

ALTIRIS
DOCUMENTATION
**BEST PRACTICES
ARTICLE**



Vista Migration and More: Auditing for Security Compliance



altiris®

Auditing for security compliance is important to do before and after migrating a Windows computer to the Windows Vista operating system. The information revealed about a computer during an audit helps you:

- prevent existing security vulnerabilities from carrying over to the Windows Vista environment.
- ensure you set up Windows Vista according to your organization's security policies.

Altiris® Audit Integration Component™ lets you audit for security compliance by comparing the current state of each computer against the security policies of your organization. The audit results show how well each computer complied with those policies. Once you know how the individual computers on the network rate in the most critical security areas, you can solve your security problems and prevent new ones on an enterprise level.

The integration component includes three security-management interfaces: SecurityExpressions™ Console, Security Expressions™ Audit and Compliance Server, and AuditExpress™. They are used together, each offering its own unique combination of auditing and compliance features optimized by different kinds of networking technology. The console application is a Windows application with the flexibility to run on servers or workstations, while the server application uses Web-server technology to communicate with all platforms with ease. Both the server and the console application share data by connecting to the same central ODBC-compliant database.

Note

AuditExpress, also a console application running on Windows, is not featured in this article. Auditing for security compliance as part of the migration process includes advanced steps that require a combination of the console and server applications.

We recommend using the integration component to audit computers being migrated to Windows Vista for security compliance in three phases:

- **Pre-Migration Assessment** - Audit all computers being migrated against a migration-focused security policy to pinpoint and resolve security vulnerabilities before you migrate.
- **Post-Migration Assessment** - Devise a security policy that focuses on running Windows Vista with the security settings you chose. Then audit all computers against the policy to ensure your configuration of Windows Vista didn't create security vulnerabilities.
- **Ongoing Compliance Audits** - Audit Windows Vista computers against this policy regularly to ensure they continue to comply with the organization's Windows Vista policies.

Each of the three phases supplies detailed information about the state of security on the organization's Windows computers, worldwide. You can analyze these audit results by displaying them in different formats and generating reports. This gives you the knowledge to make Vista-migration decisions now and regularly check migrated computers for company-wide security compliance.

What You Need

Before you begin, you must have the following:

- the Audit Integration Component installed, configured, and connected to the *security audit database*, a centrally located, ODBC-compliant database that stores audit results and management data. This requirement includes having the security-

mangement applications SecurityExpressions Console and SecurityExpressions Audit and Compliance Server installed, configured, and connected to the same security-audit database.

For more information about installing and configuring the software, see chapter 2 of the *Altiris Audit Integration Component User's Guide*. You can find this and all Altiris documentation at <http://www.altiris.com/Support/Documentation/>.

- knowledge of your organization's computer security policies.
- access to and familiarity with the *Windows Vista Security Guide*, located at <http://www.microsoft.com/technet/windowsvista/security/guide.mspx>.
- the ability to author policy files.

Pre-Migration Assessment

Before you migrate the Windows computers in your organization to a Windows Vista environment, audit them all using the integration component, looking for possible security issues. If you resolve these issues before migrating computers, the computers will be at peak security in time for migration.

Determine what issues to audit for, based on migration plans and existing corporate policies. Customize one or more policy files to check for these issues. Then audit the computers in bulk using those policy files. The audit results will show the security strengths and weaknesses.

Process Overview

This phase is divided into the following tasks:

<i>Step 1: Determining the Issues</i> (page 3)	<ul style="list-style-type: none">• Determine what issues to audit for.
<i>Step 2: Customizing Policy Files</i> (page 4)	<ul style="list-style-type: none">• Customize policy files.
<i>Step 3: Auditing Target Computers</i> (page 6)	<ul style="list-style-type: none">• Audit all Windows computers migrating to Windows Vista.
<i>Step 4: Analyzing Results</i> (page 13)	<ul style="list-style-type: none">• Analyze the results.
<i>Double click a row to view details about a particular security check.</i> (page 14)	<ul style="list-style-type: none">• Solve any problems you found.

Step 1: Determining the Issues

Determining what issues to audit for will be a combination of your organization's existing security policies, plus your migration plans and goals. The integration component offers dozens of policy files containing hundreds of rules to check against the migrating computers. Pinpoint your needs in advance so you know exactly which policy files and rules to look for while customizing your own policy files.

Step 2: Customizing Policy Files

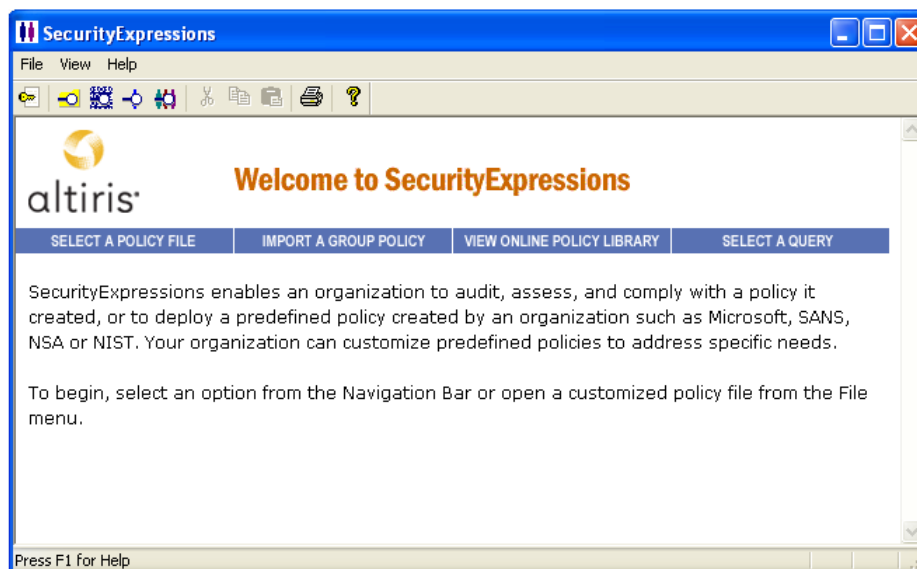
A *policy file* is a configuration file that checks a computer for evidence of whether or not the computer complies with corporate policies. Policy files consist of *rules* that check a computer for particular conditions, settings, hardware, and software. Policy files have a .sif extension. The file format is the standard INI format used by many Windows applications. It consists of sections and a list of key/value pairs for each section.

Use the SecurityExpressions Console to create one or more custom policy files from the existing policy files and the rules they contain. Although you can audit computers against any of the policy files in their original form, it's more efficient to customize your own. The auditing process can take hours. Instead of auditing the same computers against each policy file that happens to contain relevant rules, you can combine those rules into one policy file that enforces your organization's security policies.

To view the contents of existing policy files

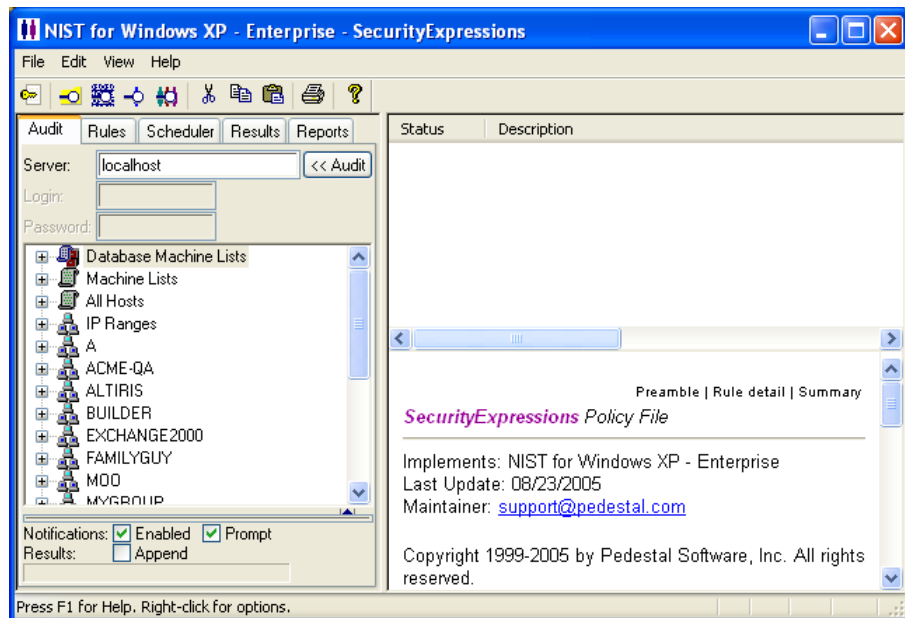
1. Open the console application.

