Quest® InTrust 11.4.2

Deployment Guide

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.**

i **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

InTrust Deployment Guide
Updated - September 2020
Version - 11.4.2

Contents

InTrust Deployment Options

You have two InTrust deployment options:

- Default
  Install a lean streamlined set of components that closely implement best practices for auditing and regulations compliance without much variation.
- Extended
  Customize your InTrust component choice, workflows and security roles for auditing, real-time monitoring, advanced SQL Server Reporting Services-based reporting and regulations compliance.

This set of topics deals with extended deployment. For details about the default installation, see Getting Started with InTrust.

Performing Extended Deployment of InTrust

Before You Run Setup

Consider some preliminary procedures you may need to carry out prior to launching InTrust setup. Make sure you have read about the key features, components and workflow of InTrust in the Product Overview.

For more details, see the following topics:

- Providing Database Access
- Planning for InTrust Accounts

Providing Database Access

An important thing to consider when installing InTrust is security for the databases that it is going to use. The accounts used by InTrust to access these databases can have the **dbo** role for the databases, or minimal privileges provided by special scripts.

If you use an account that has the **dbo** role, no database pre-configuration is needed. You can create databases as you proceed with the setup. If you cannot or do not want to use the system administrator account, make sure that your account is the owner of at least the InTrust configuration, audit and alert databases.

Access to the databases accounts without the **dbo** role is also possible, but database cleanup is disallowed to such accounts. If this is an acceptable limitation for the account you want to use, ask your database administrator to configure the account using the procedure below.

To provide access to SQL Server 2005 and later databases

1. Create a Windows group (for example, **InTrustAccounts**), and add the following accounts to it:
   a. The account under which InTrust setup will be run, for example, **InTrustSetupAccount**
   b. The account that will be used for InTrust operations (later you will have to enter it during the InTrust setup), for example, **InTrustServiceAccount**

   You can use the same account for both purposes.
2. In SQL Server Management Studio, select the SQL Server that will host InTrust databases.
3. Right-click **Security | Logins**, and select **New Login**. Create a login that will be used for database access; in the **Login name** field, specify the **InTrustAccounts** group (created on step 1).
4. Create the databases (configuration, audit, and alert) to be used by InTrust.
5. Run the corresponding scripts for them:
   a. for the configuration database: **configdb.sql** and **InTrust9_0_configuration_schema.sql** scripts
   b. for the audit database: **auditdb.sql** and **ITFE80_EventsData.sql** scripts
   c. for the alert database: **alertdb.sql** and **InTrust9_0_alerts_schema.sql** scripts

   These scripts automatically create database schemas and roles required for InTrust operations.
6. Select the database you created (for example, audit database); under that database, select **Security | Users**, and create a new user (for example, **Non_dbo**). In the **Login name** for that user, provide the account created on step 3.
7. Check the following:
   a. **InTrust Gathering** is set as the default schema for the user.
   b. This user has the appropriate database roles (**InTrust Audit DB Cleanup**, **InTrust Gathering**, and **Reporting Console User**).
8. Repeat step 6 for the alert database.
9. Check the following:
   a. **InTrust Real-Time Monitoring** is set as the default schema for the user.
   b. This user has the appropriate database roles (**InTrust Real-Time Monitoring**, **InTrust AlertDB Cleanup**, **InTrust Monitoring Console**, and **Reporting Console User**).
10. Repeat step 6 for the configuration database.
11. Check the following:
    a. **AdcCfgUser** is set as the default schema for the user.
    b. This user has the appropriate database roles (**AdcCfgUser**, **Reporting Console User**).

Once you have completed these steps, your databases and accounts are ready to be specified during the installation. They will have the privileges required for proper InTrust operation without the **dbo** role (with the limitation described above).

Planning for InTrust Accounts

This topic gives an overview of the accounts you will need to install and configure InTrust. Detailed information is provided in System Requirements.

1. To install Knowledge Packs containing reports and other predefined objects, this account also requires the following:
    a. Membership in the local **Administrators** group on the computer where the setup is run
    b. **Content Manager** role for the **Home** folder in SQL Server Reporting Services.
    c. **System Administrator** site-level role in SQL Server Reporting Services (for creating item-level roles and shared schedule)
2. During the setup, you will be prompted for InTrust account. This account will be used for InTrust services operation (data gathering, real-time monitoring, scheduled task processing) and agent installation (by default).
   In order to provide automatic creation of Service Connection Point (SCP) by InTrust means, do one of the following before the setup:
    - Open the ADSI Edit snap-in and create **CN=Quest InTrust, CN=System, DC=<*Domain*>** in the "Domain" Active Directory partition. You have to assign the following rights for this container for the account under which you will run the setup: **Create All Child Objects**, **Read Permissions**, **Modify Permissions**.
    - Open the ADSI Edit snap-in and specify the following rights for the **CN=System, DC=<*Domain*>** in the "Domain" Active Directory partition for the account under which you will run the setup: **Create All Child Objects**, **Read Permissions**, **Modify Permissions**, **Read All Properties**, **Write All Properties**. These permissions must be applied onto **This object and all descendant objects** scope.

What you have after you have performed all these actions and setup has finished:

- The **CN=Quest InTrust** container is created.
- The account under which you install the Quest InTrust Server service has sufficient rights to create child objects.
- The account under which you run the Quest InTrust Server service has sufficient rights to create child objects.
- The **serviceConnectionPoint** object is created.

If you need to change an account after the InTrust installation, use the **adcsrvacc** command-line utility. For more details, see Special-Purpose Commands and Utilities.
The rights and permissions required for InTrust operations are described in System Requirements.

Installing and Configuring InTrust Components

To install InTrust, run the Autorun application from your InTrust distribution on the computer where your InTrust server will be located. On the **Install** tab, click **InTrust Extended Suite**. Follow the steps, as described in the related topics:

- Installing the First Server in InTrust Organization
- Installing Servers Into an Existing InTrust Organization
- Installing InTrust in Unattended Mode

Participation in the Quest Software Improvement Program

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 Opting In and Out below.

Participation is enabled or disabled on a per-computer basis. It is configured independently on every computer where you install software using InTrust setup.

Opting In and Out

To change your choice regarding participation in the Quest Software Improvement Program at any time after InTrust setup is complete, use the **sipcfg.exe** command-line utility, which is located in the **InTrust\Tools\Software Improvement Program** folder in your InTrust distribution. Run the command without parameters to see usage information.

The command will have an effect only on the computer where it is performed. For example, if you run it on an InTrust server, it will not affect any other servers in the InTrust organization.

If you want to opt out, you can also use the Autorun application from your InTrust distribution. Launch Autorun, select the **Customer Feedback** tab, and click the **Opt Out** button. This action will prevent automatic opt-in on the same computer if you use InTrust setup to install other components later.

Installing the First Server in InTrust Organization

Accept the License Agreement

On the first step of the setup, accept the license agreement to proceed.

Select Your Country

Select the country where you are performing InTrust installation. This choice affects whether your participation in the Quest Software Improvement Program is enabled automatically. For details about the program, see the Installing and Configuring InTrust Components topic.

Make Your Software Improvement Program Participation Choice (Conditional)

This step is displayed only if the country you selected has legislation that prohibits automatic opt-in for software that transmits data back to the vendor. If you want to take part in the initiative, select the “yes” option.

Select the Components to Install

Next, you are prompted to select any of the following features to install:

1. InTrust Server; it will be installed with the following:
    - InTrust Administrative Knowledge Pack for tracking and reporting on server operation
    - Objects for common best-practice auditing and reporting scenarios
2. InTrust Resource Kit
3. InTrust Manager—the user interface for InTrust configuration.
4. The Monitoring Console application, which allows you to work with real-time monitoring alerts.

Check Your Readiness

After you have selected the components you need, setup runs an automatic check to see if your system meets the requirements for your selection. You can proceed only if all of the listed items check out as **Passed**. Issues with the items marked as **Failed** need to be addressed before you deploy InTrust. To find out the exact requirements for an item, click its **Failed** or **Passed** status label.

For some **Failed** items, an automatic fix is possible; in such cases, a **Fix Issues** link is available for them. For example, if you have chosen to install Monitoring Console but Microsoft IIS is not configured properly, clicking **Fix Issues** for the **IIS** item will activate IIS and enable the necessary features of it.

Supply the User Account

Next, you need to specify the account for InTrust operation.

This account will be used for agent installation by default, audit data gathering, and processing of scheduled tasks. You can use this account to access the configuration and alert databases as well.

The rights and permissions required for InTrust operations are described in System Requirements.

Specify InTrust Organization

When you install the first InTrust server in your environment, a new *InTrust organization* is created. An organization is a set of InTrust servers that share a single configuration database.

Supply the new organization’s name and password. This password is used for the configuration database encryption when you add a new InTrust server to the InTrust organization or register a manually installed agent with the server.

Specify the Configuration Database

Next, specify the configuration database.

You can do one of the following:

- Create a new configuration database.
- Specify a database created in advance by a script (described in the Providing Database Access topic).

For that, launch SQL Server Connection Wizard by clicking the button next to the **SQL Server** text box.

You will be asked to specify the SQL server, database name and connection settings to be used for access to the database. By default, Windows authentication will be used for database access; you can select to use SQL Server authentication when prompted.

> **NOTES:**
>
> 1. You can use InTrust service account to access the configuration database. In this case, select Windows authentication method. Alternatively, you can use the SQL Server standard user account for the database access. In this case, select SQL Server authentication.
> 2. The configuration database must be located on a Microsoft SQL server that has a reliable broadband connection with the computer where you are installing InTrust server.

Review and Modify Default InTrust Settings

On the next step, the default choices for InTrust configuration are displayed. These choices have been made automatically by the installer based on established practices and what you have already specified.

Review the configuration of the following:

- Default InTrust databases
- Communication ports

> **CAUTION:**
>
> - **Communication ports are not configurable if you are performing extended InTrust deployment on top of a default deployment; in this case, it is assumed that the ports are already set up and working thanks to the default deployment.**
> - **Selecting the Allow InTrust traffic through Windows Firewall option will change Windows Firewall rules accordingly. It will not affect any other firewall software you may be using.**
> - **Make sure the ports specified here are open for inbound traffic and not blocked by any firewalls.**

- Monitoring Console
- InTrust notification
- SQL Server Reporting Services

To change any of the default settings, select the **Change automatic configuration** option. The following steps will then let you change the settings.

