Quantum

User's Guide

Vision

Version 4.4

6-68534-01

Vision User's Guide, 6-68534-01, December 2016, Product of USA.

COPYRIGHT STATEMENT

TRADEMARK STATEMENT

Contents

Preface

This manual introduces Vision and discusses:

- Installation and Upgrades
- Configuration
- System operations

Document Organization

The following chapters are included in this manual:

Notational Conventions

This manual uses the following conventions:

Convention	Example
User input is shown in bold monospace font.	**`./DARTinstall`**
Computer output and command line examples are shown in monospace font.	`./DARTinstall`
User input variables are enclosed in angle brackets.	**http://<ip_address>/cgi-bin/stats**

For UNIX and Linux commands, the command prompt is implied.	`./DARTinstall`
	is the same as
	`# ./DARTinstall`

File and directory names, menu commands, button names, and window names are shown in bold font.	**/data/upload**
Menu names separated by arrows indicate a sequence of menus to be navigated.	**Utilities > Firmware**

The following formats indicate important information:

Note: Note emphasizes important information related to the main topic.

Caution: Caution indicates potential hazards to equipment or data.

WARNING: Warning indicates potential hazards to personal safety.

- Right side of the system - Refers to the right side as you face the component being described.
- Left side of the system - Refers to the left side as you face the component being described.
- Data sizes are reported in base 1000 rather than base 1024. For example:
  - 1 MB = 1,000,000 bytes
  - 1 GB = 1,000,000,000 bytes
  - 1 TB = 1,000,000,000,000 bytes

Product Safety Statements

Quantum will not be held liable for damage arising from unauthorized use of the product. The user assumes all risk in this aspect.

This unit is engineered and manufactured to meet all safety and regulatory requirements. Be aware that improper use may result in bodily injury, damage to the equipment, or interference with other equipment.

WARNING: Before operating this product, read all instructions and warnings in this document and in the *Quantum Products System, Safety, and Regulatory Information Guide*.

ADVARSEL: Læs alle instruktioner og advarsler i dette dokument og i *Informationsvejledning vedrørende system-, sikkerheds- og lovbestemmelser for Quantum produkter, før produktet betjenes*.

AVERTISSEMENT : Avant d'utiliser ce produit, lisez toutes les instructions et les avertissements de ce document et du *Guide d'informations sur le système, la sécurité et la réglementation de Quantum*.

WARNUNG: Lesen Sie vor der Inbetriebnahme dieses Produkts alle Anleitungen und Warnungen in diesem Dokument und im *System-, Sicherheits- und Betriebsbestimmungen-Handbuch für Quantum-Produkte*.

ADVERTENCIA: Antes de hacer funcionar este producto, lea todas las instrucciones y advertencias de este documento y de la *Guía de información normativa, del sistema y de seguridad de los productos de Quantum*.

VARNING: Läs igenom alla instruktioner och varningar i detta dokument och i *Quantums produktsystem, säkerhet och reglerande informationsguide* innan denna produkt används.

ВНИМАНИЕ! Перед началом эксплуатации данного изделия прочтите все инструкции и предупреждения, приведенные в настоящем документе и в *Руководстве по системе, технике безопасности и действующим нормативам компании Quantum*.

警告：本製品を使用される前に、本書と『*Quantum製品システム、安全、規制情報ガイド*』に記載されているすべての説明と警告をお読みください。

경고: 본 제품을 작동하기 전에 본 문서와 *Quantum 제품 시스템, 안전 및 규제 정보 설명서*에 있는 모든 지침과 경고를 참조합니다.

警告：在操作本产品之前，请阅读本文档和 *Quantum 产品系统、安全和法规信息指南*中的所有说明和警告。

警告：操作此產品前，請閱讀本檔案及 *Quantum 產品系統、安全與法規資訊指南*中的指示與和警告說明。

אזהרה: לפני ההפעלה של מוצר זה, קרא את כל ההוראות והאזהרות הכלולות במסמך זה וכן *במדריך המידע בנושא מערכת, בטיחות ותקינה עבור מוצרי Quantum*.

Related Documents

The following Quantum documents are also available for Vision:

Document Number	Document Title
66900	Vision Release Notes

For the most up to date information on Vision, see:

http://www.quantum.com/serviceandsupport/get-help/index.aspx#contact-support

Contacts

For information about contacting Quantum, including Quantum office locations, go to:

http://www.quantum.com/aboutus/contactus/index.aspx

Comments

To provide comments or feedback about this document, or about other Quantum technical publications, send e-mail to:

doc-comments@quantum.com

Getting More Information or Help

StorageCare™, Quantum's comprehensive service approach, leverages advanced data access and diagnostics technologies with cross-environment, multi-vendor expertise to resolve backup issues faster and at lower cost.

Accelerate service issue resolution with these exclusive Quantum StorageCare services:

- **Service and Support Website** - Register products, license software, browse Quantum Learning courses, check backup software and operating system support, and locate manuals, FAQs, firmware downloads, product updates and more in one convenient location. Get started at:

  http://www.quantum.com/serviceandsupport/get-help/index.aspx#contact-support

- **eSupport** - Submit online service requests, update contact information, add attachments, and receive status updates via email. Online Service accounts are free from Quantum. That account can also be used to access Quantum's Knowledge Base, a comprehensive repository of product support information. Get started at:

  http://www.quantum.com/customercenter/

For further assistance, or if training is desired, contact the Quantum Customer Support Center:

Region	Support Contact
North America	1-800-284-5101 (toll free) +1-720-249-5700
EMEA	+800-7826-8888 (toll free) +49 6131 324 185
Asia Pacific	+800-7826-8887 (toll free) +603-7953-3010
For worldwide support: http://www.quantum.com/serviceandsupport/get-help/index.aspx#contact-support	

Worldwide End-User Product Warranty

For more information on the Quantum Worldwide End-User Standard Limited Product Warranty:

http://www.quantum.com/serviceandsupport/warrantyinformation/index.aspx

Chapter 1: Quantum Vision

This chapter contains the following topics:

Quantum Vision

Quantum Vision is a data protection solution that allows you to monitor, analyze, and report on your Quantum backup environment. You can view the status and track the performance of the following using a single flexible interface:

- Multiple DXi® disk backup systems
- Q-Cloud Protect
- Scalar® libraries
- Scalar LTFS
- vmPRO 4000 and vmPRO software

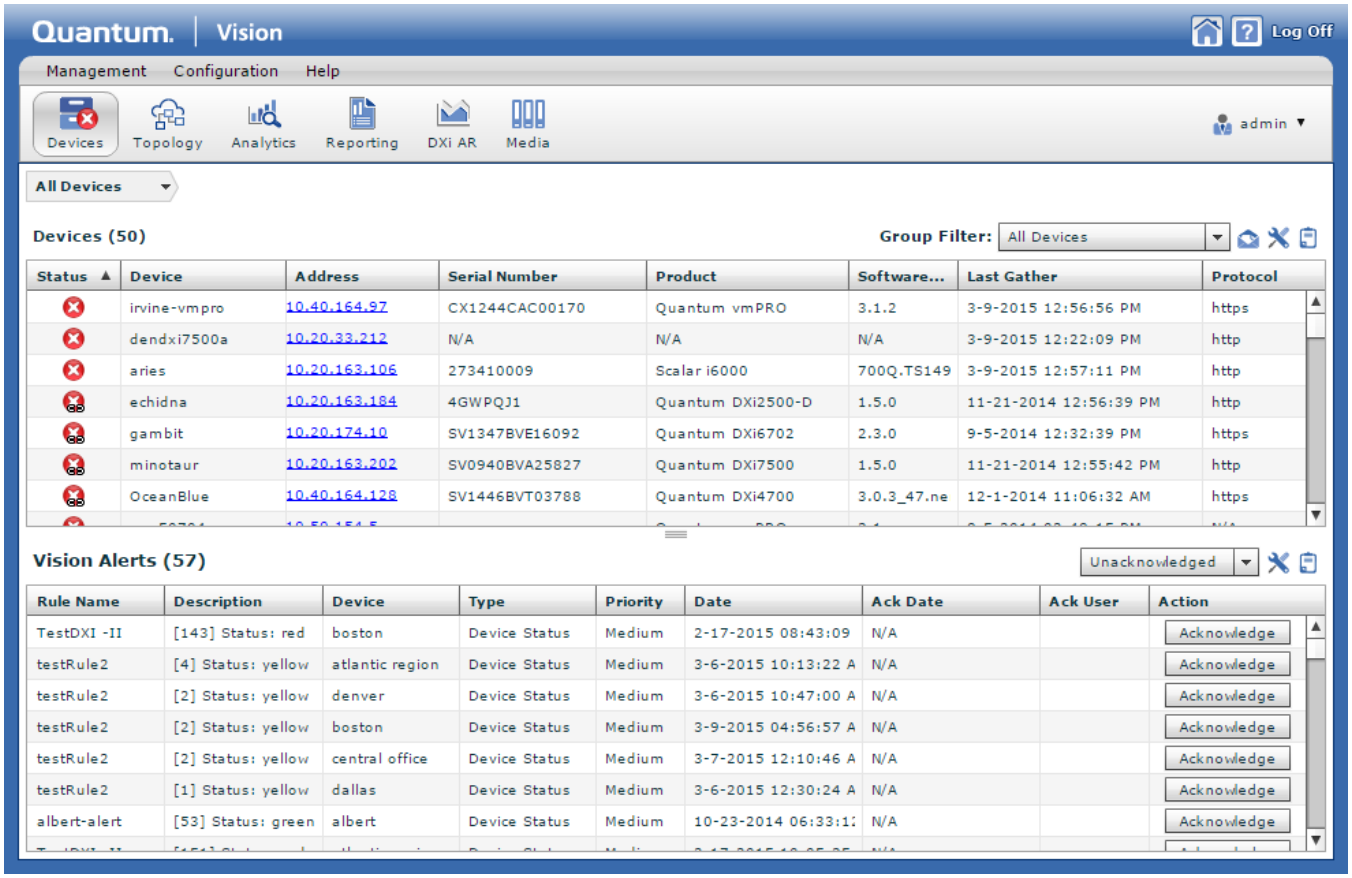
Quantum Vision Features and Benefits		
Identify and initiate software updates for one or more vmPRO appliances from Vision.	Receive notification of and initiate a Vision software update using the Vision GUI (virtual appliance only).	Provide a chargeback report, based on individual shares, partitions, or OST LSU system usage, in both print and e-mail versions.
Monitor the status and health of DXi devices, Q-Cloud Protect appliances, Scalar libraries, Scalar LTFS, and vmPRO.	Visualize data on demand to track capacity usage, analyze performance, and identify trends.	Access a Topology map to view the devices and their relationships.
Automatically generate reports and graphs, and send them to multiple recipients.	Define alert rules to monitor thresholds and manage alert notifications.	Access the native management interface of any monitored Quantum device.
View and compare DXi Advanced Reporting graphs for one or more DXi disk backup or Q-Cloud Protect systems.	Generate a Capacity Upgrade Estimate for DXi devices Q-Cloud Protect appliances.	Monitor the usage and health of media in Scalar libraries (including Extended Data Life Management [EDLM] status), change media location, and delete media.

The Vision Window

Vision provides a flexible Web-based graphic user interface (GUI) from which to monitor, analyze, and report on your backup environment. The information displayed in the Vision GUI depends on your user role, your user group, and the devices assigned to your user group. See Manage Groups in Vision on page 68.

To access Vision, you must first log in with the user name and password assigned to you by your Vision administrator.

Figure 1: Vision Window



Vision Requirements

Vision supports installation and operation on both physical servers and virtual machines (VMs) functioning as servers. To properly install and use Vision on a physical or VM server, ensure the following requirements are met.

Server Requirements

Make sure that the Vision server, which hosts Vision software, meets the requirements outlined below.

Server Component	System Requirement
Processor	• Intel or AMD server class processor • 2 CPUs for up to 50 devices • 4 CPUs for more than 50 devices
Memory	• 4 GB for monitoring up to 50 devices • 8 GB for monitoring more than 50 devices
Available Disk Space	• 200 GB for monitoring up to 50 devices • 400 GB for monitoring more than 50 devices
Operating System	One of the following operating systems: • Windows Server 2003 32-bit • Windows Server 2003 R2 64-bit • Windows Server 2008 32-bit • Windows Server 2008 R2 64-bit • Windows Server 2012 Standard 64-bit • Windows Server 2016 Standard 64-bit • Red Hat Enterprise Linux 5 32-bit • Red Hat Enterprise Linux 5 64-bit • Red Hat Enterprise Linux 6 64-bit • Red Hat Enterprise Linus 7 64-bit • SUSE Linux Enterprise 11 Service Pack 3 • SUSE Linux Enterprise 11 Service Pack 4
Virtual Appliance	• Server system with at least an i7 quad-core Intel processor (or AMD equivalent) • 2 virtual CPUs for up to 50 devices • 4 virtual CPUs for more than 50 devices • At least one IP address available for use by the Vision appliance • One or more ESX4, ESXi4, ESXi5, or ESXi 6 servers • Same memory requirements as that of a physical server installation
Additional Software	(Windows only) Microsoft .NET Framework 2.0 or higher

Server Port Requirements

Before using Vision, you need to open and enable specific firewall ports on the Vision server.

For Vision to operate correctly, open the following firewall ports:

- Port 80 - Web server (http)
- Port 443 - Web server (https)
- Port 162 - SNMP

To enable monitoring of storage devices, open the following firewall ports to outgoing traffic:

- Port 80 - Web server (http)
- Port 443 - Web server (https)
- Port 22 - SSH

Note: Ports 80 and 443 are the default web server ports. If you specified different web server ports when installing Vision software, open those ports in the firewall instead.

Browser Requirements

Before running Vision software on your system, review following browser requirements:

- Vision 4 is designed to run in any modern Web browser that supports the Adobe Flash Player plug-in.
- Vision 4.3.5 and later requires Adobe Flash Player version 11.4 or higher. Web browser software is not included with Vision. You must obtain and install it separately. To download and install Flash Player, go to http://www.adobe.com.
- Vision does not support the 64-bit version of the Flash Player plug-in on Linux. Instead, use the 32-bit Flash Player plug-in and a 32-bit browser. For 64-bit Linux, the Chrome browser and its built in pepper flash player are compatible with Vision.