The welcome window appears.

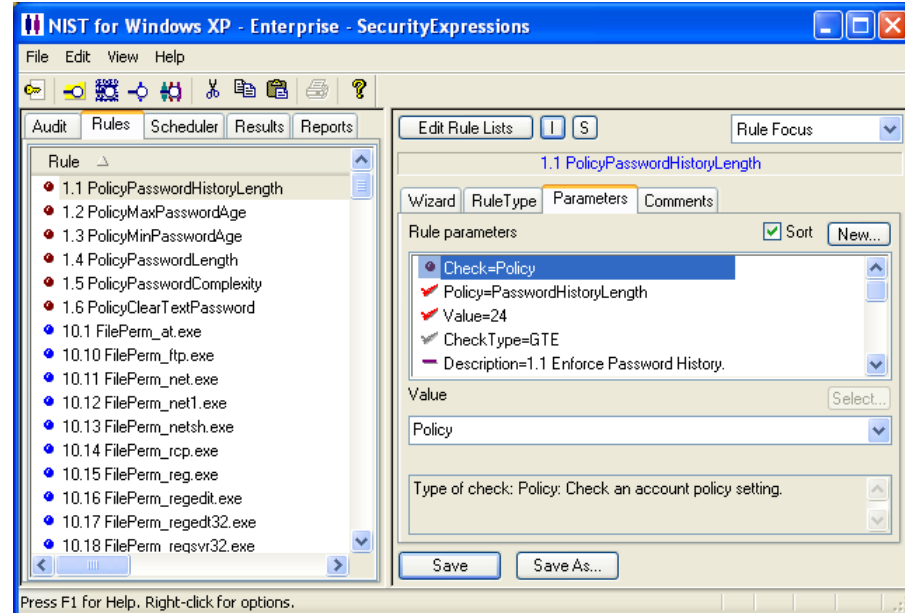


2. Click **SELECT A POLICY FILE** to display Altiris' library of preconfigured policy files.
3. Select a policy file that you think addresses your issues and open it.

The console application appears.



4. Click the **Rules** tab.
This displays all the rules in the open policy file.
5. Use the Wizard, Rule Type, and Parameters tabs in the lower right pane to learn more about what the rule does.



Most likely, your organization has different security requirements for computers used in different ways. Create one policy file to cover each set of requirements. When it comes time to audit, you can group computers with the same security requirements together and audit them against the policy file created just for them.

You can customize policy files in several ways. You can use the rules from any existing policy files in your own policy files, or even design your own rules.

Caution

It's up to you to make sure the rules you use and create are relevant to the computers you're auditing. Irrelevant rules are ignored during the audit and don't appear in audit results.

- You can start with an existing policy file and modify it to include your organization's security policies. Choose a policy file that's designed to audit the version of Windows running on the computers you plan to audit, such as *NIST for Windows XP - Enterprise* for Windows XP computers.

Caution

If you modify the policies installed with the software, save them under a new name. Not only does this preserve the original policy file, but it also ensures your modifications carry over when you upgrade the software. Upgrading the software updates all preconfigured policy files from Altiris' library.

- If you don't find one policy file that you want to modify, you might want to create a new policy file and then create or copy rules into it.
- Authoring policy files is an advanced technical skill similar to programming. Altiris offers professional services that can help you create policy files or create them for you. See <http://www.altiris.com/Services/> for details.

For details on how to use the console to create and modify policy files and rules, check the *SecurityExpressions Console User Guide* at <http://www.altiris.com/Support/Documentation/>.

Step 3: Auditing Target Computers

Once you've created your policy files, you're ready to configure audit tasks and run them. The process includes installing the audit agent on the *target computers* (computers you want to audit) as necessary, grouping computers into machine lists to be audited at once, scheduling the audits, and scheduling Notification Server to import the audit results.

Note

Each program that's part of the integrated component is best suited for certain tasks. In order to take advantage of the integration component's high-level security and flexible maintenance, use the program noted in each task to perform that task.

To perform audits

- Integration Component:** Decide which target computers should use the audit agent to connect to the software.

You have the option of auditing target computers with or without the *audit agent*. The audit agent, separate from the Altiris Agent, is distributed with the integration component. Consider which is the best way to connect to each target computer.

Agentlessly

Altiris' audit technology is capable of connecting to target computers without using agents. If your network setup enables you to connect to a target directly and you'd rather not use an agent, agentless auditing is a simpler model. Perform agentless auditing through Windows Networking or UNIX SSH.

Using an agent

If a target computer is behind a firewall, has Windows Networking or SSH disabled, or if you find connecting through agents more efficient, install the audit agent on the target computer before auditing. The agent runs with privilege, authenticates its users directly, and performs tasks on the target computer only if the authentication is passed.

Through a proxy

If a target computer is behind a firewall or other router that blocks Windows Networking or hides the computer through Network Address Translation (NAT), you can proxy a connection to the computer through the agent on a remote computer. You install the agent on a Windows computer, making that computer a proxy computer.

Tip

To learn more about agents and proxies, see "Connecting to Remote Systems" in the *SecurityExpressions User's Guide*. You can find this guide at <http://www.altiris.com/Support/Documentation/>.

Agentless audits require you to have administrative credentials for the target computers, which you'll have to configure in the console application. When making this decision for each target computer, keep in mind the audit agent:

- must be installed on the target computers.
- requires a Windows access group that can access the target computer.

Each method has different credential requirements, so decide now which target computers will use the audit agent. Then put them in a Notification Server collection. Finally, install the audit agent on the entire collection from the Security Audit Agent Installation page in Altiris Console.

To install a security audit agent on a collection of computers

1. In Altiris Console, click the **Resources** tab.
2. In the left pane, right click **Resource Management > Collections** and select **New > Collection** from the menu that appears. In the New Collection page, create a collection containing all computers using the same operating system on which you want to install the agent.
3. Click the **Configuration** tab.
4. In the left pane, select **Configuration > Solution Settings > Security Management > Audit and Compliance > Security Audit Agent**.

The Security Audit Agent folder contains subfolders named for each operating system the agent supports.


5. Open the folder containing the agent you want to install, and then open the Rollout subfolder.
6. Click **Security Audit Agent Installation**.


The Security Audit Agent Installation page appears in the right pane.