Change Miscellaneous Default Settings (Optional)

This step is shown if you selected the **Change automatic configuration** option on the Automatic Configuration step. Here you can configure the following:

- Default InTrust alert and audit databases
- Communication ports
- Virtual directory that InTrust Monitoring Console should use

Make sure the ports specified here are open for inbound traffic and not blocked by any firewalls.

> ! **CAUTION:**
>
> - **If you place the InTrust server behind a firewall, you need to allow incoming packets to the specified listening port at the server's IP address and also both incoming and outgoing packets on the RPC endpoint port.**
> - **Port 8341 must be open on the server for incoming packets; this is not configurable.**

Specify Mail Settings (Optional)

This step is shown if you selected the **Change automatic configuration** option on the Automatic Configuration step. Here you can configure mail settings for notifications sent by InTrust.

Specify the following:

- SMTP server name and port for connection
- Email addresses to be used as the default From and To address when the InTrust server sends notifications. Also this email addresses are used for default recipients.
- NETBIOS computer name for default notification recipient

Specify Reporting Settings (Optional)

This step is shown if you selected the **Change automatic configuration** option on the Automatic Configuration step. If you do not want SSRS-based reporting, leave all the options on this step blank.

SQL Reporting Services GUI URL

InTrust interactive operations with reports are based on the web application that facilitates interaction with SQL Server Reporting Services.

Supply the URL of this web application’s virtual directory. In a default Reporting Services installation, the name of the virtual directory is **Reports**. Setup displays the following in the text box: **http://<server name>/Reports** or **http://<server name>/Reports$<instance name>** (for report server instance), where **<server name>** is the name of SQL server that was specified for the configuration database.

If your SSRS installation differs from the default, supply the necessary virtual directory name.

SQL Reporting Services URL

SQL Server Reporting Services provide a web service (Report Server) that exchanges data with applications. Scheduled InTrust reporting jobs use this service.

Supply the URL of the Report Server web service’s virtual directory. In a default Reporting Services installation, the name of the virtual directory is **reportserver**. Setup displays the following in the text box: **http://<server name>/reportserver** or **http://<server name>/reportserver$<instance name>** (for report server instance), where **<server name>** is the name of SQL server that was specified for the configuration database.

If your SSRS installation differs from the default, supply the necessary virtual directory name.

Path to a local folder where InTrust reports will be stored

This setting specifies the location of the folder where SSRS-based InTrust reports will be stored.

This folder will be shared automatically by InTrust setup in order to provide access to the reports from the network.

Complete the Installation

Click **Next** to install the selected features. Wait for the setup to complete.

Installing Servers Into an Existing InTrust Organization

To install additional InTrust servers into an existing InTrust organization, run the setup on the target computers.

> **NOTE:** Do not perform server installations simultaneously—servers must be installed sequentially, one after another.
>
> Consider that all accounts under which you are going to run the setup are listed as InTrust organization administrators. To make sure this requirement has been met:
>
> 1. Open InTrust Manager and connect to the InTrust server.
> 2. Open the properties of the root node.
> 3. Add the necessary accounts to the list that appears. You need to specify the accounts explicitly, because privilege assignment through group membership will not work.

When prompted, supply organization’s password. The configuration database is the same for all servers in the organization.

When installing a new InTrust server into existing organization, you can specify:

- Alert database location
- Mail settings
- Communication ports

> **CAUTION:**
>
> - **Communication ports are not configurable if you are performing extended InTrust deployment on top of a default deployment; in this case, it is assumed that the ports are already set up and working thanks to the default deployment.**
> - **Selecting the Allow InTrust traffic through Windows Firewall option will change Windows Firewall rules accordingly. It will not affect any other firewall software you may be using.**
> - **Make sure the ports specified here are open for inbound traffic and not blocked by any firewalls.**

- IIS virtual directory for Monitoring Console

Installing InTrust in Unattended Mode

You can install the InTrust components you need without going through all the steps of the installation wizard. To do it, use CMD files provided in the **InTrust** folder in your InTrust distribution.

Copy the necessary CMD files to your local hard drive, and open them in a text editor. Edit the lines that set variables such as paths, user names, passwords and so on. Save and run the CMD files.

The CMD files are described in the Files for Unattended InTrust Installation topic. For the meaning of options, you can also see the commented-out lines in the files themselves.

Files for Unattended InTrust Installation

The following batch files let you perform an automated installation of InTrust components without completing wizard steps:

File	Component Installed
Setup_DefaultSuite.cmd	Default set of InTrust components
Setup_Server.cmd	InTrust Server and all related components
Setup_AllComponents.cmd	InTrust Server, all related components, all data view applications and report packs
Setup_ITManager.cmd	InTrust Manager and InTrust Deployment Manager
Setup_MonitoringConsole.cmd	InTrust Monitoring Console
Setup_RepositoryViewer.cmd	InTrust Repository Viewer
Setup_Parameters.cmd	File that defines parameters for unattended installation of InTrust.
Setup_WindowsAgent.cmd	File that installs InTrust agent and registers the agent on the InTrust server.
Setup_ReportPacks.cmd	SSRS report packs for use in task-based auditing workflow; for a full list, see InTrust Reports.

The parameters within **Setup_Parameters.cmd** are listed alphabetically in the table below. The **bolded** parameters are needed for both default and extended deployment; the others only for extended deployment.

Parameter	Description
CONNECT_INTRUST_ORGANIZATION_MODE	Whether to connect to an InTrust organization.
DB_AUD	Name of the audit database. **Important:** This database must already exist when the script runs. It is not created automatically.

Parameter	Description
DB_CFG	Name of the configuration database.
DB_RTM	Name of the alert database. **Important:** This database must already exist when the script runs. It is not created automatically.
DISTRIB_PATH	Absolute path to the InTrust CD root. Normally, this is the CD drive letter. If you have copied the CD structure to a shared resource, this is the path to the share that contains the structure. The path must not end in a backslash.
InTrust_Server	Specifies the InTrust server name for agent installation
IT_PATH	Full path to the folder where InTrust component must be installed.
ITMC_SITE	Microsoft IIS Web site number. 1 sets the default Web site.
ITMC_VDIR	Name of the virtual directory.
MAIL_FROM	Identifies the sender of InTrust notification messages.
MAIL_TO	Email address of the recipient of InTrust notification messages. This address becomes a property of the default notification recipient.
MSI_LOG_OPT	Options related to MSI logging. The default is *v!. For more information about these Windows Installer logging options, search http://msdn.microsoft.com for information on the topic.
MSI_UI_OPT	Sets the user interface level. Options related to MSI logging and MSI logging interface. The default is *v!. For more information about these Windows Installer logging options, search http://msdn.microsoft.com for information on the topic.
OPERATOR_COMPUTER	NETBIOS computer name for default notification recipient.
ORG_NAME	Name of the InTrust organization.
ORG_PWD	Password for the InTrust organization.
PF_REPORTING_SHARE	Local path to a reports folder on current server.
PORT_ADMIN	Number of the port that InTrust Manager uses to connect to the InTrust server. The default is 8340.
PORT_LISTEN	Number of the port that agents use to communicate with the InTrust server. The default is 900.

Parameter	Description
RS_SERVICE_URL	Path to a SRS server to be used as default for reporting jobs.
SIP	Participation in the Software Improvement Program. For details about the program, see Installing and Configuring InTrust Components.
SMTP_PORT	Name of the port that InTrust must use for notification messages. The default is 25.
SMTP_SERVER	Name of the SMTP server that InTrust must use for notification messages.
SQL_AUTH_TYPE_AUD	Type of SQL Server connection to be used for setting up the audit database. 1 specifies a trusted connection. 0 specifies that SQL Server authentication is used.
SQL_AUTH_TYPE_CFG	Type of SQL Server connection to be used for setting up the configuration database. 1 specifies a trusted connection. 0 specifies that SQL Server authentication is used.
SQL_AUTH_TYPE_RTM	Type of SQL Server connection to be used for setting up the alert database. 1 specifies a trusted connection. 0 specifies that SQL Server authentication is used.
SQL_PWD_AUD	Related to the audit database: if SQL_AUTH_TYPE_AUD is set to 0, specifies the password for SQL Server authentication.
SQL_PWD_CFG	Related to the configuration database: if SQL_AUTH_TYPE_AUD is set to 0, specifies the password for SQL Server authentication.
SQL_PWD_RTM	Related to the alert database: if SQL_AUTH_TYPE_RTM is set to 0, specifies the password for SQL Server authentication.
SQL_SERVER_AUD	Specifies the SQL server that will host the InTrust audit database.
SQL_SERVER_CFG	Specifies the SQL server that will host the InTrust configuration database.
SQL_SERVER_RTM	Specifies the SQL server that will host the InTrust alert database.
SQL_USR_AUD	Related to the audit database: if SQL_AUTH_TYPE_AUD is set to 0, specifies the user name for SQL Server authentication.
SQL_USR_CFG	Related to the configuration database: if SQL_AUTH_

Parameter	Description
	TYPE_AUD is set to 0, specifies the user name for SQL Server authentication.
SQL_USR_RTM	Related to the alert database: if SQL_AUTH_TYPE_RTM is set to 0, specifies the user name for SQL Server authentication.
SVC_PWD	Password of the user account on whose behalf the InTrust Server services work.
SVC_USR	User account on whose behalf the InTrust Server services work.

Starting InTrust Manager

You can connect to an InTrust organization (the InTrust server will be selected automatically), or select any specific InTrust server.

If you choose to connect to a specific InTrust server, you can browse for the server only in the same domain where you are running InTrust Manager. To connect to a server in another domain, you need to explicitly specify the server name.

Licensing

When you install the product and launch InTrust Manager or InTrust Deployment Manager for the first time, you will be asked to provide a license. Supply the license that you obtained from the sales representative. If you do not supply a license, most of InTrust functionality will be unavailable to you.

To obtain a license, contact your local sales office listed at https://www.quest.com.

Deploying Agents

- Automatic Deployment
- Manual Deployment
- Monitoring the Agent Status
- Changing the Agent Account
- Setting Up Agent Security

Automatic Deployment

In most cases, you can automatically deploy agents on a site. Open the **Configuration** node, right-click the desired site, and select **Install agents**. Agents are deployed to each of the site's computers.

