NetIQ Secure Configuration Manager Dashboard

User Guide

October 2016

Legal Notice

Contents

About This Book and the Library

The *User Guide* provides steps for Secure Configuration Manager Dashboard (Dashboard) installation and configuration, and also provides an overview of the dashboard and describes how to use it.

Intended Audience

This guide is intended for Secure Configuration Manager administrators and Dashboard users.

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 *NetIQ Secure Configuration Manager User Guide*.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Understanding the Dashboard

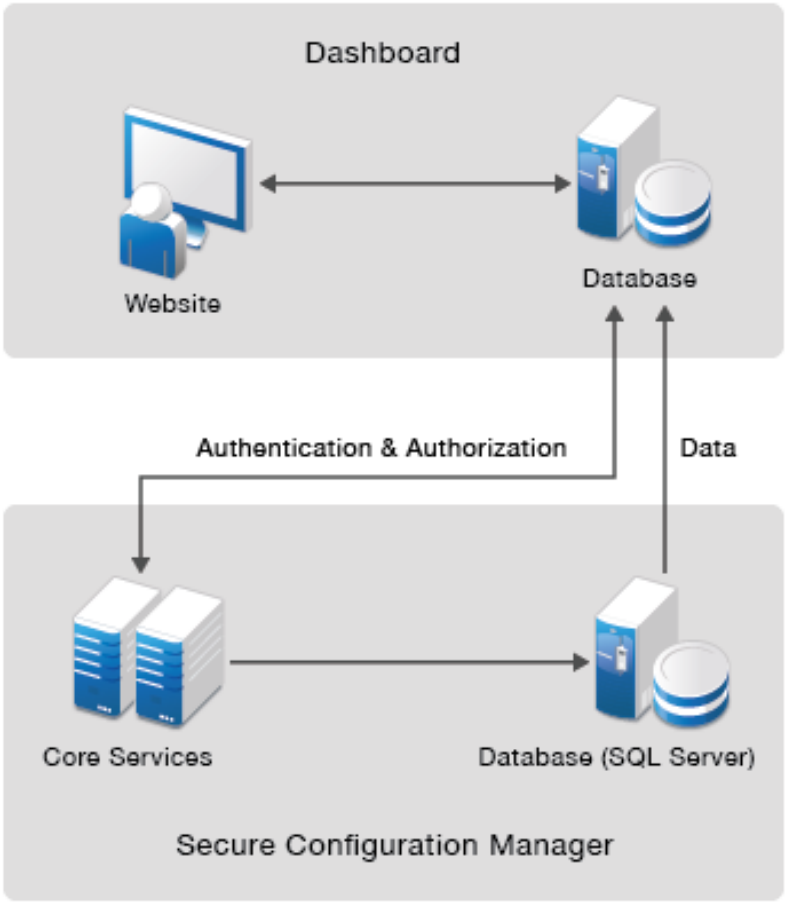
The Secure Configuration Manager Dashboard (Dashboard) expands the reporting capability of Secure Configuration Manager, and provides access through a web browser. You can quickly determine how well each IT asset in your environment complies with Secure Configuration Manager policy templates. This high-level 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 security checks in the policy template failed on exactly which endpoints.

1.1 Understanding the Dashboard Components

The Dashboard comprises a web-based application and a database. The database collects endpoint compliance data from Secure Configuration Manager, then generates charts for the Dashboard Website. The Dashboard application uses the same user accounts and roles as the Secure Configuration Manager console.

The following diagram depicts the Dashboard architecture and how it interacts with Secure Configuration Manager.



1.1.1 Dashboard Database

The Dashboard database fetches data from the Secure Configuration Manager database (SQL Server) and stores it. This data is used in Dashboard charts.

1.1.2 Dashboard Website

You can conveniently view the compliance of your computing systems in Dashboard Website from your local computer. For more information about supported web browsers, see the Secure Configuration Manager Technical Information web page.

1.2 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 authorization settings.

