Quest®

Quest® InTrust 11.3

Preparing for Gathering Audit Collection Services Data

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

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

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

InTrust Preparing for Gathering Audit Collection Services Data
Updated - May 2017
Version - 11.3

Contents

Audit Collection Services Auditing Overview

Microsoft System Center Operations Manager 2007/2012 (Operations Manager) is already being used in many organizations to facilitate monitoring of Windows-based networks in real time. Audit Collection Services (ACS) is the part of Operations Manager that collects event records generated by an audit policy on a Windows-based computer and stores them in a centralized SQL Server database for further analysis and reporting. This capability helps to collect and consolidate security events from DCs, as long as large volumes of data are generated by audit policies on these computers.

When integrated with Operations Manager, InTrust brings new, powerful means of automating and streamlining your auditing workflow:

- **Long-term data storage, archival, and backup.** With InTrust, you can use file-based or Centera-based repositories to store audit data in a compressed form for any period of time; extract events from the repository and restore them in the original format if required; import events to the database for reporting when needed. These features help organizations comply with external regulations and internal policies.
- **Consolidation of audit trails from across your enterprise-wide network.** InTrust extends the consolidation capabilities of native Windows auditing tools, providing for consolidation of data from variety of platforms and applications. This allows for comprehensive analysis of your network operations and health.
- **Quest expertise in security events analysis.** InTrust and Operations Manager integration will provide you with reports on security data, helping you with in-depth analysis of valuable information collected throughout the network.

To integrate InTrust with Operations Manager, use the InTrust Knowledge Pack for Microsoft Audit Collection Services that is provided.

How Integration Works

Typical InTrust-Operations Manager integration scheme is explained in this section. Inter-operation of the components takes place as follows:

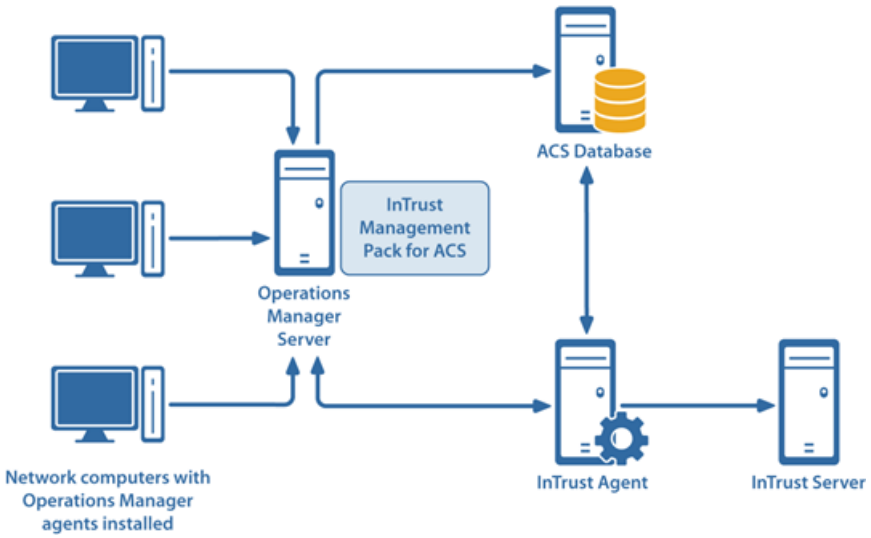
1. Audit Collection Services (ACS) of Operations Manager collects event records generated by an audit policy on Windows-based computers and stores them in a centralized SQL Server database (ACS database).
2. The InTrust component (ACSLogsCollector) obtains these event records and enriches them with the information required to comply with InTrust Audit DB format (Computer Type, time zone parameters, and Windows build number). For details, see the Pre-Processing Data topic.
3. The pre-processed event data is ready for the typical InTrust workflow, including automated gathering, storage to repository and/or database, and reporting.

This workflow can be implemented with InTrust agents (Scenario 1) or without InTrust agents (Scenario 2).