Windows Security Audit Agent Installation

Enable (currently not enabled)

Name: **Windows Security Audit Agent Installation**
Description: **Schedule deployment of the Windows Security Audit Agent.**

Package name: **Windows Security Audit Agent Package**
Program name: **Install the Windows Security Audit Agent Package** 
 Enable Verbose Reporting of Status Events

Applies to collections: **All Windows Computers requiring Security Audit Agent Install** 

Package Multicast: Disable download via multicast


Scheduling Options

Manual
 Scheduled

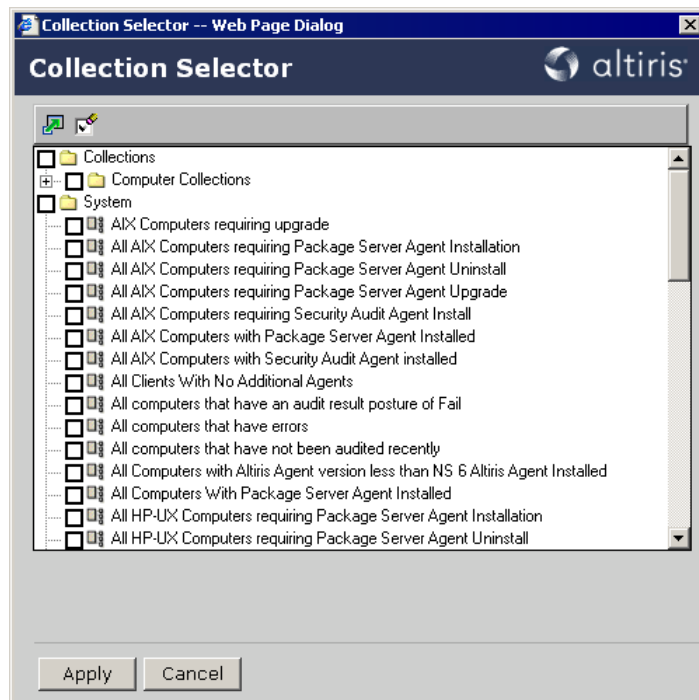
Run once **A**SAP
 Schedule: No schedule has been defined
 Only run at scheduled time
 Run as soon as possible after the scheduled time

User Can Run
 Notify user when the task is available
 Warn before running

7. Click the **Enable** checkbox.

8. In the Applies to Collections field, click the  icon.

The Collection Selector appears.



9. Locate and select the collection you created in step 2. Then click **Apply**.
10. In Scheduling Options, schedule when you want the agent installed on the computers in the collection.
11. Click **Apply** to activate an installation.

Notification Server installs the agent on the computers in the collection according to the schedule you set in step 10.

- B. **Integration Component:** Organize target computers into *machine lists* according to their audit requirements.

Note

Machine lists are similar to *computer collections* in Notification Server. When using the Audit Integration Component with Notification Server, the Audit Integration Component uses export policies to convert collections into machine lists.

Grouping target computers into machine lists makes auditing easier, whether you're performing a simple audit or auditing a large group of computers on a schedule. A machine list contains the computer names or IP addresses of the target computers you want to audit together — perhaps they have the same credentials for logging on, need to be audited using the same policy files, or that have the audit agent installed. During an audit, when the audit application tries to connect to each target computer, it can audit each target computer with ease.

Note

Computers can appear in more than one machine list.

The goal of compiling machine lists is to group computers in a way that allows the fewest and most efficient audits. The most efficient way for you to group target computers into machine lists depends on several factors unique to your audit needs. Consider the following factors and then develop a strategy for compiling machine lists.

- If you want to audit different groups of target computers against different policy files, consider grouping the target computers to be audited by a single policy file together. If you have no other factors to consider, these are the only machine lists you'll need. If you only have one policy file to audit against, then you only need one machine list containing all the target computers.
- If you're auditing any target computers without the audit agent, the audit task needs the proper credentials to access the target computers. You can store credentials in the database for use during audits. If any agentless target computers require the same credentials, you can group them in the same machine list, assign the credentials to the entire machine list, and then delegate the credentials to the server application. The console allows you to delegate credentials to the server through machine lists.
- Target computers audited using the audit agent often require credentials in order to log on to them as well. Group target computers with the same credentials in the same machine list, assign the credentials to the entire machine list, and then delegate the credentials to the server application. The console allows you to delegate credentials to the server through machine lists.
- Target computers in certain departments or geographical locations, or that have different uses, probably have different security requirements. That means you'll

want to audit them against different policy files. Group these target computers together in the same machine lists so you can audit them at once.

Since the computers in your organization are already grouped into collections in Notification Server, this solution allows you to create machine lists from existing collections. When you export a collection to the security-management application, the individual computer resources in the collection are converted to target computers that you can audit. Machine lists created from collections receive updates when changes are made to the collections, which saves you from managing separate lists of computers in each program.

To create machine lists from collections

1. In Altiris Console, click the **Configuration** tab.
2. In the left pane, select **Configuration > Solution Settings > Security Management > Audit and Compliance > Export Rules**.


The Export Rules page appears in the right pane.

Export Rules		
Name	Type	Description
Export collections based on Audit Results Summary		Creates a machine list in the Audit and Compliance applic
Export standard NS collections		Creates a machine list in the Audit and Compliance applic

3. Double click **Export standard NS collections**.

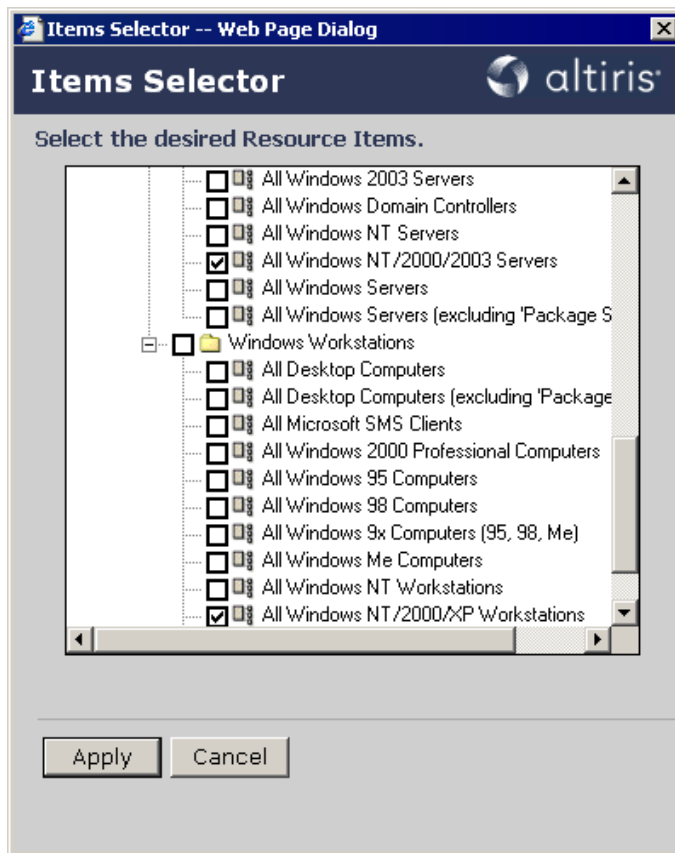
This export policy allows you to export collections used in other Notification Server solutions to the security-management application.

Export Policy

Name:	Export standard NS collections
Description:	Creates a machine list in the Audit and Compliance application's database for each specified collection
Collection:	All Windows Computers, All Windows NT/2000/XP/2003 Computers, All Windows NT/2000/2003 Servers ... 
<input type="checkbox"/> Enable Schedule:	Business Hours Every 1 hours from 8:10 AM for 9 hours every Mon, Tue, Wed, Thu, Fri of every 1 weeks, starting Wednesday, January 01, 2003
<input type="button" value="Export Now"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

4. In the Collection field, click the  icon.

The Items Selector dialog appears, listing the collections in Resource Manager.



5. Select the collections you want to export and click .

6. Click the **Enable Schedule** checkbox and select how often you want the collections to update the machine lists with their current list of computers.

The first time the policy runs, the collections are exported to the security-management application as machine lists. Whenever changes are made to the collections, the policy updates the machine lists on this schedule.

