Quest®

Quest® InTrust 11.3

Auditing and Monitoring Microsoft Windows

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 Auditing and Monitoring Microsoft Windows
Updated - May 2017
Version - 11.3

Contents

Windows Auditing and Monitoring Overview

Microsoft Windows event logs provide historical information that can help you track down the operation and security of your Windows-based network. The event-logging service controls whether events are tracked on Windows-based systems. When this service is started, you can track user actions and system resource usage events with the following event logs:

- Application Log—records events logged by applications, such as the failure of MS SQL to access a database.
- Security Log—records events set for auditing with local or global group policies, providing information about logon activity, account management, and file and object access events.
- System Log—records events logged by the operating system or its components, such as the failure of a service to start at boot-up.
- Directory Service Log—records events logged by Active Directory and its related services.
- DNS Server Log—records DNS queries, responses, and other DNS activities.
- The DFS Replication log (File Replication Service log in pre-Windows 2008 systems) contains events logged by the DFS Replication service that enables you to synchronize folders on multiple servers across local or wide area network (WAN) network connections.
- User session events—although these events are not contained in a traditional Windows event log (they are not written to any ***.evt** files and are not viewable in Event Viewer), these custom events are treated exactly like true Windows events by InTrust and are important for Windows security auditing.

The following two sections provide you with more details on Windows Security log events and user session events:

- Windows Security Log
- User Session Events

This data can help you detect suspicious activity and audit major administrative tasks.

Windows Security Log

Event records contained in the security log can be grouped according to the audit policy categories they are tracked with. Some events are generated by all versions of the Windows operating system; others are version-specific (for example, generated by Windows Server 2008). The common security event categories common to all versions are described below.

Logon Events

Logon events are generated on the computer to which the logon attempt was made, whether the attempt was an interactive or a remote logon. Events related to this category allow you to track user logons to network computers and discover suspicious activity that might lead to security incidents (such as logon failures due to bad passwords or logons during non-business hours).

Account Logon Events

Account logon events are generated when user tries to logon on the computer or domain:

- Logon attempts with domain accounts
  These events are recorded in the security log on the domain controller irrespectively where authentication was taken place.
- Logon attempts with local accounts that are stored on the local computer.
  These logon events are recorded in the security log on the computer where user tries to log in.

Account Management

These events are related to users account management, and to group and group membership management tasks. These tasks should be performed by administrators. If the administrator fails to carry out these tasks, this may lead to account misrule and security violations. The following events are included:

- User account management—events related to the creation, deletion, enabling, or disabling of user accounts
- Group management—events related to the creation, deletion, enabling, or disabling of groups
- Group membership management—events related to adding or removing user accounts from groups

System Events

The security log contains records on the important system events, allowing you to monitor for your system operation: system startup/shutdown, system time change, and other events. For example, the “Audit log was cleared” event in this category helps you discover potential intruder activity and attempts to cover the tracks.

Object Access

These events help you to find out whether an object of a certain type (printer, server, file, registry key, etc.) was accessed by a user, and what operations were performed on the object (for example, an attempt to delete).

Note, that Active Directory objects are not included in this category (for more information see Directory Service Access section below).

Policy Change

Policy change events include security event messages involving trust relationships, IPSec policy, and user rights assignments.

Privilege Use

These events help you investigate changes to a user's privileges or attempts to use privileges in an unauthorized manner.

Process Tracking

These events help you to find out what software is running on the work stations and on the servers. Information about processed tasks and object access data allow you to stay informed on users' activity in whole.

NOTE: In Event Viewer terminology the Detailed Tracking events category is the same as Process Tracking events.

Directory Service Access

Directory Service Access events allow you to monitor for AD objects access. These events are also recorded in the Windows security log.

NOTE: Since Windows Server 2008, the Audit directory service access policy is divided into the following categories:

- Directory Service Access
- Directory Service Changes
- Directory Service Replication
- Detailed Directory Service Replication

To learn more about directory service audit in Windows 2008, search Microsoft TechNet (http://technet.microsoft.com) for "AD DS Auditing Step-by-Step Guide".

