3. On the Repository Type step of the wizard, select **EMC Centera**.
4. On the Centera Settings step, either specify a Centera connection string or select **Proceed with the wizard to define settings**.

If you select to specify settings for the connection in the wizard, the remaining steps prompt you for the following:

- Connection settings
- Security settings

These settings are described in detail below.

5. Select the location for the service folder. This is a share or local folder with files used for referencing data in the Centera storage.
6. Finish the wizard.

To edit an existing repository

- If you are using InTrust Deployment Manager, start editing a collection that gathers to the repository you want to edit, and proceed to the Data Sources and Repository step of the wizard.

- If you are using InTrust Manager, find the repository you need under **Configuration | Data Stores | Repositories** and open its properties.

The same configuration options described in the procedures above (for Centera-based repositories, also the ones detailed below) are available in the repository properties.

Centera Connection and Security Settings

The New Repository Wizard can automatically generate Centera connection strings using the values you specify.

On the Connection Settings step, specify the names or IP addresses of Centera nodes with the access role. The default port for connection is 3218; specify a different port number if necessary.

On the Security Settings step, configure the Centera authentication method InTrust must use by choosing one of the following:

- Explicit credentials (profile name and secret)
- Anonymous profile
This is a profile that does not require authentication. Although the profile is supported by InTrust, EMC does not recommend using it.
- Credentials from a .pea file
Files with the **.pea** extension store Centera authentication information.

After you have created a Centera-based repository, these settings are available in the repository's properties dialog box on the **Centera** tab.

Centera Retention Policy

Every unit of data in Centera has a retention policy associated with it. The retention policy determines how long the data is kept before it expires and can be cleared.

Centera retention policy settings for audit data gathered with InTrust are not specified during repository creation. To access retention policy settings, open the properties of a Centera-based repository, select the **Centera** tab, and click **Retention Policy**.

You have three options for audit data retention, as follows:

- No retention
This option specifies that the retention period is zero.
- Retention class
This option lets you associate InTrust data with a specific retention class defined on the Centera cluster.
- Retention period
This option lets you specify precisely how long InTrust data must be retained.

Retention policy settings have precedence over InTrust repository cleanup job settings. If you run a cleanup job on a Centera-based repository where the retention period has not yet expired for the specified data, then the data is not deleted, and the repository cleanup session will contain errors. Centera permits cleanup procedures only after the retention period has expired.

Repository Indexing Configuration

InTrust repository indexing is a big topic, described separately in [Repository Indexing for Advanced Search Capabilities](#).

Cloning Repositories

If you need to make a copy of an existing production repository (for example, an idle repository for auditors' use or for Quest Support), do not use conventional file copying or regular file managers. These methods may fail, because the hierarchical file structure in InTrust repositories uses very long names. Instead, use specialized replication software such as Microsoft Robocopy, which has been shipped with Windows since Vista and was available as part of the Windows Resource Kit before Vista.

If the repository you want to clone is indexed, take the following steps:

1. On the InTrust server that processes the repository, stop the **InTrust Server** service.
2. Make a copy of the repository using replication software.
3. Start the **InTrust Server** service again.

Alternatively, if you are retiring a production repository and want to relocate it, you can do the following:

1. In InTrust Manager, delete the repository.
2. Make a copy of the repository using replication software.

If you want to convert the idle clone into a production repository, create a new repository in InTrust, and in the New Repository wizard, specify the location of the cloned repository.

Repository Tools

The following command-line utilities provide additional capabilities when working with repositories:

- Directly convert EVT files to repository format: [Evt2Repository.exe](#)
- Remove a repository: [ITRepositoryRemover.exe](#)
- Restore events in their native format: [ITEventExtractor.exe](#)
- Restore references in a Centera-based repository: [ServiceFolderRestorer.exe](#)

Converting EVT Files to Repository Format (Evt2Repository.exe)

This tool places events from an event log file to a repository without actually gathering data. Run the tool on a computer with InTrust Server installed.

Evt2Repository.exe is located in `<InTrust_installation_folder>\Server\InTrust`.

The following table lists the required parameters.

OPTION	DESCRIPTION
/FILE	Full path to the source EVT file. UNC paths are accepted.
/DOMAIN	NetBIOS name of the domain that contains the computer to which the events in the EVT file are related.
/COMPUTER	NetBIOS name of the computer from which the EVT file is retrieved.
/LOGNAME	Name of the Windows event log that the EVT file contains.
/REPOSITORY	UNC path to the InTrust repository where the events must be stored.

