Installation and Configuration Guide

NetIQ Security and Compliance Dashboard

June 2011

Legal Notice

NetIQ Secure Configuration Manager is covered by United States Patent No(s): 5829001, 7093251.

Contents

Chapter 1
Installing the Security and Compliance Dashboard 1

Chapter 2
Getting Started with the Dashboard 11

Appendix A
Upgrading the Dashboard 17

About This Book and the Library

The *Installation and Configuration Guide* provides steps for Security and Compliance Dashboard (Dashboard) installation, configuration, and integration information for the NetIQ Secure Configuration Manager (Secure Configuration Manager) product.

Intended Audience

This book provides information for individuals responsible for installing the Dashboard and configuring the Dashboard to display information from Secure Configuration Manager.

Other Information in the Library

You can use the Dashboard to display information from Secure Configuration Manager. For more information about Secure Configuration Manager, see the *User Guide for Secure Configuration Manager*.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as [*value*]	• Optional parameters of a command
Braces, such as {*value*}	• Required parameters of a command
Logical OR, such as *value1*| *value2*	• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ Corporation, an Attachmate business, is a leading provider of comprehensive systems and security management solutions that help enterprises maximize IT service delivery and efficiency. With more than 12,000 customers worldwide, NetIQ solutions yield measurable business value and results that dynamic organizations demand. Best-of-breed solutions from NetIQ Corporation help IT organizations deliver critical business services, mitigate operational risk, and document policy compliance. The company's portfolio of award-winning management solutions includes IT Process Automation, Systems Management, Security Management, Configuration Control and Enterprise Administration. For more information, please visit www.netiq.com.

Contacting NetIQ Corporation

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

Telephone: 713-418-5000
888-323-6768 (only in the United States and Canada)

Sales Email: info@netiq.com

Support: www.netiq.com/support

Web Site: www.netiq.com

Chapter 1

Installing the Security and Compliance Dashboard

As organizations are forced to comply with multiple regulations and standards, organizations need a way to clearly communicate their security compliance status to internal and external stakeholders. Communicating the security compliance status is made more difficult as each stakeholder has unique requirements on what they need and want to see. To compound the problem, various stakeholders are distributed geographically and have differing levels of technical proficiency. The ideal solution to this situation must be highly customizable, very easy to use and understand, and have the proper security to ensure stakeholders can see only what they should see.

What is the Security and Compliance Dashboard?

The Security and Compliance Dashboard (Dashboard) streamlines the audit and compliance process by expanding upon the reporting capability of Secure Configuration Manager. You can quickly determine how well each IT asset in your environment complies with Secure Configuration Manager policy templates. This high-level overview of your environment's compliance allows you to see the overall status and trends of security compliance at a single glance.

Based on your Secure Configuration Manager console user account permissions, you can remotely audit your enterprise security by reviewing your systems' compliance or risk status. When a system is out of compliance with a policy template or has a high risk score, you can browse the data for that system to see which checks in the policy template failed on exactly which endpoints.

This section provides requirements, details of supported configurations, and other information necessary for planning your Dashboard installation environment.

Accessing Data in the Dashboard

Dashboard users and administrators are based on Secure Configuration Manager user accounts. The Dashboard authenticates your Secure Configuration Manager console credentials, and then displays compliance information for Secure Configuration Manager managed groups based on your console permissions.

Users

Any user with a Secure Configuration Manager console user account with the Access IT Assets permission. Dashboard users can view tabs assigned to the Secure Configuration Manager roles for which they are members. When users access tabs in the Dashboard, they can see data for only the managed groups associated with their Secure Configuration Manager console user account permissions.

Administrators

Any Secure Configuration Manager console user who has administrator permissions in Secure Configuration Manager. You can create a console administrator by assigning the Administrators role to a console user account. A console administrator is not required to be an administrator on the Web server.

Dashboard administrators can create, publish, modify, and delete tabs, as well as update the global settings of the Dashboard.