User Session Events

InTrust lets you extend the auditing of logon activity on any Windows computer where an InTrust agent is installed. In addition to the generic logon and logoff information from the Security log, you get details about the following:

- When and how long the computer was actually in use between logon and logoff
- What caused periods of inactivity between logon and logoff (user switching, screensaver, computer lock)
- Concurrent user activity on the computer

On computers where these events are tracked, you do not have to look at the generic Security log logon and logoff events. InTrust-provided user-session auditing is more complete and (especially in the case of logoff auditing) more dependable.

These events are generated by the Quest InTrust User Session Monitor service, which is installed together with the InTrust agent. This service makes the events available to the agent through the agent cache, and the agent works with them as with any Windows events.

From the agent's perspective, these events come from the “InTrust User Session Tracking” event log, for which the **InTrust User Session Tracking** data source is provided. Gathering, real-time monitoring, reporting, browsing in Repository Viewer and other operations work for these events without limitations.

This table lists the events logged by the Quest InTrust User Session Monitor service.

Event ID	Description	Insertion Strings
100	A user session by user %IS1% took place on computer %Where%, starting at %IS13%, ending at %IS15% and lasting %IS16%. The session was started from computer %IS7% (IP address %IS8%). Reason for session start: %IS23%. Reason for session end: %IS24%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13 • End Time: %15 • Duration: %16 • Session Start Type: %17 • Session End Type: %18
101	A user session was started on computer %Where% by user %IS1% logging on at %IS13% with the %IS10% logon type.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13
102	A user session was ended on computer %Where% by user %IS1% logging off at %IS15%. The user session lasted %IS16%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13 • End Time: %15 • Duration: %16
103	A user session was ended on computer %Where% by user %IS1% locking the computer at %IS15%. The user session lasted %IS16%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13

Event ID	Description	Insertion Strings
		• End Time: %15 • Duration: %16
104	A user session was started on computer %Where% by user %IS1% unlocking the computer at %IS13%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13
105	A user session was started on computer %Where% by user %IS1% due to user switch at %IS13%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13
106	A user session was ended on computer %Where% by user %IS1% at %IS15%, because a user switch was performed. The user session lasted %IS16%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13 • End Time: %15 • Duration: %16
107	A user session was started on computer %Where% by user %IS1% making a terminal services connection from computer %IS17% (IP address %IS18%) at %IS13.	• User Name: %1 • Start Time: %15 • Duration: %16
108	A user session was ended on computer %Where% by user %IS1% logging off at %IS15% and stopping a terminal services connection from computer %IS17% (IP address %IS18%). The user session lasted %IS16%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13 • End Time: %15 • Duration: %16

Event ID	Description	Insertion Strings
110	An incorrectly finished user session by user %IS1% was found on computer %Where% while the user session monitoring service was starting. The session started at %IS13%, lasted %IS16% and ended at %IS15%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13 • End Time: %15 • Duration: %16
111	A user session was started on computer %Where% by user %IS1% before the start of the user session monitoring service. This session was detected at %IS13%.	• User Name: %1 • Domain Name: %2 • DNS Domain Name: %4 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13
120	The user session monitoring service was started on computer %Where% at %Time%.	• User Name: %1 • Domain Name: %2
121	The user session monitoring service was stopped on computer %Where% at %Time%.	• User Name: %1 • Domain Name: %2
130	A user session of user %IS1% was ended on computer %Where% by the screensaver turning on at %IS15%. The user session lasted %IS16%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13
131	A user session was started on computer %Where% by user %IS1% exiting screensaver mode at %IS13%.	• User Name: %1 • Domain Name: %2 • Logon Type: %9 • Source Workstation: %10 • Source Network Address: %11 • Start Time: %13 • End Time: %15

How to Gather Event Log Data

Audit data can be collected with InTrust from the computers running any of the following:

- Microsoft Windows 10
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 8
- Microsoft Windows Server 2008 R2
- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista

For more details, see the following topics:

- Setting Up Auditing
- Configuring InTrust

Setting Up Auditing

To turn on auditing on the target computer, configure the Audit Policy in the Group Policy Management Editor MMC snap-in.

There is an alternative to edit a local policy on every computer or propagate audit settings applying group policy to computers that are included in the certain organizational unit. Generally, you can set each policy to audit for event success or failure or both.

To collect exactly the events required for particular reports, refer to the Windows Auditing References.

To simplify Windows event data gathering and reporting, InTrust offers a special Windows Knowledge Pack containing, in particular, predefined gathering and import policies, tasks, and reports.