Supported Storage Device Requirements

To discover and monitor a Quantum backup system in Vision, the system must be a Quantum-supported device. Vision supports the following devices:

DXi Devices	Scalar Devices	Virtual Devices
• DXi8500 disk backup system • DXi7500 disk backup system • DXi6000 series (DXi6500, DXi6700, DXi6800, DXi6900, and DXi6900-S) disk backup systems • DXi4000 series (DXi4500, DXi4600, DXi4700) disk backup systems	• Scalar i6000 library • Scalar i2000 library • Scalar i500 library • Scalar i80 library • Scalar i40 library • Scalar LTFS • Scalar i3 library • Scalar i6 library	• Q-Cloud Protect • DXi V-Series (DXi V1000, DXi V2000, and DXi V4000) virtual backup systems • vmPRO 4000 (software/hardware backup solution) • vmPRO virtual backup system

Q-Cloud Protect and DXi Requirements

Review the following special requirements for Q-Cloud Protect and DXi 6900.

VPC-Private Network Connection for Q-Cloud Protect

If you are using Vision to monitor Q-Cloud Protect, you *must* configure the network connection between your Q-Cloud Protect instances, your on-site DXi appliances, and your Vision server within the same VPC-private network.

Access Control

For Vision to gather replication data for Q-Cloud Protect appliances or DXi devices running software versions 3.2 or later, it needs to identify itself through an SSH key pair.

Vision generates this key pair. The private key is Vision's secure identifier. The public key is shared with the Q-Cloud Protect appliance or DXi device. Vision has authorization to gather replication data only when the private and public keys match.

Vision Virtual Appliance Console Command Line

A limited number of functions are available from Vision's virtual appliance console command line. Access the console command line from your vSphere client. You will need the Vision user name and password to log in to the command line interface.

Command Parameters and Syntax

Parameters

You can use the following parameters when issuing Vision commands:

Command (required)

The main command being issued or the main category of the command, such as **`exit`**, **`system`**, or **`admin`**.

Subcommand (optional)

The action to perform, such as **`upgrade`**, **`reboot`**, or **`config`**.

Option (optional)

The object on which the action is being performed, such as **`service`**, **`password`**, or **`ports`**.

Syntax

Use the following syntax when issuing Vision commands:
`command subcommand option`

Example

To reset the system password, enter the following:

- command:**`system`**
- subcommand: **`reset`**
- option: **`password`**

Enter the whole command on the command line, as follows:

`system reset password`

Topics

Access the Console Command Line

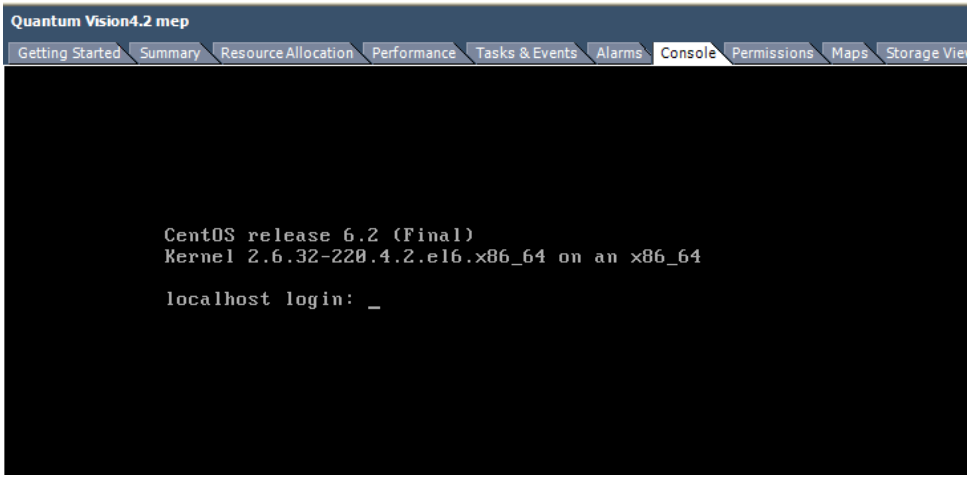
Use the following task to access your Vision VM's console command line.

Access the console command line

1. Open your vSphere client.
2. In the left pane, select your Vision virtual appliance.

3. Select the **Console** tab to display the **Console** window with the **login** command.

Figure 2: Console Window with Login Command



4. At the **login** command, enter the Vision appliance user name.
5. At the **password** command, enter the Vision appliance password.

   If this is your first time accessing the console command line, log on with the default user name (**sysadmin**) and password (**QuantumVision**).
6. Enter commands, as needed.

Issue General Commands

Use the following commands to perform general functions from your Vision VM's console command line.

Display a list of available commands

1. Access the Console Command Line on the previous page.
2. At the prompt, enter the following:
   `help`

Display help for the specific command

1. Access the Console Command Line on the previous page.
2. At the command line prompt, enter the following:
   `help <command>`

Log off the command line

1. Access the Console Command Line on page 7.
2. At the command line prompt, enter the following:
   exit

Free the cursor from the console

- Type the **<ctrl + alt>** keys on your keyboard.

  Click anywhere inside the console to return to the command line.

Issue System Commands

Use the following commands to perform system functions from your Vision VM's console command line.

Reboot the system

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   system reboot

Restart the service

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   system restart service

Shut down the system

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   system shutdown

Upgrade the system

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   system upgrade

Additional Information

- For Vision 4.3 or newer, the **`system upgrade`** command upgrades the Vision appliance from the Quantum repository by locating and downloading the upgrade RPM.
- If you are currently running Vision 4.2 or 4.2.1, you cannot access the Quantum repository. Instead, use **`system upgrade scp`** or **`system upgrade http`** to upgrade to Vision 4.3.2 or newer.

Issue Network Commands

Use the following commands to assign IP addresses and ports from your Vision VM's console command line.

Instruct DHCP to assign IP addresses

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   `net config dhcp`

Manually assign an IP address to the Vision appliance

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   `net config static`
3. At the subsequent prompts, enter the following for the Vision appliance:
   - IP address
   - NetMask
   - Gateway IP address

Enter ports for the Vision appliance

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   `net ports`
3. At the subsequent prompts, enter the names of the Vision appliance's **http** and **https** ports.

Set the IP addresses for the Vision appliance's DNS servers

1. Access the Console Command Line on page 7.

2. At the prompt, enter the following:
   `net dns`
3. At the subsequent prompts, enter each DNS server IP address to assign to the Vision appliance, in order of priority.
4. After entering all DNS IP addresses, leave the last prompt blank, and press **<enter>**.

Issue Admin Commands

Use the following commands to perform administrator functions from your Vision VM's console command line.

Change the system password

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   `admin password`
3. At the prompt, enter the new password.

Reset the system password to the default password

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   `admin password reset`

Assign a time zone to your Vision appliance

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   `admin timezone`
3. At the prompt, enter one of the following to display a list of appropriate time zones:
   - **`US timezones`**
   - **`non-US timezones`**
   - **`cancel`**
4. Select and enter the time zone to apply to your Vision appliance.

Back up the Vision appliance database

1. Access the Console Command Line on page 7.

2. At the prompt, enter the following:
   `admin backup`
3. At the subsequent prompts, enter the following:
   - Name of the server on which the Vision appliance resides
   - User name and password for the Vision appliance
   - Location to which to back up the database

Restore an archived copy of the Vision appliance database

1. Access the Console Command Line on page 7.
2. At the prompt, enter the following:
   `admin restore`
3. At the subsequent prompts, enter the following:
   - Name of the server on which the Vision appliance resides
   - User name and password for the Vision appliance
   - Location from which to retrieve the archived database

Result

a. The archived database is copied to and unpacked on the Vision appliance.
b. The Vision server is restarted.

Access Vision

When you log on to Vision, make sure that you are using a supported Web browser on a workstation that has network access to the Vision server. In addition, before logging on to Vision, you will need a user name and password defined for you by your network administrator.

Tips

Keep the following tips in mind when you are logged on to Vision:

Refresh Button

After you have logged on to Vision, do not use the browser's **Refresh** button. This will terminate your session and you will be logged out of Vision.

Browser Sessions

When accessing Vision, use only one browser and tab per session. Logging out using Vision's **Log Off** button ends your session. If you use multiple browsers or tabs during the same session, even as a different user, each session uses the same user credentials.

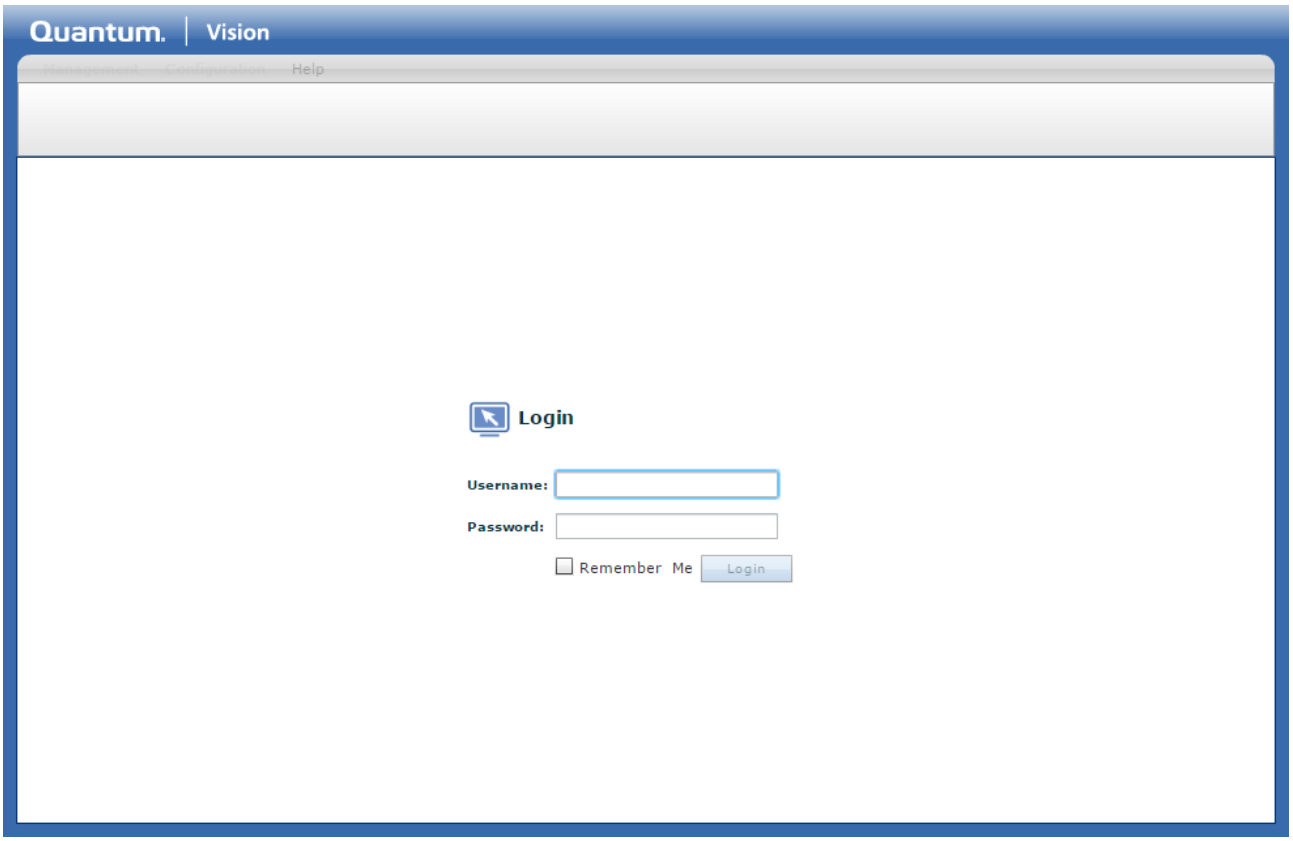
Session Termination

After you have finished using Vision, make sure to log off from the application. Otherwise messages continue to be queued on the Vision server. If this happens, the server will slowly become unresponsive and will eventually restart.

Log on and off Vision

1. Launch a supported Web browser on a workstation that has network access to the Vision server.
2. In the browser address box, enter the IP address of the Vision server to display the Vision **Login** window.

Figure 3: Vision Login Window



What if the Login window does not display?

- Verify that the IP address is correct and that the network path to the Vision server is valid.
- Verify that you are using a supported Web browser and that the correct version of Adobe Flash Player is installed.
- If you are still unable to access the Login window, contact your Vision administrator.

3. Populate the following fields:

   Username

   Enter your user name. The default is **admin**.

   Password

   Enter your password. The default is **password**.

4. Select the **Remember Me** check box to have Vision remember your user name and password the next time you log in, as applicable.

   The system encrypts the user name and password when it stores them on the client workstation. As a best practice, we recommend using the **Remember Me** option only on a workstation that is in a physically-secured location.

5. Click **Login** to display the **Devices Console**.
6. When you are finished working in Vision, click **Log Off** on the upper right corner of the Vision window to end your session.

Navigate Vision

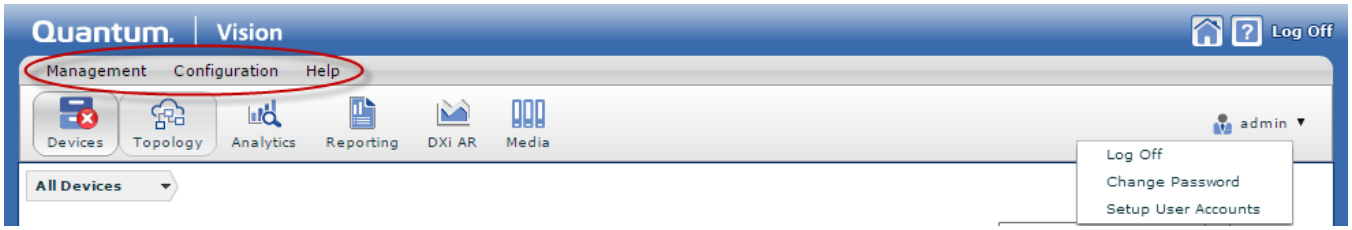
The Vision GUI provides a rich interface from which to access and manage information.

Vision Menu

The **Management**, **Configuration**, and **Help** menus are located at the top of the Vision GUI.

For information about the **Management** and **Configuration** menus, see Vision Setup and Configuration. For information about the Help menu, see Help Menu on the next page.