Example:

```
Evt2repository.exe /file=\\SERVER\TEMP\security01.evt /domain=RND /computer=SERVER /logname=Security /repository=\\Server01\InTrustRepository\Default
```

The following table lists optional parameters.

OPTION	DESCRIPTION
/VERSIONMAJOR	Major OS version for the computer from which the EVT file is retrieved.

OPTION	DESCRIPTION
/VERSIONMINOR	Minor OS version for the computer from which the EVT file is retrieved.
/COMPUTERTYPE	Type of the computer from which the EVT file is retrieved, as returned by LAN Manager. Only numeric values are accepted.
/TIMEZONE	Positive or negative difference in minutes between GMT and the local time of the computer from which the EVT file is retrieved. For example, "/timezone=-180" will return the GMT-3 time zone.
/PROPERTIESFROM	<p>If some of the optional parameters are not specified, this key defines in what order to retrieve these parameters. The following sources are available:</p> <ul style="list-style-type: none"> • REPOSITORY—If there are any events in the InTrust repository from the computer from which the EVT file was saved, all necessary information is taken from the repository. • ORIGINALCOMPUTER—NetBIOS name of the computer from which the EVT file was saved (specified in the /COMPUTER parameter). • CURRENTCOMPUTER—Computer on which the EVT file is located. <p>Example:</p> <pre>Evt2repository.exe /propertiesfrom=repository,originalcomputer</pre> <p>If this parameter is not specified, the "repository, currentcomputer" sequence is assumed.</p>
/RESOLVEDESCRIPTIONS	<p>Specifies whether to resolve event descriptions and where to take the information. Possible values are as follows:</p> <ul style="list-style-type: none"> • LOCALONLY Descriptions are resolved using the current computer's libraries. • REMOTEONLY Descriptions are resolved using libraries from the computer specified in the /COMPUTER parameter. • REMOTEFIRST Descriptions are resolved using libraries from the computer specified in the /COMPUTER parameter as long as they are available. Otherwise, the current computer's libraries are used. • LOCALFIRST Descriptions are resolved using the current computer's libraries. Otherwise, libraries from the computer specified in the /COMPUTER parameter are used. <p>The Category field is resolved for events only if you use the /RESOLVEDESCRIPTIONS option.</p>
/RESOLVESTRINGS	Specifies whether to resolve GUIDs found in event insertion strings into object names (user names, GPO names and so on).

Removing Repositories (ITRepositoryRemover.exe)

If you need to delete a repository physically, use the specially designed **ITRepositoryRemover.exe** command-line utility shipped with InTrust. (Windows tools do not let you delete a repository easily.) The utility resides in **<InTrust_installation_folder>\Server\InTrust**.

Before you run the repository removal utility, remove the repository from the InTrust configuration. For that, delete it in InTrust Manager or InTrust Deployment Manager. You may have to wait until the repository services to stop working with the repository and unlock all the locked files in it. How long you need to wait depends on the repository size and how many other repositories there are.

i NOTE:

- To confirm that the repository contents can be safely deleted, look in the InTrust Server log for the latest events from this repository. If there have been no indexing or merging events for this repository for two minutes, then you can proceed with the deletion.
- The utility removes only the audit data in the repository. The repository folder is not deleted. If the repository is indexed, the index also remains intact. You can safely remove the index and the folder with regular Windows tools.

Next, launch the utility:

1. Start the command prompt.
2. Use the `cd` command to specify the directory containing **ITRepositoryRemover.exe** as the working directory.
3. Run the command, supplying your repository path as a parameter and optionally `/y`, if you want to confirm the deletion without a prompt. For example:

```
ITRepositoryRemover.exe d:\Repositories\Repository2012 /y
```
4. Press **ENTER**.

If you start **ITRepositoryRemover.exe** without any parameters, it will display information about the correct usage of the utility.

Restoring Events in Native Format (ITEventExtractor.exe)

If you need to view audit trails in their native format, use the **ITEventExtractor.exe** command-line utility shipped with InTrust.

- ## **i** NOTE:
- Events that were filtered out when data was gathered to a repository will not be present in the extracted log files.

