Quest®

Quest® InTrust 11.3.1

Connector for Microsoft System Center Operations Manager User

Guide

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 Connector for Microsoft System Center Operations Manager User Guide
Updated - October 2017
Version - 11.3.1

Contents

Introduction to InTrust Connector for Operations Manager

InTrust Connector for Microsoft System Center Operations Manager (Operations Manager) 2007/2012 helps establish a single, comprehensive workflow for managing your Windows-based network.

With InTrust Connector for Operations Manager you can integrate the InTrust capabilities of tracking the business-critical security events into the existing enterprise-wide system of network operations management.

The product consists of the following components:

- InTrust Connector for Operations Manager
  A bridge forwarding alerts from InTrust to Operations Manager. It optionally can forward updates to the alerts from Operations Manager back to InTrust.
- InTrust Connector Management Pack
  Required for InTrust Connector's operation.

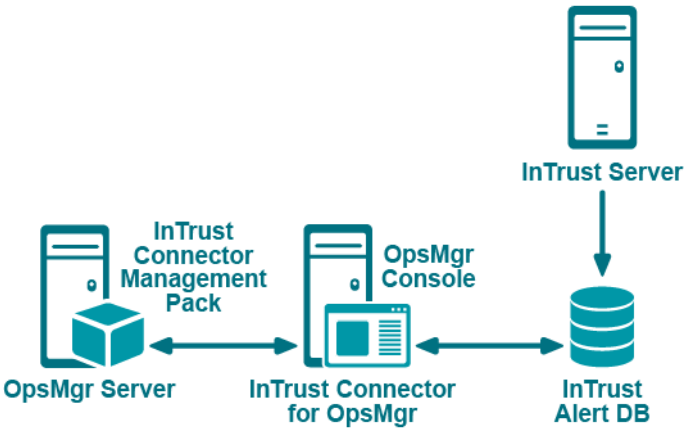
How It Works

InTrust Connector for Operations Manager allows you to forward alerts stored in the InTrust Alert database to Operations Manager so that personnel in charge can view and resolve the alerts using the Operations Manager user interface. The workflow is implemented through InTrust, InTrust Connector for Operations Manager, and Operations Manager.

NOTES:

- You can install these components using any deployment scheme that suits your network environment and meets the system requirements listed in this document. For example, to evaluate the solution in a test lab, you can install all required components on a single computer.
- A dedicated InTrust Connector is used to forward alerts from a single Alert database, so you must deploy a separate InTrust Connector instance for each Alert database you want to forward alerts from.

A sample deployment is shown in the figure below.



The steps in the process are as follows:

1. To provide for interaction between Operations Manager and InTrust Connector, a specially developed Management Pack is installed on the Operations Manager Server.
2. Alerts are generated by InTrust upon certain conditions. InTrust Server stores alerts in the InTrust Alert database.
3. InTrust Connector service scans this database, applying filters to the alerts (i.e., selecting them by severity or other criteria). Selected alerts are forwarded to Operations Manager to be processed by personnel in charge.
4. During alert forwarding process, the InTrust Connector Management Pack maps InTrust alert fields into Operations Manager alert record fields; then this record is stored to the Operations Manager database. Alert field mapping is described in the Alert Field Mapping topic.

NOTE: Alert states are adjusted after the initial synchronization completes. Until then, the original state value is kept in the alert record's custom field #9. For details, see the Working with Alerts topic.

5. An authorized operator views and resolves the alert received, changing the alert's status in the Operations Manager console.
6. Alert information is updated in both the Operations Manager and InTrust databases. InTrust Connector is subscribed to the alerts it has created and stored to the Operations Manager database (they are identified by the Connector GUID stored in the alert record's custom field #10). InTrust Connector service periodically scans the Operations Manager database and retrieves information about any alerts modified since the last scan.
7. The information retrieved is used to adjust alert state, as follows:
    - If no status changes were made by the Operations Manager operator, then the status is set to the value kept in custom field #9 (initially received from InTrust).
    - Otherwise, the status is set in accordance with the value entered by the operator.
8. Changes to alert states in Operations Manager are optionally synchronized back to InTrust by the Connector.

NOTE: If an alert is forwarded to Operations Manager by InTrust Connector and then changes were made to the alert state using InTrust Monitoring Console, these changes will not be forwarded to Operations Manager.