7. Click to save the policy.

C. **SecurityExpressions Server:** Create tasks for any audits you need done on a schedule.

This process involves creating *policies*, which are different from policy files, and setting a schedule. Since the purpose of this phase is to perform a one-time assessment, we recommend auditing all target computers on a schedule that runs once. The schedule enables you to run the audits during off-peak hours when they won't affect network performance, such as nights and weekends. The schedule also lets you control how soon the audits occur. Company-wide migration has time constraints that can't wait for computers to connect to the network on their own, which is how Audit on Connect and self-service audits initiate audits.

- Create policies, which consist of one or more policy files plus some other settings. When you associate a policy with a scheduled audit task, the target

computers are audited against all policy files in the policy and according to all settings in the policy.

- Create the scheduled audit task, assigning the appropriate machine lists and policy.

SecurityExpressions audits the target computers at the scheduled time.

For more information on using SecurityExpressions to perform this step, see the *SecurityExpressions Audit and Compliance Server User's Guide* at <http://www.altiris.com/Support/Documentation/>.

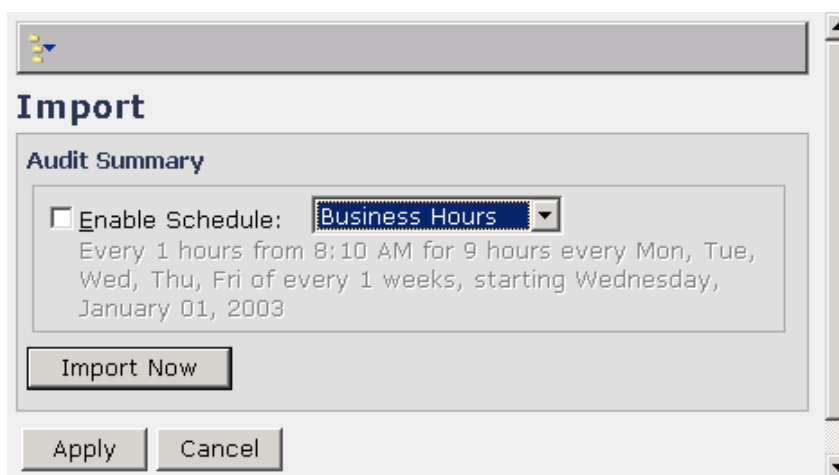
- D. **Integration Component:** Import data from the security audit database into the Notification Server database.

Once you've created machine lists using the integration component and performed an audit using the security-management application, you need to bring security audit data into Notification Server. Schedule imports to occur after scheduled audits.

To import data from the security audit database

1. In Altiris Console, click the **Configuration** tab.
2. In the left pane, select **Configuration > Solution Settings > Security Management > Audit and Compliance > Import**.

The Import page appears in the right pane.



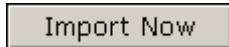
3. Select the schedule on which you want to import data from the security audit database.


When you select a schedule from the list, a description of the schedule appears below it.

4. Click **Enable Schedule**.

You can disable the schedule any time by clicking this checkbox again.

Tip

Any time you want to import data instantly, rather than wait for the next scheduled import to occur, you can click the  button.

5. Click  to set the import schedule.

Step 4: Analyzing Results

Once you have gathered data through auditing, analyze it using the integration component so you can pinpoint security issues and take action. You can view audit details online, generate reports from them, and send Helpdesk tickets.

Viewing Audit Results

If you want to know the outcome of a computer's latest audit, you can display details about the audit using the Audit Detail views. The Audit Detail views are available in the Resources tab through the computer collections. You can display audit details about one computer at a time.

Note

In order to view audit results in Altiris Console, you must belong to a user group whose security role includes audit and compliance privileges. A Notification Server administrator can grant audit and compliance privileges to your user group by enabling the **View Audit Details** global privilege for your user group in the Security Role Management page. The Security Role Management page is located in **Configuration > Server Settings > Notification Server Settings**.

To view a computer's audit results

1. In Altiris Console, click the **Resources** tab.
2. In the left pane, select **Resource Management > Collections > Computer Collections**.
3. Under Computer Collections, locate the collection that corresponds to the machine list you audited in the previous procedure and click the collection.

A table appears in the right pane, listing the computers in the collection and some basic information about the computers.

4. Right click the computer whose latest audit results you want to check and select either **Audit Details** or **Audit Details by Security Policy** from the menu that appears.

A summary of this computer's most recent results appears in a separate window. If you selected **Audit Details**, results are grouped by security category. If you selected **Audit Details by Security Policy**, results are grouped by security policy.

The columns show how many security checks in each security category or security policy rated as OK, NOT OK, Info, and Error. If results are listed by security policy, each policy's score is also listed.

The screenshot shows a web browser window with a toolbar at the top. The main content area is titled "Latest results for QACURNS". Below the title is a table with the following data:

Category	OK	Not OK	Info	Error
Antivirus	0	1	0	0
Vulnerabilities - Windows	43	11	0	0

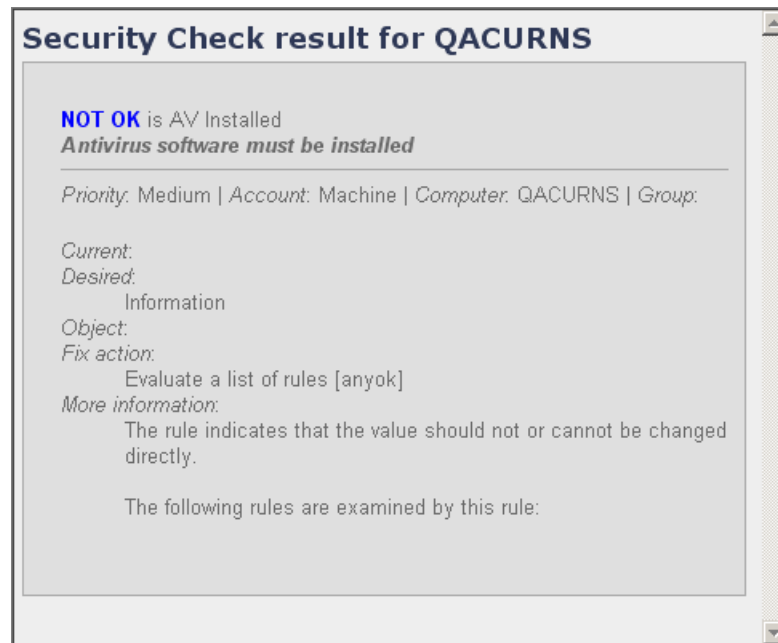
Audit Details by Security Category

- Double click a row to display that category's or policy's audit results.
A table showing each security check in the category or policy and its result appears. The table also lists the most recent date each security check was included in an audit and each security check's priority as set in the security-management application.

The screenshot shows a web browser window with a toolbar at the top. The main content area is titled "Latest results for QACURNS for category Antivirus.". Below the title is a table with the following data:

Date	Priority	Security Check Name	Result
12/5/2005 2:37:57 PM	Medium	is AV Installed	NOT OK

- Double click a row to view details about a particular security check.
A new window appears, displaying these details.



Sending Helpdesk Tickets

You can configure notification policies to alert key individuals when audits reveal a potential problem. When an audit occurs that meets the notification's criteria, the integration component automatically sends a notification to a location designated in the notification policy. The solution comes with some notification policies already configured to generate Altiris Helpdesk or Alert Management tickets based on audit results.

Exercise

The solution lets you create new notification policies and modify existing notification policies. For the purpose of this exercise, however, you will enable one of the notification policies that came with the solution. To learn how to create new notification policies or modify existing notification policies, see chapter 4 of the *Altiris Audit Integration Component User's Guide* at <http://www.altiris.com/Support/Documentation/>.

To send a Helpdesk ticket whenever a computer fails an audit

1. In Altiris Console, click the **Configuration** tab.
2. In the left pane, select **Configuration > Solution Settings > Security Management > Audit and Compliance > Notification Policies**.