Figure 4: Vision Menu



Help Menu

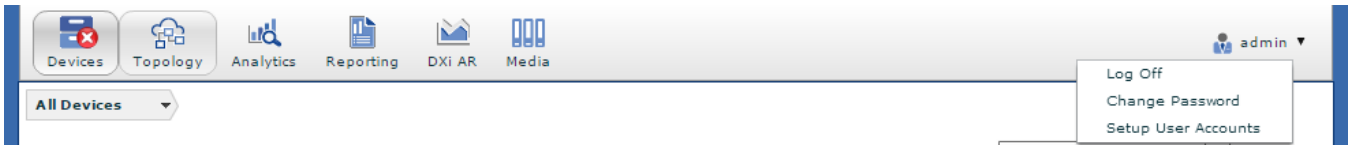
Use the **Help** menu to access the following features:

Feature	Description
About Vision	Displays the version of Vision that you are running and the Vision End-User License Agreement (EULA).
Send Us Feedback	Displays a feedback form in which you can evaluate various Vision features and provide comments that can be sent to the Vision development team.
Training and Documentation	Displays the Vision Documentation Center.

Toolbar

The Vision Toolbar displays below the Vision Menu. Use the toolbar to access the **Devices**, **Topology**, **Analytics**, **Reporting**, **DXi AR**, and **Media** consoles.

Figure 5: Vision Toolbar



Devices Console

Use the Devices console to view the status of all monitored devices and software, and to work with notifications.

The status badge, located in the **Status** column of the console, changes appearance depending on the status of monitored devices. Hold the cursor over the status badge to see a status summary.

- Indicates that all devices are operating correctly.
- Indicates that there is a problem with one or more devices.
- Indicates that there is a major problem with one of more devices.

- Indicates that Vision's connection with the device has failed.
- Indicates that the device is discovered but no data has been collected yet, or the status is unknown.

See Vision Device Consoles on page 97.

Topology Console

The Topology console is composed of topology maps that you can use to quickly view the following information:

- DXi and Q-Cloud Protect replication relationships
- PTT, vmPRO-DXi, and Scalar LTFS-scalar relationships
- Capacity usage
- Deduplication percentages

See Vision Topology Console on page 163.

Analytics Console

The Analytics console is composed of interactive graphs that you can use to quickly visualize and compare key statistics for DXi devices, Q-Cloud Protect appliances, Scalar libraries, and vmPRO.

See Vision Analytics on page 178.

Reporting Console

Use the Reporting console to generate and view reports, set up recurring schedules for automatically generating reports, and send reports to specified recipients.

See Vision Reporting on page 200.

DXi AR Console

Use the DXi AR console to view and compare Advanced Reporting graphs for one or more DXi devices or Q-Cloud Protect appliances.

Media Console

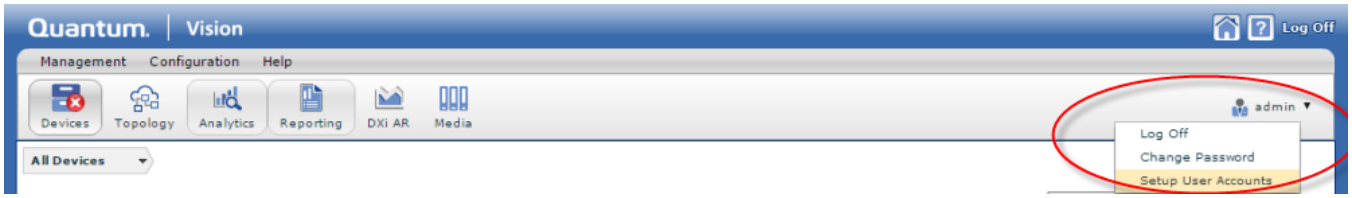
The Media console displays information for tape media within Scalar libraries. Use this console to monitor Scalar libraries, update media locations, and delete obsolete media.

See Vision Media Console on page 170.

User Menu

The **User** menu displays the name of the user who is currently logged on, such as **admin**.

Figure 6: User Menu



Click the **User** menu icon to display the following options:

Log Off

Use to log the current user off Vision.

Change Password

Use to display the **Change Password** dialog box.

Change your password

a. Enter your original password.
b. Enter the new password.
c. Enter the new password again to confirm it.
d. Click **Save**.

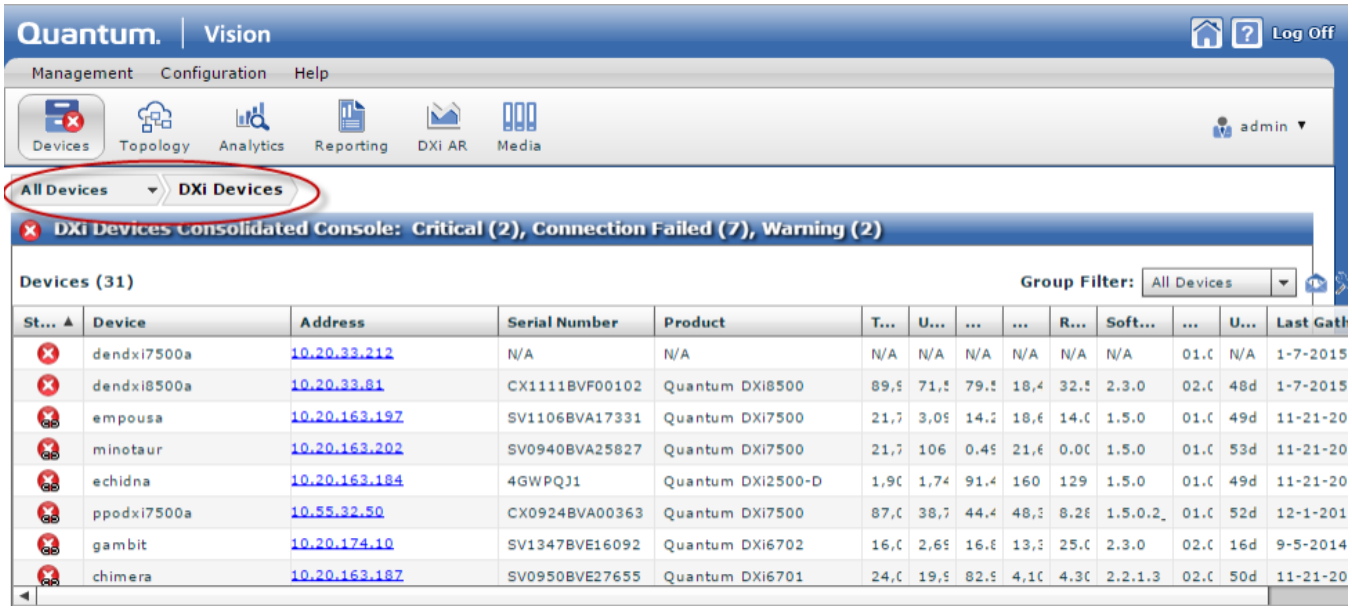
Setup User Accounts

Use to display the **User Management** dialog box. See Manage Users in Vision on page 71.

Navigation Bar and Console

The navigation bar above the console shows your current location within the Vision application. Click on any of the navigation bar's tabs to view the associated information in the Vision console. The main area of the Vision GUI displays the currently selected console. The Devices console acts as the Vision home page.

Figure 7: Vision Navigation Bar and Console



You can use the navigation bar to display the Consolidated console, which is a list of all the devices for a specific device family.

Display the Consolidated console

- Click on the family name tab.

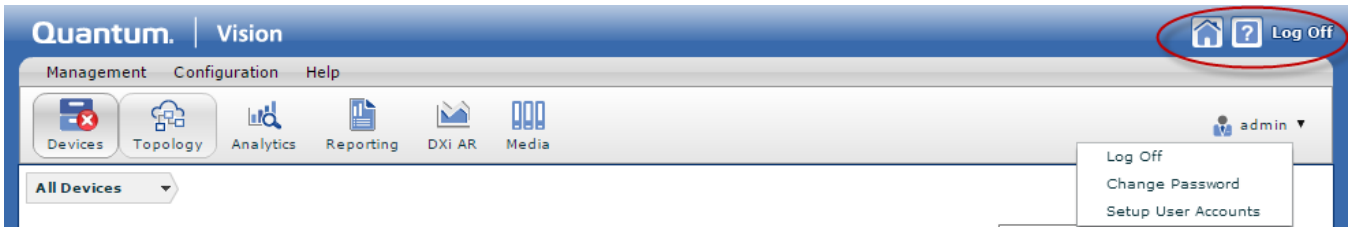
  OR

- Select the family name from the **All Devices** drop-down list.

Home, Help, and Log Off

The **Home** icon, **Help** icon, and **Log Off** button appear at the top right of the Vision GUI.

Figure 8: Home Icon, Help Icon, and Log Off Button



Use these as follows:

Icon/Button	Description
	Click to return to the **Devices** console.
	Click to open help topics associated with the displayed console.
	Click to end your Vision session.

Tooltips

Tooltips are small pop-up windows that appear when you hold the cursor over certain objects in the Vision GUI. They provide further information about the object over which the cursor is hovering.

Examples

- Hold the cursor over a field or button to learn more about using it.
- Hold the cursor over a line or bar on a chart to see details about the underlying data.

Tables

You can sort tabular data based on any of the available column headings.

Example

On the **Devices** console, click the **Status** column heading to sort all storage devices according to status, or click the **Product** column heading to sort all storage devices according to product family.

Select the columns to display

For most tables that display information, you can choose the columns of data that you want to display.

1. Click  on the upper right of the table to display the **Configure Columns** menu.
2. Select the columns to display.
3. Click **Save**.

Export the information in a table to a file

You can export most information in tables to a file. You can then import the information into other applications.

1. Click on the upper right of the table to display a list of file formats.
2. Select a file format (CSV, Text, or XML).
3. Select a location to save the file, type a name for the file, and click **Save**.

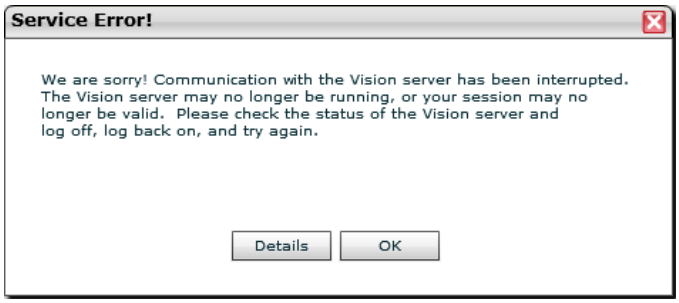
System Messages

If there are communication problems between the browser and the Vision server, Vision displays a **Service Error Message**.

Example

A timeout error can result when the browser makes a request to the server, and the server does not respond in time.

Figure 9: Service Error Message



Quantum Device Names

In some cases, Vision refers to Quantum storage devices by their product family name. Use the following information to understand how the product family name relates to specific device models:

Product Family	Device Models
DXi	DXi V-Series appliances (virtual backup systems), DXi4500, DXi4701, DXi6500, DXi6700 (including DXi6701 and DXi6702), DXi6802, DXi 6900, DXi 6900-S, DXi7500, and DXi8500 disk backup systems Q-Cloud Protect appliances
Scalar	i40, i80, i3, i6, i500, i2000, and i6000 libraries
Scalar LTFS	Scalar linear tape file system
vmPRO	vmPRO virtual backup system

Chapter 2: Installations and Upgrades

This chapter contains the following topics:

Vision Installations and Upgrades

Vision is available as either a standard software package or as a virtual appliance.

Standard Software Package

Vision software packages are available to install and upgrade for both Windows and Linux operating systems. Before installing Vision software, make sure the operating system on the Vision server is accessible on the network. For best results, we recommend configuring the Vision server with a static IP

address.

Note: Installing Vision 4 does not upgrade an existing Vision 3 installation. We recommend uninstalling any version of Vision 3 before upgrading to Vision 4. Although it is possible to run both Vision 3 and 4 simultaneously on your Vision server, we do not recommend it. See Uninstall Vision Software from a Vision Server on page 46.

Virtual Appliance

Vision 4.3.2 and newer are available as a VMware appliance in a format that installs within a vSphere infrastructure. This Vision appliance may be installed either on a physical server or as a virtual machine (VM) by OVF or other means to allow you to comply with your company's IT standards and policies. There is no technical advantage to installing Vision on a physical server or VM.

In addition, if you have Vision 4.2 to 4.3.1, you can upgrade to a Vision 4.3.2 and newer appliance by using one of the following methods:

Vision 4.2.0 and Vision 4.2.1

Use Red Hat Package Managers (RPMs) to upgrade to the Vision 4.3.2 or newer appliance.

Vision 4.3.0 and Newer

Use the Software Update feature on the Vision window to upgrade to the Vision 4.3.2 or newer appliance.

The Vision Software Update feature also allows you to choose whether you want the Vision server to automatically check for and notify you of available updates.

Note: See Vision Virtual Appliance Console Command Line on page 6 for information about using your Vision virtual appliance's console command line.

Install Vision onto a Windows-Based Server

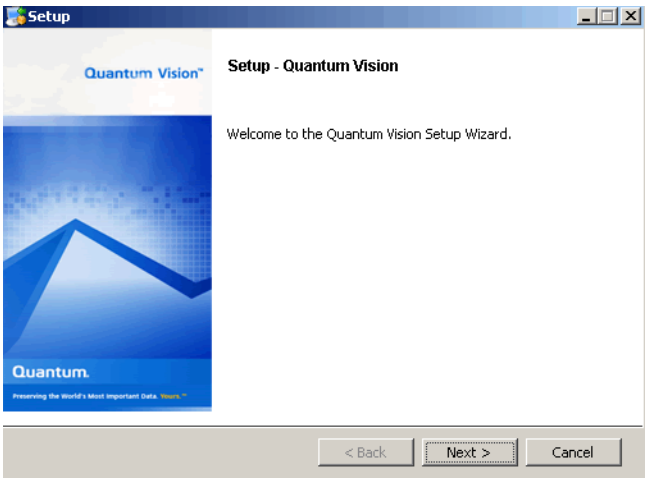
Use the Vision standard installation software package for Windows-based servers. After you have completed the installation wizard, set up and configure your Vision software.

Install Vision software onto a Windows-based server

1. Download the Vision installer file **vision-<x>-windows-installer.exe**, or insert the media with the installer file into the appropriate drive of your Vision server.
2. Browse to the location of the installer file.