Note the following:

1. It is assumed that the account under which the InTrust Server service is running has the administrative rights over the computers where you plan to install agents. If the account does not have enough rights, specify a different account (with sufficient privileges) using the Properties page of the InTrust site.
2. If you perform any operation that requires an agent to be installed on the target computer, the agent is automatically installed on that computer (for example, when you activate a real-time monitoring policy to monitor site computers).

Manual Deployment

Agents should be deployed manually on the Unix-based computers, and on the Windows-based computers under the following (or similar) circumstances:

- The InTrust server and the processed computers are connected by unreliable and slow links. Agent installation fails when the packet drop rate exceeds 5%.
- The processed computers are behind a firewall.

To install an agent manually, follow the instructions provided in the Installing Agents Manually topic or in the **InTrust_11.4.2_InstallingAgentsManually.pdf** document shipped with the agent installation package.

Monitoring the Agent Status

When an agent communicates with the InTrust server using TCP, it periodically sends a special communication packet—agent heartbeat—to inform server that this agent is running. By default, heartbeat frequency is set to 120 seconds (this value can be modified by the corresponding organization parameter in the configuration database). Heartbeats help server to monitor for agent status:

- If no heartbeat was received from an agent during 240 seconds (default value) since the last one, the server considers this agent to be not responding, and changes corresponding agent status (record in the configuration database).
- If no heartbeat was received from an agent during 600 seconds since the last one, the server considers this agent to be lost, and tries to restore (re-install) it. By default server tries to recover an agent every 300 sec.

To view current agent’s status, in InTrust Manager, select **Configuration | InTrust Servers**, expand your InTrust server’s node, and click **Agents**.

Changing the Agent Account

When installing agents to process site objects, you can select to use the LocalSystem account for agent operation on the target computers, or specify another account:

- In InTrust Manager, select **Configuration | Sites**, right-click the site where the agent is installed, and select **Properties**.
- Open the **Accounts** tab, select the account that will be used to process site objects with the agents (**LocalSystem** or another account).

If you select to use an account other than **LocalSystem**, InTrust automatically attempts to grant the account the **Log on as a service** right. However, Group Policy settings may prevent this. If the account fails to get the right, you can configure account rights using the Local Security Policy console.

To grant user rights to a service account

1. From the Windows Control Panel, go to Administrative Tools, and then double-click **Local Security Policy**. The Local Security Policy console opens.
2. In the console tree, select **Security Settings | Local Policies | User Rights Assignments**.
3. In the details pane, right-click the **Log on as a service** right, and select **Properties**.
4. Click **Add User or Group** and add the user or group you want.

To change the account for an agent that is already running

1. On the computer where the agent runs, in the Services MMC snap-in select the **Quest InTrust Agent** service.
2. Right-click it and select **Properties** from the shortcut menu.
3. Change the account on the **Log On** tab.

Setting Up Agent Security

See the following topics:

- Setting Up Authentication
- Setting Up Encryption

Extending a Default InTrust Deployment

The default InTrust deployment is mainly designed for a specific scenario: real-time collection of logs to an InTrust repository, viewing the contents of the repository and generating reports on those contents in Repository Viewer. If you want to depart from this scenario (collect a rare log, add real-time alerts, make SSRS-based reports with correlated events and so on), you should begin by extending your default deployment with new InTrust components.

For that, run the InTrust setup suite on the computer where the default set of components is installed, as described in Installing and Configuring InTrust Components. The necessary components will be added.

! CAUTION: **Due to an issue in the installer, customizing the communication ports on the Review Default Settings step currently does not work. You can specify custom ports and successfully complete the setup, but these changes will have no effect, and InTrust will keep using the default ports: 900 and 8340.**

Best Practice: Keep Real-Time Workflows Separate

After you have extended a default InTrust deployment, it is not recommended that you mix real-time event collection with classic InTrust real-time monitoring. In your new extended deployment, let the original InTrust server keep performing real-time event collection. For real-time monitoring, use other servers in the same InTrust organization (add them if necessary).

Mapping Out Your Environment for InTrust

In InTrust, your environment is represented by InTrust sites. Sites define the scope of InTrust operation and also specify the computers where InTrust agents can reside. See the following topics:

- InTrust Sites
- InTrust Agents

InTrust Sites

InTrust provides for collection, correlation, archival, and reporting on the heterogeneous audit data from your enterprise-wide network, as well as for real-time alerting and notification.

The two main processes in InTrust are audit data gathering and real-time monitoring for critical events. You can set them up using InTrust Manager—an MMC snap-in intended for InTrust configuration.

Both gathering and monitoring are performed on InTrust sites. An InTrust *site* is a representation of several computers and the settings associated with them. Sites logically group those computers for which the auditing and monitoring requirements are similar. So, by using sites you map out your environment for InTrust—this is the first step you make when configuring gathering or monitoring workflow.

InTrust provides several predefined sites but you need to populate these sites manually. Depending on the InTrust Knowledge Pack you have installed, your configuration can include different predefined sites, for example:

- InTrust for Windows Knowledge Pack offers the “All Windows Servers in the domain” site.
- InTrust for IIS Knowledge Pack brings in the “All IIS Servers” site, and so on.

Besides, you can create your own sites, following the steps described in the Creating Sites topic.

Every time you create a new InTrust object or make any other changes to the InTrust configuration, you must apply these changes. For that, right-click the **InTrust Manager** root node and select the **Commit** option from the shortcut menu or press **Commit** on the toolbar.

In InTrust Manager, sites are shown grouped by environment (such as Microsoft Windows Network and UNIX Network) under **Configuration | Sites**.

To process logs on site computers, InTrust agents can be used.

Creating Sites

To create a site

1. In InTrust Manager, double-click **Configuration | Sites**.
2. Right-click the appropriate environment (for example, **Microsoft Windows Network**); and select **New Site**.
3. Follow the instructions of the New Site Wizard.

   The wizard prompts you for the method to use for enumerating site objects and the InTrust server that will process the site.

   You can perform domain enumeration for the site, either by using the Computer Browser service, or by getting the computer list from a domain controller.

   - For InTrust gathering, site objects will be enumerated each time a gathering session starts.
   - For InTrust real-time monitoring, you can schedule enumeration using site properties.

   > **NOTE:** By default, the Computer Browser service is disabled on Windows Server 2008 and later computers, so it is recommended that you use the alternative enumeration method (that is, get the computer list from a domain controller).

4. Next, populate the site with objects. Specify computers by doing any of the following:

   - Selecting the whole network
   - Specifying or selecting particular computers
   - Specifying or selecting domains that contain the computers you are interested in
   - Specifying an IP address range
   - Selecting organizational units
   - Selecting or specifying an Active Directory site
   - Adding all domain controllers in the domain or Active Directory site
   - Supplying a list of computers in a file
   - Specifying a script that enumerates the computers (for details, see the Site Enumeration Scripts topic)

   A computer list file uses the plain text format. Each name must be a separate line in the file. You can add comments prefixed either with double slashes or with semicolons. The following is a sample file:

   ```
   ;This is a comment

   EDITOR

   Deborah

   //This is a comment using a different style

   Backup

   10.35.28.196

   \\Exchange
   ```

   A computer can appear in the list as any of the following:

- A computer name
- A NetBIOS name
- An FQDN
- An IP address

5. After that you can provide a filter that narrows your selection of site objects based on computer properties. Object filters enable you, for example, to select all computers in your environment with a particular OS installed. This way, you include the entire network as the site object and still get the required precision without having to deal with particular computer names or IP addresses. For more information about object filters, see Using Filters in InTrust Manager.
6. Finally, specify the name and description for the new site.
7. Review the settings and click **Finish** to complete the wizard. The new site will appear in the left-pane treeview.

Modifying Sites

In a site’s properties dialog box invoked from the shortcut menu, you can modify the site settings specified during the site creation procedure, as well as some other settings, including:

- An account to be used for accessing the objects in the site (in particular, the gathering engine will use this account to collect data from site computers without agents).
- An account to be used by InTrust agents installed on the site.

i **NOTE:** To supply either of these accounts, open the **Accounts** tab.

- If the role-based administration feature is enabled, you can specify users who will be able to see and edit the site or use the site objects. For that, open the **Security** tab.

You can also use the site’s shortcut menu to:

- Add objects to the site
- Install agents on the site’s computers

Site Enumeration Scripts

If you want to specify your own algorithm for the enumeration of objects in the site, you can use the **Enumeration Script** option, which prompts you for a script that will perform the enumeration. This option is available:

- During site creation: on the Site Objects step
- For an existing site: from the context menu, or in the site properties on the **Objects** tab

Selecting **Enumeration Script** prompts you for the script you want to use. The scripts are located in the **Configuration | Advanced | Scripts** container node.

InTrust comes with the example “Enumeration script: LDAP query” script for this purpose. For your sites, you can use this script, copies of it, or your own scripts.

The “Enumeration script: LDAP query” script has the following parameters, which you can customize without modifying the script itself:

Parameter	Meaning
Attribute Name	Name of the attribute that will be used as the object name in the list of site objects.
Bind String	ADSI bind string; for example, “GC:” means that the entire AD forest will be searched, “LDAP:” specifies the current domain.
Filter	LDAP filter, such as **(objectCategory=serviceConnectionPoint)**
Need Deep Search	What to do if the search in the entire forest finds objects whose names (specified by the Attribute Name parameter) cannot be read: • **0** Do nothing; the matching object is not included in the site • **1** Try searching in individual domains and reading the attributes again This parameter is considered only if the Bind String begins with **GC:**.
Search Scope	Search scope in LDAP terms, with the following values: • **0** Base • **1** One level • **2** Subtree

InTrust Agents

You can deploy InTrust *agents* on site computers to locally perform audit data gathering and monitoring. An agent is an executable that keeps track of events logged on the computer, filters data, compresses it and sends it to the InTrust server it responds to.

> CAUTION: **Agents are optional for audit data gathering, but required for real-time monitoring. Using agents for gathering, however, helps minimize network impact when communicating data from the target computer to the InTrust server.**

Usually, agents are installed automatically, but in some cases you need to deploy them manually (for example, if a computer is behind a firewall or if it is a Unix host).

- To install agents on all site computers in bulk, right-click that site and select **Install Agents**.
- To avoid automatic agent installation on site computers, right-click that site, select **Properties**, and on the **General** tab, select the **Prohibit automatic agent deployment on site computers** option.

For more details about agent installation, see Deploying Agents.