The Notification Policies page appears in the right pane.

Notification Policies		
Name	Type	Description
All computers that have an audit result posture of Fail	Notification Policy	
All computers that have errors	Notification Policy	
All computers that have not been audited recently	Notification Policy	
Create New Notification Policy		Create new notification po

3. Double click **All computers that have an audit result posture of Fail**.

This policy sends a ticket to Helpdesk when an audit completes and one or more computers failed the audit.

All computers that have an audit result posture of Fail

Enable (currently not enabled)

Name: All computers that have an audit result posture of Fail

Description:

Source: Query -- Edit Query -- -- Edit Parameters --

Schedule: Daily
At 2:00 AM every 1 days, starting Wednesday, January 01, 2003

Automated Actions		
Name	Type	Description
<input checked="" type="checkbox"/> Create Workitem	New Incident Automated Action	

Add action type: Edit Incident Automated Action Add

Test Notification Policy

Apply Cancel

4. Click **Enable**.

You may disable the policy any time by checking this box again.

5. Click **Apply** to enable the policy.

Generating Web Reports

The solution offers ready-made reports you can use to share the results of the most recent audits with others. You can generate reports that show all audit results or just the results that relate to a particular security policy or category within a security policy. You can also designate which computers the report classifies as Passed and Failed, depending on how many Not OKs you find acceptable for the audit in question. The reports display data in chart and table format.

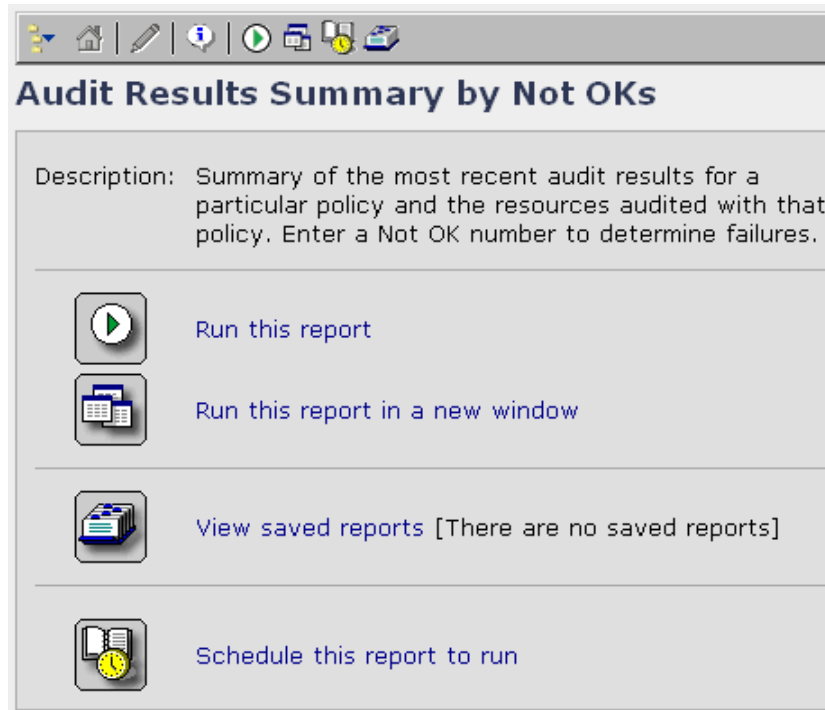
1. In Altiris Console, click the **Reports** tab.
2. In the left pane, select **Reports > Security Management > Audit and Compliance**.


The Audit and Compliance page appears in the right pane.

Audit and Compliance		
Name	Type	Description
Audit Results Summary by Not OKs	Report	Summary of the most recent audit results for a particula
Audit Results Summary by Score	Report	Summary of the most recent audit results for a particula

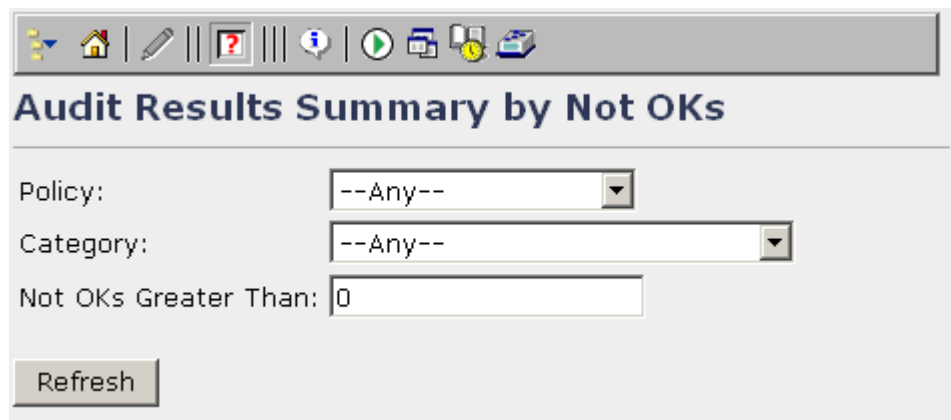
3. Double click **Audit Results Summary by Not OKs**.

The report's home page appears.



4. Click  to run the report based on the latest audit results.

The report's options appear. These options let you choose what data appears in the report and how it appears.

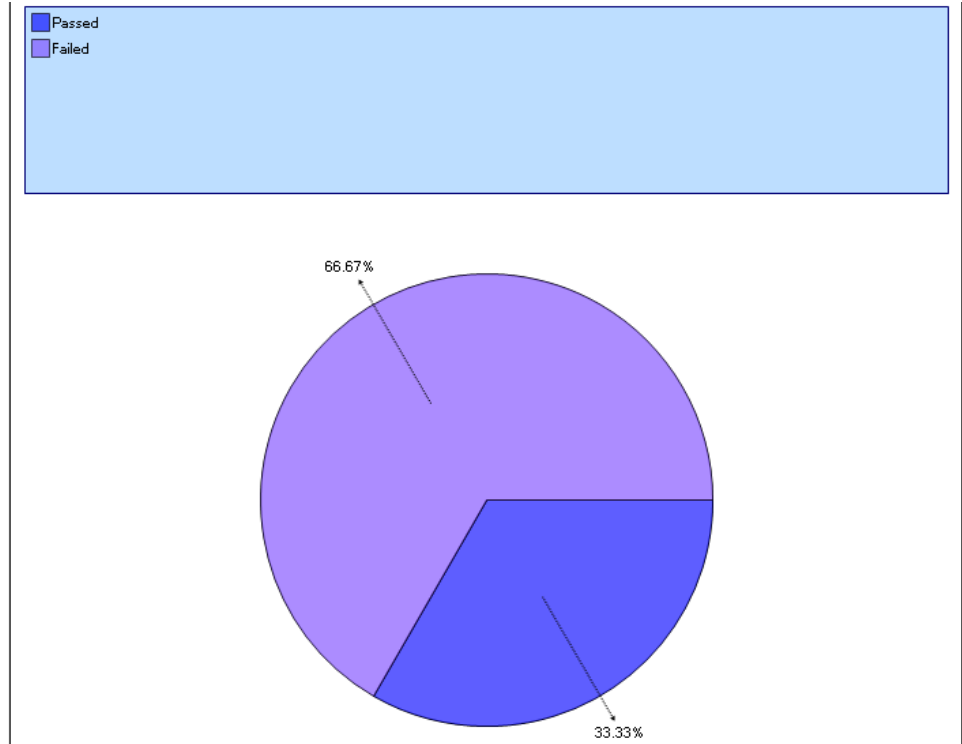


The Policy and Category fields are filters that let you limit the data appearing in the report to just one security policy or one category in one policy.