Scenario 1

An agent communicates with the ACS database and with the Operations Manager server to pre-process event records and execute InTrust gathering jobs.

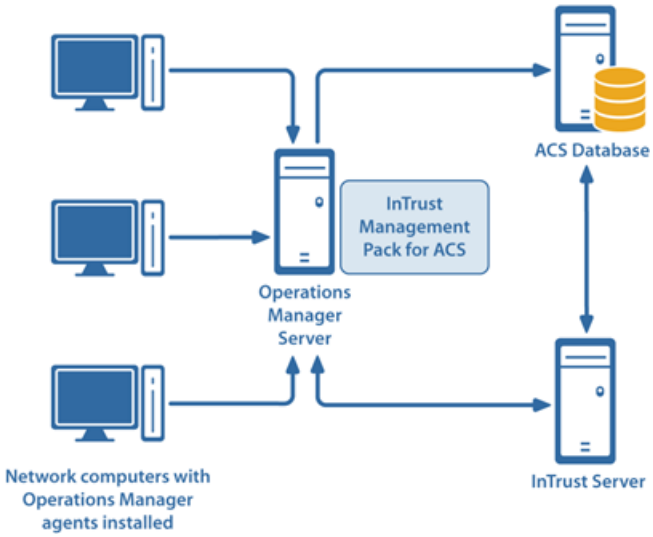
CAUTION: If you plan to deploy an InTrust agent on a dedicated computer, then Operations Manager console must be installed on the computer hosting the InTrust agent. (This component provides the Operations Manager API SDK required for interaction between Operation Manager and InTrust.) Make sure that target computer is running the same version of the Operations Manager console as your Operations Manager server.



Scenario 2

If so, an InTrust server will communicate with Operations Manager server and the ACS database; it will also pre-process event records and execute gathering jobs. Note, however, that server load will significantly increase if data is gathered without agents.

> **CAUTION: If you plan to collect data without using InTrust agents, then the Operations Manager console must be installed on the computer hosting the InTrust server. Make sure this console is of the same version as the Operations Manager console running on the Operations Manager server.**



Pre-Processing Data

In order for event records to be stored in the ACS database, native Windows event format is converted according to transformation rules defined in the EventSchema.xml file stored on Operations Manager server. Writing these events into the InTrust Audit database requires reverse transformation, and therefore authorized InTrust components must have access to the transformation rules (that is, to **EventSchema.xml**). For details, see the Gathering with and without Agents topic.

In addition, to comply with in the InTrust audit database format, the records obtained from the ACS database need to be supplemented with the computer type, time zone parameters, and Windows build number.

To summarize, in order for event data to be stored in an InTrust repository and/or audit database, the following information is required:

1. **EventSchema.xml and ACS database connection parameters.** This data can be obtained directly from the Operations Manager server.
2. **Time zone parameters.** This information is obtained from the following sources:
    - Operations Manager server; its parameters are obtained directly from that server.
    - Each network computer whose events are stored in ACS database; this information is obtained using a specially designed Management Pack (see the Gathering with and without Agents topic).
3. **Computer type and OS (Windows) build number.** This information is retrieved by the Operations Manager server from network computers after the server is forced by the Management Pack to collect this data.

So, for ACS data to be processed correctly, you have to deploy Quest InTrust for ACS Management Pack. The installation procedure is described in the Step 1. Install the InTrust Knowledge Pack for ACS topic.

ACS Data Gathering and Reporting With InTrust

This topic explains the steps you need to take in order to enable ACS data gathering and reporting with InTrust:

1. Install the InTrust Knowledge Pack for ACS feature from the InTrust suite setup.
2. Configure an InTrust site using automatic or manual resource discovery procedure, and deploy the Quest InTrust for ACS Management Pack (as prescribed by the corresponding procedure).
   If needed, configure specific access rights required for processing.
3. Install agents, if necessary.
4. Configure the InTrust policies, tasks, and jobs you need.
5. Install the Report Pack for the Operations Manager console; run the InTrust task and use the Operations Manager console to view reports on the collected data.

Each step is described in detail in the related topics.