You can configure the alert synchronization by running InTrust Connector Configuration Wizard. In particular, it helps you to do the following:

- Specify connection settings for the Connector to access InTrust Alert database
- Select the alerts that should be synchronized by applying filters
- Set up the alert synchronization process (i.e., select whether to forward the alerts only from InTrust to Operations Manager, or to synchronize them back to InTrust)

NOTE: By default, the alerts displayed in the Operations Manager Console can have a state of either 'New' or 'Closed', while the InTrust alert status can be “New”, “Acknowledged”, or “Resolved”. Therefore, to properly process the alerts, you may need to assign a custom state that will present the Acknowledged InTrust alerts displayed in Operations Manager. For details, refer the Configuring InTrust Connector for Operations Manager topic.

Contents of the Package

The solution package includes the following:

- **ITC4SCOM.<version>.msi**—the InTrust Connector installation file
- **System.Connectors.Library.InTrustIntegration.xml**—InTrust Connector Management Pack
- **InTrust Connector for Microsoft System Center Operations Manager User Guide**—this document
- **Readme.htm**—last-minute product information and updates to the documentation

Using InTrust Connector for Operations Manager

Software Requirements

For InTrust Connector installation and functioning, your network environment must meet the following requirements:

- InTrust Server (remote or local)
- Microsoft System Center Operations Manager 2007 or Microsoft System Center Operations Manager 2012 (remote or local)
- One of the following must be installed on the computer where InTrust Connector will be deployed:
    - Management Server component of Operations Manager
    - Operations Console
    - Authoring Console for SCOM 2007
- Microsoft SQL Server Native Client 11.0.6538.0 or later (version 11.0.6538.0 redistributable package of the client is included in the InTrust distribution)

User Rights

InTrust OpsMgr Connector Admins Group

To allow a user to configure InTrust Connector (apply filters to the alerts that should be forwarded, set up alert forwarding process, etc.), you must add the user's account to the **InTrust OpsMgr Connector Admins** local group. This group is automatically created on the computer where InTrust Connector is installed, and the group is granted the permissions described in the Connection to Alert Database and Operations Manager Server topic.

The following accounts are added to the InTrust OpsMgr Connector Admins group during installation:

- Service account (specified during installation) under which InTrust Connector for Operations Manager service (**ITConOpsMgrService**) will run
- User account under which the installation is performed

NOTE: The **InTrust OpsMgr Connector Admins** group is not removed when you uninstall InTrust Connector; you need to remove it manually.

The **InTrust OpsMgr Connector Admins** group is granted the following permissions:

- For the ***<InTrust Connector working folder>*\ITConMOM.xml** file where the connector's configuration is stored:
  - Read
  - Write
  - Append Data
  - Read Extended Attributes
  - Write Extended Attributes
  - Execute
  - Read Attributes
  - Write Attributes
  - Read Permissions
  - Synchronize

NOTE: The **Synchronize** permission is not displayed in the standard Properties window. To show it, use the **Subinacl.exe** utility available from the Resource Kit.

- For the **HKEY_LOCAL_MACHINE\SOFTWARE\Dell\InTrust Connector for SCOM** registry entry:
  - Query Value
  - Set Value
  - Enumerate Subkeys
  - Notify
  - Read Control
- For the InTrust Connector service (**ITConOpsMgrService**):
  - Start
  - Stop
  - Query Status
  - Read Control

NOTE: When granting the necessary permissions manually, clear the **Allow inheritable permissions from parents to propagate to this object** check box.

Connection to Alert Database and Operations Manager Server

To connect to the InTrust Alert database, InTrust Connector can use either the ITConOpsMgrService account (supplied during the setup) or a specific different account (which you can supply using the Configuration Wizard). Whatever account is used, it should be assigned the following:

1. **db_datareader** and **db_datawriter** SQL Server roles for the alert database
2. **InTrust Real-Time Monitoring** or **InTrust Monitoring Console** roles (which are created during InTrust setup) for the alert database

If specific Windows account will be used to access the Alert database (see the Configuring InTrust Connector for Operations Manager topic for details), then it also must be granted the **Log on as a batch job** right.

The account used for connecting to the Operations Manager server must be a member of the domain global group included in the **Operations Manager Administrators** role (this group is created during Operations Manager setup).

Installing InTrust Connector for Operations Manager

- Step 1: Install InTrust Connector Management Pack
- Step 2: Install InTrust Connector
- Unattended Installation

Step 1: Install InTrust Connector Management Pack

Prior to installing InTrust Connector, you should deploy the specially designed InTrust Connector Management Pack (**System.Connectors.Library.InTrustIntegration.xml**) on your Operations Manager server. This Management Pack is required for InTrust Connector operation.