The Not OKs Greater Than field lets you designate how many Not OK checks you'll allow for a computer to pass the audit. Any computers that have more Not OK checks than the number entered here are classified in the report as Failed.

- Click **Refresh** to generate the report.

The report appears, using one pie chart to illustrate how many computers passed the audit and how many failed.




- To learn which computers make up each segment of the chart, click the segments. When you click a segment, a table appears in a new browser window, listing the computers.

A screenshot of a browser window displaying a table titled "Audit Results Summary by Not OKs". The table lists three rows of data, each representing a computer that failed an audit. The columns include Computer Name, Policy, Category, Posture, Score, OK, Not OK, Info, and Error.

Computer Name	Policy	Category	Posture	Score	OK	Not OK	Info	Error
JMVM-W2003	Windows - Detailed	Minimum Security Configuration	Fail	13.64	3	19	0	0
JMVM-W2003	Windows - Detailed	Vulnerabilities - Windows	Fail	72.22	13	5	0	0
QALEGW2K3P1	Windows - Detailed	Minimum Security Configuration	Fail	13.64	3	19	0	0

Rows: 1 to 3 of 3
Page: 1 of 1
Rows per page: All

- To produce a copy of the report you can show to others, click  on the toolbar to print the report.

Step 5: Solving Problems

Now that you are aware of security issues, you can solve those issues before beginning migration. The following Altiris products provide remediation capabilities:

- **SecurityExpressions Console** - The console application lets you perform automated fixes on rules that rated Not OK. After the audit, go to the Rules tab and right click on rules that rated Not OK. Select either **Fix Item** to fix the highlighted rule or select **Fix All Problems** to fix all Not OK rules.

For more information on using SecurityExpressions to perform this step, see the *SecurityExpressions Console User Guide* at <http://www.altiris.com/Support/Documentation/>.

- **Notification Server** - In general, you can use collections to pass audit data to other Altiris products from the integration component. See Notification Server's documentation for more information. You can find this and all Altiris documentation at <http://www.altiris.com/Support/Documentation/>.

After solving security issues, repeat steps 3, 4, and 5 in this phase until you're pleased with the level of compliance.

Post-Migration Assessment

Windows Vista offers a multitude of new security settings. Determine which ones you want to enable, using tools from Microsoft such as the *Windows Vista Security Guide*, found at <http://www.microsoft.com/technet/windowsvista/security/guide.aspx>. Then perform the migration.

Right after migration, audit for vulnerabilities caused by implementing or not implementing the new settings to ensure you chose the right ones for your organization. Create custom policy files that check for possible issues with the settings you did and didn't choose. Then audit all computers against the policy file to ensure the Windows Vista security settings you enabled didn't create vulnerabilities.

Process Overview

This phase is divided into the following tasks:

<i>Step 1: Determining the Issues</i> (page 3)	<ul style="list-style-type: none"> • Determine what issues to audit for.
<i>Step 2: Customizing Policy Files</i> (page 4)	<ul style="list-style-type: none"> • Customize policy files.
<i>Step 3: Auditing Target Computers</i> (page 20)	<ul style="list-style-type: none"> • Audit all Windows computers migrated to Windows Vista.
<i>Step 4: Analyzing Results</i> (page 23)	<ul style="list-style-type: none"> • Analyze the results.
<i>Step 5: Solving Problems</i> (page 24)	<ul style="list-style-type: none"> • Solve any problems you found.

Step 1: Determining the Issues

Compile a list of the Windows Vista security settings you enabled and didn't enable on the migrated computers. In this phase, you want to investigate whether or not you chose the right settings for your organization.

Step 2: Customizing Policy Files

Use the SecurityExpressions Console to create one or more custom policy files to audit Windows Vista computers. You'll need to add rules that check for the conditions and behavior you expected when you chose which security settings to enable in Windows Vista.

Because your organization has different security requirements for computers used in different ways, you'll want to keep in mind which policy file covers which set of requirements and make sure to add the right rules to the right policy files.

You can customize policy files in several ways. You can use the rules from any existing policy files in your own policy files, or even design your own rules.

Caution

If you're using existing policy files and rules in your custom policy files, beware that some of the files, registry keys, and registry settings might not be the same in Windows Vista as in the other versions of Windows. You might have to alter some rules so they can check Windows Vista computers.

It's up to you to make sure the rules you use and create are relevant to the computers you're auditing. Irrelevant rules are ignored during the audit and don't appear in audit results.

- You can start with an existing policy file and modify it to include your organization's security policies. For example, you might want to choose a policy file that's designed to audit the version of Windows closest to Windows Vista, such as *NIST for Windows XP - Enterprise*.

Caution

If you modify the policies installed with the software, save them under a new name. Not only does this preserve the original policy file, but it also ensures your modifications carry over when you upgrade the software. Upgrading the software updates all preconfigured policy files from Altiris' library.

- If you don't find one policy file that you want to modify, you might want to create a new policy file and then create or copy rules into it.
- Authoring policy files is an advanced technical skill similar to programming. Altiris offers professional services that can help you create policy files or create them for you. See <http://www.altiris.com/Services/> for details.

For details on how to use the console to create and modify policy files and rules, check the *SecurityExpressions Console User Guide* at <http://www.altiris.com/Support/Documentation/>.

Step 3: Auditing Target Computers

When it comes time to audit, you can probably use the same machine lists you created for the pre-migration assessment. The integration component, the audit agents, and credentials should already be in place.

To perform audits

- A. **Integration Component:** If you need to change which target computers use the audit agent to connect to the software, do so now.

Agentless audits require you to have administrative credentials for the target computers, which you'll have to configure in the console application. When making this decision for each target computer, keep in mind the audit agent:

- must be installed on the target computers.
- requires a Windows access group that can access the target computer.

Each method has different credential requirements, so decide now which target computers will use the audit agent. Then put them in a Notification Server collection. Finally, install the audit agent on the entire collection from the Security Audit Agent Installation page in Altiris Console.

To review how to install the audit agent, see step step A in *Step 3: Auditing Target Computers* (page 6).

- B. **Integration Component:** If you need to move target computers to different machine lists or create new machine lists, do so now.

Note

Computers can appear in more than one machine list.

Recall the following factors before changing machine lists or creating new ones.

- If you want to audit different groups of target computers against different policy files, consider grouping the target computers to be audited by a single policy file together. If you have no other factors to consider, these are the only machine lists you'll need. If you only have one policy file to audit against, then you only need one machine list containing all the target computers.
- If you're auditing any target computers without the audit agent, the audit task needs the proper credentials to access the target computers. You can store credentials in the database for use during audits. If any agentless target computers require the same credentials, you can group them in the same machine list, assign the credentials to the entire machine list, and then delegate the credentials to the server application. The console allows you to delegate credentials to the server through machine lists.
- Target computers audited using the audit agent often require credentials in order to log on to them as well. Group target computers with the same credentials in the same machine list, assign the credentials to the entire machine list, and then delegate the credentials to the server application. The console allows you to delegate credentials to the server through machine lists.
- Target computers in certain departments or geographical locations, or that have different uses, probably have different security requirements. That means you'll want to audit them against different policy files. Group these target computers together in the same machine lists so you can audit them at once.

To review how to create machine lists from collections, see step step B in *Step 3: Auditing Target Computers* (page 6).

- C. **SecurityExpressions Server:** Create scheduled tasks to audit the target computers against the Vista-focused policy files.

- Create policies, which consist of one or more policy files plus some other settings. When you associate a policy with a scheduled audit task, the target computers are audited against all policy files in the policy and according to all settings in the policy.

- Create the scheduled audit task, assigning the appropriate machine lists and policy.

SecurityExpressions audits the target computers at the scheduled time.