Users

Any user with a Secure Configuration Manager console user account. When users access charts in the Dashboard, they can see data for only the groups and templates associated with their user account.

Administrators

Any Secure Configuration Manager console user who has administrator permissions in Secure Configuration Manager.

2 Installing the Dashboard

This chapter describes how to install the Dashboard.

2.1 Planning the Dashboard Installation

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

2.1.1 System Requirements

This section provides hardware, software, and permissions requirements for the Dashboard computer.

Category	Minimum Requirements and Recommendations
Processor	See the NetIQ Secure Configuration Manager Technical Information web page.
Disk Space	
Memory	
Operating System	
Monitor	
Installation Permissions	The user account you use to install the Dashboard must be a member of the Administrators local group on the computer.
Usage Permissions	Any Secure Configuration Manager user account can use the Dashboard.
Ports	Keep the required ports open. For more information, see Section 2.1.4, “Default Ports,” on page 14.

2.1.2 Supported Web Browsers

For information about the supported browsers, see the NetIQ Secure Configuration Manager Technical Information web page.

If you are using Internet Explorer 10, enable TLS 1.1 and TLS 1.2 protocols by performing the following steps:

1. In Internet Explorer, go to **Settings** > **Internet Options** > **Advanced**.
2. Scroll down to the Security settings options and perform the following:
   - Unselect **Use TLS 1.0**.
   - Select **Use TLS 1.1** and **Use TLS 1.2**.

2.1.3 Considerations for Installation

Dashboard supports various types of installations. You can choose the installation type that is best suited to your environment. Also see the Supported Configurations for Secure Configuration Manager, and align your Dashboard installation with your Secure Configuration Manager installation.

Following are the installation options:

- You can install the Dashboard where you install Secure Configuration Manager components. For more information, see Section 2.2, “Installing the Dashboard,” on page 15.
- You can install the Dashboard on a separate computer. For more information, see Section 2.2, “Installing the Dashboard,” on page 15.
- You can install the Dashboard in a distributed environment. You can install components of the Dashboard - Website and Database - in separate computers. For more information, see Section 2.2, “Installing the Dashboard,” on page 15. You can install the Dashboard in the Secure Configuration Manager multiple Core Services setup. For more information, see “Supported Configurations” in the *NetIQ Secure Configuration Manager Installation Guide*.

2.1.4 Default Ports

Open the ports listed in the following table for proper communication between Secure Configuration Manager components and the Dashboard components.

Port Number	Component Computer	Port Use
TCP 9200	Dashboard database	Used for communication with Dashboard database using its REST services.
TCP 8045	Dashboard website	Used for communication with the Dashboard website.
TCP 8044	Core Services computer	Used for communication with the Secure Configuration Manager Core Services computer.
TCP 9300	Dashboard database	Used for communication with Dashboard database using its native protocol.

NOTE: If you have used non-default ports for the Dashboard database, Dashboard website, and Core Services computers, ensure that those ports are open.

2.2 Installing the Dashboard

You can install the Dashboard in one of the following two ways:

- Installing the Dashboard along with Secure Configuration Manager

  You can install the Dashboard while installing or upgrading to Secure Configuration Manager 6.1. For more information, see the *NetIQ Secure Configuration Manager Installation Guide*.

- Standalone Installation of the Dashboard

To install the Dashboard standalone:

1. Copy the Dashboard installer, `NetIQDashboard.msi`, from the Secure Configuration Manager installation CD image to the computer where you want to install the Dashboard, and double-click `NetIQDashboard.msi` to run the Dashboard installation wizard.

   NOTE: If you have the Secure Configuration Manager installation setup in the computer where you want to install the Dashboard, you can also click **Install Dashboard** after you run the Secure Configuration Manager **Setup.exe**.