To deploy the Management Pack

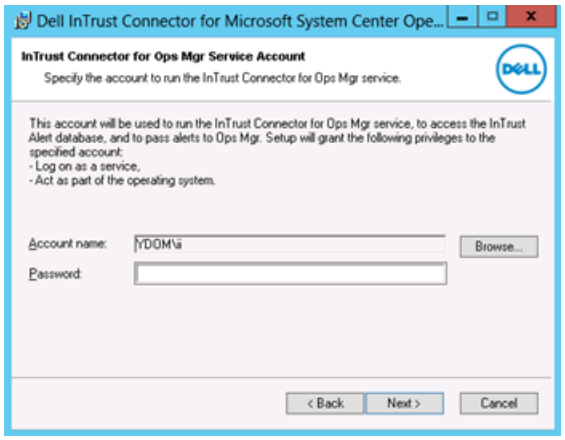
1. In the Operations Manager console, go to the Administration page and select **Management Packs**.
2. Right-click the node and select **Import Management Packs**. In the **Select Management Pack to import** dialog box, browse to the **System.Connectors.Library.InTrustIntegration.xml** file, and click **OK**. When imported, it appears in the list of Management Packs on the right.

Step 2: Install InTrust Connector

NOTE: The account under which you run the setup will automatically be added to the InTrust OpsMgr Connector Admins group on the computer where InTrust Connector is installed.

To install InTrust Connector for Operations Manager

1. Run the **ITC4SCOM.<*version*>.msi** file. The InTrust Connector for Operations Manager Installation Wizard starts.
2. Select InTrust Connector for Operations Manager to be installed. Change the installation folder, if necessary.
3. On the next step, you will be prompted for the account under which the InTrust Connector service will run, connecting to Operations Manager and InTrust Alert database. Provide the account in **DOMAIN\username** format.
   Make sure the account you supply meets the requirements stated in the Connection to Alert Database and Operations Manager Server topic.



4. Review the settings you have specified and complete the wizard. To configure InTrust Connector for Operations Manager immediately after the installation, select the **Run configuration wizard now** check box.

Unattended Installation

Installation Using Command Prompt

You can install InTrust Connector for Operations Manager from a command prompt, as shown below:

```
Msiexec.exe /q[n|b|r|f] /i IT4SCOM.<version>.msi
IT_SCOM_SVC_USER=ABC\MJack IT_SCOM_SVC_PASSWORD=abc
```

Here:

- **/q**—specifies the user interface level to be used by the program:
  - **n**—no UI
  - **b**—basic UI
  - **r**—reduced UI
  - **f**—full UI (default)
- **IT_SCOM_SVC_USER**—specifies the service account name
- **IT_SCOM_SVC_PASSWORD**—specifies the password of the service account

Installation Using Group Policy

InTrust Connector for Operations Manager can also be installed using Group Policy (administrative installation).

The command prompt for administrative installation looks like this:

```
Msiexec.exe /A IT4SCOM.<version>.msi

IT_SCOM_SVC_USER=ABC\MJack IT_SCOM_SVC_PASSWORD=abc
```

Here:

- • IT_SCOM_SVC_USER—specifies the service account name
- • IT_SCOM_SVC_PASSWORD—specifies the password of the service account

CAUTION: If the InTrust Connector service is installed using Group Policy, it will be run on the target computer under the account specified in that command prompt.

Configuring InTrust Connector for Operations Manager

Before You Begin: Preparing a Custom Alert State

This section describes an optional procedure you can follow if you want the full range of InTrust alert resolution states to be represented in Operations Manager Console.

By default, the alerts displayed in the Operations Manager Console can have one of the following states:

- New
  State ID= 0
- Acknowledged
  State ID= 249
- Closed
  State ID = 255

The InTrust alert status also can be New, Acknowledged, or Closed.

You may want to assign a custom state that will represent the Acknowledged InTrust alerts displayed in the Operations Manager console. Otherwise, both New and Acknowledged states of InTrust alerts will appear in the Operations Manager Console as New.