> **CAUTION: For reports on collected data to work properly, it is strongly recommended that you use a dedicated InTrust Audit database to collect only event data provided by ACS. If you also want to collect Windows event data in the standard way (that is, directly from the audit trails, using the InTrust workflow) from the same computers (Operations Manager servers), configure a separate Audit database.**

Step 1. Install the InTrust Knowledge Pack for ACS

The InTrust Knowledge Pack for ACS brings in several predefined objects required for the InTrust auditing workflow.

To install the Knowledge Pack, launch the InTrust suite setup, and from the list of features to install, select **Knowledge Pack for ACS**.

After the setup is complete, the following predefined objects become available in InTrust Manager (for a detailed list with descriptions, see Predefined Objects for ACS Data Collection and Reporting):

- **All OpsMgr ACS Servers in the domain**—An InTrust site used to arrange your Operations Manager servers with Audit Collection Services installed.
- **Microsoft OpsMgr ACS**—A predefined data source of Microsoft ACS Events type that represents Windows security log events stored in the Microsoft Audit Collections Services database.
- **Gathering, consolidation, and import policies**—InTrust policies defining the events to be collected, consolidated, or imported.
- **OpsMgr ACS events collection**—A task containing gathering and notification jobs.
- **OpsMgr ACS events collection**—A gathering job.

Step 2. Configure an InTrust Site

To arrange your Operations Manager servers with Audit Collection Services installed into the InTrust site, perform the following steps:

1. Deploy the Quest InTrust for ACS Management Pack on the Operations Manager servers, as described in the related topics. Keep a record of the Operations Manager servers where the Management Pack is installed.
2. In InTrust Manager, create a new site. Populate it with the computers from the list created on the previous step.

NOTE: It is recommended that you arrange Operations Manager servers into sites considering their location and/or administrative boundaries.

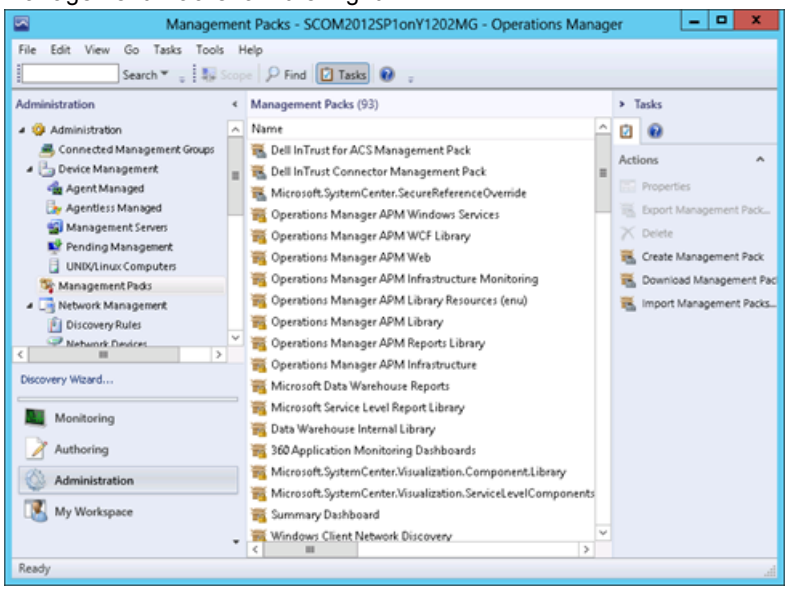
To install agents on the site computers, refer to the Gathering with and without Agents topic.

InTrust for ACS Management Pack Deployment

This section describes how to install the Quest InTrust for ACS Management Pack using the Operations Manager console. Alternatively, the Management Pack can be deployed in a centralized manner (for example, via Group Policy or SMS).