NOTE: The Windows Knowledge Pack is always installed together with InTrust Server. This component is not included in an explicit form in the InTrust feature list. The Windows Knowledge Pack is installed by default.

Configuring InTrust

To configure the gathering of Windows event data with InTrust:

1. In InTrust Manager, select **Configuration | Sites | Microsoft Windows Network**, than select the **All Windows servers in the domain** site, or select another existent site (**All Windows workstations in the domain**, etc.) or create a new one.
2. To automatically install agents on the site computers, clear the **Prohibit automatic agent deployment on site computers** option in the site's properties and select **Install Agents** from the site's context menu. Gathering with and without agents is described below in detail.
3. Either select the **Windows and AD Security Daily Collection and Reporting** task, or configure a new task you need, with a gathering job that involves the necessary gathering policy and site.
4. Configure a reporting job, if necessary.

Gathering With and Without Agents

Usually, audit trails are collected using agents. If the agent is not running under the **LocalSystem** account, then its account must be granted **Manage auditing and security log** right to gather events from the Security event log. To run the gathering job with agents, select the **Windows and AD Security Daily Collection and Reporting** task, click the **Gathering** tab on the right, and make sure the **Use agents to execute this job on target computers** check box is selected.

However, in some cases you may need to work without agents (for example, if running extra services on the certain computers is not allowed). If so, you can prevent agents from being installed automatically on those computers; for that, do the following:

1. Use InTrust Manager to arrange those computers into a site.
2. In the site properties, select the **Prohibit automatic agent deployment on site computers** check box.

The account under which the gathering service will access site computers (which is either specified explicitly in the site's settings, or inherited from the InTrust server or task) requires the following:

- **Access this computer from the network** right must be granted.
- **Deny access to this computer from network** right must be disabled.
- **Manage auditing and security log** right must be granted to gather events from the Security log; members of the local Administrators group have this right by default.
- To clear logs after gathering, account membership in the local **Administrators** group is required.

The **Admin$** share must exist and should be open on target computer.

> **CAUTION: If you want to gather events from an event log on a computer, make sure the agent or, for agentless gathering, the gathering job account has Read access in the ACEs of the appropriate logs. You can use Group Policy to grant these permissions automatically. For details, refer to Microsoft Knowledge Base article 323076.**

Collecting Event Descriptions

Events from the Microsoft Windows event logs have standard descriptions which InTrust collects as follows:

- If the events are gathered to a repository, event descriptions are collected automatically.
- If the events are gathered to an audit database and you need the event descriptions to be collected, locate the necessary log in **Quest InTrust Manager | Configuration | Data Sources**, and open its Properties dialog box from the context menu. Click the **Microsoft Windows Events** tab and select **Store event descriptions to database**.
- Also, on that tab you can select whether to resolve SIDs and GUIDs in insertion strings.

> **NOTE:** This option can be used for Security log only.

Collecting Without Agents

If you are not using agents for gathering, you can select what libraries to use when retrieving standard descriptions for Windows events. The descriptions can be taken from libraries that exist locally on processed computers or from remote computers.

To select which libraries to obtain descriptions from

1. In the Data Sources, select the Microsoft Windows log you need, and open its properties.
2. On the **Microsoft Windows Events** tab, specify the order in which the libraries should be used:
    - Select **Only local** to retrieve the descriptions from libraries that exist on the InTrust server.
    - Select **Local, then remote** to first retrieve the descriptions from the InTrust server libraries; if they cannot be retrieved, libraries on the remote (processed) computer will be used.
    - Select **Remote, then local** to first retrieve the descriptions from libraries on the remote (processed) computer as long as they are available; if they cannot be retrieved, libraries on the InTrust server will be used.

Keeping Event Data Backup on the Agent Side

To ensure the integrity of event data from the specified data source, you can create agent-side log backups. This helps protect data from being lost event if accidental or malicious log cleanup occurs on the target machine. Log backups can be created for the most frequently used data sources, including Windows Event logs.

Agent-side log backup uses a compression method similar to that used in InTrust repositories. On average, the contents of the event cache are compressed to 1/40th their original size. Nevertheless, consider that using this feature requires additional space on the agent side. So it is recommended that you specify a reasonable retention period for agent-side log backups.