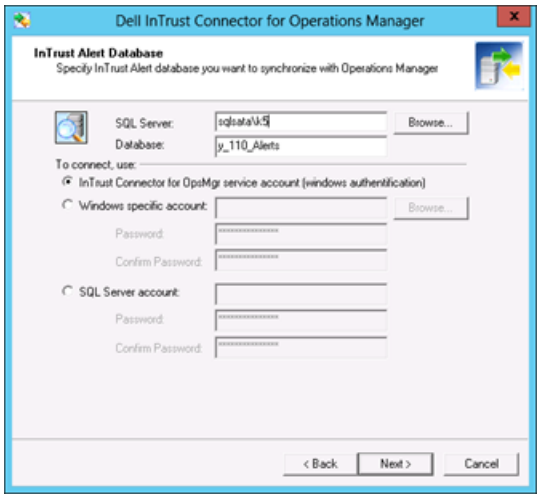
Running Configuration Wizard

To help you set up InTrust Connector for Operations Manager, the Configuration Wizard is launched automatically if you select the **Run configuration wizard now** check box during the setup. Alternatively, you can

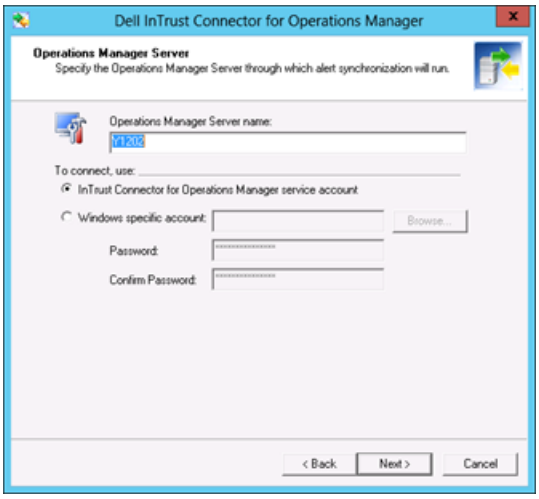
run the Configuration Wizard using the InTrust Connector for Operations Manager shortcut at **Start | Programs | Quest | InTrust | InTrust Connector for OpsMgr**.

To configure InTrust Connector for Operations Manager

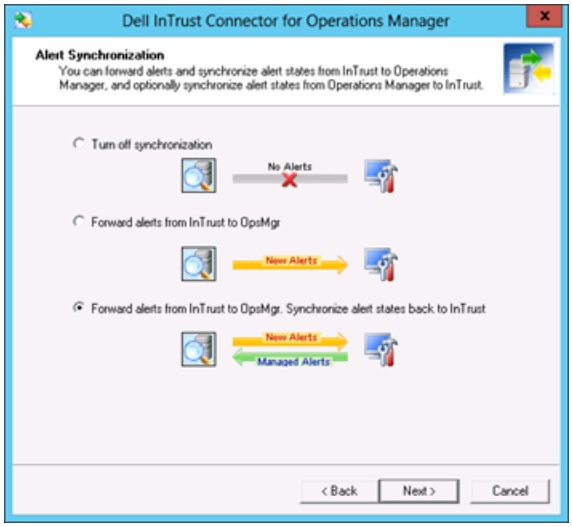
1. On the **InTrust Alert Database** step of the Configuration Wizard, specify the Alert database location and name, and the account that should be used for connection. You can use either the InTrust Connector service account (specified during its setup) or another account with sufficient rights (see the Software Requirements and User Rights topics).



2. On the Operations Manager Server step of the wizard, specify the following:
   - The Operations Manager Server to connect to.
   - The account to be used for connection. You can use either the InTrust Connector service account (specified during its setup) or another account with sufficient rights. If you select the **Windows specific account** option, then you can click **Browse** to look for the account you need (otherwise, this button is inactive).