To import the Management Pack

1. In Operations Manager console, go to the Administration page and select **Management Packs**.
2. Right-click the node and select **Import Management Packs**. In the Select Management Pack to import dialog box, browse to the corresponding XML file (**Microsoft.SystemCenter.OperationsManager.mx4ACS.xml** located at **Knowledge Packs\Knowledge Pack for ACS Add-ins** folder in your InTrust distribution, or in the **Server\InTrust** subfolder of the InTrust working folder). When imported, it appears in the list of Management Packs on the right.



3. Wait for the new configuration to be distributed to the Operations Manager agents running on the network computers, and for these agents to submit the data back to the Operations Manager server.

NOTE: Meanwhile, you can proceed with the remaining configuration steps. After installing the InTrust for ACS Reports Report Pack, use the 'InTrust for ACS management pack deployment status' report for Operations Manager console to discover the results of Management Pack deployment to Operations Manager agents (ACS-forwarders).

This report can be used as metrics for the following:

- Decision-making on the gathering process start
- Analysis of session results (if any errors occur while processing the specified computers)

4. Record the names of the Operations Manager servers where the Management Pack was installed.

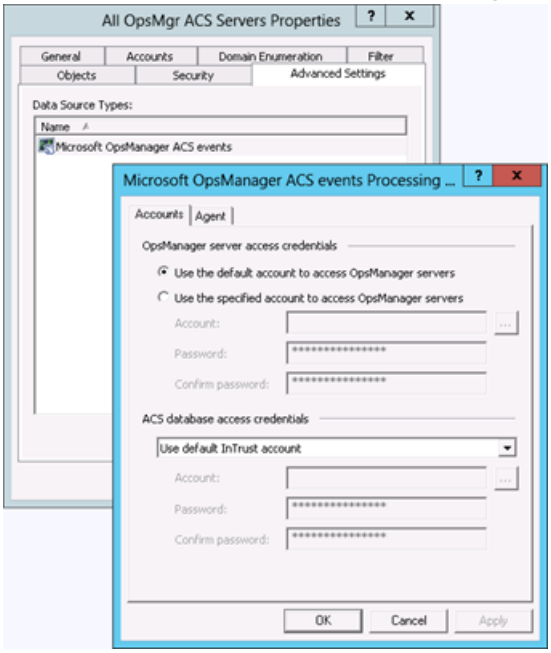
Step 3 (optional). Specify a Data Source and Related Settings

If you want your Operations Manager server and ACS database to be accessed under a specific account (not inherited from a site, job, task, or InTrust server), and/or you want to install the InTrust agent on a dedicated computer (other than the Operations Manager servers included in the All OpsMgr ACS Servers in the domain site), you have to take the following steps:

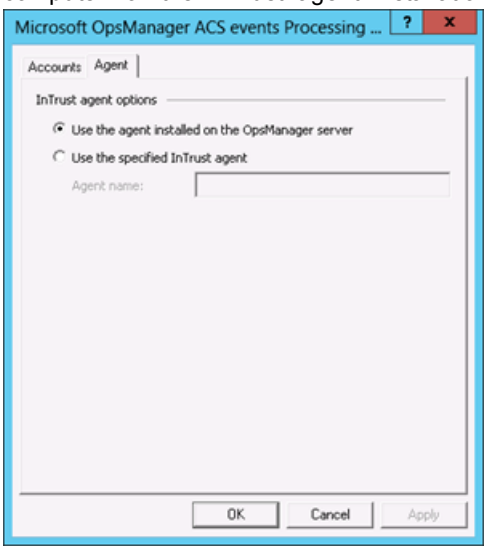
1. In InTrust Manager, open the **All OpsManager ACS Servers in the domain** site properties. On the Advanced Settings tab, click **Add** and select the **Microsoft OpsMgr ACS** data source.