Agent-side log backup is unavailable for gathering-only data sources such as Microsoft ISA Server logs and Microsoft Proxy Server logs.

To use agent-side log backup

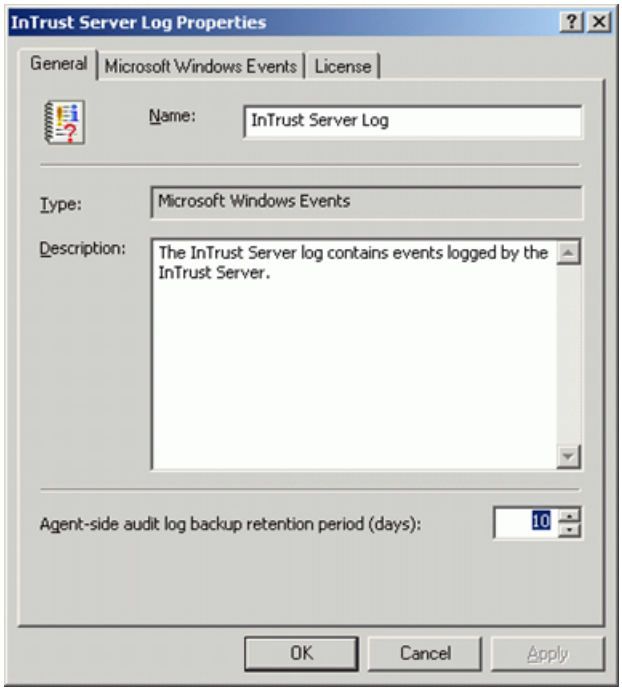
1. Select the data source under the gathering policy.
2. Select **Properties** from the context menu, and select the **Enable log backup and use it to gather events** option on the **General** tab.
3. Click **OK** to save your settings and close the dialog box.
4. Commit the changes by clicking the **Commit** button in the InTrust toolbar.

> **CAUTION: An agent-side log backup will be created if all of the following conditions are met:**
>
> 1. **At least one gathering policy processing this log uses it with this option selected**
> 2. **At least one task involving this policy has the task schedule enabled**
> 3. **The gathering job in this task has the Use agents to execute this job on target computers checkbox selected.**

To set the log backup retention period

1. Select **Configuration | Data Sources**, and select the necessary data source.
2. From its context menu, select **Properties**.

3. On the **General** tab, specify the agent-side log backup retention period:

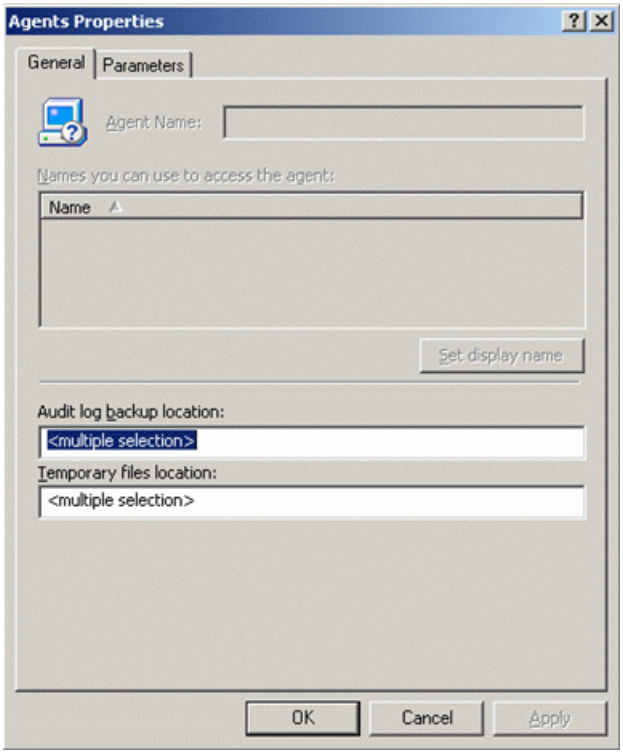


4. Click **OK** to save your settings and close the dialog box.

To change the location of agent log backup and temporary files

1. From **Configuration | InTrust Servers**, select the InTrust server the the agent you need responds to.
2. Expand the server node, and click **Agents**. The list of agents is displayed on the right.
3. Right-click the required agent, and from its shortcut menu select **Properties**.
4. On the **General** tab, specify agent temporary files location and agent log backup location you need.