   ---

2. In the NetIQ Secure Configuration Manager Dashboard Setup window, click **Next**.
3. Select the Dashboard components you want to install. By default, both the Website and Database components are installed in the local hard drive, in the `C:\Program Files(x86)\NetIQ\Secure Configuration Manager\Dashboard` folder.
4. Click **Next**.
5. Provide or verify the following settings:
   - **Cluster Name**: Name of the Dashboard cluster for database configuration.
   - **Database Port**: Port used for communication with Dashboard database. Default port is 9200.
   - **Website Port**: Port used for communication with Dashboard website. Default port is 8045.
   - **Core Host Name**: IP address/name of the Secure Configuration Manager Core computer.

     This value is auto-populated if you are installing the Dashboard on a computer in which Secure Configuration Manager is already installed. Specify the host name if you are installing the Dashboard on a different computer.
   - **Core Port**: Port used for communication with Secure Configuration Manager Core computer. Default port is 8044.
   - **Protocol**: Select the type of protocol for communication between Secure Configuration Manager Core computer and the Dashboard.

   NOTE: If you are installing the Dashboard in a distributed environment, and have selected only one of the components (either website or database), you will be prompted to specify the configuration information for only that component.

   ---

6. (Optional) Click **Test Connection** to test the connection with the specified Secure Configuration Manager Core computer IP address/name.

   When you click **Next**, the program verifies connection with the specified Secure Configuration Manager Core computer. Installation proceeds only if the connection is established.
7. Click **Next**.
8. Review the installation summary, and click **Install** to start the installation.

2.2.1 Configuring the Dashboard in a Distributed Setup

If you have installed the Dashboard in a distributed setup, you must configure unicast discovery. For more information about unicast discovery, see the Elastic Search documentation.

To configure unicast discovery, perform the following steps in both Dashboard Website and Database host computers:

1. Open the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Dashboard\Database\config\elasticsearch.yml` file.
2. Uncomment the following line:

   ```
   # discovery.zen.ping.unicast.hosts: ["host1", "host2"]
   ```
3. In the above line, add the IP addresses of Dashboard Website and Database hosts that you want to add for unicast discovery.

   For example:

   ```
   discovery.zen.ping.unicast.hosts: ["255.0.0.0", "127.0.0.1"]
   ```
4. Save the `elasticsearch.yml` file.
5. Restart the **Elastic Search 2.0.0 (NetIQDatabaseService)** service.

2.3 Customizing the Installation

After installing the Dashboard, you can customize your installation by changing the default settings. To customize the Dashboard installation:

1. Go to the directory where you have installed the Dashboard. By default, the Dashboard is installed in the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Dashboard` directory.
2. (Conditional) To customize the Dashboard database, go to the `Database\config` directory and open the `db.properties` file. You can change the protocol, database port, and the Core computer name in this file.

   Save the file.
3. (Conditional) To customize the Dashboard website, go to the `Website` directory and open the `website.properties` file. You can change the website protocol, website port, database protocol, and the database port in this file.

   Save the file.
4. Restart the **Elastic Search 2.0.0 (NetIQDatabaseService)** and the **NetIQ Dashboard Website Service**, in that order.

3 Getting Started with the Dashboard

After you have installed the Dashboard, you are ready to define how you want to view Secure Configuration Manager compliance information in the Dashboard.

3.1 Logging on to the Dashboard

You can launch the Dashboard from the Start menu of your computer where Secure Configuration Manager and the Dashboard are installed. For quick and easy access, add the Dashboard URL to the Favorites tab of your browser. For more information about supported browsers, see Section 2.1.2, “Supported Web Browsers,” on page 14.

To log on to the Dashboard:

1. Go to Start menu and select **Secure Configuration Manager Dashboard**.
2. Specify your Secure Configuration Manager user name and password.
3. Click **Log In**.

All the Secure Configuration Manager Console users can log in to the Dashboard. However, the data users can view depends on the privileges their role has been assigned by the Secure Configuration Manager administrator. For more information about Secure Configuration Manager users and roles, see the relevant sections in “Chapter 3, Setting Security on the Secure Configuration Manager Console” in the *NetIQ Secure Configuration Manager User Guide*.