Viewing Compliance Information in the Dashboard

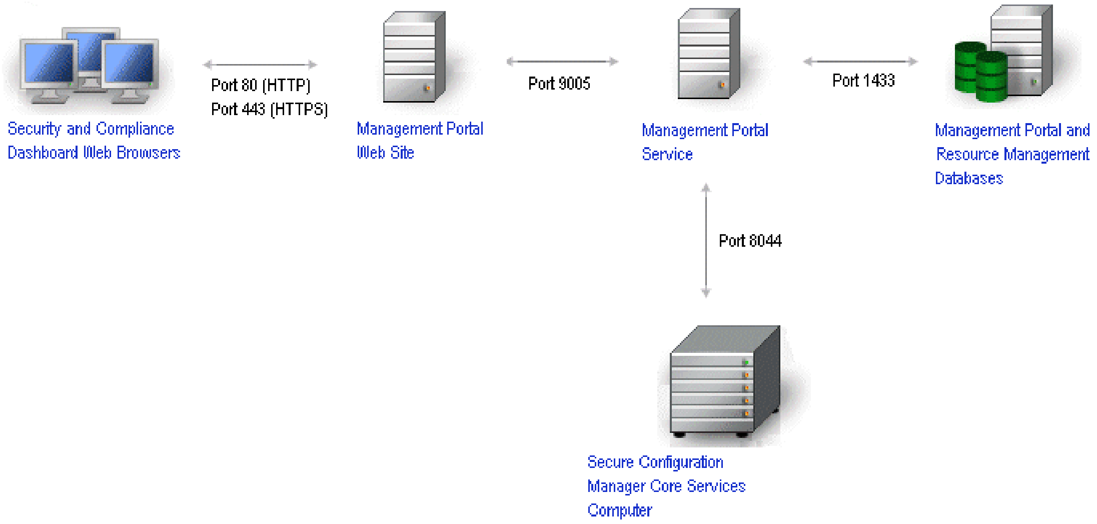
Tabs are subsets of compliance data based on the specified managed groups, scoring type, and policy templates. Tabs provide a way to filter Secure Configuration Manager compliance information and provide the status for various levels of management in your organization. You can determine which users you want to see compliance information for specific managed groups as well as define how the compliance results are calculated. Depending on how your managed groups are defined in Secure Configuration Manager, you may create tabs based on geography, business unit, or area of responsibility.

Planning Your Dashboard Environment

This section provides requirements, details of supported configurations, and other information necessary for planning your Dashboard installation environment.

Understanding the Dashboard Infrastructure

The Dashboard allows you to remotely view your environment's policy compliance. This product includes the Management Portal infrastructure components that you install in your environment to facilitate communication with Secure Configuration Manager. The Management Portal infrastructure hosts the Dashboard to allow users to remotely connect to the Web-based interface. You should plan to install these components over a number of computers.


Security and Compliance Dashboard Web Browsers
Port 80 (HTTP)
Port 443 (HTTPS)
Management Portal Web Site
Port 9005
Management Portal Service
Port 1433
Management Portal and Resource Management Databases
Port 8044
Secure Configuration Manager Core Services Computer

The Dashboard includes the following major components:

Dashboard Web Browsers

A Web-based user interface that allows users to view compliance data for their environment based on Secure Configuration Manager policy templates.

Portal Web Site

Web site components that support the Dashboard Web-based interface. The NetIQ Management Portal Setup Wizard installs the Dashboard on the Portal Web Site computer along with the Web Site components.

Portal Service

Services that manage communication with remote users, the Portal Web Site, the Portal and Resource Management databases, and the Secure Configuration Manager Core Services computer.

Portal Database

Microsoft SQL Server database that stores all Management Portal information, such as processes and supporting analysis.

Resource Management Database (IQRM)

Microsoft SQL Server database that stores information needed to display resource data such as services, users, and computers. The NetIQ Management Portal Setup Wizard remotely installs the Resource Management database on the Portal Database computer while installing the Portal Service component.

Resource Management Namespace Provider

The Resource Management Namespace Provider facilitates communication with the Portal Database and Secure Configuration Manager.

Supported Configurations

NetIQ Corportaion recommends you install the Management Portal components strategically over a number of computers. If you are installing the Management Portal components in a test environment, you can install all components on one computer.

Portal Database Computer

Install the Portal and Resource Management (IQRM) databases on one computer.

Web Site Computer

Install the Portal Web Site components, which include the Management Portal application and Dashboard, on one computer.

Portal Service Computer

Install the Portal Service component, which includes the Resource Management Namespace Provider, on one computer.

For more information about installing Management Portal components, see “Installing Management Portal Infrastructure Components” on page 7.