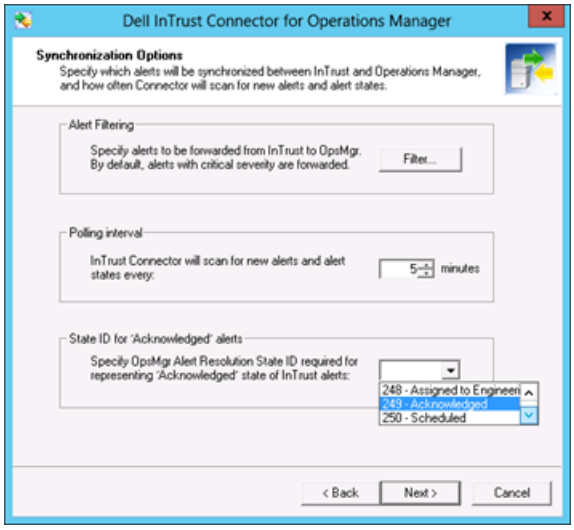


3. Next, specify the InTrust Connector operation mode:

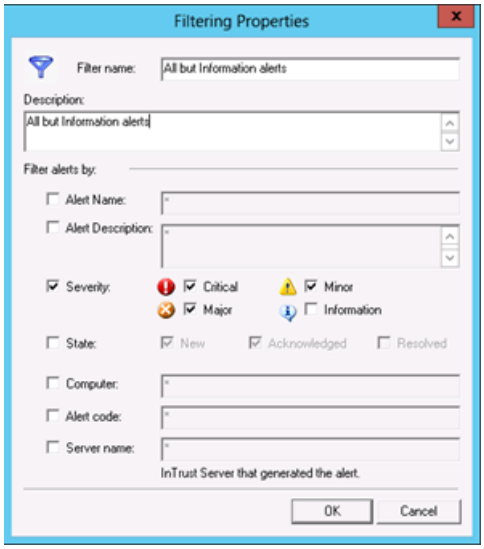


- Select **Forward alerts from InTrust to OpsMgr. Synchronize alert states back to InTrust** to receive the alert state back into InTrust.
- Select **Forward alerts from InTrust to OpsMgr** if you want to have InTrust alerts forwarded to Operations Manager (alert states will not be synchronized back to InTrust).
- Select **Turn off synchronization** if you want to cancel alert forwarding to Operations Manager.

4. On the next step, specify the synchronization options.



Click **Filter** to configure the criteria for selecting alerts to be forwarded to Operations Manager. The Filtering Properties dialog box is displayed:

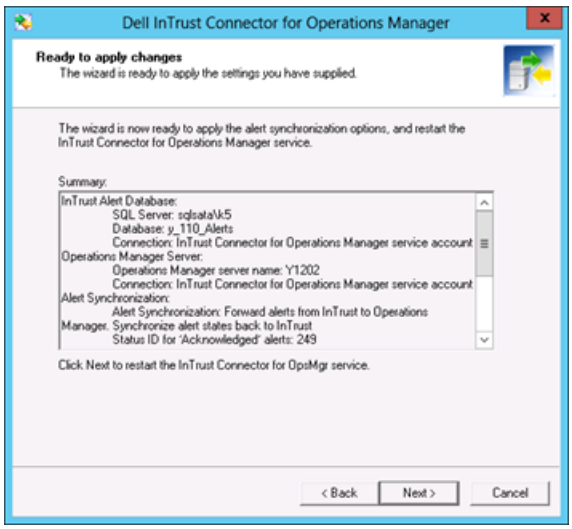


Here you can select which alerts to synchronize. Consider using wildcards (asterisks or question marks) in the filtering criteria, as well as Transact-SQL wildcard characters (described in the LIKE (Transact-SQL) MSDN article).
InTrust Connector will forward any alert containing a custom field with the field name **ForwardToMOM**, regardless of the filter settings.
After setting the filters, click **OK** to save them and return to the **Synchronization Options**.

   a. Specify how often InTrust Connector will scan the InTrust Alert database for new alerts to be forwarded to Operations Manager.

b. Specify which Operations Manager State ID will be used to represent the Acknowledged state of InTrust alerts. By default, this value is set to 0 (i.e., the Acknowledged alert will be represented as New in Operations Manager Console). If you configured a custom value for it before starting the wizard (as described in the Before You Begin: Preparing a Custom Alert State topic), select it from the list.