If using an agent on the target computer, you can set a limit for the agent so that its CPU usage does not go beyond the specified percentage. For that, do the following:

1. Under the **InTrust Server** node, select **Agents**, right-click the agent you need.
2. In the agent’s properties, go to the **Parameters** tab; select the **Agent_ThrottleCPU** parameter, click **Edit** and set parameter value to **1**—to activate CPU throttling.
3. Select **Agent_ThrottleCPUPercent** parameter, click **Edit** and specify value for the limit. Note that if an agent responds to multiple InTrust servers, and this option is configured on more than one of those servers, the least of the specified values is used.

Besides, on the **General** tab of the agent's properties page, you can specify the location of temporary files and agent log backup (for more information on agent log backup, refer to the Keeping Event Data on the Agent Side topic). You can change these settings for a list of agents responding to the InTrust server that InTrust Manager is connected to.

Using Filters in InTrust Manager

In some parts of InTrust configuration, filters can be used for fine tuning. See below for details about setting up filters for data and objects.

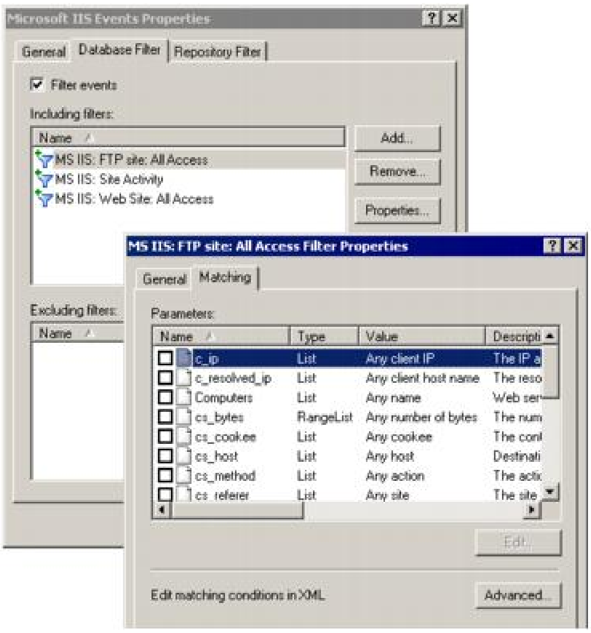
Data Filters

Data filters specify what kind of data is retrieved. Data filters are associated with individual data sources within policies. Data filtering is configured separately for repositories and databases.

When creating a new data source, the New Data Source Wizard will offer you to create the data filters you want to be used. There are two varieties of filters: including and excluding. Apply including filters to include the selected events in the data store. Apply excluding filters to ignore the selected events.

> **NOTE:** You can configure excluding filters only if at least one including filter exists.

To configure the data filters of existing data sources, expand the policy which involves the necessary data source, and from the data source’s shortcut menu, select Properties. Use the **Repository Filter** and **Database Filter** tabs to modify the filters as you need.



☑ Filter events

Including filters:

Name
MS IIS: FTP site: All Access
MS IIS: Site Activity
MS IIS: Web Site: All Access

Excluding filters:

Name

Parameters:

	Name	Type	Value	Descripti
□	c_ip	List	Any client IP	The IP a
□	c_resolved_ip	List	Any client host name	The reso
□	Computers	List	Any name	Web ser
□	cs_bytes	RangeList	Any number of bytes	The num
□	cs_cookee	List	Any cookee	The con
□	cs_host	List	Any host	Destinati
□	cs_method	List	Any action	The actic
□	cs_referer	List	Any site	The site

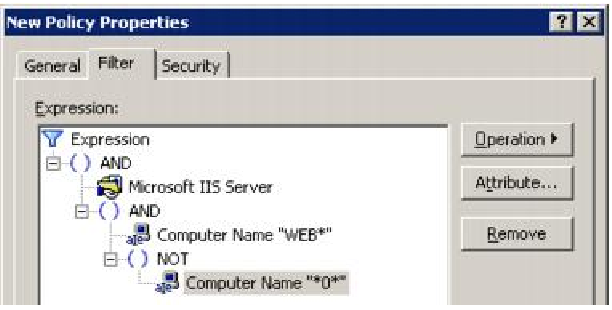
Edit matching conditions in XML

Object Filters

Object filters specify the objects from which data is retrieved. Object filters are associated with the following:

- Entire gathering policies (not individual data sources in those policies)
- InTrust sites (both predefined and custom) involved in gathering and real-time monitoring

Object selection for the site filters is based on the logical operators AND, OR and NOT. Highlight an item in the Filter tab tree and select an expression or attribute to supplant or expand the item. Filter attributes are selected from an extensible list.



Expression:

```
Expression
( ) AND
    Microsoft IIS Server
    ( ) AND
        Computer Name "WEB*"
        ( ) NOT
            Computer Name "*0*"
```

For example, if you need to include all IIS servers whose names start with “WEB” and do not contain the character “0”, do the following:

1. Open the properties of the site or policy for which you are configuring the filter, and to the **Filter** tab.
2. Click the root item **Expression**, click **Operation** and select **AND**. An AND node appears, expanded by two placeholders for expressions or attributes.
3. Click the first placeholder and click **Attribute** to select the **Microsoft IIS Server** attribute from the list.
4. Highlight the second placeholder, click **Operation** and select **AND**. Again, two placeholders appear.

5. Click the first, click **Attribute**, select Computer Name and type “**WEB***”.
6. Click the second placeholder, click **Operation** and select **NOT**. A placeholder appears.
7. Click the placeholder, click **Attribute**, select **Computer Name** and type “***0***”.

Click **OK** to save the changes and close the dialog box.

Role-Based Administration of InTrust

By default, after your InTrust installation is complete, the role-based administration feature of InTrust is disabled.

In large, complex environments, InTrust administration can require multiple people. Often, it makes sense to define several scopes of control, or roles, for these InTrust administrators to clearly delineate their responsibilities. For example, you might use the roles of auditing administrator, monitoring administrator, and InTrust server administrator.

A role can be represented by an Active Directory group. You implement roles by setting InTrust object permissions for each group, thereby granting or denying the group members access to InTrust configuration objects or InTrust features.

A user can belong to more than one group and so have more that one role. For example, a user might be both an auditing administrator and an InTrust server administrator.

It is up to you what roles you introduce in your InTrust framework. Consider that your roles can control the following:

- Access to specific content
  For example, you might want an Active Directory team, a Linux team, or an InTrust Server team.
- Level of responsibility
  For example, a user might be an InTrust administrator or a notification recipient.
- Geographical location
  For example, users are located in the United States or Europe.

This list is just a starting point. You may want to define your roles based on different criteria.

> ! CAUTION: **By default, after your InTrust installation is complete, the role-based administration feature of InTrust is disabled. After upgrade, the enabled or disabled state of this feature does not change.**

When role-based administration is disabled, the following object access configuration is in effect:

- Accounts from the list of InTrust organization administrators have full control of InTrust objects: they can use, create, modify and delete objects. For details about this list, see the *Users with Unrestricted Access* section of the Default Roles topic.
- Accounts from the computer local **AMS Readers** group on the InTrust server have read-only access to objects—most importantly, this means that they can run tasks and jobs. For details about this group, see the *Users Who Can View Configuration Objects in InTrust Manager* section of the Default Roles topic.
- Accounts that are not included in the organization administrators list or **AMS Readers** group cannot connect InTrust Manager to an InTrust server.

Default Roles

Users with Unrestricted Access

Accounts (users or groups) in the list of InTrust Organization Administrators are not affected by the security settings on InTrust objects; they have unlimited rights over the configuration in an InTrust organization.

To access this list, right-click the root node in the InTrust Manager treeview and select **Properties**. In the dialog box that opens, use the **Add** and **Remove** buttons to work with the list. Only users who are already in the list can add or remove accounts.

By default, the organization administrators list contains the following:

- The user account under which you install InTrust Server
- The user account specified as the InTrust Server service account

> **NOTE:** If you decide that using roles is not justified in your environment, you can add to this list either the accounts of all your InTrust administrators or a group that they are members of. This way, you can disregard administration role considerations entirely.

Importantly, in the current version of InTrust, several configuration objects can be created only by accounts that are listed as InTrust organization administrators. These are objects under the following Configuration nodes: **Notifications**, **Data Stores**, and **Advanced**. Other users, however, can be assigned any rights they need to access the configuration objects under these nodes.

Users Who Can View Configuration Objects in InTrust Manager

By default, **Everyone** has **Read** access to InTrust configuration objects. However, to use InTrust Manager, a user must be a member of the **AMS Readers** computer local group on the InTrust server or an InTrust organization administrator. The **AMS Readers** group initially has no members. To enable users to view InTrust configuration in InTrust Manager, take the following steps:

1. Create an Active Directory security group named, for example, **Configuration Readers**.
2. Include the necessary accounts in this group.
3. Add this group to the local **AMS Readers** group on your InTrust server.

Then, any time you need to grant **Read** access to another account, simply make it a member of the **Configuration Readers** group.