2. Next, you must configure the settings that are specific for ACS event processing. Select **Microsoft OpsManager ACS events** from the list, and click **Edit**.

   a. If you want to access the Operations Manager server and ACS database under a specific account, supply the account's credentials on the Accounts tab, as shown below. Rights required for InTrust to access the Operations Manager servers and ACS database are described in the Access Rights topic.



   b. To use the agent for data collection, open the **Agent** tab and specify the target computer for the InTrust agent installation, as follows:



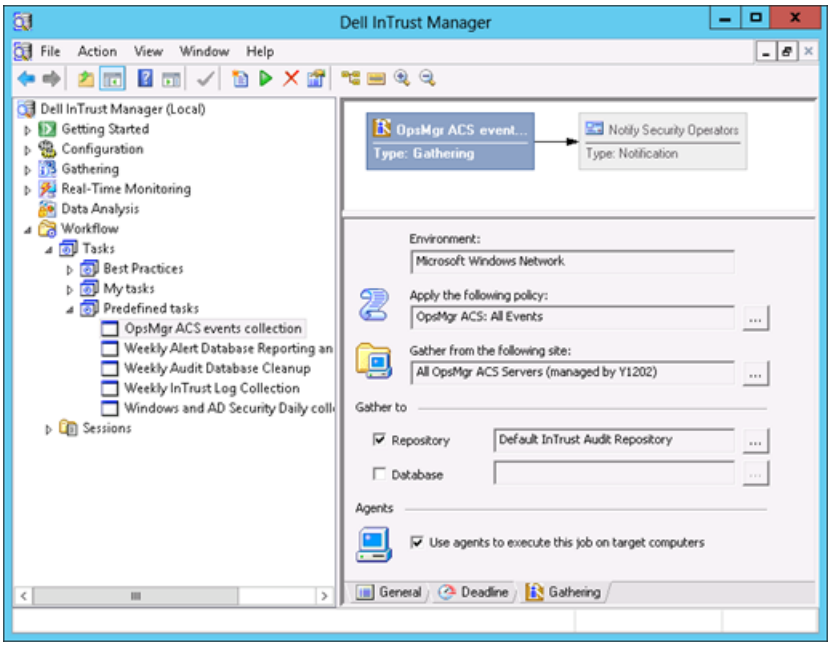
NOTE:

- It is recommended to install the agent on a computer other than the Operations Manager server.
- Gathering with and without agents is described in detail in the Gathering with and without Agents topic.

Step 4. Configure an InTrust Policy, Task, and Job

Configure InTrust predefined objects that will be used for data collection and reporting.

- You can use any of the predefined gathering policies (for example, **OpsMgr ACS: All Events**), or create a gathering policy that will collect data from the Microsoft OpsMgr ACS data source.
- You can either use the **OpsMgr ACS events collection** predefined task, or create a new task that will contain the jobs you need.
- Similarly, you can use the **OpsMgr ACS events collection** predefined job, or create a new gathering job that involves the desired gathering policy and site.



Access Rights

Access to Operations Manager Server

An account under which site computers (Operations Manager servers) will be accessed is either specified explicitly in the site's settings (**Advanced** tab), or inherited from the site, job, task, or InTrust server, as described in this section. To access Operations Manager servers, this account requires the following:

- **Access this computer from the network** right must be granted.
- **Deny access to this computer from network** right must be disabled.

- **Read** access to the **HKEY_LOCAL_MACHINE\Services\AdtServer\Parameters and HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI** registry entries of the computer hosting the Operations Manager server.
- **Read** access to the **EventSchema.xml** (path to this location is stored in the **EventSchema** registry value at **HKEY_LOCAL_MACHINE\Services\AdtServer\Parameters**).

All available accounts are listed below in order of usage priority (inheritance order). If an account with higher priority is not specified in the corresponding entity's properties, then the account with lower priority that follows will be used:

Usage Priority	Account	Where the Account Is Set
1	Account intended for connection to Operations Manager server	On the **Accounts** tab of the data source-related site properties (site's **Advanced Settings | data source properties | Accounts**)
2	Account used for site objects access	On the **Accounts** tab of the site properties (if the site is processed without agents)
3	Account specified for site-processing job	In the job properties
4	Account specified for the task containing site-processing job	In the task properties
5	Account used for InTrust Server operation (if gathering without agents) or for agent operation (if gathering with agents)	During the setup. The account for the currently-running agent can be changed in the **Quest InTrust Agent** service properties.