CAUTION: These settings can be also specified for the whole list of agents responding to InTrust Server that InTrust Manager is connected to. Select all agents in the list, then right-click and select Properties.


Agents Properties
General
Parameters
Agent Name:
Names you can use to access the agent:
Name
Set display name
Audit log backup location:
<multiple selection>
Temporary files location:
<multiple selection>
OK
Cancel
Apply

How to Gather User Session Data

As with event log gathering, you can collect user session data with InTrust from the computers running any of the following:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 8
- Microsoft Windows Server 2008 R2
- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista

To configure the gathering of Windows event data with InTrust

1. In InTrust Manager, select **Configuration | Sites | Microsoft Windows Network**, than select the **All Windows servers in the domain** site or some other site (such as **All Windows workstations in the domain**). Alternatively, create a new one.
2. To automatically install agents on the site computers, clear the **Prohibit automatic agent deployment on site computers** option in the site's properties. For user session data, this is a requirement. Select **Install Agents** from the site's context menu.
3. Either select an existing task, or configure a new task as necessary, with a gathering job that involves the necessary gathering policy and site. The gathering policy must include the **InTrust User Session Tracking** data source.
4. Configure a reporting job, if necessary.

How to Monitor for Critical Events

To monitor for critical events on Windows-based computers, InTrust agents are used on target sites. If the agents are not yet installed, they will be deployed automatically as soon as you activate a real-time monitoring policy.

To simplify the configuration of the real-time monitoring workflow, InTrust Knowledge Pack for Windows offers predefined monitoring rules and policies.

To configure monitoring for Windows events with InTrust

1. In InTrust Manager, carry out the following:
    a. Enable the rule that will handle the events you need, for example, failed logons, or any other rule from **Real-Time Monitoring | Rules | Windows/AD Security**.
    b. Activate a monitoring policy that will bind this rule to your InTrust site, such as the **Real-Time Monitoring | Policies | Windows/AD Security: Detecting Common Attacks** policy, or any other policy you need.
    c. If you want to set notification upon alert generation, select the monitoring policy and from its context menu select **Properties**. Click **E-mail** or **Net send** tab to choose a notification method. Select Notify the following operators checkbox to specify recipients that will be notified. To add desired operators to the notification group in the **Configuration | Personnel**, select **Notification Groups** and add the recipient to a group.

> **NOTE:** Make sure this notification method is also specified in the corresponding rule's properties.

    d. Select the site you will monitor, and from its context menu, select **Properties**. Click **Security**, and make sure the list of accounts includes users you want to be able to work with the alerts (as alert readers or alert managers). Check the same for the rule group containing the rule you are using.
2. In Monitoring Console, do the following:
    a. Open the profile you want to work with, or create a profile by running Monitoring Console Administration from the Start menu.
    b. Configure an alert view to display the necessary alerts.

For detailed information on configuring gathering and monitoring processes, refer to the Auditing Guide and Real-Time Monitoring Guide.

Gathering Windows DHCP Server Events

You can use InTrust to gather the following audit trails from Microsoft DHCP Server:

- Microsoft DHCP Server Audit log
- Windows System log (events generated by DHCP Server)

The DHCP server audit log stores information about events generated when IP addresses are assigned, revoked and so on.

> **CAUTION: The Microsoft DHCP Server Log data source type treats event times as local time. If you collect events for a period during which time was set back due to daylight saving time adjustments, the event times will be incorrect after the adjustment for the duration of the difference.**

To enable DHCP server logging

1. Click **Start | Settings | Control Panel**, double-click **Administrative Tools**, and then double-click **DHCP**.
2. In the console tree, click the applicable DHCP server. If working on a Windows 2008-based computer, select the applicable IP version.
3. On the **Action** menu, click **Properties**.
4. On the **General** tab, select **Enable DHCP audit logging**, and then click **OK**.

To collect data from Microsoft DHCP Server Audit Log

1. Turn on DHCP server logging
2. Use the **Windows/AD: DHCP** gathering policy provided with InTrust Knowledge Pack for Windows.

Rights and Permissions for Data Gathering Without Agent

The following is required to gather DHCP server audit data without agents:

- **Access this computer from the network** right. (**Deny access to this computer from network** right must be disabled.)
- **Read** permission to the **HKLM\SYSTEM\CurrentControlSet\Services\ DHCPServer\Parameters** registry key.
- **Read** permission to the **HKLM\SYSTEM\CurrentControlSet\Control\ TimeZoneInformation** registry key.