Support for Non-English Language Versions

The Management Portal components support Microsoft Windows in English, Spanish, German, and Portuguese, and Microsoft SQL Server in United States - English. The language version for the Microsoft Windows operating system should be the same across all computers where you install the Portal Web Site, Portal Service, and Portal Database.

Core Services Computer

Each installation of the Dashboard can display information for only one Secure Configuration Manager Core Services computer. Connecting the Portal Service component to multiple Core Services computers is not supported.

Default Ports

Open the ports listed in the following table for proper communication between Management Portal infrastructure components.

Port Number	Component Computer	Port Use
80 (HTTP) 443 (HTTPS)	Portal Web Site computer	Used by the Portal Web Site computer to allow remote users to log on to the Dashboard. The Portal Web Site computer uses port 80 by default.
9005	Portal Service computer	Used by the Portal Service computer to communicate with the Portal Web Site computer.
1433	Portal Database computer	Used by the Portal Service computer to communicate with the Portal and Resource Management databases.
8044	Core Services computer	Used by the Portal Service to communicate with the Secure Configuration Manager Core Services computer.

Planning to Install the Portal Database

The following table lists requirements for the Database Server..

Category	Requirement	Recommendation
Processor	500 MHz Intel Pentium III server class or equivalent	3 GHz Intel Xeon server processor or equivalent
Disk Space	20 GB free disk space* **If you plan to install the Portal and Resource Management databases on the same computer as the Secure Configuration Manager database, you need a total of 40 GB free disk space.*	100 GB free disk space* **If you plan to install the Portal and Resource Management databases on the same computer as the Secure Configuration Manager database, NetIQ Corporation recommends you have a total of 200 GB free disk space.*
Memory	1.5 GB	6 GB
Operating System	One of the following operating systems: • 32-bit and 64-bit Windows Server 2003 Service Pack 2 or later • 32-bit and 64-bit Windows Server 2003 R2 • 32-bit and 64-bit Windows Server 2008 • 64-bit Windows Server 2008 R2	
Database	One of the following database versions: • 32-bit Microsoft SQL Server 2005 Service Pack 1 or later • 32-bit and 64-bit Microsoft SQL Server 2008 • 64-bit Microsoft SQL Server 2008 R2	
Additional Software	Microsoft SQL Server Native Client 2005 or 2008	

Installing and Configuring Microsoft SQL Server

The Portal Database computer requires Microsoft SQL Server 2005 Service Pack 1 (United States - English version) or 2008 with mixed-mode authentication. Non-U.S. language versions of Microsoft SQL Server are not supported.

Follow the instructions provided in the Microsoft SQL Server documentation to install the database software.

You can also install the Portal Database in a Microsoft cluster environment. For more information about setting up SQL Server clusters, see the appropriate Microsoft documentation.

Planning to Install the Portal Web Site

The following table lists requirements for the Portal Web site computer.:

Category	Requirement	Recommendation
Processor	500 MHz Intel Pentium III or equivalent	3 GHz Intel Xeon server processor or equivalent
Disk Space	4 GB free disk space	100 GB free disk space
Memory	1 GB	6 GB
Operating System	One of the following operating systems: • 32-bit and 64-bit Windows Server 2003 Service Pack 2 or later • 32-bit and 64-bit Windows Server 2003 R2 • 32-bit and 64-bit Windows XP Service Pack 2 or later • 32-bit and 64-bit Windows Vista Service Pack 1 or later • 32-bit and 64-bit Windows Server 2008 • 64-bit Windows Server 2008 R2 • 32-bit and 64-bit Windows 7	
Additional Software	• Microsoft Internet Information Services 6.0, 7.0, or 7.5 (32-bit mode) • Microsoft ASP.NET 2.0 (32-bit extensions) • Microsoft Chart Control 3.5.0.0 • Microsoft .NET Framework 3.5 Service Pack 1	
Web Browsers	The Dashboard supports the following Web browsers: • Internet Explorer 7.0* • Internet Explorer 8.0* • Firefox 3.5 The minimum supported resolution for these Web browsers is 1024x768. The Dashboard is optimized for a resolution of 1152x864. ** If your Internet Options Security Settings or Privacy Settings are set to **Medium** or **High**, you must add the Dashboard URL as a trusted site.*	

Securing Your Management Portal Infrastructure

The Management Portal infrastructure uses the following technologies to secure your Portal Web Site computer:

- ASP.NET security provides application-level security for the Portal Web Site computer. You can lock down the computer using best practices for ASP.NET security.
- Security features in IIS control access to the Portal Web Site virtual directory.