For more information on using SecurityExpressions to perform this step, see the *SecurityExpressions Audit and Compliance Server User's Guide* at <http://www.altiris.com/Support/Documentation/>.

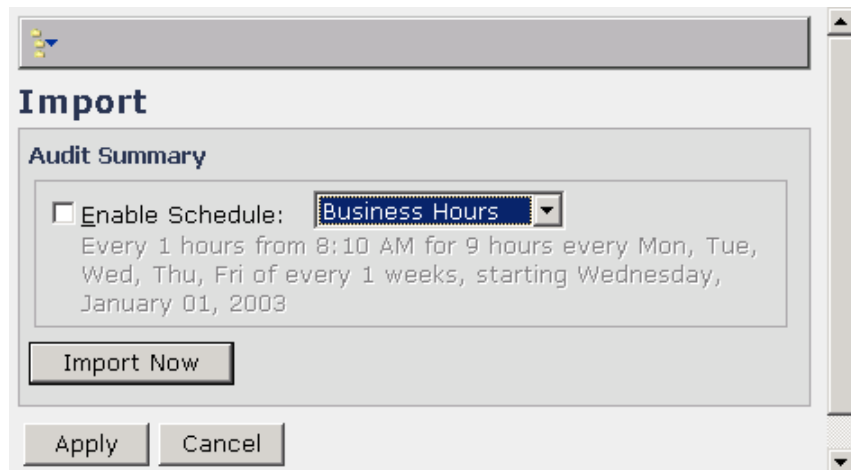
- D. **Integration Component:** Import data from the security audit database into the Notification Server database.

Schedule imports to occur after scheduled audits.

To import data from the security audit database

1. In Altiris Console, click the **Configuration** tab.
2. In the left pane, select **Configuration > Solution Settings > Security Management > Audit and Compliance > Import**.

The Import page appears in the right pane.



3. Select the schedule on which you want to import data from the security audit database.

When you select a schedule from the list, a description of the schedule appears below it.

4. Click **Enable Schedule**.

You can disable the schedule any time by clicking this checkbox again.

Tip

Any time you want to import data instantly, rather than wait for the next scheduled import to occur, you can click the **Import Now** button.

5. Click **Apply** to set the import schedule.

Step 4: Analyzing Results

Once you have gathered data through auditing, analyze it using the integration component so you can pinpoint security issues and take action. You can view audit details online, generate reports from them, and send Helpdesk tickets.

Viewing Audit Results

If you want to know the outcome of a computer's latest audit, you can display details about the audit using the Audit Detail views. The Audit Detail views are available in the Resources tab through the computer collections. You can display audit details about one computer at a time.

Note

In order to view audit results in Altiris Console, you must belong to a user group whose security role includes audit and compliance privileges. A Notification Server administrator can grant audit and compliance privileges to your user group by enabling the **View Audit Details** global privilege for your user group in the Security Role Management page. The Security Role Management page is located in **Configuration > Server Settings > Notification Server Settings**.

To review how to view a computer's audit results, see *Viewing Audit Results* (page 13).

Sending Helpdesk Tickets

You can configure notification policies to alert key individuals when audits reveal a potential problem. When an audit occurs that meets the notification's criteria, the integration component automatically sends a notification to a location designated in the notification policy. The solution comes with some notification policies already configured to generate Altiris Helpdesk or Alert Management tickets based on audit results.

Exercise

The solution lets you create new notification policies and modify existing notification policies. For the purpose of this exercise, however, you will

To review how to enable one of the notification policies that came with the solution, see *Sending Helpdesk Tickets* (page 15). To learn how to create new notification policies or modify existing notification policies, see chapter 4 of the *Altiris Audit Integration Component User's Guide* at <http://www.altiris.com/Support/Documentation/>.

Generating Web Reports

The solution offers ready-made reports you can use to share the results of the most recent audits with others. You can generate reports that show all audit results or just the results that relate to a particular security policy or category within a security policy. You can also designate which computers the report classifies as Passed and Failed, depending on how many Not OKs you find acceptable for the audit in question. The reports display data in chart and table format.

To review how to generate Web reports, see *Generating Web Reports* (page 16).

Step 5: Solving Problems

Now that you are aware of security issues caused by the Windows Vista settings you chose and didn't choose, you can solve those issues. The following Altiris products provide remediation capabilities:

For more information on using SecurityExpressions to perform this step, see the *SecurityExpressions Console User Guide* at <http://www.altiris.com/Support/Documentation/>.

- **Notification Server** - In general, you can use collections to pass audit data to other Altiris products from the integration component. See Notification Server's documentation for more information. You can find this and all Altiris documentation at <http://www.altiris.com/Support/Documentation/>.

After solving security issues, repeat steps 3, 4, and 5 in this phase until you're pleased with the level of compliance.

Ongoing Compliance Audits

Performing the migration and optimizing security company wide was a big job. Protect your investment of time and resources by performing audits on the migrated computers on an ongoing basis. Checking regularly for compliance ensures the security settings you carefully set up don't change once in place.

Process Overview

This phase is divided into the following tasks:

<i>Step 1: Determining the Issues</i> (page 3)	• Determine what issues to audit for.
<i>Step 2: Customizing Policy Files</i> (page 4)	• Customize policy files.
<i>Step 3: Auditing Target Computers</i> (page 25)	• Audit all Windows computers migrated to Windows Vista.
<i>Step 4: Analyzing Results</i> (page 28)	• Analyze the results.
<i>Step 5: Solving Problems</i> (page 29)5	• Solve any problems you find.

Step 1: Determining the Issues

Compile a list of the Windows Vista security settings you changed on the migrated computers based on your findings during the post-migration assessment. These are the changes you want to make to your audits so you can perform them regularly.

Step 2: Customizing Policy Files

Chances are, you can use the Windows Vista policy files you created for the post-migration assessment. If you need to change any policy files, use the console application to modify them as documented in *Step 2: Customizing Policy Files* (page 20). Most

likely, you'll be changing rules based on the conditions or behavior you expect Windows Vista computers to have going forward.

Step 3: Auditing Target Computers

When it comes time to audit, you can probably use the same machine lists you already created. The integration component, the audit agents, and credentials should already be in place. The difference in this phase is now you have to decide when, how, and how often you want audits to run.

- **Audit on Connect** is suited for computers that aren't always connected to the network. If a computer isn't connected to the network, you can't audit it.
- **Self-service audits** enable special users to perform audits whenever they want. This is usually in addition to scheduled or Audit-on-Connect audits. The self-service user typically is not a SecurityExpressions user. However, any user, casual or advanced, can audit their local system if they have administrator privileges on that computer.
- **Scheduled audits** are suited for computers that are connected to the network at predictable times.

To perform audits

- A. **Integration Component:** If you need to change which target computers use the audit agent to connect to the software, do so now.

Agentless audits require you to have administrative credentials for the target computers, which you'll have to configure in the console application. When making this decision for each target computer, keep in mind the audit agent:

- must be installed on the target computers.
- requires a Windows access group that can access the target computer.

Each method has different credential requirements, so decide now which target computers will use the audit agent. Then put them in a Notification Server collection. Finally, install the audit agent on the entire collection from the Security Audit Agent Installation page in Altiris Console.

To review how to install the audit agent, see step A in *Step 3: Auditing Target Computers* (page 6).

- B. **Integration Component:** If you need to move target computers to different machine lists or create new machine lists, do so now.

Note

Computers can appear in more than one machine list.

Recall the following factors before changing machine lists or creating new ones.

- If you want to audit different groups of target computers against different policy files, consider grouping the target computers to be audited by a single policy file together. If you have no other factors to consider, these are the only machine lists you'll need. If you only have one policy file to audit against, then you only need one machine list containing all the target computers.
- If you're auditing any target computers without the audit agent, the audit task needs the proper credentials to access the target computers. You can store credentials in the database for use during audits. If any agentless target

computers require the same credentials, you can group them in the same machine list, assign the credentials to the entire machine list, and then delegate the credentials to the server application. The console allows you to delegate credentials to the server through machine lists.