3. Double-click the file to display the Quantum Vision Setup Wizard.

Figure 10: Quantum Vision Setup Wizard

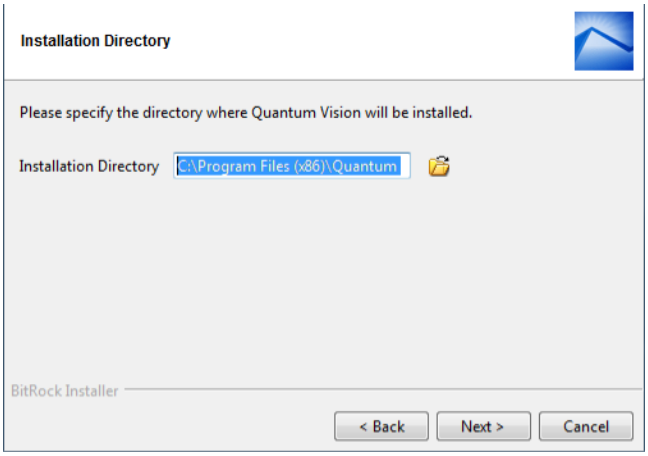


4. Click **Next** to display the **License Agreement** window.

Figure 11: License Agreement Window

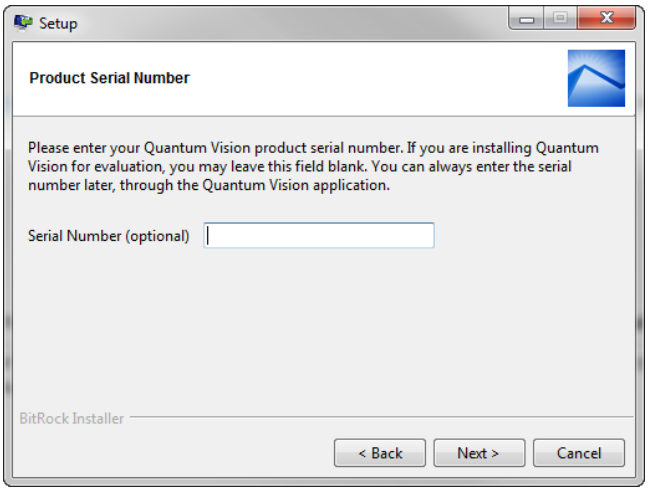
5. Select **I accept the agreement** and click **Next** to display the **Installation Directory** window.

Figure 12: Installation Directory Window



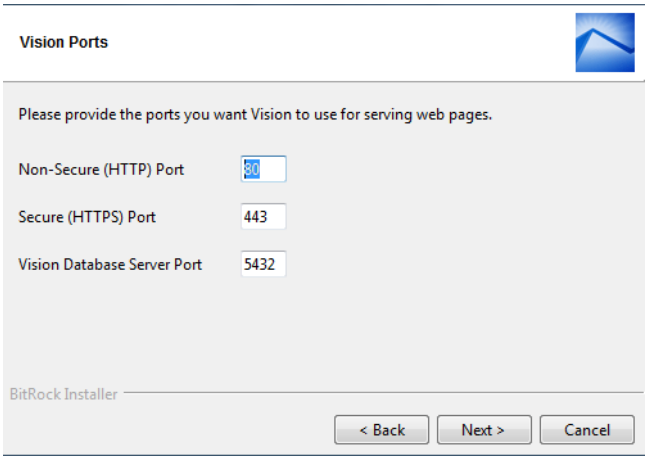
6. In the **Installation Directory** field, edit the location in which to install the Vision software as needed, and click **Next** to display the **Product Serial Number** window.

Figure 13: Product Serial Number Window



7. In the **Serial Number** field, enter your Vision serial number as needed, and click **Next** to display the **Vision Ports** window.

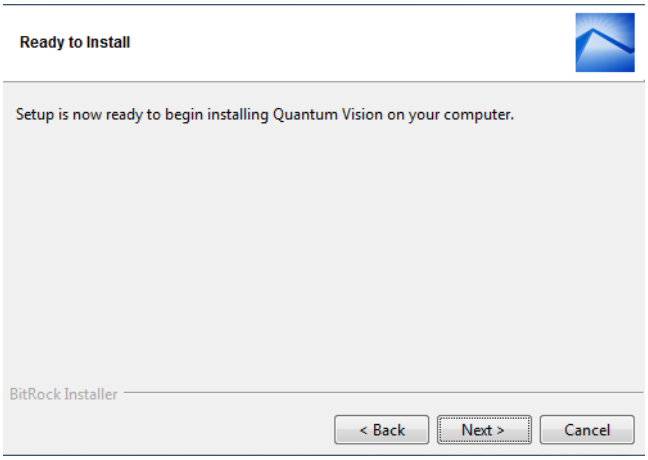
Figure 14: Vision Ports Window



8. In the **Port** fields, edit the ports that Vision will use as needed, and click **Next** to display the **Ready to Install** window.

Note: You can change your network ports using Vision's Security feature. When using this feature to change ports, check your existing firewall configuration to ensure that the appropriate firewall ports are open.

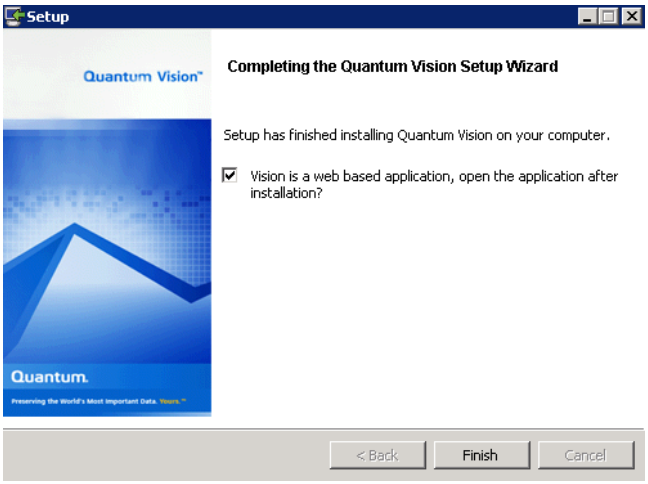
Figure 15: Ready To Install Window



9. Click **Next** to start the installation.

   The setup wizard installs the software, initializes the database, and starts Vision. When the setup wizard is finished, the **Completing the Quantum Vision Setup Wizard** window displays.

Figure 16: Completing the Quantum Vision Setup Wizard Window



10. Select the **Vision is a web based application, open the application after installation?** check box to launch Vision after the setup wizard is closed.
11. Click **Finish** to close the setup wizard.
12. Continue with the Vision setup.

Install Vision onto a Linux-Based Server

Use the Vision standard installation software package for Linux-based servers. After you have completed the installation wizard, set up and configure your Vision software.

Install Vision software on a Linux-based server

1. Use one of the following options to display the Quantum Vision Setup Wizard.

   If you are accessing the Vision Linux installer from removable media

   a. Insert the media into the appropriate drive of your Vision server.
   b. In a terminal window, execute the following commands as the root user:

   ```
   umount /media/<device>
   mkdir /tmp/VISION
   mount /dev/<device> /tmp/VISION/
   cd /tmp/VISION/
   ./setup-linux.bin
   ```

If you have downloaded the Vision Linux installer vision-<x>-linux-installer.run from the Internet

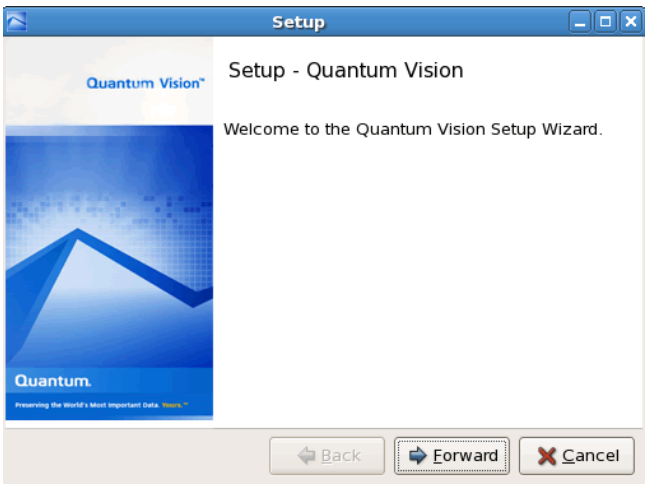
a. In a terminal window, execute the following command as the root user:

```
chmod +x /root/Desktop/vision-<x>-linux-installer.run
```

b. Do one of the following:

- If you are in a desktop environment, double-click the installer file.
- If you are in a command line environment, type `./vision-<x>-linux-installer.run` and press **<Enter>**.

Figure 17: Quantum Vision Setup Wizard

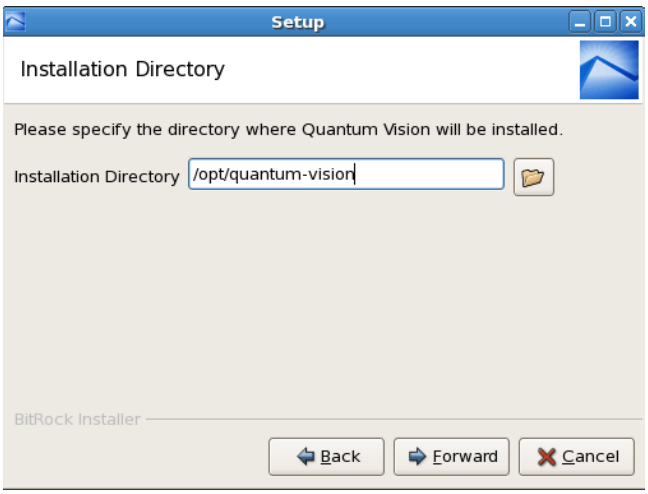


2. Click **Forward** to display the **License Agreement** window.

Figure 18: License Agreement Window

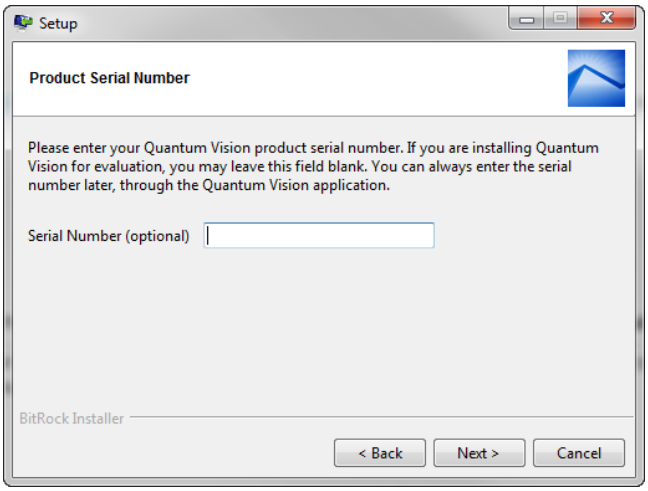
3. Select **I accept the agreement**, and click **Forward** to display the **Installation Directory** window.

Figure 19: Installation Directory Window



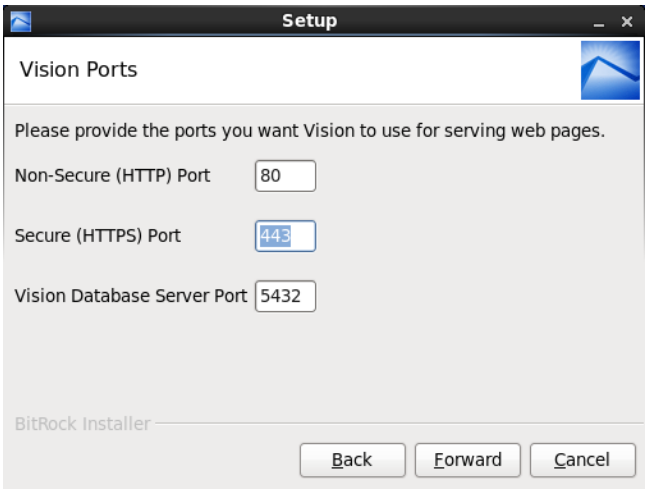
4. In the **Installation Directory** field, edit the location in which to install the Vision software as needed, and click **Forward** to display the **Product Serial Number** window.

Figure 20: Product Serial Number Window



5. In the **Serial Number** field, enter your Vision serial number as needed, and click **Forward** to display the **Vision Ports** window.

Figure 21: Vision Ports Window



6. In the **Ports** fields, edit the ports that Vision will use as needed, and click **Forward** to display the **Ready to Install** window.

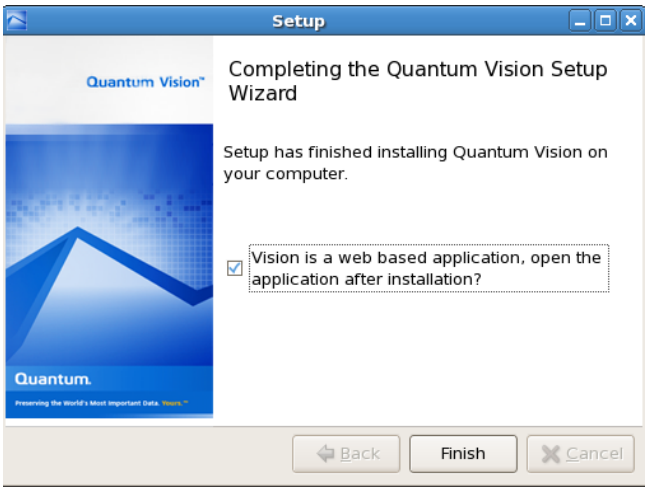
Note: You can change your network ports using Vision's Security feature. When using this feature to change ports, check your existing firewall configuration to ensure that the appropriate firewall ports are open.

Figure 22: Ready to Install Window

7. Click **Forward** to start the installation.

   The setup wizard installs the software, initializes the database, and starts Vision. When the setup wizard is finished, the **Completing the Quantum Vision Setup Wizard** window displays.

Figure 23: Completing the Quantum Vision Setup Wizard Window



8. Select the **Vision is a web based application, open the application after installation?** check box to launch Vision after the setup wizard is closed.
9. Click **Finish** to close the setup wizard.

Additional Steps for Removable Media Installations

a. If you installed the Vision software with removable media, execute the following commands to safely remove the media:

```
cd/
umount/tmp/VISION
```

b. Remove the media from the drive.

10. Continue with the Vision setup.

Upgrade Vision with the Standard Software Package

Use the Vision standard update software package to upgrade an existing installation of Vision to the latest version for either a Windows or Linux operating system (OS).

Important

After you run the software updater, Vision must update and convert the database for optimum performance. This process can take two hours for large configurations. The Vision Web-based interface is not available during this time.

Upgrade Vision with the standard software package

1. Access the Quantum Web site at http://www.quantum.com/vision.
2. Click **Vision Software Download**.
3. Click **Vision 4.4.0 Software Upgrade**.
4. Locate and download the correct update software for the OS on which the Vision server is running, either Windows or Linux.