To use the **ITEventExtractor.exe** utility

1. Start the command prompt.
2. Use the `cd` command to specify the directory containing **ITEventExtractor.exe** as the working directory. The utility resides in **%ProgramFiles%\Common Files\Quest\InTrust** (on 64-bit systems, in **%ProgramFiles(x86)%\Common Files\Quest\InTrust**).
3. Type **ITEventExtractor.exe <parameters>**.
4. Press **ENTER**.

The syntax depends on the environment to which the required audit trails are related.

Microsoft Windows:

```
ITEventExtractor /REPPATH:<Path> /LOGNAME:<Name> /COMPUTER:<Computer> /FILE:<FileName>
/DOMAIN:<Domain> [/SRVPORT:protocol:server[port]] [/DATEFROM:<Date>] [/DATETO:<Date>]
```

PARAMETER	DESCRIPTION
/REPPATH:	UNC path to the repository from which to extract the events.
/LOGNAME:	Specifies the logs that contained the events you need.
/COMPUTER:	The computers from which the events you need were retrieved. When specifying several computer names, separate them with white spaces.
/FILE:	The path to the file to which the utility writes information.
/DOMAIN:	The name of the domain or domains that include computers from which the events you need were retrieved.
/SRVPORT:	The communication port and protocol, and the server that processed the events you need.
/DATEFROM:	Date in MM/dd/YY or MM/dd/YYYY:HH:mm format; events recorded before this date are ignored. If you omit this parameter, events are extracted starting with the earliest.
/DATETO:	Date in MM/DD/YY or MM/dd/YYYY:HH:mm format; events recorded after this date are ignored. If you omit this parameter, events up to the latest are extracted.

Unix:

```
ITEventExtractor /REPPATH:<Path> /LOGNAME:<Name> /HOST:<Object> /FILE:<:FileName>
[/SRVPORT:protocol:server[port]] [/DATEFROM:<Date>] [/DATETO:<Date>]
```

PARAMETER	DESCRIPTION
/REPPATH:	UNC path to the repository from which to extract the events.
/LOGNAME:	Specifies the logs that contained the events you need.
/HOST:	The hosts from which the audit trails you need were retrieved. When specifying several hosts, separate them with white spaces.
/FILE:	The path to the file to which the utility writes information.
/SRVPORT:	The communication port and protocol, and the server that processed the events you need.

PARAMETER	DESCRIPTION
-----------	-------------

/DATEFROM:	Date in MM/dd/YY or MM/dd/YYYY:HH:mm format; events recorded before this date are ignored. If you omit this parameter, events are extracted starting with the earliest.
------------	---

/DATETO:	Date in MM/DD/YY or MM/dd/YYYY:HH:mm format; events recorded after this date are ignored. If you omit this parameter, events up to the latest are extracted.
----------	--

i | **NOTES:**

- Do not type spaces between a parameter's variable and invariable parts (/REPPATH: \\Server01\InTrustRepository\Default is incorrect).
- If the variable part of a parameter contains spaces, put quotation marks around it (/COMPUTER:Stone Wilson is incorrect; /COMPUTER:"Stone Wilson" is correct).

Restoring Centera-Specific References (ServiceFolderRestorer.exe)

The **ServiceFolderRestorer** command-line utility recreates the contents of the service folder used by a Centera-based InTrust repository. The service folder is used for referencing Centera clips created within the time range you specify, without checking whether those clips are referenced from anywhere else. You can use this to restore damaged service folders.

The utility is located in **<InTrust_installation_path>\InTrust\Server\InTrust**. Use the following syntax:

```
ServiceFolderRestorer.exe <path> <pool> ["<start time>"] ["<end time>"] [/y]
```

PARAMETER	DESCRIPTION
-----------	-------------

<path>	The path to the service folder of the Centera-based repository; the supporting file structure is created automatically.
--------	---

<pool>	The Centera connection string (for example, 212.3.248.12:3128?c:\mercom.pea)
--------	--

<start_time> and	Optional parameters that specify the time range of the Centera clips you are interested in. These times must be in YYYY.MM.DD hh:mm:ss format.
---------------------	---

<end_time>	Mind that these times reflect when the clip was created in the Centera storage, not when the gathered events occurred.
------------	--

/y	Optional parameter that enables silent mode.
----	--

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 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