- Target computers audited using the audit agent often require credentials in order to log on to them as well. Group target computers with the same credentials in the same machine list, assign the credentials to the entire machine list, and then delegate the credentials to the server application. The console allows you to delegate credentials to the server through machine lists.
- Target computers in certain departments or geographical locations, or that have different uses, probably have different security requirements. That means you'll want to audit them against different policy files. Group these target computers together in the same machine lists so you can audit them at once.

To review how to create machine lists from collections, see step B in *Step 3: Auditing Target Computers* (page 6).

- C. **SecurityExpressions Server:** Set up Audit-on-Connect for systems you need to audit whenever they connect to the network.

Some computers aren't always connected to the network, which makes it hard to schedule a time to audit them. For these computers, perhaps Audit on Connect is a more appropriate way to audit.

This process involves creating profiles, which associates policies with scopes.

- Create policies, which consist of one or more policy files plus some other settings. When you associate a policy with an Audit-on-Connect profile, the target computers are audited against all policy files in the policy and according to all settings in the policy.
- Create scopes, assigning the appropriate credentials to them and arranging them in the order you want them checked.
- Create profiles, associating policies with scopes.

For more information on using SecurityExpressions to perform this step, see the *SecurityExpressions Audit and Compliance Server User's Guide* at <http://www.altiris.com/Support/Documentation/>.

- D. **SecurityExpressions Setup program:** Install and configure connection monitors to detect Audit-on-Connect activity.

Complete a configuration file (dmconfig.txt) for each connection monitor installed. Then, on the Connection Monitors page in the server application, compile a list of all connection monitors installed and their passwords.

For more information on using SecurityExpressions to perform this step, see the *SecurityExpressions Audit and Compliance Server Getting Started Guide* at <http://www.altiris.com/Support/Documentation/>.

- E. **Server:** If necessary, create Audit-on-Connect profiles and install and configure connection monitors for anyone who needs to perform self-service auditing using multiple policy files at once.

Use the process outlined in step C and step D.

- F. **SecurityExpressions Server:** Modify the scheduled audit tasks you already created and create new scheduled audit tasks as needed. Schedule them to run regularly.

- If you need to modify the policies you already created to account for any changes made based on the post-migration assessment, do so now. When you associate a policy with a scheduled audit task, the target computers are audited against all policy files in the policy and according to all settings in the policy.
- Modify the scheduled audit task, scheduling it to run regularly and assigning the appropriate machine lists and policy.

SecurityExpressions audits the target computers at the scheduled time.

For more information on using SecurityExpressions to perform this step, see the *SecurityExpressions Audit and Compliance Server User's Guide* at <http://www.altiris.com/Support/Documentation/>.

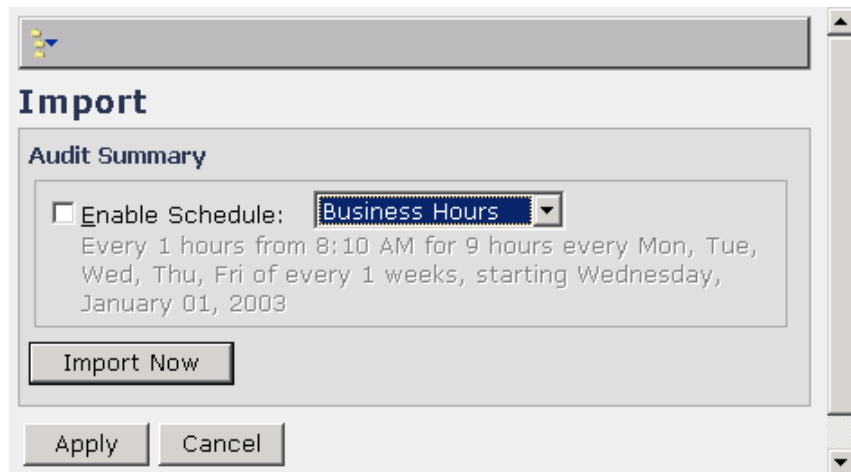
- G. **Integration Component:** Import data from the security audit database into the Notification Server database.

Schedule imports to occur after scheduled audits.

To import data from the security audit database

1. In Altiris Console, click the **Configuration** tab.
2. In the left pane, select **Configuration > Solution Settings > Security Management > Audit and Compliance > Import**.

The Import page appears in the right pane.



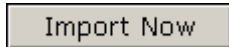
3. Select the schedule on which you want to import data from the security audit database.


When you select a schedule from the list, a description of the schedule appears below it.

4. Click **Enable Schedule**.

You can disable the schedule any time by clicking this checkbox again.

Tip

Any time you want to import data instantly, rather than wait for the next scheduled import to occur, you can click the  button.

5. Click  to set the import schedule.

Step 4: Analyzing Results

Once you have gathered data through auditing, analyze it using the integration component so you can pinpoint security issues and take action. You can view audit details online, generate reports from them, and send Helpdesk tickets.

Viewing Audit Results

If you want to know the outcome of a computer's latest audit, you can display details about the audit using the Audit Detail views. The Audit Detail views are available in the Resources tab through the computer collections. You can display audit details about one computer at a time.

Note

In order to view audit results in Altiris Console, you must belong to a user group whose security role includes audit and compliance privileges. A Notification Server administrator can grant audit and compliance privileges to your user group by enabling the **View Audit Details** global privilege for your user group in the Security Role Management page. The Security Role Management page is located in **Configuration > Server Settings > Notification Server Settings**.

To review how to view a computer's audit results, see *Viewing Audit Results* (page 13).

Sending Helpdesk Tickets

You can configure notification policies to alert key individuals when audits reveal a potential problem. When an audit occurs that meets the notification's criteria, the integration component automatically sends a notification to a location designated in the notification policy. The solution comes with some notification policies already configured to generate Altiris Helpdesk or Alert Management tickets based on audit results.

Exercise

The solution lets you create new notification policies and modify existing notification policies. For the purpose of this exercise, however, you will

To review how to enable one of the notification policies that came with the solution, see *Sending Helpdesk Tickets* (page 15). To learn how to create new notification policies or modify existing notification policies, see chapter 4 of the *Altiris Audit Integration Component User's Guide* at <http://www.altiris.com/Support/Documentation/>.

Generating Web Reports

The solution offers ready-made reports you can use to share the results of the most recent audits with others. You can generate reports that show all audit results or just the results that relate to a particular security policy or category within a security policy. You can also designate which computers the report classifies as Passed and Failed, depending on how many Not OKs you find acceptable for the audit in question. The reports display data in chart and table format.

To review how to generate Web reports, see *Generating Web Reports* (page 16).

Step 5: Solving Problems

Whenever a target computer doesn't comply with the organization's policies, you can solve the problem. The following Altiris products provide remediation capabilities:

- **SecurityExpressions** - The console application lets you perform automated fixes on rules that rated Not OK. After the audit, go to the Rules tab and right click on rules that rated Not OK. Select either **Fix Item** to fix the highlighted rule or select **Fix All Problems** to fix all Not OK rules.

For more information on using SecurityExpressions to perform this step, see the *SecurityExpressions Console User Guide* at <http://www.altiris.com/Support/Documentation/>.

- **Notification Server** - In general, you can use collections to pass audit data to other Altiris products from the integration component. See Notification Server's documentation for more information. You can find this and all Altiris documentation at <http://www.altiris.com/Support/Documentation/>.

After solving security issues, repeat steps 3, 4, and 5 in this phase until you're pleased with the level of compliance.