   If the Vision server is unable to access the Internet, download the update software onto another computer, and then copy it to the Vision server using a USB flash drive or other removable storage.
5. On the Vision server, stop the Vision service by doing one of the following:

   Windows OS

   Use the **Services** control panel to stop the Vision service.

   Linux OS

   At a terminal prompt, enter `service vision stop`.
6. On the Vision server, run the Vision update software by doing one of the following:

   Windows OS

   Double-click the downloaded updater software file.

   Linux OS

   From a terminal window as the root user, execute the following command in the directory storing the update software file:

   `./<vision_updater_filename>`
7. At the prompt, click **OK** to display the Quantum Vision Setup Wizard.
8. Click **Next** or **Forward** to display the **License Agreement** window.
9. Select **I accept the agreement**, and click **Next** or **Forward** to display the **Installation Directory** window.
10. In the **Installation Directory** field, edit the location in which to install the Vision software as needed, and click **Next** or **Forward** to display the **Ready to Install** window.

    Windows (32-bit)

    The default location is: **\Program Files\Quantum Vision**.

Windows (64-bit)

The default location is: **\Program Files (x86)\Quantum Vision**.

Linux

The default location is: **/opt/quantum-vision/**.

11. Click **Next** or **Forward** to initiate the upgrade.

    When the setup wizard has completed the upgrade, the **Completing the Quantum Vision Setup Wizard** window displays.

12. Click **Finish** to close the setup wizard.

    Your Vision software is updated to the latest version.

13. Close your browser to clear its cache before accessing the updated version of Vision.

Install Vision as a Virtual Appliance

You can install Vision 4.3.2 and newer as a VMware appliance within a vSphere infrastructure.

Use the following task to walk through a typical OVF deployment. Keep in mind that the actual sequence of deployment windows depends on your system's configuration and may not appear exactly as shown here. With a basic knowledge of your system, the selections that you need to make, such as hosts or clusters, should be intuitive.

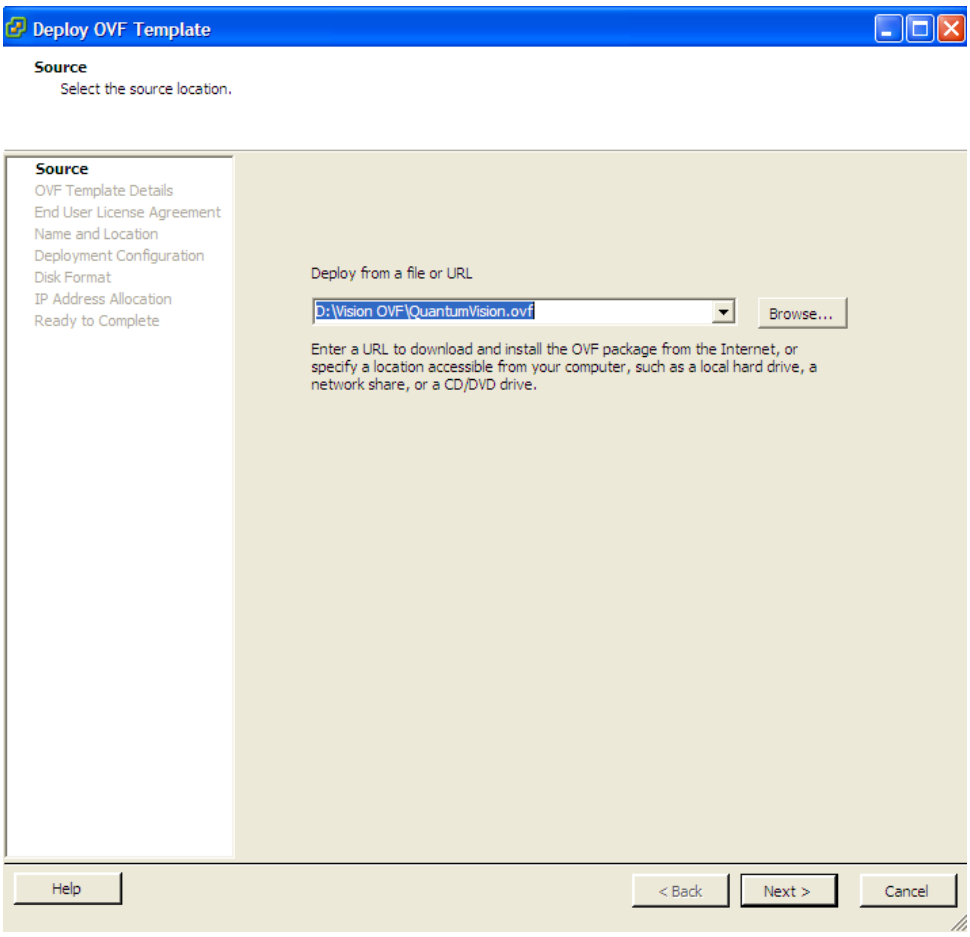
Note: If you have downloaded a Vision OVA file from Quantum.com, simply use it as you would an OVF file.

Install Vision as a virtual appliance

1. Download the Vision OVA or OVF file, or insert the media with the installer file into the appropriate drive of your Vision server.
2. Display the **vSphere Client** window.

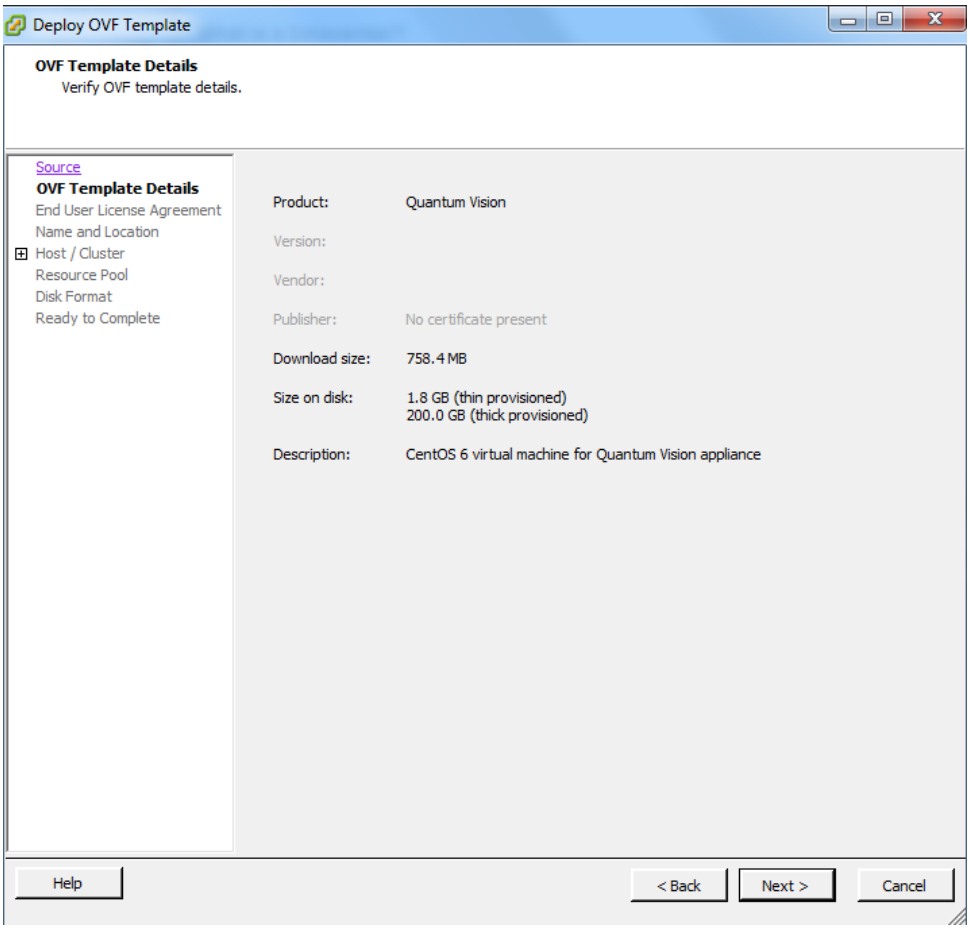
3. On the **File** menu, select **Deploy OVF Template** to display the **Source** window.

Figure 24: Source Window



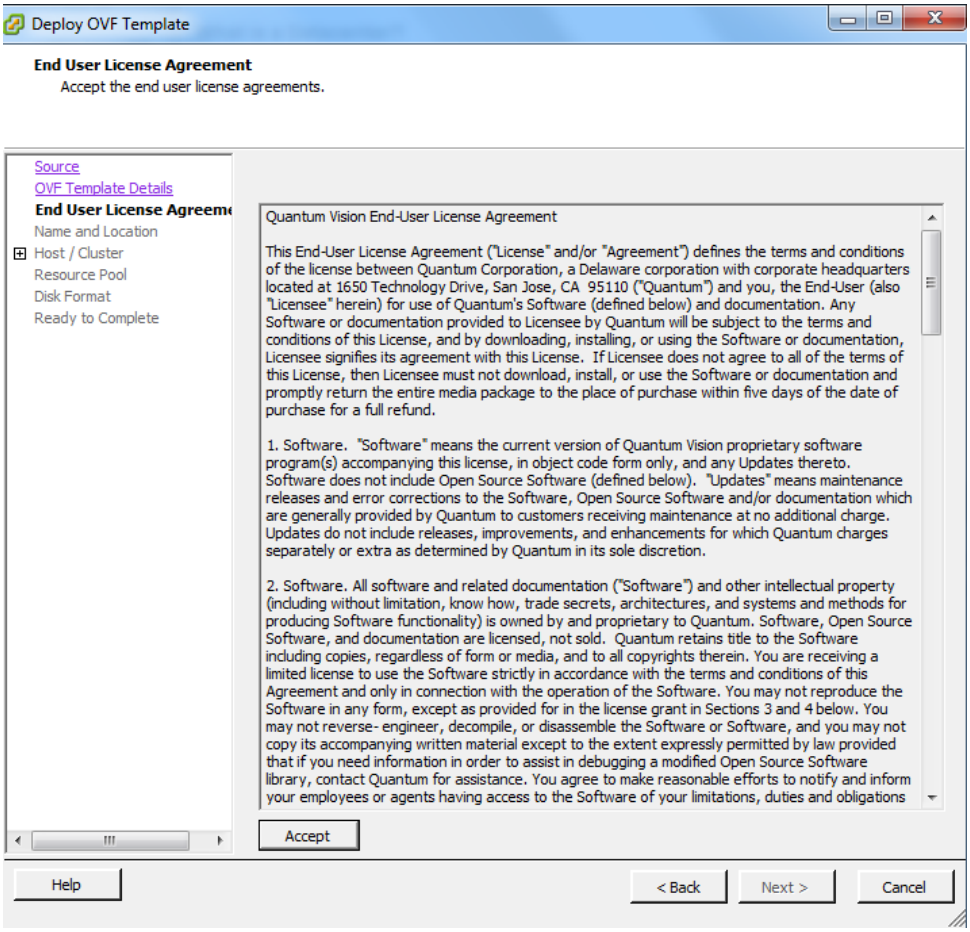
4. Click **Browse** to locate and select the **QuantumVision.ovf** file, and click **Next** to display the **OVF Template Details** window.

Figure 25: OVF Template Details Window



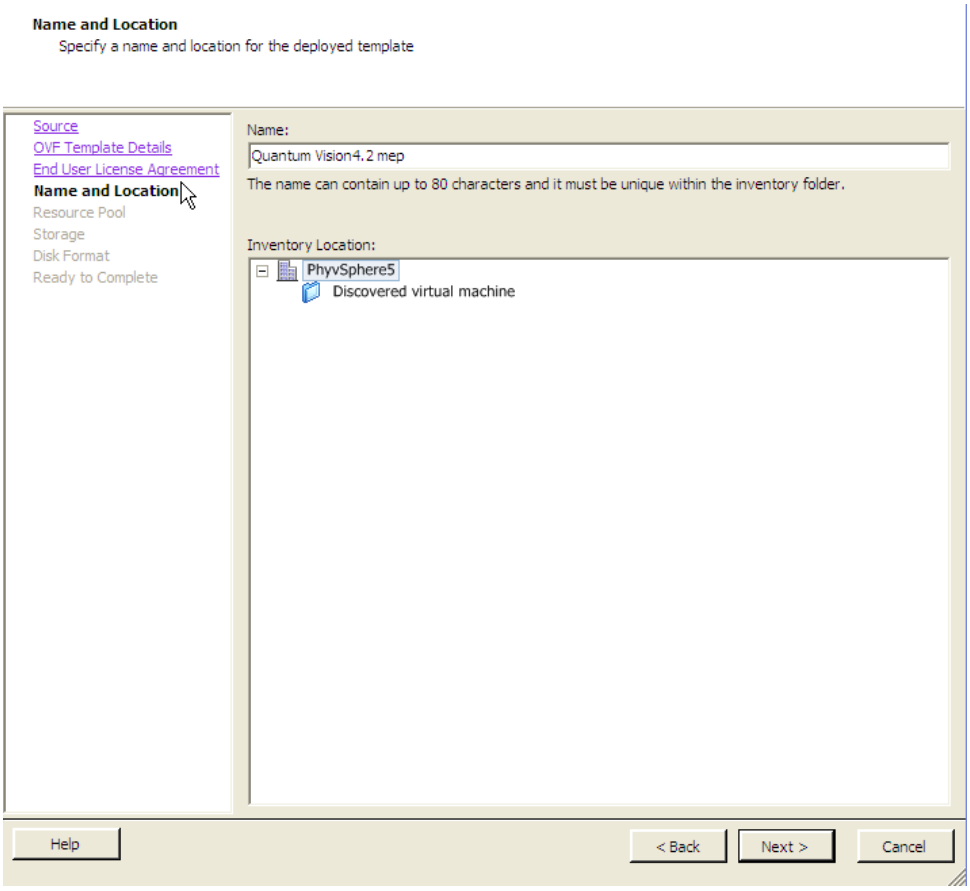
5. Make note of any information you need, and click **Next** to display the **End User License Agreement** window.

Figure 26: End User License Agreement Window



6. Click **Accept** to accept the license agreement, and click **Next** to display the **Name and Location** window.

Figure 27: Name and Location Window



7. In the **Name** field, enter a name for the appliance, and in the **Inventory Location**field, select a location, as needed.
8. Click **Next** to make any of the following selections that apply to your vSphere configuration:

If your configuration has multiple hosts or clusters

Select your host or cluster and click **Next**. This option is not available if you have only one host or a single cluster.