If your role has been configured with a session limit value, it will be applicable for your Dashboard session too. For more information about session limit, see “Assigning Session Limit to Roles” in the *NetIQ Secure Configuration Manager User Guide*.

If your user account is deleted by the Secure Configuration Manager administrator while you are using the Dashboard, your session will be terminated whenever the session is revalidated. For more information about session revalidation interval, see the **Validate User in Every** field in Section 3.2.3, “Working with General Dashboard Settings,” on page 19.

3.2 Setting up the Dashboard as an Administrator

If you are an administrator, you can configure the Dashboard settings and assign access rights to other users.

Click your user name and select **Configuration** in the Kibana menu bar. The Dashboard Settings page has General Settings, Geolocation, and Authorization options.

3.2.1 Working with Authorization Settings

As an administrator, you can configure authorization settings for other user roles. To configure the authorization settings, click **Authorization** in the Dashboard Settings page.

To configure authorization settings for user roles:

1. Select the user role for which you need to configure the authorizations settings from the **User Roles** list.
2. Click **Edit** in the **Groups** tab. The corresponding groups associated with the user role you have selected in step 1 are displayed in this list. Select the groups about which the user role you have selected can view the data, and click **Save**.
3. Click **Edit** in the **Templates** tab. The corresponding templates associated with the user role you have selected in step 1 are displayed in this list. Select the templates about which the user role you have selected can view the data, and click **Save**.

For example, if you are configuring authorization settings for the NetIQ Windows Admin user, you can select the Windows group from the Groups list, and select only the Windows templates from the Templates list. This results in the NetIQ Windows Admin users viewing only the data about Windows groups and from Windows templates.

NOTE: The Administrator role is not displayed in the **User Roles** list to select for configuring authorization settings, because the users belonging to this role will have full privileges. As an administrator, you can view the data from all the template runs on all the groups.

3.2.2 Working with Geolocation Settings

The Dashboard comprises three geolocation charts, which display compliance data in world map view. For these chart to be functional, you must set the geographical locations of your environment, so that the data is displayed in these charts.

To configure the geolocation settings as an administrator:

1. Click **Geolocation** in the Dashboard Settings page.

   A table with already existing geolocation mappings, if any, is displayed.
2. To add a new geolocation mapping, click the **New** icon adjacent to the table.

   Select geolocation window is displayed.

   2a Specify the following information:

   - Location: Name of the location that you want to add as a geolocation.

- IP Range: The IP address range of the endpoints that you want to monitor and view the data for.

  NOTE: You must specify a value for at least one of the above two fields.

- Latitude: Latitude of the location.
- Longitude: Longitude of the location.

  Alternatively, click the **Map** icon to select the latitude and longitude of the location on the map.

  NOTE: You must have internet connection in your computer to be able to use the **Map** feature.

2b Click the **Save** icon.

The geolocation mapping you added is displayed in the Geolocation Mapping table.

You can edit or delete the geolocation mappings in the table by clicking the **Edit** or **Delete** icons that are present adjacent to the geolocation mapping record.

You can also add multiple geolocation mappings to this table by following the same procedure.

You can also import and export geolocation mappings as `.Xlsx` files. Click the **Import** icon to import geolocation mappings that you might have already saved in your computer and want to apply those mappings to the Dashboard. Also, you can export the existing geolocation mappings by clicking the **Export** icon.

3 Click **Apply Geolocation** after adding the necessary geolocation mappings.

This updates the existing geolocation data which is already synchronized to the Dashboard database from Secure Configuration Manager, and enables you to view the geolocation data in the charts. After a geolocation mapping is applied, any new data that is synchronized to the Dashboard database will displayed in the geolocation charts.

4 A confirmation message is displayed. Click **Apply** to apply the geolocation mappings.

After configuring the geolocation settings, you can view the geolocation charts in the Dashboard populated with data whenever applicable.