Planning to Install the Portal Service

The following table lists requirements for the Portal Service computer..

Category	Requirement	Recommendation
Processor	500 MHz Intel Pentium III server class or equivalent	3 GHz Intel Xeon server processor or equivalent
Disk Space	20 GB free disk space	100 GB free disk space
Memory	512 MB	6 GB
Operating System	One of the following operating systems: • Windows Server 2003 Service Pack 2 or later • 32-bit and 64-bit Windows Server 2003 R2 • 32-bit and 64-bit Windows Server 2008 • 64-bit Windows Server 2008 R2	
Additional Software	Microsoft SQL Server Native Client 2005 or 2008	

Planning to Access the Dashboard from Web Browsers

Computers used to remotely access the Dashboard must be running one of the following Web browsers:

- Internet Explorer 7.0*
- Internet Explorer 8.0*
- Firefox 3.5

The minimum supported resolution for these Web browsers is 1024x768. The Dashboard is optimized for a resolution of 1152x864.

* If your Internet Options Security Settings or Privacy Settings are set to **Medium** or **High**, you must add the Dashboard URL as a trusted site.

Installing Management Portal Infrastructure Components

To successfully install the Management Portal infrastructure, you must install all of the components. Use the following checklist to install the Management Portal components in your production environment. This checklist assumes that you already have Secure Configuration Manager installed in your environment.

☑	Checklist Items
☐	**1.** Review product architecture information to learn about Management Portal infrastructure components. For more information, see “Understanding the Dashboard Infrastructure” on page 3.
☐	**2.** Install the Portal Database component. For more information, see “Installing the Portal Database Component” on page 8.
☐	**3.** Install the Portal Web Site component. For more information, see “Installing the Portal Web Site Component” on page 8.
☐	**4.** Install the Portal Service component. For more information, see “Installing the Portal Service Component” on page 9.

Installing the Portal Database Component

These steps guide you through the process of installing the Management Portal database on the Portal Database computer.

To install the Management Portal Database:

1. Log on with a local administrator account to the Portal Database computer.
2. Ensure the computer meets the minimum requirements. For more information, see "Installing the Portal Database Component" on page 8.
3. Run the setup program from the root folder of the installation kit.
4. Click **Begin Setup**.
5. On the Select Features window, clear the following checkboxes:
    - **Portal Web Site**
    - **Portal Service**
6. Click **Next**.
7. Follow the instructions in the NetIQ Management Portal Setup wizard until you finish installing the Management Portal database, and then click **Finish**.

Installing the Portal Web Site Component

These steps guide you through the process of installing the Portal Web Site component on the Portal Web Site computer.

To install the Portal Web Site component:

1. Log on with a local administrator account to the computer where you want to install the Portal Web Site component.
2. Ensure the computer meets the minimum requirements. For more information, see "Planning to Install the Portal Web Site" on page 6.
3. ***If you are running IIS on a 64-bit computer***, complete the following steps:
    a. Enable IIS to run 32-bit applications on a 64-bit computer. For more information, see the following Microsoft Web site: http://technet.microsoft.com/en-us/library/cc737351(WS.10).aspx).
    b. Install the 32-bit version of ASP.Net 2.0.
    c. Restart the World Wide Web Publishing service.
4. Run the setup program from the root folder of the installation kit.
5. Click **Begin Setup**.
6. On the Select Features window, clear the following checkboxes:
    - **Portal Service**
    - **Portal Database**
7. Click **Next**.

8. Ensure the computer meets all of the prerequisites for the Portal Web Site component, and then click **Next**.
9. Specify the short name or alias for the Dashboard, and click **Next**.

   This alias is part of the URL for the Dashboard. For example, if you use the default alias SCMDashboard, the URL to access the Dashboard is `http://servername/SCMDashboard`, where *`servername`* is the name of the server where you are installing the Portal Web Site component.
10. Specify the type of communication you want to use when communicating with the Dashboard.