If you configuration supports resource pools

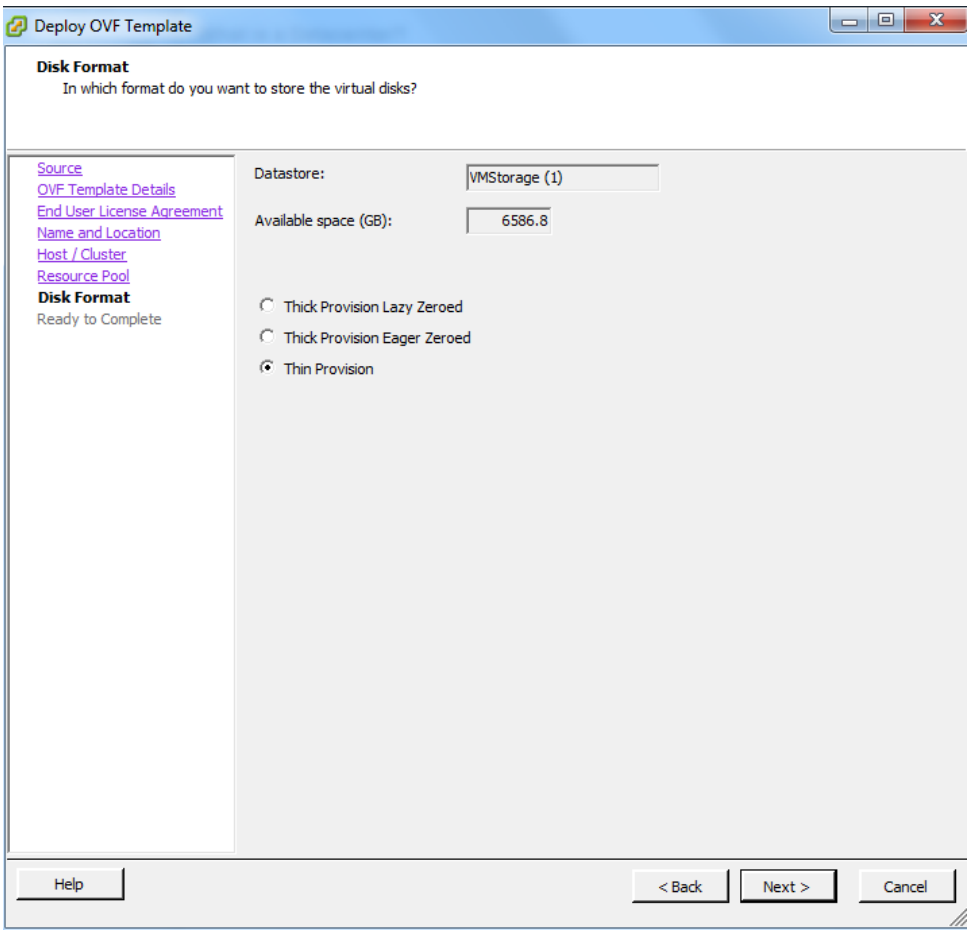
Select your resource pool and click **Next**. This option is not available if you are not using the resource pool capability.

If you have multiple storage destinations

Select your storage destination and click **Next**. This option is not available if you have only one storage device.

The **Disk Format** window displays.

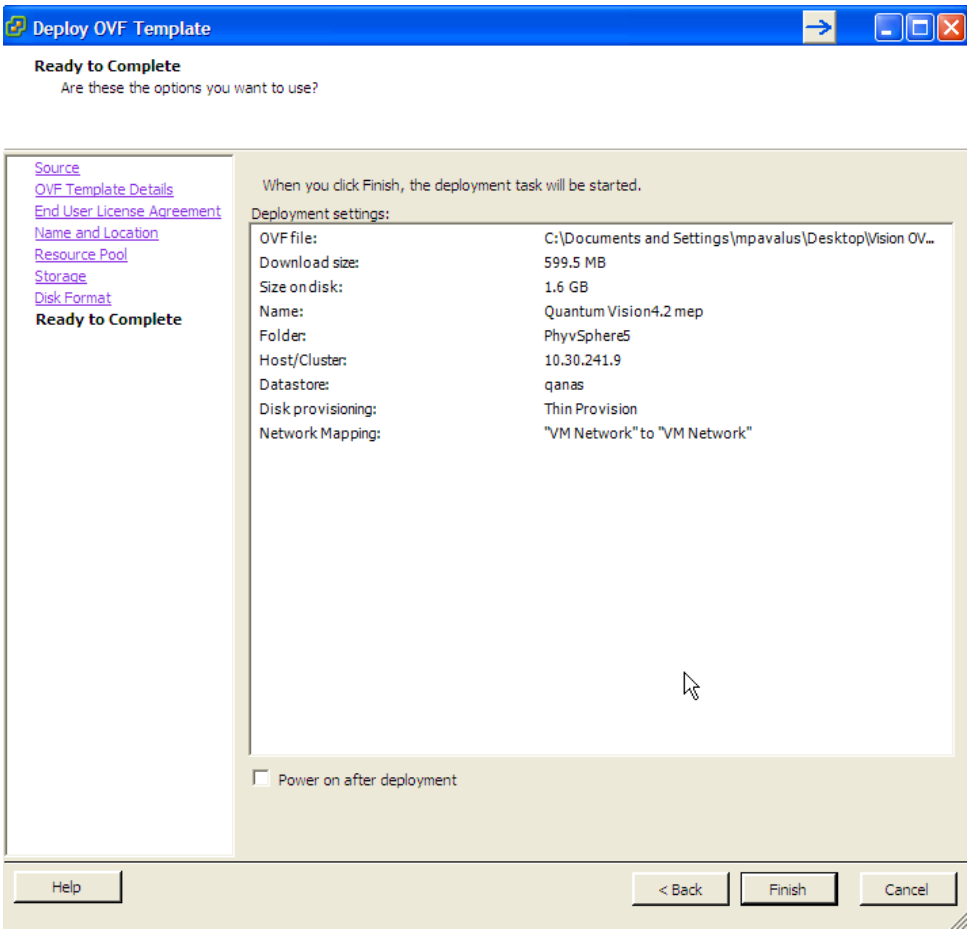
Figure 28: Disk Format Window



9. Make sure that **Thin Provision** is selected and click **Next** to display the **Ready to Complete** window.

   If you have multiple vSwitches configured in your environment, select the appropriate network and click **Next** to display the **Ready to Complete** window. This option is not available if you have a single vSwitch configuration.

Figure 29: Ready to Complete Window



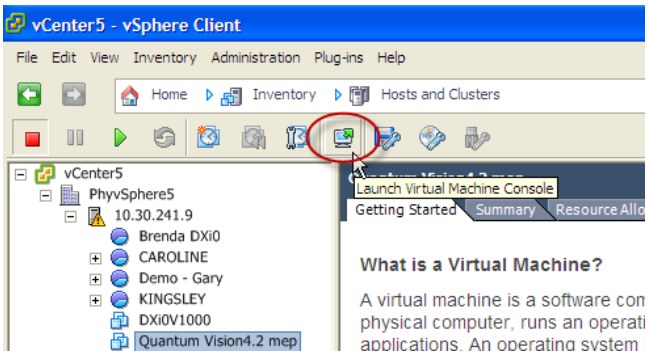
10. On the **Ready to Complete** window, verify that the settings are correct and click **Finish** to initiate the deployment process.

    When the Vision appliance has been deployed, the **Deployment Completed Successfully** dialog box displays.

11. Click **Close** to return to the **vSphere Client** window.

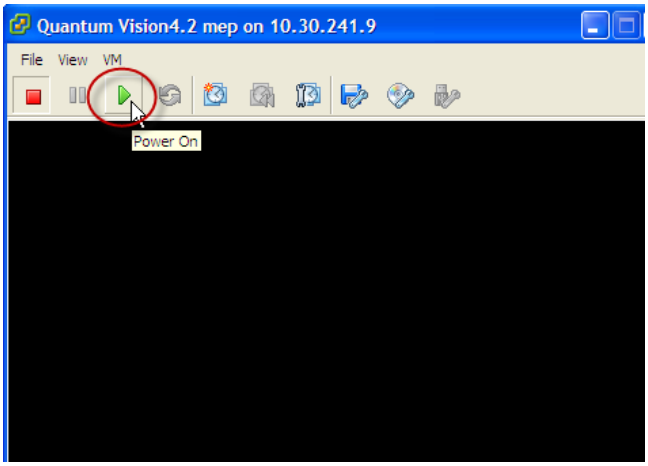
12. In the left panel, select the new Vision appliance's name and click the **Launch Virtual Machine Console** icon to display the appliance's virtual machine console window.

Figure 30: Launching your Virtual Machine Console



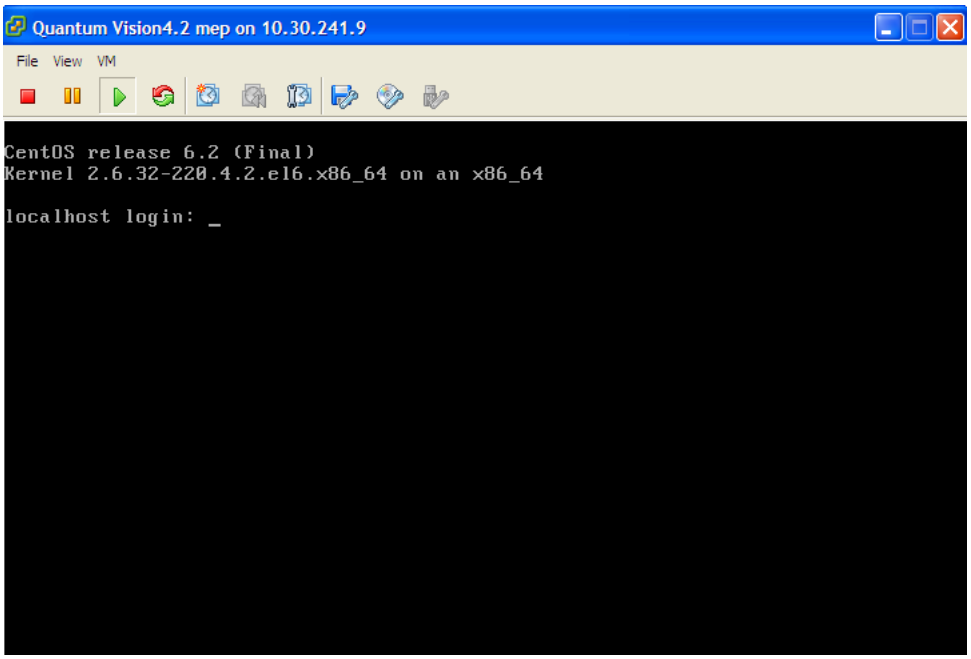
13. On the appliance's virtual machine console window, click the **Power On** icon.

Figure 31: Console Window with Power On Icon



The Power On process takes several minutes. When it is complete, the appliance's console command line window displays.

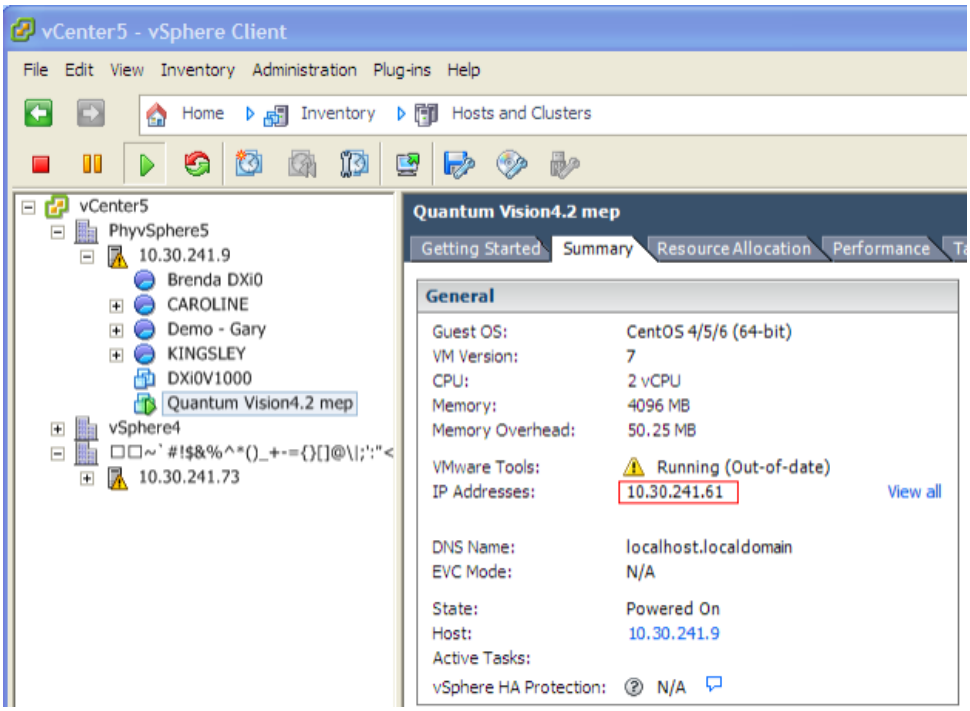
Figure 32: Console Window with Command Line



14. Log on with your appliance's user name and password, as needed. See Access the Console Command Line on page 7.

    The system will establish an IP address for the Vision appliance and display it on the **vSphere Client Summary** tab's right panel.

Figure 33: vSphere Client Summary Tab



For enhanced stability, it is recommended that you replace your DHCP assigned IP address with a static IP address. See Issue Network Commands on page 10.

15. Continue with the Vision setup.

Upgrade to a Vision Virtual Appliance

If you have Vision 4.2 to 4.3.1, you can upgrade to a Vision 4.4.0 virtual appliance by using one of the following methods.

Important

As a precautionary measure, we recommend that you use your vSphere client or other ESXi management client to take a snapshot of your Vision server before beginning any update.

Vision 4.2.0 and Vision 4.2.1

Use Red Hat Package Managers (RPMs) to upgrade to the Vision 4.4.0.

Upgrade Vision 4.2.0 to Vision 4.4.0

1. Access the Quantum Web site at http://www.quantum.com/vision.
2. Click **Vision Software Download**.
3. Click **Vision 4.4.0 Software Upgrade** to access the RPMs.
4. Locate the following 3 PostgreSQL 8.4 RPMs and the Vision-install RPM:
   - **postgresql-libs-8.4.13-1.el6_3.x86_64.rpm**
   - **postgresql-8.4.13-1.el6_3.x86_64.rpm**
   - **postgresql-server-8.4.13-1.el6_3.x86_64.rpm**
   - **vision-install-4.4.0-<build_number>.x86_64.rpm**

   Note: The Vision and PostgresSQL version numbers will change when the software is updated. You should use the most recent versions.
5. Download the RPMs to a server that is both on your network and that can be accessed from the appliance by either HTTP or SCP/SSH, as follows:

   HTTP servers

   Place the RPMs anywhere within the Web server's directory structure, for example:

   http://<server>/directory/path/vision-install-4.4.0-<build_number>.x86_64.rpm

   For this example, you would use the http command in step 8.