- **Read** permission to the **HKLM\SYSTEM\CurrentControlSet\Control\Nls\Language** registry key.
- Membership in the local **Administrators** group.
- **Read** and **List Folder Contents** permissions to log file folders; the **Delete** permission must also be granted if the **Clear log files after gathering** option is turned on for the data source.

Rights and Permissions for Data Gathering With Agent

The following is required to gather DHCP server audit data using agent:

- **Read** permission to the **HKLM\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters** registry key.
- **Read** permission to the **SYSTEM\CurrentControlSet\Control\TimeZoneInformation** registry key.
- **Read** and **List Folder Contents** permissions to log file folders; the **Delete** permission must also be granted if the **Clear log files after gathering** option is turned on for the data source.

InTrust Predefined Objects for Windows-Based Computers

InTrust offers a set of predefined objects that will help you configure the gathering and monitoring event data from your Windows-based computers. The following is a list of these objects. For a list of Windows reports, see Reports for Microsoft Windows.

Gathering Policies

- Windows/AD: Security: All Events
  Defines all Windows/AD security events to be collected to a repository. The most critical security events, such as Failed Logons, Account Management, etc. are to be collected into database for analysis. The policy is intended to be used for gathering on a daily basis.
- Windows/AD: Security: All Logons
  Defines the Logon events to be collected both to a repository and a database.
- Windows/AD: Security: Failed Logons
  Defines the Failed Logon events to be collected to both a repository and a database.
- Windows/AD: Security: Account Management
  Defines the Account Management events to be collected both to a repository and a database.
- Windows/AD: Security: Policy Changes
  Defines the Policy Changes to be collected both to a repository and a database.
- Windows/AD: Security: Objects Access
  Defines the Object Access events to be collected both to a repository and a database.
- Windows/AD: Security: Misc
  Defines all Windows/AD miscellaneous security events to be collected to a repository. The most critical of miscellaneous security events such as Security Subsystem and Audit Subsystem Faults are to be collected into database for analysis.
- Windows/AD: DHCP
  Collects all the DHCP events from both the Windows System Log and the DHCP Audit Log to a repository and a database.
- Windows/AD: Security: Objects Access: Registry Access
  Defines the Registry Access events to be collected both to a repository and a database.
- Windows/AD: Successful AD Administrator Logons
  Defines the AD Administrator events to DC to be collected both to a repository and a database.

- Auditing Domain Controllers: Events from DCs
  Defines all events from domain controller logs to be collected to the repository and then imported to an audit database as part of the “Auditing Domain Controllers” best practice scenario. No filters are applied.
- Auditing Domain Controllers: Events from DCs for the Last 24 Hours
  Defines all events from domain controller logs to be collected to the repository and then imported to an audit database as part of the “Auditing Domain Controllers” best-practice scenario. All events older than 24 hours are filtered out.
- Auditing Exchange Servers: Events from Exchange Servers
  Defines all Exchange-related events to be collected to the repository and then imported to an audit database as part of the “Auditing Exchange Servers” best practice scenario. No filters are applied.
- Auditing Exchange Servers: Exchange Events for the Last 24 Hours
  Defines all Exchange-related events to be collected to the repository and then imported to an audit database as part of the “Auditing Exchange Servers” best practice scenario. All events older than 24 hours are filtered out.
- Auditing File Servers: Events from File Servers
  Defines all file server-related events to be collected to the repository and then imported to an audit database as part of the “Auditing File Servers” best practice scenario. No filters are applied.
- Auditing File Servers: File Server Events for the Last 24 Hours
  Defines all file server-related events to be collected to the repository and then imported to an audit database as part of the “Auditing File Servers” best practice scenario. All events older than 24 hours are filtered out.
- Auditing Workstations: Events from Workstations
  Defines all events from desktop logs to be collected to the repository and then imported to an audit database as part of the “Auditing Workstations” best practice scenario. No filters are applied.
- Auditing Workstations: Events from Workstations for the Last 24 Hours
  Defines all events from desktop logs to be collected to the repository and then imported to an audit database as part of the “Auditing Workstations” best practice scenario. All events older than 24 hours are filtered out.