    Note

    NetIQ Corporation recommends you use Secure Sockets Layer (SSL) for Dashboard communication. Otherwise, any person using a sniffer on your network could access passwords and other privileged information.

    For more information about configuring SSL in Microsoft Certificate Services, see the Microsoft documentation.

    ---
11. Specify the port, logon information, and installation path you want to use for the Management Portal application. You must specify a user account that is a member of the local Administrator group.
12. Specify the computer, logon information, and installation path for the Portal Service computer. The Dashboard uses the Resource Management Provider on the Portal Service computer to communicate with the Portal Web Site. You must specify a user account that is a member of the local Administrator group.
13. Click **Install**.

Installing the Portal Service Component

These steps guide you through the process of installing the Management Portal services, Resource Management Namespace Provider on the Portal Service computer. This installation also installs the Resource Management database on the Portal Database computer.

To install the Portal Service component:

1. Log on with a local administrator account to the computer where you want to install the Portal Service components.
2. Ensure the computer meets the minimum requirements. For more information, see “Planning to Install the Portal Web Site” on page 6.
3. Run the setup program from the root folder of the installation kit.
4. Click **Begin Setup**.
5. On the Select Features window, clear the following checkboxes:
   - **Portal Web Site**
   - **Portal Database**
6. Click **Next**.
7. Specify the computer, logon, and installation path where you installed the Portal Web Site component.

8. Specify the Secure Configuration Manager Core Services computer information for which you want the Dashboard to display compliance data.

Notes

- Ensure you specify the same protocol specified on the Core Services Configuration Utility Web Services tab.
- Specify the Secure Configuration Manager console user account you want to access the Core Services computer. Ensure the user account you specify is a member of the Administrator role.

9. Specify the Portal Database computer name.

   The Portal Service component remotely installs the Resource Management database on the Portal Database computer.

10. Specify a user account that is an Administrator on the Portal Database computer, and a member of the db_owner role on the SQL Server instance containing the Resource Management database (IQRM).
11. Follow the remaining instructions in the NetIQ Management Portal Setup Wizard until you finish installing the Management Portal services and Resource Management database, and then click **Finish**.

Chapter 2

Getting Started with the Dashboard

Once you have installed the Portal Web Site, Portal Service, and Portal Database components, you are ready to define how you want to view Secure Configuration Manager compliance information in the Dashboard and which users you want to see this information.

Logging on to the Dashboard

You can launch the Dashboard from any computer with connectivity to the Internet. For quick and easy access from remote computers, add the Dashboard URL to the Favorites tab of your browser. For more information about supported browsers, see “Planning to Access the Dashboard from Web Browsers” on page 7.

To log on to the Dashboard:

1. ***If you are accessing the Dashboard from the Portal Web Site computer***, double-click the Dashboard shortcut.
2. ***If you are accessing the Dashboard remotely***, use the URL `https://`*`HostComputer`*`/`*`AliasName`*`/`*`Portal.aspx`* where *`HostComputer`* is the name of the Portal Web Site computer and *`AliasName`* is the name of the Dashboard alias you provided during installation. If you specified `HTTP` protocol during installation, use the URL `http://`*`HostComputer/AliasName/Portal.aspx`*

   Provide this URL to all users who will remotely access the Dashboard
3. Specify your Secure Configuration Manager console user name and password.

   To create tabs and view configuration settings, you must log in with a Secure Configuration Manager user account that is a member of the Administrator role.
4. Click **Log In**.

Troubleshooting Logon Errors

Each time a user attempts to log on to the Dashboard, information is recorded in a log file. This file provides the computer name and port of the computer the user tried to access, as well as the account name and password provided. You can use this information to display the exception and error details to determine if the user tried to log on using a valid Secure Configuration Manager console user account.

To troubleshoot logon errors:

1. Log on to the Portal Web Site computer with a domain or local Administrator account.
2. Use Windows Explorer to open the `NetIQEMP_IQConnect.log` file.

   By default, you can locate the `NetIQEMP_IQConnect.log` file in:

   `Program Files\NetIQ\ManagementPortal\Website\log\`
3. Review the log to see the exception and error details.

Viewing Secure Configuration Manager Compliance Data

The Dashboard leverages compliance data collected from Secure Configuration Manager policy templates to allow you to easily identify the compliance of your environment. In order to provide the most appropriate view of your environment for your stakeholders, the Dashboard displays compliance data based on the Secure Configuration Manager managed groups and scoring types you want each user role to see.