5. On the next step, review your configuration settings:

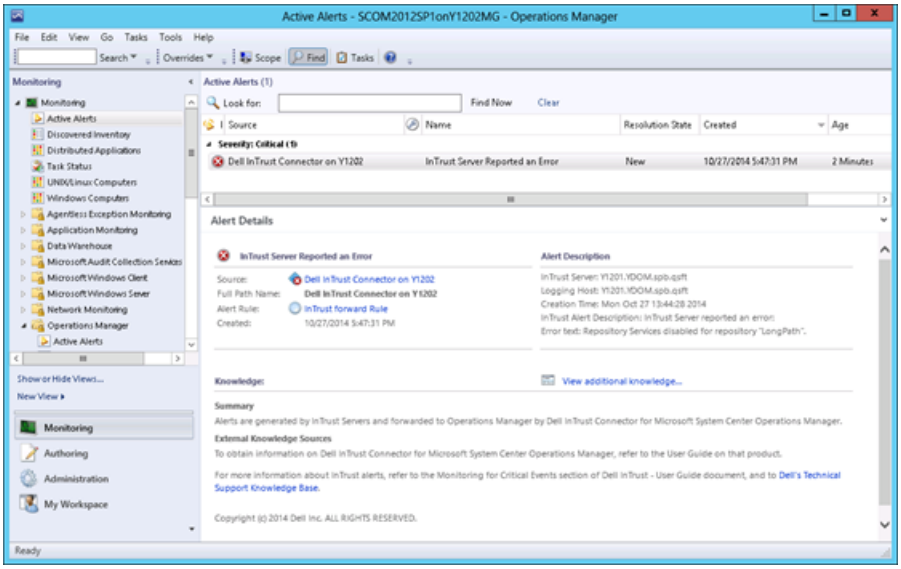


6. Click **Next** to apply the configuration; wait until the service is restarted, and then finish the wizard.

Working with Alerts

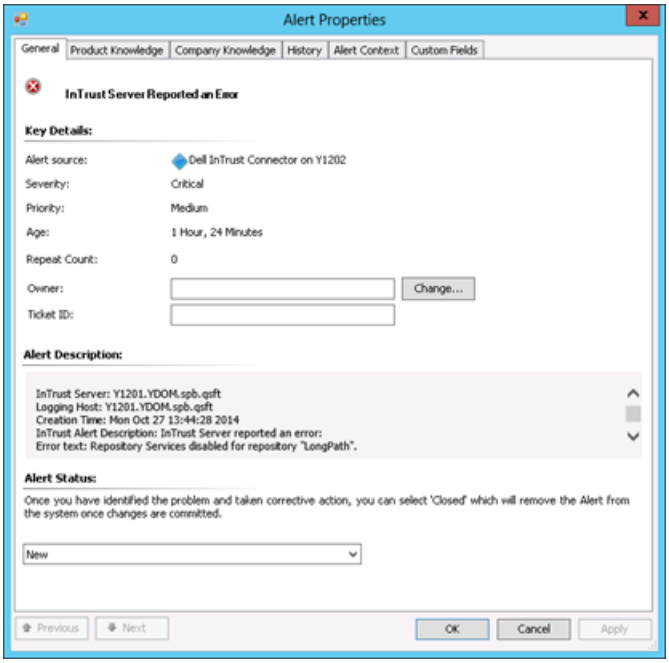
Alert View Interface

To view the alerts forwarded from InTrust, use the Operations Manager console. After you select **Monitoring | Active Alerts**, they will be displayed as shown below:



You can examine each alert in detail after opening by double-clicking it to open its properties.

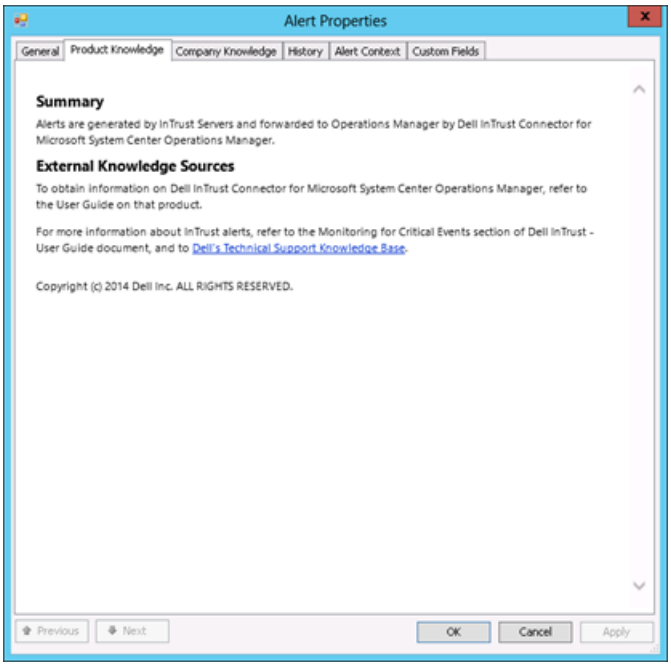
Alert Properties—General



Here you can find general information about the alert, including its severity, description, status, etc.