   Servers other than HTTP servers

   Place the RPMs anywhere on the server, for example:

   /tmp/vision/updates/vision-install-4.4.0-<build_number>.x86_64.rpm

   For this example, you would use the SCP command in step 8.
6. Make note of the location in which you place the RPMs.
7. Log in to one of the following Vision appliances as a **sysadmin** user, as appropriate:

   Linux/Unix/Mac systems

   Use SSH or a comparable application.

   Windows systems

   Use PuTTY or a comparable application.

   VMware vSphere client

   Use the appliance's VM console.

8. Depending on how you are transferring the PostgrSQL RPMs from the server to your appliance (see step 5), run one of the following upgrade commands to upgrade RPMs:

   HTTP

   At the appliance's admin command line prompt, enter **`system upgrade http`**.

   SCP

   At the appliance's admin command line prompt, enter **`system upgrade scp`**.

9. Respond as appropriate to each upgrade command. The following occurs:
   - The upgrade command retrieves and installs the PostgreSQL RPMs onto the appliance.
   - After the RPMs are installed, a message displays notifying you that the Vision service is being restarted.
   - When the Vision service has restarted, the updated PostgreSQL is installed.
10. At the **admin** prompt, repeat steps 7 and 8 for the Vision-install RPM.

    The upgrade command retrieves and installs the Vision-install RPM onto the appliance. This installation configures and starts the PostgreSQL service.
11. At the **admin** prompt, enter **exit**.

    Vision has been upgraded.

Upgrade Vision 4.2.1 to Vision 4.4.0

1. Access the Quantum Web site at http://www.quantum.com/vision.
2. Click **Vision Software Download**.
3. Click **Vision 4.4.0 Software Upgrade** to access the RPM.
4. Locate the **vision-install-4.4.0-<build_number>.x86_64.rpm** RPM.

   Note: The Vision and PostgresSQL version numbers will change when the software is updated. You should use the most recent versions.

5. Download the above RPM to a server that is both on your network and that can be accessed from the appliance by either SCP/SSH or HTTP, as follows:

   HTTP servers

   Place the RPM anywhere within the Web server's directory structure, for example:

   http://<server>/directory/path/vision-install-4.4.0-<build_number>.x86_64.rpm

   For this example, you would use the http command in Step 8.

   Servers other than an HTTP server

   Place the RPM anywhere on the server, for example:

/tmp/vision/updates/vision-install-4.4.0-<build_number>.x86_64.rpm

For this example, you would use the SCPcommand in Step 8.

6. Make note of the location in which you place the RPM.
7. Log in to one of the following Vision appliances as a **sysadmin** user, as appropriate:

   Linux/Unix/Mac systems

   Use SSH or a comparable application.

   Windows systems

   Use PuTTY or a comparable application.

   VMware vSphere client

   Use the appliance's VM console.

8. Depending on how you are transferring the PostgrSQL RPMs from the server to your appliance (see step 5), run one of the following upgrade commands to upgrade RPMs:

   HTTP

   At the appliance's admin command line prompt, enter **`system upgrade http`**.

   SCP

   At the appliance's admin command line prompt, enter **`system upgrade scp`**.

9. Respond as appropriate to each upgrade command. The following occurs:
   - The upgrade command retrieves and installs the RPM onto the appliance.
   - After the RPM is installed, a message displays notifying you that the Vision service is being restarted.
   - When the Vision service has restarted, the admin application displays a prompt.
10. At the **admin** prompt, enter **`system upgrade`** to run the system upgrade command.
11. At the **admin** prompt, enter **exit**.

    Vision has been upgraded.

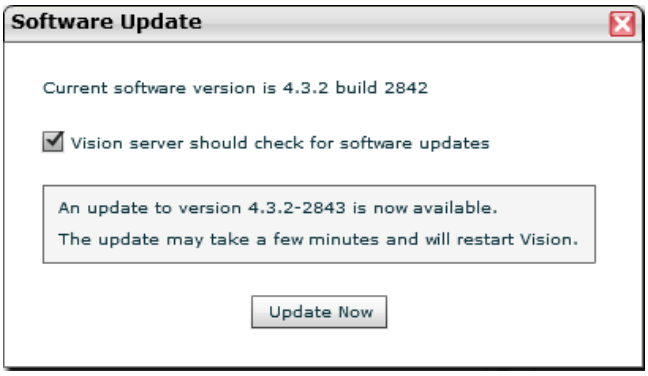
Vision 4.3.0 and Newer

Use the Software Update feature on the Vision window to upgrade to the Vision 4.4.0.

Upgrade Vision 4.3 or newer to Vision 4.4.0

1. Log on to Vision as a **sysadmin** user to display the Vision window.
2. On the **Configuration** menu, select **Software Update** to display the **Software Update** dialog box with the **Update Now** button activated.

Figure 34: Software Update Dialog Box – Update Now

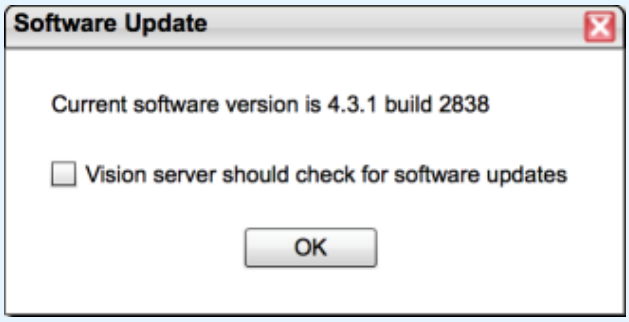


3. Click **Update Now** to upgrade your Vision software.

What if software updates are not available?

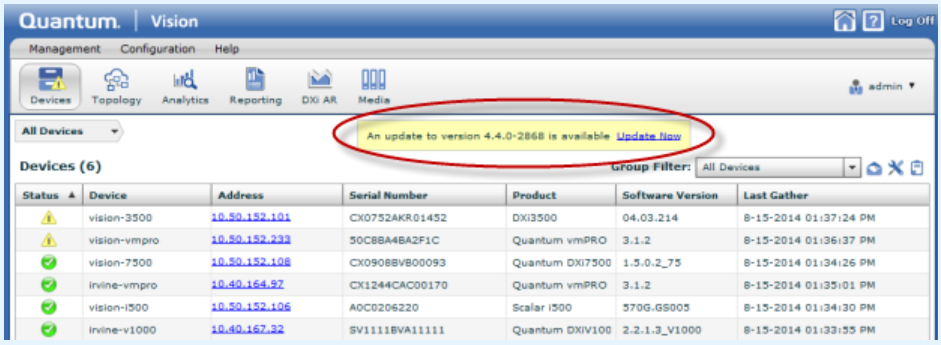
When you display the **Software Update** dialog box, the **Update Now** button does not appear. Instead a **Vision server should check for software updates** check box and an **OK** button display.

Figure 35: Software Update Dialog Box – Configure Settings



Select this check box and click **OK** to check for software updates. If software updates are available, a notification banner displays to the right of the toolbar. You can install the software updates by clicking **Update Now**.

Figure 36: Software Update Notification



By leaving the **Vision server should check for software updates**check box selected, your Vision server automatically checks for software updates.

If you do not want your Vision server to automatically check for updates, clear the **Vision server should check for software updates** check box. By deselecting this check box, you can control when your Vision server checks for updates.

Uninstall Vision Software from a Vision Server

Use the following procedures to uninstall Vision software from a Vision server running on either a Windows or Linux operating system.

When you uninstall Vision software, you have the opportunity to save the Vision database. The database contains configuration and status information for the Vision server.

Uninstall Vision software from a Vision server running on Windows:

1. In Windows, navigate to the **Control Panel**, and then to **Uninstall or change a program**.
2. In the list of currently installed programs, select **Quantum Vision**.
3. Click **Uninstall** to display a message asking if you want to uninstall Vision.
4. Click **Yes** to run the uninstall wizard.
5. At the message asking if you want to save the Vision database, click **Yes** to save the database or **No** to delete the database.
6. At the message indicating that the uninstall process is complete, click **OK**.
7. Depending on the version of Windows that you are running, a message stating that you must restart Windows to complete the uninstall process might display. if it does, click **Yes** to restart Windows and complete the uninstall process.

Uninstall Vision software from a Vision server running on Linux

1. In a terminal window, execute the following commands as **root**:

   cd/opt/quantum-vision

   ./unistall

2. At the message asking if you want to uninstall Vision, click **Yes** to run the uninstall wizard.
3. At the message asking if you want to save the Vision database, click **Yes** to save the database or **No** to delete the database.
4. At the message indicating that the uninstall process is complete, click **OK**.

Chapter 3: Setup and Configuration

This chapter contains the following topics:

Vision Setup and Configuration

Before using Vision, you need to set up and configure your system to define how it interacts with users, devices, and other servers.

Example

Use the management capabilities in Vision to define when users are notified about changes in device status, or to define which devices are monitored by Vision.

OR

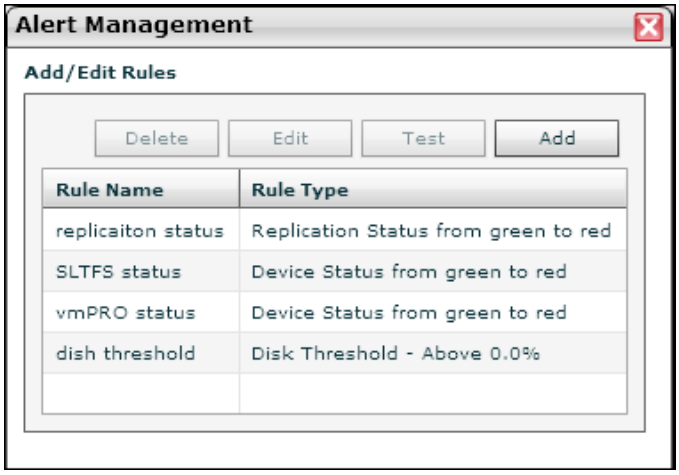
Define configuration settings for email, licenses, and authentication, in addition to other parts of the Vision system.

Alert Management

With alerts, Vision can automatically notify users and administrators by e-mail about important changes in device status. You define alert rules to specify both the conditions for when Vision generates an alert and the recipients to whom Vision sends the alert. In addition, Vision sends an e-mail in response to SNMP traps generated by devices.

Use the **Alert Management** dialog box to view all current rules, and to add, edit, or delete rules. See Manage Alert Rules in Vision on page 59.

Figure 37: Alert Management Dialog Box



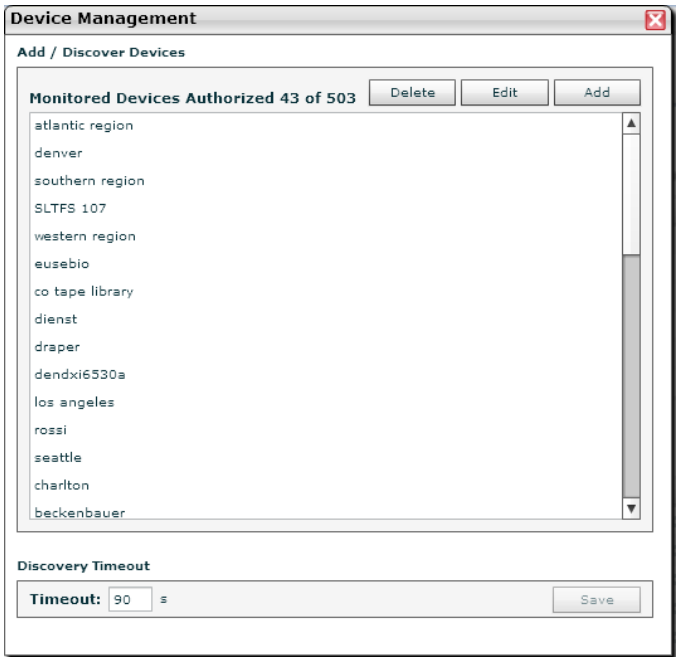
Prerequisite

Before Vision can send alert notifications to recipients, you must configure e-mail server settings.

Device Management

In Vision, a device is the backup system being monitored, such as a Scalar tape library, DXi disk backup system, Q-Cloud Protect, or Scalar LTFS. Before you can use Vision to monitor your devices, you must first run a process in which Vision discovers the devices within your network. After devices are discovered, use the **Device Management** dialog box to view, edit, and delete devices. See Manage Devices in Vision on page 64.

Figure 38: Device Management Dialog Box



Groups Management

In Vision, a group is a named collection of users. Vision uses groups to manage device access. When you run the device-discovery process, you can assign one or more groups to the device. Only users who belong to the assigned groups can access the device. Keep in mind that a user can belong to more than one group.

Use the **Groups Management** dialog box to add, edit, and delete groups. See Manage Groups in Vision on page 68.

Figure 39: Groups Management Dialog Box

User Management

Vision supports three user roles: administrators, users, and monitors. Each role determines the type of access a user has to devices within Vision, and the functions a user can perform in Vision.

Admin

Administrators have access to all devices. They can schedule reports, configure Vision, and manage users, groups, and devices. Multiple administrators can log on to Vision at the same time.

User

Users have access to devices to which their groups have been assigned. Users can view information in Vision but cannot make changes.

Monitor

Monitors can view information in Vision but cannot make changes. Multiple users can log on as monitor at the same time. However, there is only one Monitor user account. To enable the Monitor user account, see Enable Vision Monitor Access on page 74.