Understanding Managed Groups

In the Secure Configuration Manager console, a managed group is a view that presents endpoints organized into logical groups. You can create user-defined groups to provide a view of your company's assets, such as organizational hierarchy, physical location of computers, or type of service the computers perform.

You must define managed groups in Secure Configuration Manager before you can create tabs in the Dashboard. If you change your managed group structure after creating tabs, you need to unpublish tabs that contained the changed managed groups and re-select the managed groups included in the tab.

For more information about creating managed groups, see the *User Guide for Secure Configuration Manager*.

Understanding Scoring Types

The Dashboard gathers security checkup report results for the Overall Status and Detail charts each time you refresh the Dashboard so you can see the most recent run of the specified Secure Configuration Manager policy templates. By default, Secure Configuration Manager retains the most recent run data for the past 30 days, but you can customize this number on the Out of Compliance Alerts tab of the Core Services Configuration Utility. For more information, see the *User Guide for Secure Configuration Manager*.

The Dashboard also gathers the results of the most recent run of security checkup reports nightly to create trend data. You can specify the interval (daily, weekly, or monthly) you want to display for the trending charts. The Dashboard does not display data in the trend charts until the interval is complete. For example, if you specify that you want to display trend data on a monthly basis, the trend charts do not contain data until the first day of the next month.

The Dashboard displays compliance data only for scored security checks. Security checks with a scoring method of `Informational only` are not included in the compliance data.

To customize the view of your environment's compliance, you can specify whether the Dashboard uses the System, Technical Control, or Risk scoring type to display compliance results.

System Compliance

Allows you to see the compliance of your environment based on the compliance status of each system. Systems are considered out-of-compliance if any security check fails on the system. For example, if you have a system with three endpoints and you run five policy templates against each of those three endpoints and only one security check fails on an endpoint, the Dashboard displays the compliance of the system as `Failed`.

Technical Control Compliance

Allows you to see the compliance of your environment based on passed and failed security checks. Security checks provide a way for you to determine if your systems are in compliance with specific technical controls. This scoring type provides you the ability to track progress with technical controls and show improvement in overall compliance.

Risk Compliance

Allows you to see the compliance of your environment based on Secure Configuration Manager risk scoring. Risk scores help you identify which endpoints have the most serious exposures based on discovered threats and endpoint importance. For more information about risk scoring, see the *User Guide for Secure Configuration Manager.*

Since risk scores are calculated for each template run for an endpoint, the Dashboard reviews the risk score level for each endpoint template combination and uses the most conservative risk level to determine the compliance for the system. For example, if you have two endpoints on one system, and one endpoint failed and the other endpoint passed, the Dashboard displays the compliance of the system as `Failed`.

Understanding Roles

A role is a set of permissions that controls access to specific Secure Configuration Manager features. Assigning Secure Configuration Manager console users to roles allows you to easily maintain and update permissions while consistently enforcing the same level of security across your organization.

You use these same roles in the Dashboard to assign access to tabs. If you want to use roles other than those provided by Secure Configuration Manager, you can create user-defined roles in Secure Configuration Manager to meet your organization's needs.

For more information about Secure Configuration Manager roles, see the *User Guide for Secure Configuration Manager.*

Creating Tabs

Tabs provide a way to filter Secure Configuration Manager compliance information and provide the status for various levels of management in your organization. Secure Configuration Manager administrators can determine which users they want to see compliance information for specific managed groups as well as define how the compliance results are calculated when they create tabs. Administrators can also publish, modify, and delete tabs they have created. You cannot modify or delete a tab created by another Secure Configuration Manager administrator.

To create a tab:

1. Ensure your Secure Configuration Manager managed group structure is organized according to the setup of your organization. For more information, see "Understanding Managed Groups" on page 12.
2. Ensure you have the latest policy templates from AutoSync. For more information, see the *User Guide for Secure Configuration Manager.*

3. Ensure the appropriate roles are defined in Secure Configuration Manager. For more information, see “Understanding Roles” on page 13.
4. Log on to the Dashboard with a Secure Configuration Manager administrator account.
5. Click the tab with the green plus (+) sign.
6. Follow the instructions in the wizard until you have finished creating the tab.