Access to the ACS Database

The ACS database will be accessed using the account from those listed below (also listed in descending priority order).

Usage Priority	Account	Where the Account Is Set
1	Account intended for ACS database connection	On the **Accounts** tab of the data source-related site properties (site's **Advanced Settings | data source properties | Accounts**)
2	Account used for connection to Operations Manager server	On the **Accounts** tab of the data source-related properties (site's **Advanced Settings | data source properties | Accounts**)
3	Account used for site objects access	On the Accounts tab of the site properties (if the site is processed without agents)
4	Account specified for site-processing job	In the job properties
5	Account specified for the task containing site-processing job	In the task properties

Usage Priority	Account	Where the Account Is Set
6	Account used for InTrust Server operation (if gathering without agents) or for agent operation (if gathering with agents)	During the setup. The account for the currently-running agent can be changed in the **Quest InTrust Agent** service properties.

Gathering with and without Agents

Usually audit trails are collected using agents. You can install an InTrust agent to a dedicated computer (recommended) or to the Operations Manager server. In some cases you may need to gather event data without agents. Each option is described below.

To use an agent on a dedicated computer

1. In InTrust Manager, open the **All OpsManager ACS Servers in the domain** site properties.
2. Open the **Advanced Settings** tab, select the **Microsoft OpsManager ACS events**, and click **Add**.
3. Select **Microsoft OpsManager ACS events** from the list, and click **Edit**.
4. In the dialog displayed, open the **Agent** tab.
5. Select the **Use the specified InTrust agent** option, and enter the agent location.
6. Click **OK** to save the settings and close the dialog.
7. In the site properties, open the **General** tab and clear the **Prohibit automatic agent deployment on site computers** check box (to allow for agent installation).
8. In the gathering job properties, open the **Gathering** tab, and select the **Use agents to execute this job on target computers** check box.
9. Commit the changes.

> **CAUTION: For data to be collected using an InTrust agent on a dedicated computer, the Operations Manager console must be installed on that computer. Make sure that the console is the same version as the Operations Manager console running on your Operations Manager server.**

When the gathering job starts, InTrust agents will be automatically deployed on the specified computers.

To use an agent on the Operations Manager server

1. In InTrust Manager, select the gathering job that will collect ACS data.
2. On the **Gathering** tab of the job properties, select the **Use agents to execute this job on target computers** check box.
3. Select the **All OpsManager ACS Servers in the domain** site, open the **Advanced Settings** tab, select the **Microsoft OpsManager ACS events**, and click **Add**.
4. Select **Microsoft OpsManager ACS events** from the list, and click **Edit**.

5. In the dialog displayed, open the Agent tab, and select Use the agent installed on the OpsManager server option.
6. From site's shortcut menu, select **Install Agents** (to install agents on Operations Manager servers right away)
7. To prevent superfluous agent installation, open the site properties, go to the General tab and select the **Prohibit automatic agent deployment on site computers** check box.

To gather data without agents

1. In the site properties, select the **Prohibit automatic agent deployment on site computers** check box.
2. In the gathering job properties, on the **Gathering** tab, clear the **Use agents to execute this job on target computers** check box.

CAUTION: If you plan to collect data without using InTrust agents, then the Operations Manager console must be installed on the computer hosting the InTrust Server. Make sure that the console is the same version as the Operations Manager console running on your Operations Manager server.

Running Reports

To enrich native reporting with reports on consolidated data collected by InTrust, a special Report Pack for the Operations Manager console (named Quest InTrust for ACS Reports) is provided with the Quest solution. It offers ten predefined reports on various aspects of network security, including user and computer management, file and object access, and user and administrator activity, along with a special report that helps you discover the InTrust for ACS management pack deployment status.

This Report Pack should be deployed on the Microsoft SQL Server Reporting Services (SSRS) that is used to run the Operations Manager console.