Implementing Role-Based Administration

To implement role-based InTrust administration, do the following:

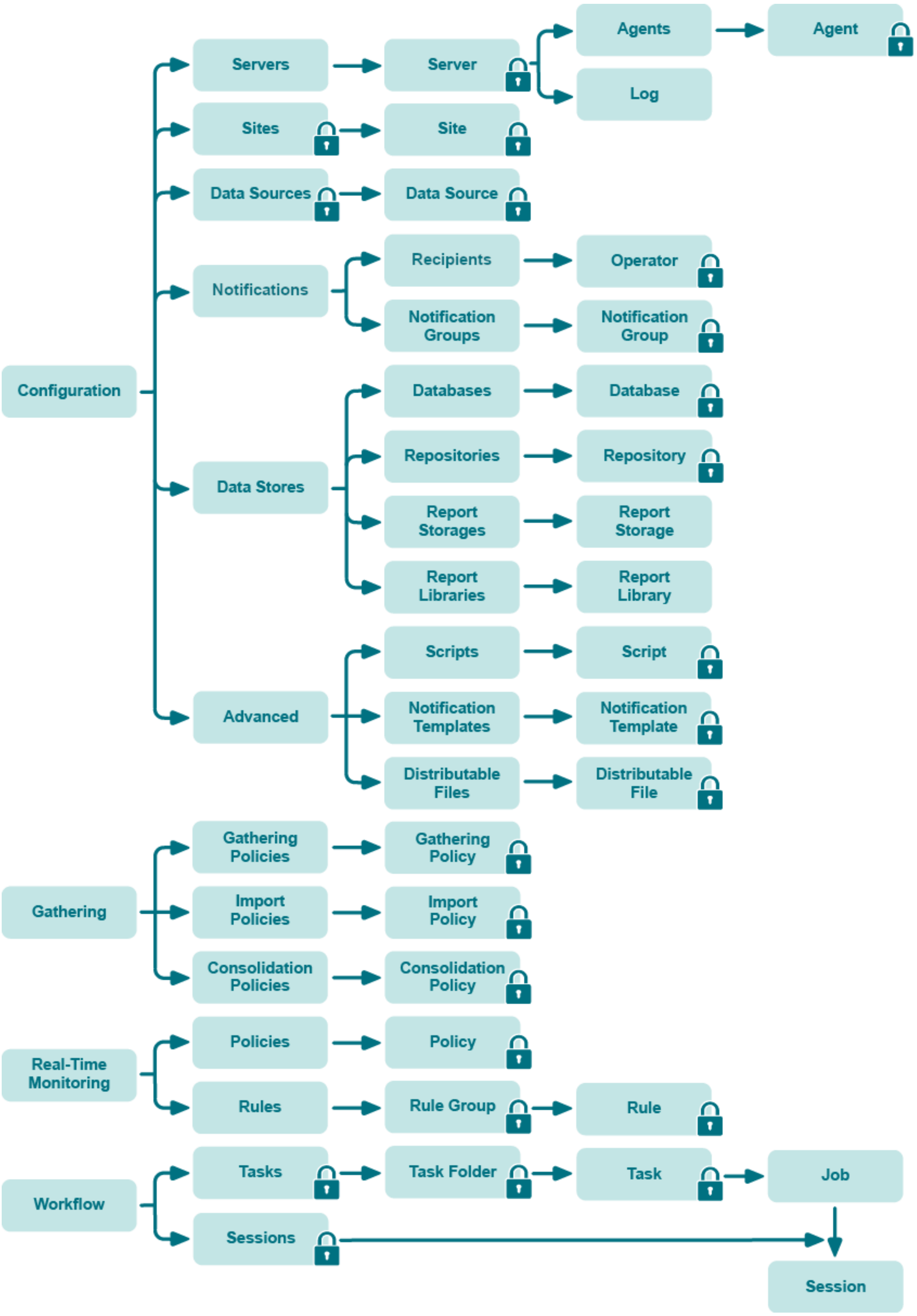
1. Make an Active Directory security group for each new role.
2. Populate the group with accounts that must have the role.
3. Set permissions on InTrust objects for the group.

It is recommended that you create groups with descriptive names. For example, if you need to define an auditing administrator role, you should create a group called **InTrust Auditing Admins** or something similar, depending on the naming conventions in your environment.

InTrust Object Security

Objects can inherit security permissions from their parents or have them assigned directly. You can specify security settings to a number of InTrust configuration objects using InTrust Manager snap-in. Setting permissions on these objects affects the objects' availability in the InTrust Manager snap-in and the InTrust operations, if the respective jobs or tasks are running under an account other than the InTrust Server account. Permissions control whether specific people can access objects in the snap-in and whether an account under which a certain job is running can access objects used by this job.

The following figure illustrates the inheritance of security permissions of InTrust configuration objects available in the InTrust Manager snap-in. Containers are shown as folders. The lock icon means that you can edit security settings of the marked object using the **Security** tab in its properties dialog box.



Consider the following examples:

- If you select **Deny** for **Read**, **Modify** and **Full Control** on an object for a specific group, users in that group will not see that object in the snap-in.
- Changing InTrust-specific permissions on a database has no effect on real database permissions; similarly, role-based administration-specific repository permissions are not in any way associated with the NTFS permissions on actual repository files.

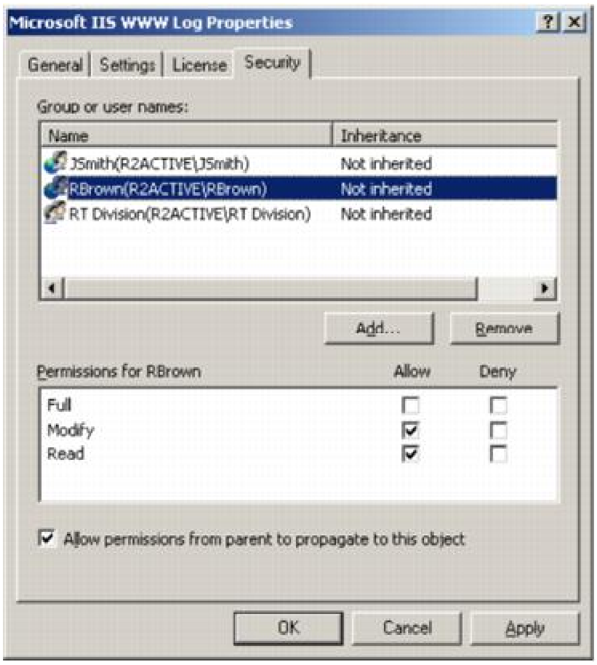
To set object security

1. In InTrust Manager, right-click an object and select **Properties**.
2. Go to the **Security** tab.
3. Click **Add** to specify the groups (or users if necessary) for which you want to define permissions.
4. Select the check boxes you need in the **Permissions** section.

For convenience, InTrust offers a simplified security model with only three options: **Full Control**, **Modify**, and **Read**. The state of each of these options can be either **Allow** or **Deny**.

Internally, however, security is more granular and resembles the NTFS model. For example, extended privileges over InTrust objects are given to users who create those objects. This is analogous to users retaining the Creator Owner permission on an NTFS file or folder that they create—object creators can change their own permissions.

NOTE: Selecting the **Allow permissions from parent to propagate to this object** option means that object parent permissions will be inherited by the object. If you clear the option, the parent permissions will no longer be applied to this object.



Group or user names:

Name	Inheritance
JSmith(R2ACTIVE\JSmith)	Not inherited
RBrown(R2ACTIVE\RBrown)	Not inherited
RT Division(R2ACTIVE\RT Division)	Not inherited

Permissions for RBrown	Allow	Deny
Full	□	□
Modify	☑	□
Read	☑	□

☑ Allow permissions from parent to propagate to this object

Switching Role-Based Administration On and Off

To enable or disable the InTrust role-based administration feature, use the **adccfgsec.exe** utility from the Resource Kit (located in the ***<InTrust_installation_folder>*\Server\ADC\SupportTools** folder on the InTrust Server computer). You can run this command-line utility with the following parameters:

Parameter	Description
-querymode	Use this parameter if you need to find out whether the role-based administration feature is currently enabled. One of the following values is returned: • **Server_level** Role-based administration is inactive; security settings for configuration objects cannot be modified on the Security tab of object properties. • **Object_level** This feature is active, and security settings are available for modification.
-setmode	Use this parameter to switch role-based administration on or off.
-setmode object_level	Activates role-based administration.
-setmode server_level	Deactivates role-based administration.

IMPORTANT: After you have enabled or disabled role-based administration using **adccfgsec.exe**, you need to restart the following services on all InTrust servers in the organization:

- Quest InTrust Server
- Quest InTrust Real-Time Monitoring Server

This will make sure your configuration changes are fully applied.

Examples: Who Can Do What

View Configuration Objects

If you need to enable a group of users to use several configuration objects in their InTrust workflow, consider the following:

- To specify an InTrust configuration object when configuring other InTrust objects, a user must have at least the **Read** permission on that object.
- The default permissions that an object inherits from its parent can enable an unintended user to use and modify the object.

Manage Configuration Objects

An administrator who creates an InTrust configuration object automatically gets the **Full Control** permission on that object. In addition, unrestricted access to the object is given to the accounts in the list of InTrust organization administrators. If you want another group of users to be able to manage an object, delete it, or associate it with other InTrust objects, you must grant them the desired permissions explicitly. Specifically, consider the following:

- To modify or delete an InTrust configuration object, a user must have the **Modify** or **Full Control** permission on the object.
- Account under which a certain job is running must have at least **Read** permission on objects used by this job.
- Every newly created configuration object inherits permissions from its parent node by default. These inherited permissions can enable an unintended user to use or modify the object.

View Alerts

To authorize a group of users to read alerts from a certain InTrust site and a certain rule group, keep in mind the following:

- You must have a real-time monitoring policy that uses the rules you need and the InTrust sites you want to monitor.
- To configure read access to alerts for users or groups, you need to give their accounts the **Read** right in the properties of the policy on the **Alert Security** tab.

Manage Alerts

You may want to enable a group of users to view and modify alert records generated by rules in a specific rule group in a specific InTrust site. Alert records are available to users only if their accounts have sufficient permissions. To do this, consider the following:

- You must have a real-time monitoring policy that uses the rules you need and that works on the InTrust sites you want to monitor.
- To configure access (read and modify) to alerts for users or groups, enable the **Change Alert State** right in the properties of the policy on the **Alert Security** tab.

Case Study: Regional Scenario

Suppose that Acme Corporation has its headquarters in London and branch offices in Mexico and Tokyo. The desired configuration is as follows:

- An administrator from the Tokyo office is authorized to manage a set of configuration objects created by an InTrust organization administrator. These objects might include sites, servers, tasks, databases, repositories, and notification groups.
- An administrator from Mexico office is authorized to manage a different set of configuration objects created by InTrust organization administrator.

- Import and gathering policies are unified. InTrust administrators from regional agencies can view these objects but cannot delete or modify them.

To implement this scenario, consider the following:

- The organization administrator must create the InTrust configuration objects that will be used by regional InTrust administrators in the Tokyo and Mexico offices.
- Object permissions inherited from parent objects must not break the desired security policy.
- The regional InTrust administrators must have at least the **Modify** permission on configuration objects that are used in the InTrust workflow in their offices.
- If a regional administrator has the **Full Control** permission on an object he or she can assign permissions to other users.
- The **Read** permission on the **Gathering** node is sufficient for both regional administrators.

Case Study: Managing Access to Reporting Configuration

Suppose an InTrust administrator creates a task that generates reports on superuser access to Linux hosts. Only users from the **Linux01** group can view and modify this reporting task. When a user from the **Linux01** group opens InTrust Manager, only the **Tasks** node and the prepared task with the reporting job are available.