Import Policies

- Windows/AD: Security: All Events
  Defines all Windows/AD security events to be imported to a database for analysis.
- Windows/AD: Security: All Logons
  Defines the Logon events to be imported to a database.
- Windows/AD: Security: Failed Logons
  Defines the Failed Logon events to be imported to a database.
- Windows/AD: Security: Account Management
  Defines the Account Management events to be imported to a database.
- Windows/AD: Security: Policy Changes
  Defines the Policy Changes to be imported to a database.
- Windows/AD: Security: Objects Access
  Defines the Object Access events to be imported to a database.

- Windows/AD: Security: Misc
  Defines the most critical of miscellaneous security events such as Security Subsystem and Audit Subsystem Faults to be imported to database for analysis.
- Windows/AD: DHCP
  Imports the DHCP events from both the Windows System Log and the DHCP Audit Log to a database.
- Windows/AD: Security: Objects Access: Registry Access
  Defines the Registry Access events to be imported to a database.
- Windows/AD: Successful AD Administrator Logons
  Defines the AD Administrator events to DC to be imported to a database.
- Auditing Domain Controllers: Weekly Reporting
  Defines events from the Windows Security, System and Application logs and the InTrust for AD log to be imported to an audit database. Events older than one week are excluded.
- Auditing Domain Controllers: Daily Reporting
  Defines events from the Windows Security, System and Application logs and the InTrust for AD log to be imported to an audit database. Events older than one day are excluded.
- Auditing Exchange Servers: Weekly Reporting
  Defines events from the Windows Security, System, Directory Service and Application logs, Exchange tracking log and CA for Exchange log to be imported to an audit database. Events older than one week are excluded.
- Auditing Exchange Servers: Daily Reporting
  Defines events from the Windows Security, System, Directory Service and Application logs, Exchange tracking log and CA for Exchange log to be imported to an audit database. Events older than one day are excluded.
- Auditing File Servers: Weekly Reporting
  Defines events from the Windows Security, System, Directory Service and Application logs and CA for file servers log to be imported to an audit database. Events older than one week are excluded.
- Auditing File Servers: Daily Reporting
  Defines events from the Windows Security, System, Directory Service and Application logs and CA for file servers log to be imported to an audit database. Events older than one day are excluded.
- Auditing Workstations: Weekly Reporting
  Defines events from the Windows Security, System and Application logs to be imported to an audit database. Events older than one week are excluded.
- Auditing Workstations: Daily Reporting
  Defines events from the Windows Security, System and Application logs to be imported to an audit database. Events older than one day are excluded.

Jobs

- All Windows and AD Security Events collection
  Collects all the Windows/AD security events to the default repository. The most critical security events such as failed logons are also collected to the default database for analysis
- DHCP Events collection
  Collection of the DHCP events to the default repository and the default database.
- Daily Windows and AD Security Events Reporting
  Controls daily reporting of the most critical Windows/AD security events

- Notify Security Operators
  Notifies the Security Operators notification group of task completion.
- InTrust Log Collection
  Collection of the InTrust log from all InTrust servers in the organization.
- Audit Database Cleanup
  Clears all default InTrust audit database contents older than one week.
- Event Collection
  Gathers all domain controller-related, all Exchange-related events, or all desktop-related events to the default repository.
- Reports on DCs
  Builds reports as part of the “Auditing Domain Controllers” best-practice scenario.
- Windows Event Log Reports
  Builds Windows log-based reports as part of the “Auditing Domain Controllers” best-practice scenario.
- ChangeAuditor for AD Reports
  Builds ChangeAuditor for AD reports as part of the “Auditing Domain Controllers” best-practice scenario.
- Event Import
  Imports all domain controller-related events, all Exchange-related events or all desktop-related events from the default repository to the default audit database.
- Reports on Exchange Servers
  Builds reports as part of the “Auditing Exchange Servers” best-practice scenario.
- CA for Exchange Servers Reports
  Builds CA for Exchange log reports as part of the “Auditing Exchange Servers” best-practice scenario.
- Reports on Workstations
  Builds reports based on the most common events as part of the “Auditing Workstations” best-practice scenario.
- Comprehensive Reports on Workstations
  Builds diverse reports as part of the “Auditing Workstations” best-practice scenario.