3.2.3 Working with General Dashboard Settings

To configure the general Dashboard settings, click **General** in the Dashboard Settings page. You can configure the following settings:

Startup Dashboard

This is the name of the dashboard that will be displayed when users log in to the Dashboard. For more information about these dashboards, see Section 3.3.3, “Viewing Charts in the Dashboard,” on page 21.

Validate User in Every

This is the time interval at which the user sessions are revalidated. The Dashboard communicates with Secure Configuration Manager at this interval and validates the user whose session is presently on.

Data Pull Interval

This is the time interval at which the Dashboard connects to the Secure Configuration Manager database and receives fresh data.

Retain Data For

This is the time interval till which the Dashboard retains the data in the Dashboard database.

NOTE: When you update the above three fields, the new value is applied only after the current intervals are completed. If you want to update the values immediately, restart the **Elastic Search 2.0.0 (NetIQDatabaseService)** service.

Click **Save** after you update the value in any of these fields.

If you update these values, new values will be applied only for a new session of the Dashboard. If you want the new values to be applied immediately, log out of the Dashboard and log in again.

Resetting Built-in Dashboards

Click **Reset built-in dashboards** to reset any updates done to the four built-in dashboards. Any customization done to any of these dashboards will be overridden, and the dashboards will be set to the default configurations. Any custom dashboards you might have created will not be affected by this operation.

3.3 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.

3.3.1 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 start using the Dashboard.

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

3.3.2 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.

The same roles are applicable in the Dashboard too. Secure Configuration Manager users can view all of the charts in the Dashboard, but the data populated in the charts depends on the user's role and associated permissions.

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

3.3.3 Viewing Charts in the Dashboard

The charts in the Dashboard are categorized into four logical groups, and these are put together in the following four dashboards. Click the **Load Saved Dashboard** icon on the menu bar to navigate to any of these dashboards.

Secure Configuration Manager

This is the default dashboard displayed when you log in to the Dashboard. This dashboard is used to visualize the results of template runs over various endpoints/managed groups. This dashboard provides an overview of the compliance, risk status, and distribution of assets, endpoints, and groups added or created in Secure Configuration Manager.

System Compliance

This dashboard is used to visualize the important compliance related information of your network. When a template is run over any endpoint, it can result in "In compliance", "Out of compliance", or "Unknown compliance".

Technical Compliance

This dashboard is used to visualize the check level information of the network. When the check is run on an endpoint it can either result in "passed", "failed", or "Excepted".

Risk Compliance

This dashboard is used to visualize the important risk related information of your network. When a template is run on any endpoint, it can result in "low risk", "medium risk", "high risk", or "unknown risk".

For more information about the charts available in each of these dashboards, see Appendix A, "Charts in the Dashboard," on page 23.

3.3.4 Customizing the Dashboard

You can perform the following tasks using the options in the menu bar, to customize the Dashboard:

Creating New Dashboard

If you need your own, customized dashboard apart from the four dashboards provided, click the **New Dashboard** icon to create it. When you click this icon, an empty dashboard is displayed. In this dashboard, you can add the charts based on your requirement.

Adding Charts to Existing Dashboard

You can add charts to your dashboard by clicking the **Add Visualization** icon.

Saving the Dashboard

If you have created you own dashboard, you can save it by clicking the **Save Dashboard** icon, and providing a name of your dashboard.

Select **Store time with dashboard** while saving the dashboard to change the time filter for the dashboard to the currently applied time filter.

Loading Saved Dashboard

You can load any default or saved dashboard by clicking the **Load Saved Dashboard** icon and selecting the dashboard you want to load.

Changing the Dashboard Theme

You can update the dashboard to use the dark theme by clicking the **Options** icon and then selecting the **Use dark theme** option.

NOTE: The Secure Configuration Manager Dashboard leverages Kibana, a browser-based analytics and search dashboard, that helps you to visualize and analyze data. Apart from the customizing functionality that the Dashboard offers, you can also use the Kibana functionality to customize the Dashboard. For more information, see the Kibana documentation.