To install the Report Pack

1. Run the Report Pack setup (launch **IT_ACS4SCOM.10.x.<build_number>.msi** from the **Knowledge Packs\Knowledge Pack for ACS Add-ins** folder in your InTrust distribution).
2. Specify your name and organization.
3. Specify the URL of the Report Server (web service) where Operations Manager console runs, for example:
   http://My_SQL_Srv/ReportServer
   -or-
   https://My_SQL_Srv/ReportServer
4. On the Configure Data Sources step, make sure the data source is associated with InTrust Audit database where events from ACS are stored. (If you want to re-configure the data source later, you can use SSRS Report Manager.)
5. Complete the wizard.

NOTE: Some reports may create temporary tables in the data source. To clean them up, a special job is created and scheduled during Report Pack setup. For the Temporary Tables Cleanup job schedule to be applied, make sure the SQL Server Agent is running. If not, start the Agent, and then use data source's properties in SSRS Report Manager to schedule the cleanup.

After the setup is complete, you can open the Operations Manager console and go to the **Reporting** tab. Select the **Quest InTrust for ACS Reports** node in the tree to see the newly installed reports. To generate a report, select it and click **Open** from the shortcut menu, or use the toolbar button.

Predefined Objects for ACS Data Collection and Reporting

InTrust offers a set of predefined objects that will help you configure gathering and reporting on event data from the ACS database.

NOTE: Import policies have the same names as gathering policies and are intended to import the corresponding data from the repository to the Audit database.

Object	Description
“All OpsMgr ACS Servers in the domain” site	This InTrust site is used to arrange your Operations Manager servers with Audit Collection Services installed.
“Microsoft OpsMgr ACS” data source	This data source of Microsoft ACS Events type represents Windows security log events stored in the Microsoft Audit Collections Services database.
“OpsMgr ACS: Successful AD Administrator Logons” gathering policy	This gathering policy defines the AD Administrator Logons to DC events to be collected to both a repository and a database.
“OpsMgr ACS: All Events” gathering policy	This policy defines all security events from Audit Collection Services to be collected to a repository. The most critical security events (such as Failed Logons and Account Management) are to be collected into a database for analysis. The policy is intended to be used for gathering on a daily basis.
“OpsMgr ACS: All Logons” gathering policy	This policy defines the Logon events to be collected from Audit Collection Services to both a repository and a database.
“OpsMgr ACS: Failed Logons” gathering policy	This policy defines the Failed Logon events to be collected from Audit Collection Services to both a repository and a database.
“OpsMgr ACS: Account Management” gathering policy	This policy defines the Account Management events to be collected from Audit Collection Services to both a repository and a database.
“OpsMgr ACS: Policy Changes” gathering policy	This policy defines the Policy Changes to be collected from Audit Collection Services to both a repository and a database.
“OpsMgr ACS: Objects Access: Registry Access” gathering policy	This policy defines the Registry Access events to be collected to both a repository and a database.
“OpsMgr ACS: Objects Access” gathering policy	This policy defines the Object Access events to be collected from MS Audit Collection Services to both a repository and a database.
“OpsMgr ACS: Misc” gathering policy	This policy defines all Windows/AD miscellaneous security events to be collected from MS Audit Collection Services to a repository. The most critical of miscellaneous

Object	Description
	security events (such as Security Subsystem and Audit Subsystem Faults) are to be collected into a database for analysis.
“Standard OpsMgr ACS events consolidation” consolidation policy	This policy consolidates data from the Audit Collection Services without applying any time range filter. The standard Microsoft Operations Manager log is the Security log.
“Standard OpsMgr ACS events consolidation for the last month” consolidation policy	This policy consolidates data from the Audit Collection Services for the last month only. The standard Microsoft Operations Manager log is the Security log.
“OpsMgr ACS events collection” task	A task containing gathering and notification jobs.
“OpsMgr ACS events collection” job	A gathering job used to collect data from the ACS database.
“LDAP Query” enumeration script	A predefined enumeration script that returns the list of computers satisfying the LDAP query.
“MS OpsMgrs” enumeration script	A predefined enumeration script that returns the list of computers where Microsoft Operations Manager servers are running.

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