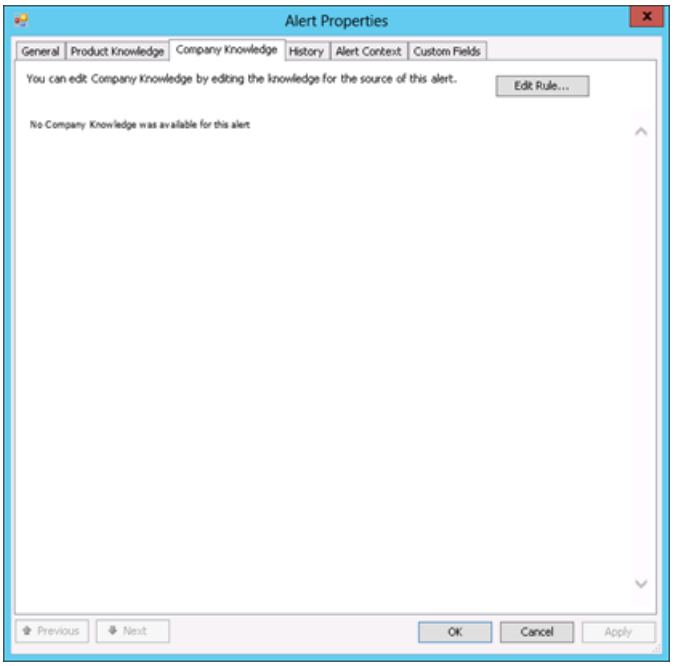
NOTE: When an alert is forwarded to Operations Manager, the Alert Source field value is set to **Quest InTrust Connector on <*Connector_host_name*>**.

Alert Properties—Product Knowledge



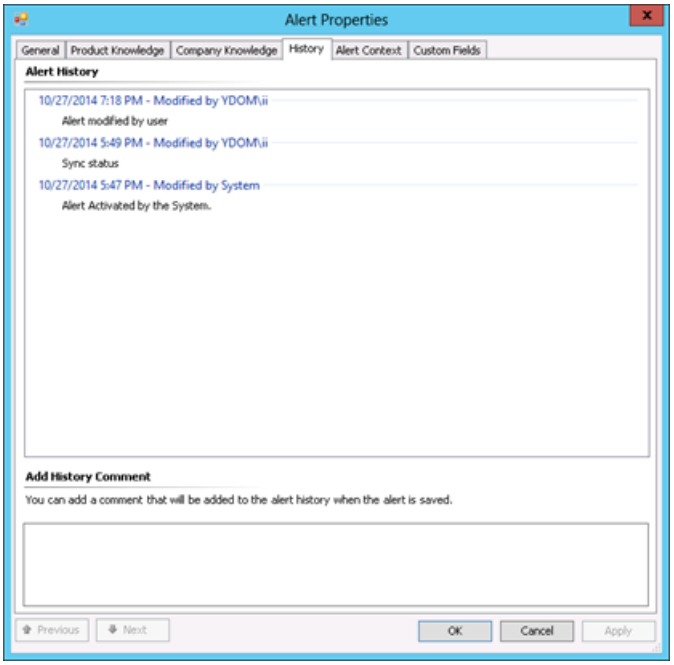
This tab contains a brief description of the product operation and references to detailed information on InTrust and InTrust Connector for Operations Manager.

Alert Properties—Company Knowledge



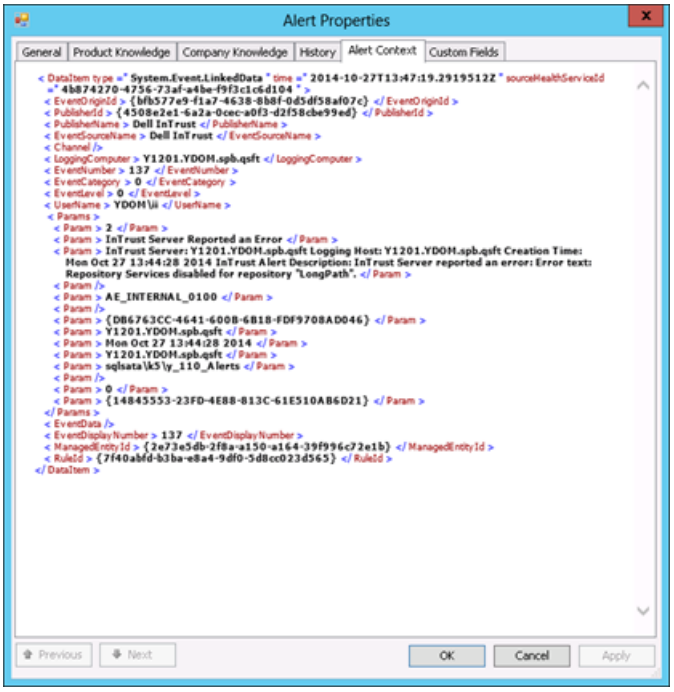
This tab can be used to enter your company knowledge for the alert (if any). For that, click **Edit Rule**, and edit the **Knowledge** field of the rule which is the source of the selected alert.