3.4 Screen Capturing and Report Sharing

The Dashboard offers reporting capabilities, which enables you to take screenshot of your dashboard and export it in multiple formats. NetIQ recommends FireShot as the screen-capturing and sharing tool. When you download FireShot and install it in your computer, you will see the FireShot icon in your browser bar. Click on that icon to start using FireShot for screen capturing and sharing tasks.

With FireShot, you can perform the following reporting tasks:

- **Capture screenshot**: You can capture entire dashboard screen, or a selected screen area.
- Save screenshots as image or PDF: You can save the captured screenshot in various formats – image (.jpg or .png) or as PDF.
- **Print screenshot**: You can directly print the screenshot, or copy it to a clipboard.

You can send the saved screenshot file (image or pdf) though email, and use it for any other report sharing purpose.

NOTE: You can also use any other screenshot capturing tool to achieve screen-capturing and reporting with the Dashboard.

A Charts in the Dashboard

This charter describes all the charts available in the Dashboard.

A.1 Charts in the Secure Configuration Manager Dashboard

Following are the charts in the Secure Configuration Manager Dashboard:

Chart Name	Description
Compliance Distribution	This is a pie chart that displays the distribution of the compliance information of the latest runs of templates over the network. The size of each slice indicates the number of template runs on the endpoints of the network, which ended with corresponding compliance level. Only unique template runs are considered for this chart; multiple runs of same templates are not considered. For example, if you run four different templates, the chart will have four slices. If you run two templates twice, the chart will have two slices.
Group Hierarchy	This is a multi-level pie chart created to visualize the hierarchy and size of the groups on which templates have been run. The size of each slice will be reflective of the number of endpoints that are part of the corresponding group.
Policy Template Risk Over Time	This is a trend chart that displays the trend of the sum of total risk of each run of a particular template. By default, the chart follows an interval of one day. The 10 templates with highest sum of total risk are shown in the chart. ALL templates run (including multiple runs of same templates) are considered for this chart.
Platform Distribution	This is a pie chart that displays the distribution of the network based on the platform of endpoints. The size of each slice reflects the number of endpoints of corresponding platform.

Chart Name	Description
Endpoint Distribution	This is a pie chart that displays the distribution of the network in terms of the endpoints. Each slice represents one endpoint.
Policy Template Distribution	This is a pie chart that displays the templates that have been ran over the network. Each slice represents one template.
Group Compliance Detail	This is a bar graph that displays the distribution of compliance levels of the latest runs of the templates ran over the groups. The groups are ordered in descending order according to the number of templates run on them.
Asset Compliance Detail	This is a bar graph that displays the distribution of compliance levels of the latest runs of the templates ran over the assets. The assets are ordered in a descending order according to the number of templates run over them.
Check Status Detail	This is a bar graph that displays the status of the execution of different security checks. The security checks will be visible in this graph only if they were executed as a part of a template run. The status of a security check can be “Passed”, “Failed”, “Excepted”, or “Unknown”. The security checks are ordered in the descending order of the number of times they have been run.
Risk Score Detail	This is a bar graph that displays the risk distribution of the latest runs of templates on respective endpoints. The size of each bar area indicates the number of template runs having that risk level. The endpoints are ordered in descending order based on the number of templates run on them.
Geolocation of Out of Compliance Endpoints	This is a world map (tile map) that shows the location of endpoints that have template runs which were out of compliance. **NOTE:** You must have internet connection in your computer to be able to view this chart.