Tasks

- Windows and AD Security Daily collection and reporting
  Daily collection of all the Windows/AD security events to the default repository. The most critical security events such as failed logons are collected also to the default database for analysis.
- Weekly InTrust Log Collection
  Collection of the InTrust log from all InTrust servers in the organization.
- Auditing Domain Controllers: Daily Gathering
  Gathers all domain controller-related events to the default repository three times a day: about 6 AM, noon and 6 PM. This task is used in the “Auditing Domain Controllers” best-practice scenario when it is set to use a schedule.
- Daily Audit Database Cleanup
  Clears all default InTrust audit database contents older than one week. This task runs daily and is shared by all best-practice scenarios: “Auditing Domain Controllers”, “Auditing Exchange Servers”, “Auditing File Servers” and “Auditing Workstations”.

- Auditing Domain Controllers: Ad-Hoc Reporting for the Last 24 Hours
  Gathers domain controller-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing Domain Controllers” best-practice scenario.
- Auditing Domain Controllers: Daily Reporting
  Gathers domain controller-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing Domain Controllers” best-practice scenario. This task runs daily.
- Auditing Domain Controllers: Weekly Reporting
  Gathers domain controller-related events for the last week, imports them to the default audit database and creates reports as part of the “Auditing Domain Controllers” best-practice scenario. This task runs weekly.
- Auditing Exchange Servers: Daily Gathering
  Gathers all Exchange-related events to the default repository three times a day: about 6 AM, noon and 6 PM. This task is used in the “Auditing Exchange Servers” best-practice scenario when it is set to use a schedule.
- Auditing Exchange Servers: Ad-Hoc Reporting for the Last 24 Hours
  Gathers Exchange-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing Exchange Servers” best-practice scenario.
- Auditing Exchange Servers: Daily Reporting
  Gathers Exchange-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing Exchange Servers” best-practice scenario. This task runs daily.
- Auditing Exchange Servers: Weekly Reporting
  Gathers Exchange-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing Exchange Servers” best-practice scenario. This task runs weekly.
- Auditing File Servers: Daily Gathering
  Gathers all file server-related events to the default repository three times a day: about 6 AM, noon and 6 PM. This task is used in the “Auditing File Servers” best-practice scenario when it is set to use a schedule.
- Auditing File Servers: Ad-Hoc Reporting for the Last 24 Hours
  Gathers file server-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing File Servers” best-practice scenario.
- Auditing File Servers: Daily Reporting
  Gathers file server-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing File Servers” best-practice scenario. This task runs daily.
- Auditing File Servers: Weekly Reporting
  Gathers file server-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing File Servers” best-practice scenario. This task runs weekly.
- Auditing Workstations: Daily Gathering
  Gathers all workstation-related events to the default repository three times a day: about 6 AM, noon and 6 PM. This task is used in the “Auditing Workstations” best-practice scenario when it is set to use a schedule.
- Auditing Workstations: Ad-Hoc Reporting for the Last 24 Hours
  Gathers desktop-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing Workstations” best-practice scenario.

- Auditing Workstations: Daily Reporting
  Gathers desktop-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing Workstations” best-practice scenario. This task runs daily.
- Auditing Workstations: Weekly Reporting
  Gathers desktop-related events for the last 24 hours, imports them to the default audit database and creates reports as part of the “Auditing Workstations” best-practice scenario. This task runs weekly.

Sites

- All MS Windows NT based computers in the domain
  All supported Microsoft Windows-based computers in the domain
- All Windows servers in the domain
- All Windows desktops in the domain
- All DHCP servers in the domain
- All InTrust servers
- Auditing Domain Controllers: DCs
- Auditing Exchange Servers: Exchange Servers
- Auditing File Servers: File Servers
- Auditing Workstations: Workstations

Real-Time Monitoring Policies

- Windows/AD Security: full
  Specifies monitoring of all the security events on all the NT-based computers in the domain
- Windows/AD Security: Detecting Common Attacks
  Specifies only common attacks to be monitored on all the NT-based computers in the domain
- Windows/AD Security: Administrative Activity Monitoring
  Specifies administrative activity to be monitored on all the NT-based computers in the domain
- InTrust: Tracking Log Monitoring
  Specifies monitoring of critical events from all the InTrust servers in the organization.

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 https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

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