To implement this scenario, be sure to do all of the following:

- Deny access to all second-level nodes in the InTrust Manager treeview, except the **Tasks** node.
- Give the **Linux01** group the **Read** permission on the **Tasks** node and the task folder that contains the necessary task.
- Give the **Linux01** group the **Modify** permissions on the task itself.
- Make sure that account under which the reporting job runs has the **Read** permission on the nodes of the InTrust server and data stores used by the reporting job.

InTrust Configuration

Configuring Access Rights

During InTrust installation, the following groups are created on the InTrust server:

- AMS Organization Servers
- AMS Readers

In addition, access to InTrust configuration is controlled by the following:

- List of organization administrators (see InTrust Organization Administrators)
- Permissions on individual InTrust objects

These settings are closely related to the role-based administration capabilities of InTrust, that is, help to control who has access to which InTrust objects. Role-based administration feature is disabled by default after the installation. For more information about enabling and using this feature, see the Role-Based Administration of InTrust topic.

InTrust Organization Administrators

InTrust organization administrators are members of a special list maintained in the InTrust configuration database. Accounts included in this list can do the following:

- Install InTrust servers
- Override permissions on objects in InTrust Manager (if role-based administration is used in your InTrust organization)

When you install the first InTrust server in the organization, the following accounts automatically become members of this list:

- The account you are using to run the setup
- The account of the InTrust Server service (supplied during the setup)

Before you install subsequent servers, you should add all the accounts you are going to use for setup to this list. For that, in InTrust Manager, open the properties of the root node and use the **Add** and **Remove** buttons to edit the list.

> **!** CAUTION: **If you configured non-dbo accounts to access InTrust databases (as described in the Providing Database Access topic), make sure that the corresponding group is included in the list of InTrust organization administrators.**

AMS Organization Servers

The local **AMS Organization Servers** group includes the accounts under which the organization's InTrust servers run. To allow your organization's InTrust servers to communicate with the server you are setting up, add its account to this group.

For example, if you have two InTrust servers installed (IT1 and IT2), to allow data communication between IT1 and IT2, you can take the following steps:

- Create a global domain group named, for example, All Org InTrust Servers
- Include the InTrust server accounts (both IT1 and IT2) in this group
- Add All Org InTrust Servers to the local groups AMS Organization Servers on both IT1 and IT2

Then, each time you add a new InTrust server to the organization and need to allow communication between all servers in the organization, you should do as follows:

- Include the new server's account in the All Org InTrust Servers domain global group
- Add All Org InTrust Servers to the local AMS Organization Servers group on this new server

> **!** CAUTION: **If you configured non-dbo accounts to access InTrust databases (as described in the Providing Database Access topic), include the corresponding group in the AMS Organization Servers group on all InTrust servers.**

AMS Readers

The local **AMS Readers** group includes the accounts that are permitted to connect to InTrust servers using InTrust Manager in order to run tasks, view the configuration and so on. Include in this group all personnel who are supposed to work with InTrust Manager.

This group is granted the **Log on as a batch job** right on the InTrust server where the task or job is executed. When you create a task or a job with a specific account, this account is automatically granted the **Log on as a batch job** right and included in the **AMS Readers** group.

Members of this group automatically have read access to all objects available in InTrust Manager. This lets the group's members run existing jobs and tasks but not delete or change them. To let an account perform configuration, make the account an InTrust organization administrator, as described in InTrust Organization Administrators.

Configuring InTrust Sites

InTrust offers a number of predefined sites for Microsoft Windows Network and UNIX network; you can use them by selecting the **Configuration | Sites** node in InTrust Manager.

NOTE: It is recommended that you do not change predefined sites directly to conform to your environment. Instead, consider copying existing predefined sites that correspond to the sites you need, and making changes to the copies.

You can populate a site with the following objects:

- Whole network
- Domains
- Computers
- IP address ranges
- Computer lists (loaded from a text file)
- AD organizational units
- AD sites
- All domain controllers in domains
- All domain controllers in AD sites
- Script object

You can use filters to populate InTrust sites basing on:

- Computer roles
- OS versions
- Specific applications installed on computers, such as Microsoft IIS, (you can define your own applications based on registry values.)
- Registry keys and registry values present on target computers

For example, you want to create an InTrust site with all domain controllers of the domain. For that on the Site Objects step of the New Site Wizard you should click **Add** button and select **All Domain Controllers in | Domain**.

InTrust automatically discovers and enumerates site resources in case shortcuts to domains, Active Directory organizational units, Active Directory sites, or IP ranges are used. This means, if you add a new domain controller to a domain processed by InTrust, it will be automatically discovered and included in the corresponding site.

You can perform domain enumeration for the site either by using the Computer Browser service, or by getting the computer list from a domain controller.

- For InTrust gathering process, site objects will be enumerated each time a gathering session starts.
- For InTrust real-time monitoring, you can schedule enumeration using site properties.
- To display the computers included in the site at the moment, select the site and on the right pane, click Enumeration. On the enumeration pane, click Refresh.

CAUTION: In some cases, when an InTrust site is configured to include computers by matching a filter, 'excessive' computers may appear in the site after enumeration.

This happens if the filter matching cannot be done for some computers in the scope of the site (domain, OU, IP range, etc.) due to specific reasons (for example, if a computer cannot be accessed at the enumeration time).

However, to reduce a probability of data loss, such computers are included in the site as if they matched the filter defined for the site objects. InTrust tries to process such computers. If filter matching fails, users are notified by a message.

Configuring Notification Groups and Recipients

InTrust uses the terms *operator* and *recipient* interchangeably. They define who or what is the addressee of notifications from InTrust jobs and real-time monitoring rules. Recipients can be grouped into notification groups for notifying multiple recipients at once.

To create a new recipient

1. In InTrust Manager click **Configuration**, select **Notifications** and right-click **Recipients**. Select **New Operator**. A new recipient named “New Operator” is created, and its Properties dialog box pops up.
2. In the dialog box, specify the following:
   - Name and optional description
   - Computer name to be used with the Net Send Notification Provider
   - Email address to be used with the Email Notification Provider

Dynamic Operators

Recipients are not necessarily fixed accounts. InTrust provides a way to make a single recipient represent appropriate accounts for multiple situations. These dynamic operators are designed for real-time monitoring purposes, and the account selected for notification depends on the event that triggers the real-time alert.

For example, if your rule uses "Dynamic Operator: Manager of Account in Who Field" as the notification recipient, then InTrust will analyze the contents of the **Who** field in the alert-triggering event, query Active Directory to find out the initiator's manager and send a message to this manager's address. There are several predefined recipients like this; their names start with "Dynamic Operator".

The dynamic recipient selection is script-based. The scripts that implement it are located under the **Configuration | Advanced | Scripts** node in InTrust Manager. The names of the predefined scripts for this purpose start with "Address Discovery". You can create your own scripts of this kind by making copies of the predefined scripts and modifying the copies to suit your needs.

To create a new dynamic operator

1. In InTrust Manager click **Configuration**, select **Notifications** and right-click **Recipients**. Select **New Dynamic Operator**. A new operator named “New Dynamic Operator” is created, and its Properties dialog box pops up.
2. In the dialog box, specify the following:
   - Name and optional description
   - Script to use for dynamic recipient selection; this is one of the script objects from the **Configuration | Advanced | Scripts** container.

> **NOTE:** Dynamic operators are best used together with rules of the "Single event" type. Using them with rules of other types (such as "Events threshold" or "Missing event") may result in irrelevant notifications or may not make sense.

Event Log Recipient

Event Log Recipient is a non-messaging type of notification recipient that uses the InTrust event log as the notification destination. If this recipient is specified for a real-time monitoring rule, then every time the rule is matched, InTrust generates an event about the rule match instead of sending a message to someone. The intended use for this feature is to integrate real-time monitoring and forwarding to SIEM systems, which customarily work with log data. This method provides a SIEM-compliant alternative to InTrust alerts.

There is only one event log recipient; you cannot delete it or create new ones.

Where the Notification Events End Up

Event Log Recipient puts all rule match events in the InTrust log. The destination log is located on the InTrust server that processes the site containing the computer where the rule match occurs. Therefore, to avoid losing any of these events, you should get them from all InTrust servers in the organization.

The events always have event ID 17408. For details about the event, see Events from InTrust Notification Engine.

The InTrust Log Becomes More Important

If you start using the InTrust log for rule match events, you turn it from an InTrust-specific resource into a significant security asset. Make sure you treat the log accordingly. For example, think twice before you clear the log and consider tracking user access to it.

Bulk Configuration of Event Log Recipient for Rules

If you rely heavily on logging rule match events in your workflow, then it can be tedious to specify **Event Log Recipient** for individual rules. Consider using the **NotifyThroughEventLog.exe** utility, which enables **Event Log Recipient** for all existing rules. You can download the utility from the link provided in Quest Support Knowledge Base article 312739.

Where to Enable Event Log Notification: Real-Time Monitoring Policies and Rules

This feature relies on the InTrust notification framework, so for logging of the rule match event to work, the following two settings need to be configured:

1. Enable the **Event Log** notification type for the rules that you want to generate match events.
2. Enable **Event Log Recipient** in the real-time monitoring policies that apply those rules to your sites.

Enabling just one or the other is not enough for the logging to begin. For details about real-time monitoring policies, see Understanding Real-Time Monitoring Policies.

IMPORTANT: Use the **Event Log** notification type only in real-time monitoring rules. Specifying it in notification jobs is pointless, because it has no effect there.

Forwarding Rule Match Events with InTrust

If you use InTrust as your SIEM forwarding tool, see Example: Emulating InTrust Real-Time Alerts in SIEM for details.

If you use SIEM agents, refer to the documentation of your tool for information about integrating events with a specific event ID.

Configuring InTrust Monitoring Console

To configure InTrust Monitoring Console after the setup is completed, open the Monitoring Console Administration page, for example, from the Start menu.

Here you can manage the profiles which allow authorized users to work with InTrust alerts.

> ! CAUTION: **Alert records are available to users only if their accounts were granted sufficient rights to view the alerts or modify their state. For more information about how to configure alert security settings, see the Alert Security Settings topic.**

Users can work with the alerts they need using the alert views. To create or modify a view, open the Monitoring Console, for example, from the Start menu, select the necessary profile, and follow the procedures described in the Monitoring Console Help.