A.2 Charts in the Risk Compliance Dashboard

Following are the charts in the Risk Compliance Dashboard:

Chart Name	Description
Overall Risk Status	This is a pie chart that displays the distribution of the risk levels of all the latest runs of templates over the network. The size of each slice indicates the number of template runs having that risk level. Only unique template runs are considered for this chart; multiple runs of same templates are not considered. For example, if you run four different templates, the chart will have four slices. If you run two templates twice, the chart will have two slices.
Overall Risk Status Over Time	This is a bar chart that displays the risk distribution of templates over the network on specific dates. The size of each slice of the bar indicates the number of templates having corresponding risk level. ALL templates run (including multiple runs of same templates) are considered for this chart.
Risk Score Detail	This is a bar graph which displays the risk distribution of the latest runs of templates on respective endpoints. The size of each bar area indicates the number of template runs having that risk level. The endpoints are ordered in descending order of the number of template runs on them.
Low Risk Score Over Time	This is a trend chart which displays the number of template runs which have resulted in low risk at a given point of time.

A.3 Charts in the System Compliance Dashboard

Following are the charts in the System Compliance Dashboard:

Chart Name	Description
Overall Compliance Status	This is a pie chart that displays the compliance distribution of all the latest runs of templates over the network. The size of each slice indicates the number of template runs having corresponding compliance level. Only unique template runs are considered for this chart; multiple runs of same templates are not considered. For example, if you run four different templates, the chart will have four slices. If you run two templates twice, the chart will have two slices.

Chart Name	Description
Overall Compliance Status Over Time	This is a bar chart that displays the risk distribution of templates over the network on specific dates. The size of each slice of the bar indicates the number of templates having corresponding compliance level. ALL templates run (including multiple runs of same templates) are considered for this chart.
System Compliance Detail	This is a bar chart which displays the compliance distribution of the latest runs of templates on respective endpoints. The size of each bar area indicates the number of template runs having that compliance level.
Passed Compliance Over Time	This is a trend chart that displays the number of templates that are in compliance at a given point of time.

A.4 Charts in the Technical Compliance Dashboard

Following are the charts in the Technical Compliance Dashboard:

Chart Name	Description
Overall Compliance Status	This is a pie chart that displays the distribution of all the check runs on the endpoints based on their returned status. The size of each slice of the chart indicates the number of checks that returned with that status. Only unique template runs are considered for this chart; multiple runs of same templates are not considered. For example, if you run four different templates, the chart will have four slices. If you run two templates twice, the chart will have two slices.
Overall Compliance Status Over Time	This is a bar chart which displays the risk distribution of templates over the network on the particular dates. The size of each slice of the bar indicates the number of checks having corresponding compliance level. ALL templates run (including multiple runs of same templates) are considered for this chart.
Compliance Detail	This is a bar chart that displays the distribution of the check results for all the checks that have been run on a particular endpoint. The size of each area of bar indicates the number of checks ran on that endpoint, which returned in corresponding status. The endpoints are ordered in descending order of the number of checks that have run on them.

Chart Name	Description
Passed Compliance Over Time	This is a trend chart that displays the number of passed or excepted checks over time. The trend is shown for each template that has such checks.

B Troubleshooting

B.1 Updating the Dashboard Keystore When SSL is Configured on SQL Server

Issue: The Dashboard does not display any charts when the SQL Server is configured to use SSL protocol. This issue occurs because the Dashboard does not recognize and validate the SQL server certificate.

Fix: Perform the following steps:

1. Open Certificate Manager in the computer in which SQL Server is located.

   Type `certmgr.msc` in the **Start** menu of your computer.
2. Export the certificate (without private key) that the SQL server is using.

   Right-click the certificate and select **All Tasks** > **Export**. Follow the steps in the Certificate Export Wizard.
3. In the computer where the Dashboard is located, run the following commands to add the certificate to the default truststore:

   ```
   cd C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Dashboard\jre\lib\security
   ```

   ```
   ..\..\bin\keytool -importcert -keystore cacerts -storepass changeit –file certificate.cer
   ```
4. Restart the **Elastic Search 2.0.0 (NetIQDatabaseService)** service.

B.2 Starting New Sessions Upon Exceeding the Session Limit Value

Issue: Dashboard does not close the older sessions after exceeding the session limit value, and displays an error when you try to start a new session.

Fix: Manually close the older sessions when the Dashboard displays the session limit warning, and then open the new session.