Alert Properties—History



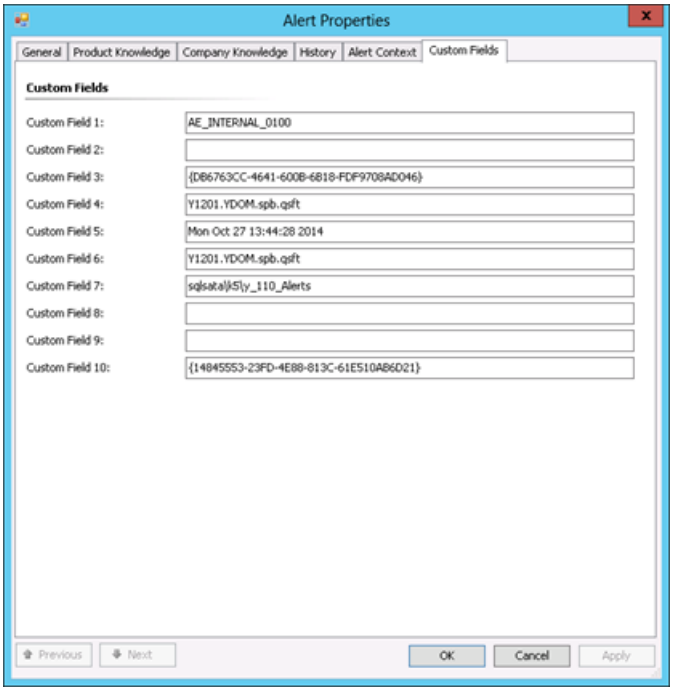
Use this tab to track the alert history (from the moment it was activated), including all modifications and their initiators.

Alert Properties—Alert Context



The alert context (structure) is displayed in XML format.

Alert Properties—Custom Fields



This tab contains a list of custom fields described in the Alert Field Mapping topic. This data is filled in automatically by the product and should not be changed.

Alert Field Mapping

The table below shows how InTrust alert fields are mapped to the Operations Manager alert fields displayed in the Operations Manager console:

InTrust Alert Field	Operations Manager Alert Field	Details
Description	Alert Description	The Operations Manager alert description is derived from InTrust alert fields using the following rule: InTrust Server: <InTrustServer> Logging Host: <HostName> Creation Time: <TimeGenerated> InTrust Alert Description: <Description>
Name	Name	Alert display name, for example, “Successful Logons During Non-Business Hours”.
AssignedTo	Owner	Not forwarded.
State	Alert Status	Operations Manager offers the following predefined alert resolution states:

InTrust Alert Field	Operations Manager Alert Field	Details
		• New State ID= 0 • Acknowledged State ID= 249 • Closed State ID = 255 The InTrust alert states are as follows: • New State ID = 0 • Acknowledged State ID = 128 • Closed State ID = 255 To represent this state in Operations Manager, you can follow the instructions provided in the Configuring InTrust Connector for Operations Manager topic. The settings you configure will take effect for all alerts forwarded to Operations Manager.
Severity	Alert Severity	Alert severity values are mapped, as follows: InTrust— OpsMgr Information— Information Minor— Warning Major— Critical Critical— Critical Custom— Warning
	Creation Time	Filled in by Operations Manager.
ForwardToMOM		If an InTrust Alert contains a custom field named 'ForwardToMOM', it is forwarded to Operations Manager regardless of the filtering settings in the InTrust Connector.
AlertCode	Custom Field 1	
Comment	Custom Field 2	
idAlert	Custom Field 3	InTrust alert ID.
HostName	Custom Field 4	This field is mapped to Custom Field 4 in order to be filled in with the proper data (since the 'Computer Name' Operations Manager alert field is reserved

InTrust Alert Field	Operations Manager Alert Field	Details
		for Operations Manager data only).
TimeGenerated	Custom Field 5	InTrust alert generation time in GMT format. This field is mapped to Custom Field 5 in order to be filled in with the proper data (since the 'Time Created' Operations Manager alert field is reserved for Operations Manager data only).
InTrustServer	Custom Field 6	This is the InTrust alert field's display name in the InTrust Monitoring Console. Tn the Alert database this field is named “ServerName”.
	Custom Field 7	InTrust Alert database providing the alerts.
	Custom Field 8	Not used.
	Custom Field 9	Used as a temporary storage for the initial alert state value received from InTrust: if InTrust alert's initial state is not 'New', the state will be kept in this field (the Resolution State in Operations Manager will first appear as 'New' but will be changed to the value from this field when the synchronization process completes).
	Custom Field 10	InTrust Connector instance's GUID (used to identify alerts stored in the Operations Manager database by this instance).

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

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