You can configure Monitoring Console to notify you of a new alert when you are working with the alerts in the certain alert view. For that, in the Monitoring Console, go to **My Preferences** tab, and select the **Pop up a message box when new alerts arise** checkbox. When a new alert arises, a message will be displayed asking whether to refresh the current view. Refresh means the following:

- New alerts are incorporated into the view
- The view is reloaded, opening on the first page (regardless of the page you have been working with)

> i NOTE: The message is displayed only when the **Alerts** tab is active (when the **Search** tab is active, no message is displayed even if the corresponding check box was selected).

Licensing

When you install the product and launch InTrust Manager or InTrust Deployment Manager for the first time, you will be asked to provide a license. Supply the license that you obtained from the sales representative. If you do not supply a license, most of InTrust functionality will be unavailable to you.

To obtain a license, contact your local sales office listed at https://www.quest.com.

Sample Deployment and Configuration Scenario

The following topics describe a simple custom InTrust deployment and its post-installation configuration:

- Lab Configuration Overview
- InTrust Organization Configuration Overview
- Gathering Configuration Overview
- Real-Time Monitoring Configuration Overview
- Installing Servers
- Installing Agents
- Configuring and Populating InTrust Sites
- Setting Up Gathering and Reporting on Events
- Setting Up Real-Time Monitoring of Security Events

Lab Configuration Overview

The deployment scenario described below was designed to fit the following test lab configuration:

- 4 trusted domains within a well-connected area
- Standalone IIS servers behind a firewall

The deployment scenario assumes the following:

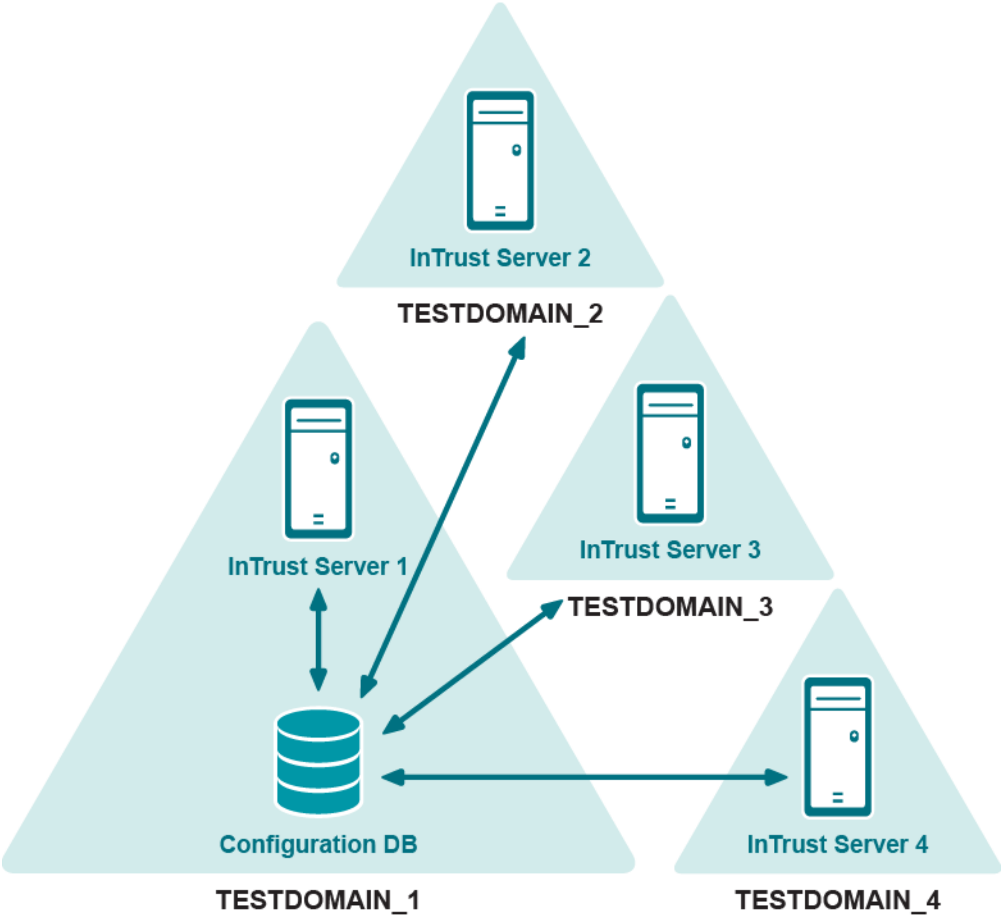
- One of the test domains is considered central.
- Audit data will be gathered into domain-level repositories and then consolidated into a central repository.
- Both domain-level reports and consolidated reports on data from all 4 domains will be generated.
- Real-time monitoring alerts will be viewed in both the central console and local consoles in each domain.
- For the sake of simplicity, you can create a single service account with the Domain Admins rights and supply this account for all InTrust operations.

In a production environment, we recommend that you granularly assign the required permissions to InTrust service accounts. For details, see System Requirements.

InTrust Organization Configuration Overview

In the InTrust organization that you are going to set up in this scenario:

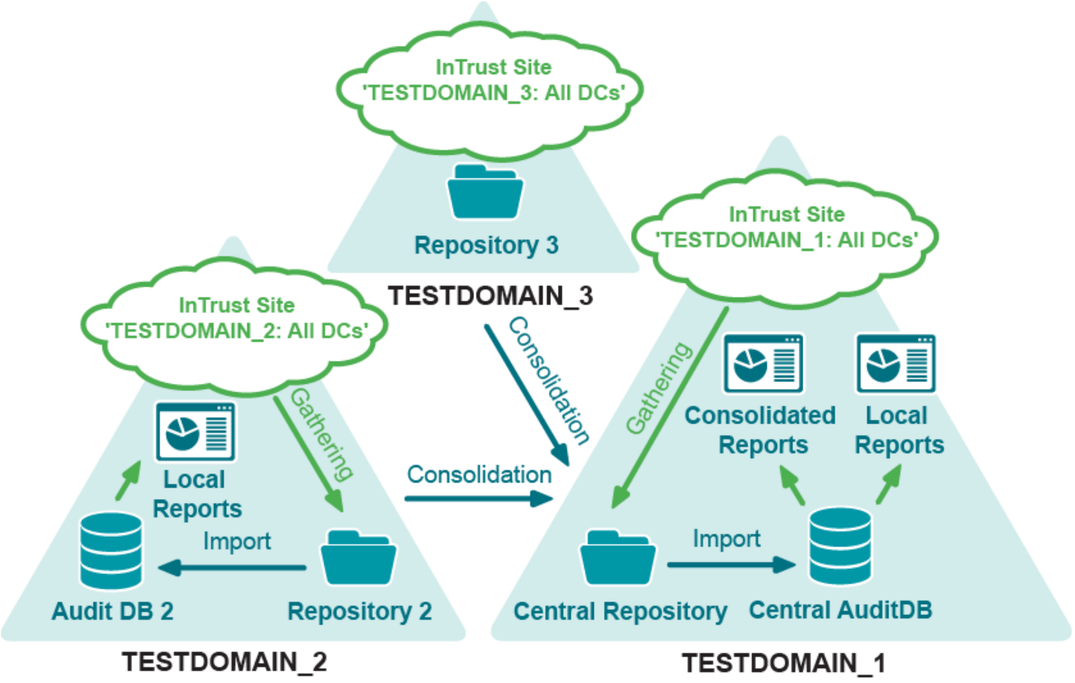
- InTrust servers are installed in each domain
- All InTrust servers are installed into one organization (this way it is possible to view all alerts in one central Monitoring Console)
- All InTrust servers share a single configuration database



Gathering Configuration Overview

Gathering is configured as follows in this scenario:

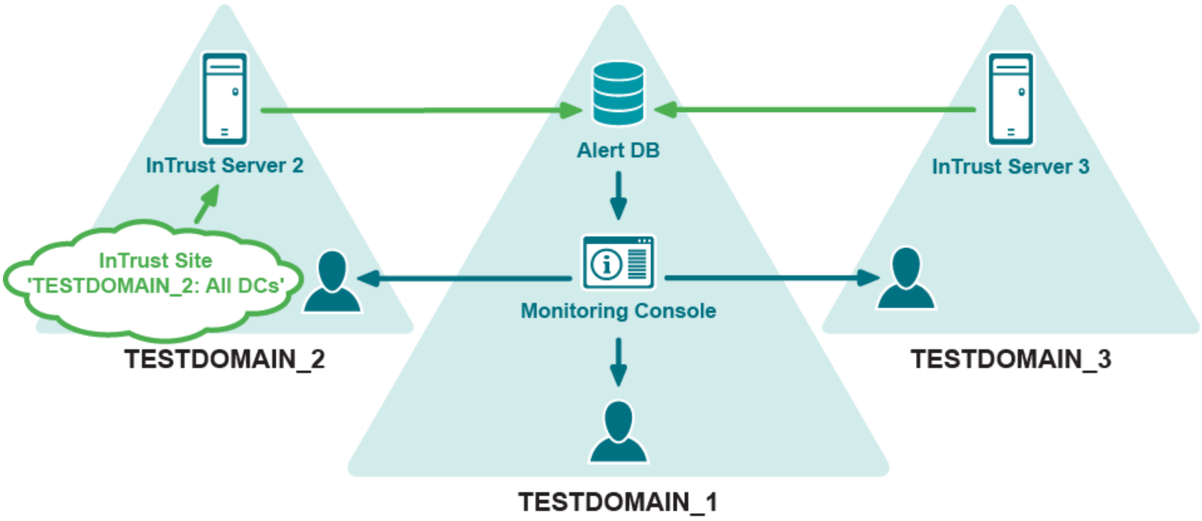
- Audit data is collected into local repositories and audit databases in each domain.
- The central repository and central audit database stand for the local ones in TESTDOMAIN_1 (in a production environment, it would be reasonable to separate the central repository and audit database from the local ones in TESTDOMAIN_1 to speed up local report generation).
- Domain-level reports are generated and distributed in domains 2, 3, and 4.
- Local repositories from domains 2, 3 and 4 are consolidated into the central repository in TESTDOMAIN_1.
- Audit data is imported from the central repository into the central audit database.
- Consolidated reports and local reports for TESTDOMAIN_1 are generated using the central audit database.