Copying a Tab

You can create a new tab by copying an existing tab. Copying a tab provides a quick and easy way to create multiple new tabs. For example, you can create a tab that contains specific policy templates, and then copy the tab to ensure the same policy templates are specified across multiple tabs. You can copy only those tabs that you created.

To copy a tab:

1. Log on to the Dashboard with a Secure Configuration Manager administrator account.
2. Click a tab that you created and want to copy.
3. Click **Edit Tab**.
4. Specify the appropriate settings and role assignments.
5. Change the name of the tab.
6. Click **Finish**.
7. Click **Yes**.
8. Click **Yes**.

Managing Configuration Settings

During installation, you specify the Portal Web Site, Portal Service, and Portal Database computers along with all of the necessary authentication methods and credentials the components use to communicate with each other. You also specify the Secure Configuration Manager Core Services computer for which you want to view compliance data.

In the Dashboard Web interface, users logged on with a Secure Configuration Manager administrator account can view the Management Portal application computer information and Secure Configuration Manager Core Services computer name and port. Users can also view or upload license information.

Using the standalone NetIQ Security and Compliance Dashboard Configuration Utility, you can modify the configuration settings for the Resource Management service computer, Resource Management database, Management Portal database, and Secure Configuration Manager Core Services computer.

To change configuration settings:

1. ***If you want to modify the Resource Management service information***, log on to the Portal Web Site computer with a domain or local Administrator account.
2. ***If you want to modify the Resource Management database, Management Portal database, or Secure Configuration Manager Core Services computer information***, log on to the Portal Service computer with a domain or local Administrator account.
3. Click **Start > Programs > NetIQ Security and Compliance Dashboard > NetIQ Security and Compliance Dashboard Configuration Utility**.

Appendix A

Upgrading the Dashboard

If you already have the Dashboard installed in your environment, perform the following upgrade steps to install the most recent version of the Dashboard. This procedure includes steps for all-in-one and distributed environments.

To upgrade the Dashboard:

1. Close all Dashboard consoles.
2. Close all Secure Configuration Manager consoles.
3. On the Portal Service and Portal Web Site computers, stop the following services:
   - NetIQ Management Portal Namespace service
   - World Wide Web Publishing service (if applicable)
4. On the Secure Configuration Manager Core Services computer, stop the NetIQ Core Services service.
5. Back up the IQRM database to a work folder using Microsoft SQL Server Management Studio.
6. Back up the NQITMgmtPortalService database to a work folder using Microsoft SQL Server Management Studio.
7. Back up the VigilEnt database to a work folder using Microsoft SQL Server Management Studio.
8. On the Secure Configuration Manager Core Services computer, start the NetIQ Core Services service.
9. On the Portal Service and Portal Web Site computers, start the NetIQ Management Portal Namespace service.
10. Run `Setup.exe` from the NetIQ Security and Compliance Dashboard 1.1 installation kit.
11. On the Install Security and Compliance Dashboard window, click **Start Installation**.
12. On the Welcome window, verify the currently installed version is 1.0.*x.xx*, where *x* is the service pack level and *xx* is the build number.
13. Click **Next**.
14. Click **Remove**.
15. Complete the wizard to successfully uninstall the Security and Compliance Dashboard 1.0.
16. On the Portal Service and Portal Web Site computers, navigate to the `...\NetIQ\ManagementPortal` folder in Windows Explorer and delete the `ManagementPortal` folder.

17. ***If you installed the Dashboard components in a distributed environment***, repeat Steps 10 through 16 on each computer where the components are installed.

18. ***If you installed all Dashboard components on a single computer***, restart the computer.

19. If applicable, start the World Wide Web Publishing service on the Portal Service and Portal Web Site computers.

20. Install the Dashboard components by performing the following steps:

    Note

    Ensure you install the Dashboard components in the following order:

    - Portal Database
    - Portal Service
    - Portal Web Site

    ---

    a. On the Install Security and Compliance Dashboard window, click **Start Installation**.

    b. On the Welcome window, verify the current version is 1.1.*x.xx*, where *x* is the service pack level and *xx* is the build number.

    c. Click **Next**.

    d. Clear the components you do not want to install and click **Next**.

    e. When installing the Portal Database, click **No** when you receive a message that the setup program has detected an existing database.