Real-Time Monitoring Configuration Overview

Real-time monitoring is configured as follows in this scenario:

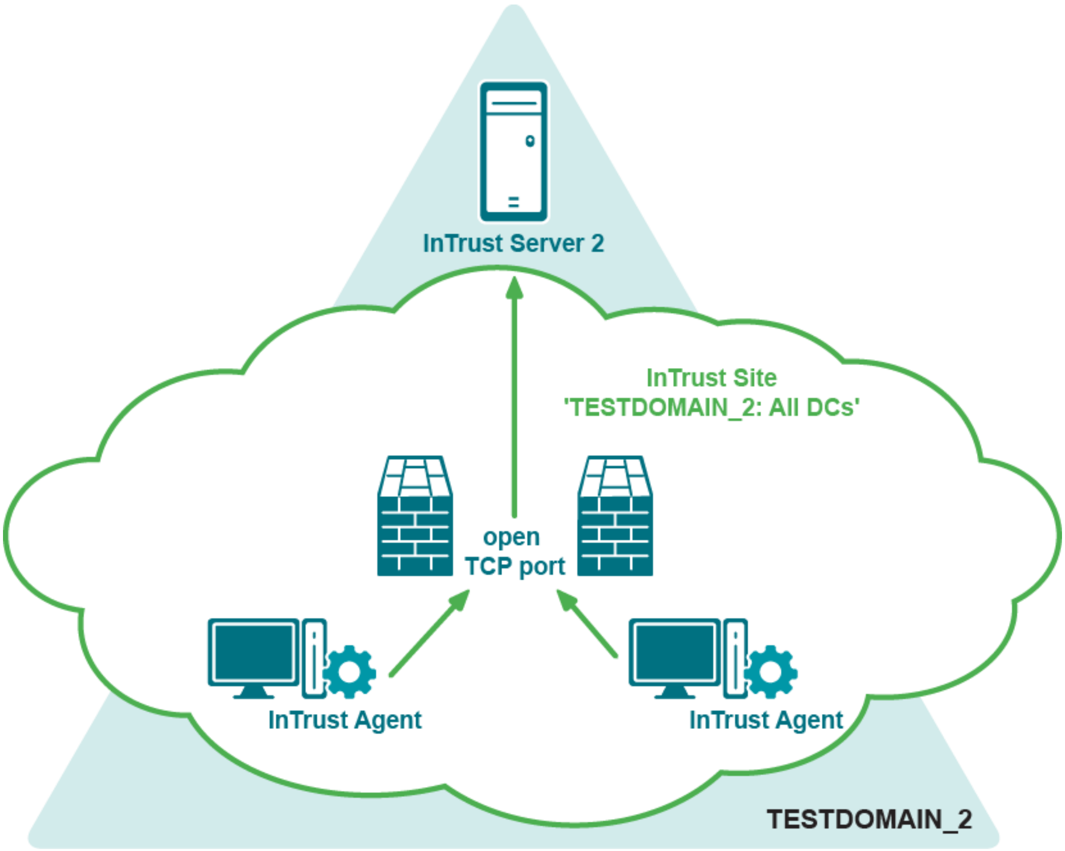
- InTrust Monitoring Console is installed in TESTDOMAIN_1.
- InTrust servers send alerts to the central alert database.
- Users from all domains access Monitoring Console using their alerting profiles and get the alerts they are allowed to view (for an explanation of alerting profiles, see the Handling Alerts topic).



Gathering and Monitoring over the Firewall

To make InTrust agents operate over a firewall, you must open a port on the firewall to allow incoming traffic from outside to the address/port of the specific InTrust server (listening port). The listening port number that the InTrust server will use is specified during InTrust Server installation.

InTrust agents must be installed manually on computers behind the firewall; see Installing Agents Manually for details.



Installing Servers

To install InTrust servers, follow the setup steps, as described in the Performing Extended Deployment of InTrust topic. When installing the first server in the organization, you will need to specify a configuration database, and InTrust organization's name and password. When installing servers into existing organization, you will have to supply this password.

NOTE: Do not perform server installations simultaneously—servers must be installed sequentially, one after another.

Installing Agents

The InTrust agent installation procedure (for auto and manual installation) is described in the Deploying Agents topic and in Installing Agents Manually.

By default, agents run under the LocalSystem account. For information on how to change the agent account, refer to the Changing the Agent Account topic.

Configuring and Populating InTrust Sites

InTrust is shipped with a number of predefined elementary configuration objects, such as InTrust sites, gathering policies and tasks, monitoring rules, and so on.

It is recommended that you not change predefined sites directly to conform to your environment. Instead, consider copying existing predefined sites that correspond to the sites you need, and making changes to the copies.

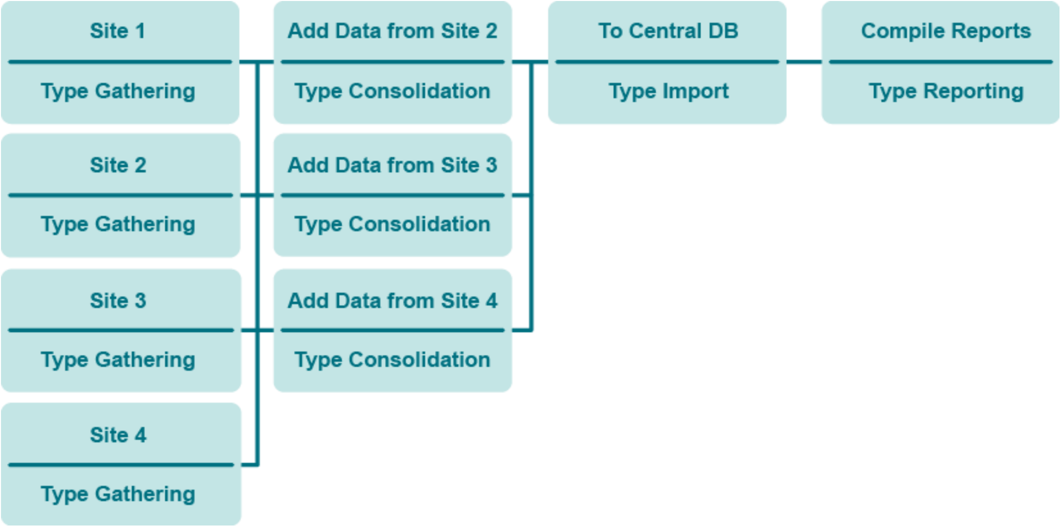
To configure sites that will be used within your gathering task and monitoring policy, take the following steps:

1. Run InTrust Manager.
2. Based on the "All Windows servers in the domain" site, create sites corresponding to your domains that include all servers, give them descriptive names, and assign each of the sites the InTrust server from the corresponding domain.
3. In each site, add a shortcut to the corresponding domain.
4. Add computers located behind the firewall (agents must be installed manually).
5. Commit the configuration.

Setting Up Gathering and Reporting on Events

You are going to make InTrust do the following:

- Gather data to several repositories
- Consolidate from repositories to a central repository
- Import from the central repository to an audit database (for centralized reporting)



Take the following steps:

1. Remove the link between the predefined gathering job and the predefined reporting job; to do it, right-click either job and select **Dependencies** to open the corresponding dialog box.
2. Configure the gathering job to collect data from an InTrust site to the central repository.
3. Create more gathering jobs on the InTrust servers from other sites. These jobs collect data to separate repositories.
4. Create consolidation jobs that consolidate the gathered data from the repositories to the central repository.
5. Link each of the gathering jobs except the first with each of the consolidation jobs (you can use the drag and drop operation to create a link); this will ensure that the consolidation does not start until the gathering is finished.
6. Create an import job that imports the data from the central repository to the central audit database.
7. Link the each of the consolidation jobs with the import job to ensure that the import follows the consolidation.
8. Link the import job with the predefined reporting job.
9. Modify the reporting job as necessary. Configure a notification option in the reporting job to stay informed about the reporting process.
10. Commit the configuration.

You can also add notification jobs next to the gathering jobs to stay informed of the data gathering process.

For details about setting up tasks and jobs, see the Auditing Guide.

Extra: Configure Gathering of Microsoft IIS Events

1. Use a copy of the predefined InTrust site for Microsoft IIS servers.
2. Add servers located behind the firewall to the site.
3. Configure the "IIS Daily Collection task" similar to the "Windows and AD Security Daily Collection and Reporting" task.

Setting Up Real-Time Monitoring of Security Events

To deploy the predefined Windows/AD Security: full policy

1. Specify parameters for predefined rules, such as authorized groups.
2. Right-click the **Windows/AD Security: full** policy and select **Properties**.
3. On the **General** tab, select **Activate**.
4. On the **Sites** tab, specify the sites to be monitored (**TESTDOMAIN_1: All servers** and so on).
5. Click **OK**.
6. Commit the configuration.

Monitoring Your Environment

The following are instructions on testing real-time monitoring of business critical security events in your network. The “Member added to administrative group” rule will be involved. When an account is added to an administrative group, this rule generates an alert, removes the account from the group and disables the account that added it. Take the following course of action:

1. In Monitoring Console, use the default profile or create a new one, than create an alert view for user accounts (those which have sufficient rights to view the alerts and modify their state for specified sites and rule groups).
2. In the InTrust Manager, right-click the “Member added to administrative group” rule, from the shortcut menu select **Properties**, and in the Properties dialog box enable the rule; on the **Response Actions** tab, select to execute two scripts (**Disable User** and **Remove User from Group**).
3. Verify that the rule is applied to the right InTrust site via the right monitoring policy; to do it, open the Properties dialog box of the corresponding policy.
4. Make sure that the users for which you created the profile have sufficient rights to work with alerts in Monitoring Console. This step is optional.For that, open InTrust Manager and right-click the policy bounding the rules you need to the InTrust sites you want to monitor, and from its shortcut menu, select **Properties**. Click the **Alert Security** tab and configure access rights for user or group accounts you need.
5. Enable the monitoring policy.
6. Commit the changes.
7. Verify that the rule works as expected: open the Active Directory Users and Computers snap-in under an account that is not an InTrust organization administrator (see InTrust Organization Administrators for details) and not the InTrust agent account, and add a user to the administrative group:
    - Check the Monitoring Console view for the alert generated by the rule.
    - Check in the Active Directory Users and Computers snap-in that the account responsible for the addition has been disabled.

Once the rule has done the following, consider the test passed:

- Disabled the account that added the user to the administrative group
- Removed the user from the administrative group
- Generated an alert viewable in Monitoring Console

For details about real-time monitoring in InTrust, see the Real-Time Monitoring Guide.

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