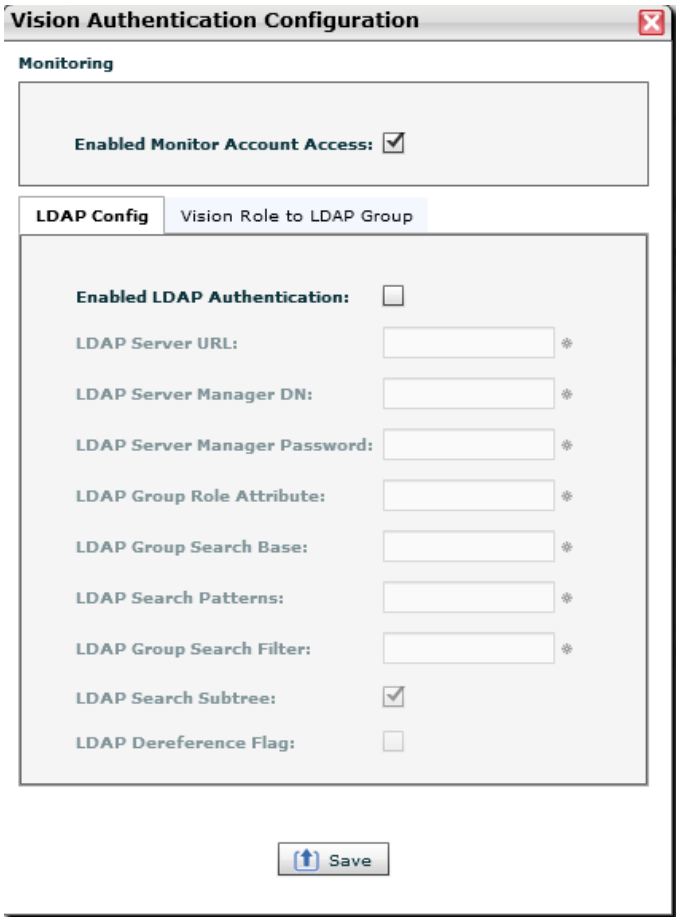
Use the **User Management** dialog box to add users, specify their roles, and assign them to groups. From this dialog box, you can also edit and delete users. See Manage Users in Vision on page 71.

Figure 40: User Management Dialog Box

Authentication Configuration

You can use Vision along with Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory (AD) to authenticate and authorize users. From the **Vision Authentication Configuration** dialog box, you can configure Vision to access the information stored in LDAP or AD, assign authorization levels to groups and users, and enable Monitor account access in Vision. See Configure LDAP Directory Services for Vision on page 76.

Figure 41: Vision Authentication Configuration Dialog Box

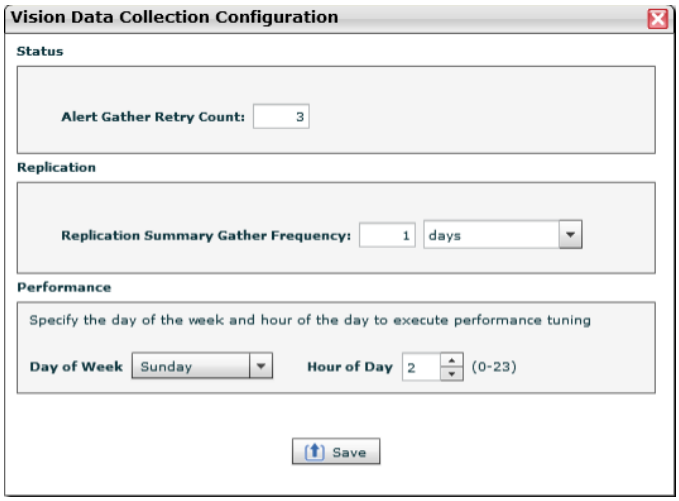


Data Collection Configuration

Use Data Collection Configuration to define the frequency at which Vision collects status and reporting data from monitored devices, and to configure maintenance settings for your Vision database, as needed.

Use the Vision **Data Collection Configuration** dialog box to configure Vision data collection and database maintenance settings. See Configure Data Collection in Vision on page 80.

Figure 42: Vision Data Collection Configuration Dialog Box



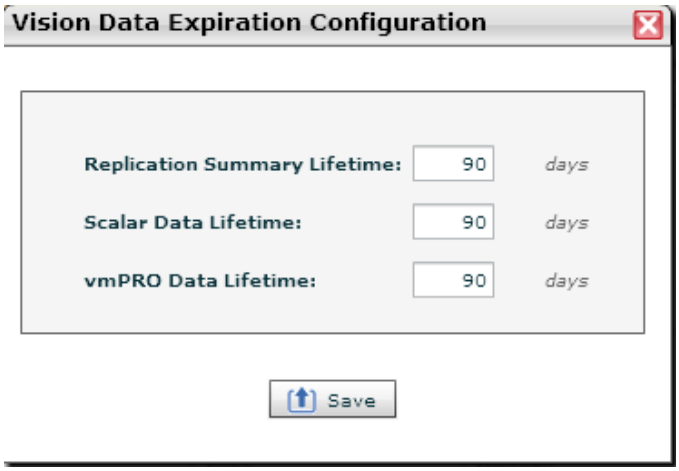
Data Expiration Configuration

Use Data Expiration Configuration to define the amount of time that Vision retains data collected from monitored devices. Any data that is older than a specified age is expired and removed from the Vision database, and this information is no longer available for reporting. When configuring data-retention time periods, keep in mind that aggregated values are retained in the Vision database for a predefined time:

- 15 minute values are retained for 6 months
- 1 hour values are retained for 12 months
- 1 day values are retained for 18 months

Use the **Vision Data Expiration Configuration** dialog box to configure data-retention settings. See Configure Data Expiration Settings in Vision on page 82.

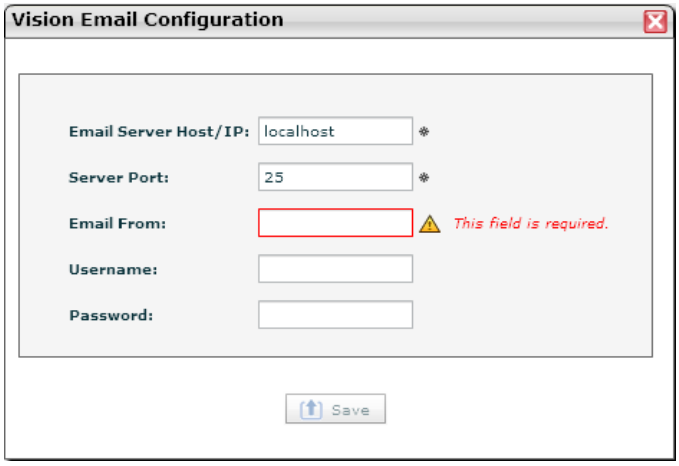
Figure 43: Vision Data Expiration Configuration Dialog Box



Email Configuration

You must configure your outgoing email server for Vision to send email notifications and reports. Use the **Vision Email Configuration** dialog box to configure these outgoing email server settings. See Configure Email Server Settings in Vision on page 83.

Figure 44: Vision Email Configuration Dialog Box

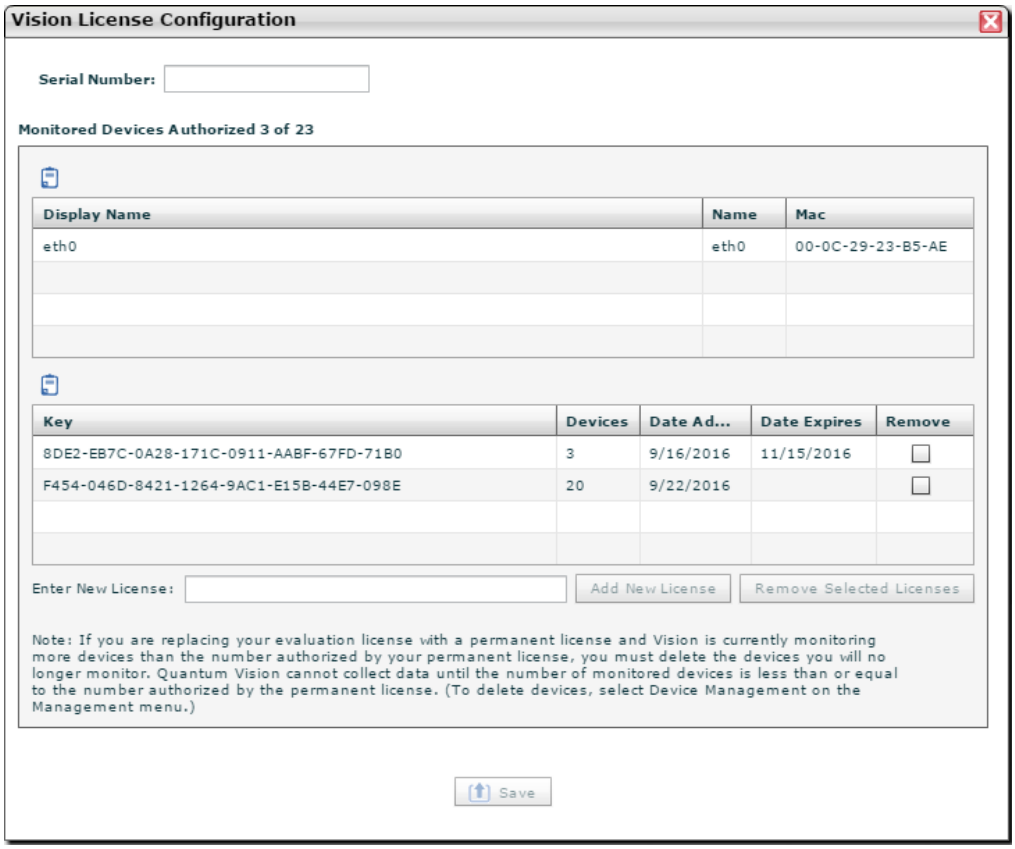


Licensing Configuration

The temporary license installed with Vision authorizes you to monitor up to 3 devices for up to 60 days. To monitor more devices, or to use Vision for more than 60 days, you must add a permanent license. To add a license to Vision, contact your Quantum Sales representative for information about purchasing a license. After you receive the license certificate, you can obtain a license key and add it to Vision.

Use the **Vision License Configuration** dialog box to configure new licenses on your vision server, to view information about your installed licenses, and to delete evaluation licenses. See Add a New Vision License on page 84.

Figure 45: Vision License Configuration Dialog Box

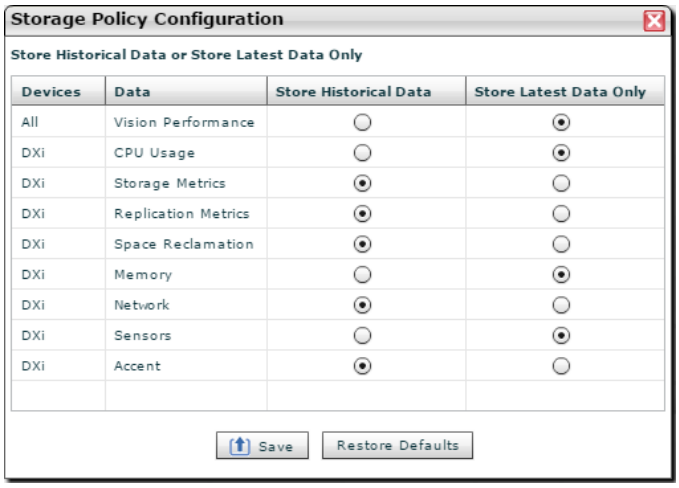


Storage Policies

Use Vision's Storage Policy Configuration to improve performance and increase scalability by reducing the amount of data stored in the Vision database. With this application, you can define the type of data to include in Vision reporting and analytic results for devices and their specified data groups.

Use the **Storage Policy Configuration** dialog box to configure group storage. See Configure Storage Policies in Vision on page 91.

Figure 46: Storage Policy Configuration Dialog Box



Security

Use the Vision's Security Configuration to define the following:

- HTTP and HTTPS ports for Windows and Linux installed Vision servers.

  For a Vision appliance, log on to the Vision Console Command Line and run the **`net ports`** command to configure ports. See Issue Network Commands on page 10.

- A public key required for Vision to access certain devices from which it is collecting data, such as DXi or Q-Cloud Protect.

  Vision generates a public key that you can add to a device requiring this level of authorization. For more information, see the documentation of the product from which your Vision server is accessing data

Use the **Security Configuration** dialog box to configure security settings. See Configure Security Settings for Vision on page 95.

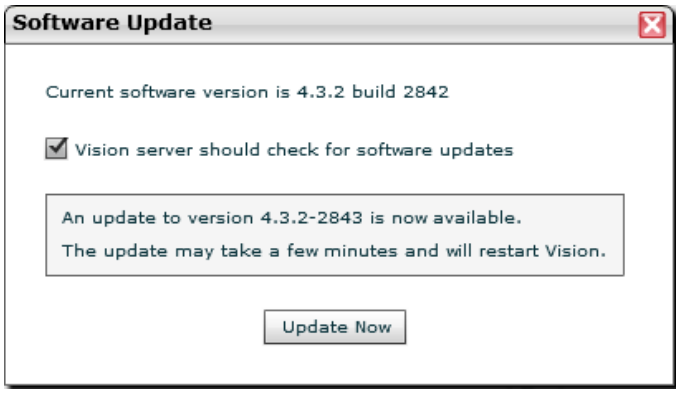
Figure 47: Security Configuration Dialog Box

Software Update

Use the Vision **Software Update** dialog box to update your Vision virtual appliance when software updates are available. Through this application, you can also choose whether you want the Vision server to automatically check for and notify you of updates that are available. See Vision Installations and Upgrades.

Note: The Software Update feature supports only the Vision virtual appliance (installations from an OVF). The Software Update feature does not update Vision when it has been installed using the standard software installer.

Figure 48: Software Update Dialog Box



Manage Alert Rules in Vision

Use Alert Management to manage alert rules, as follows:

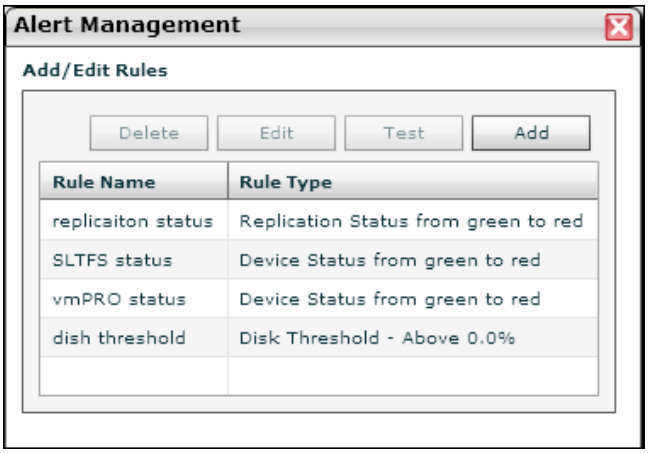
- Specify the conditions for when Vision generates an alert, and define the recipients who receive the alert.
- Change the properties or actions for the rule.
- Remove an alert rule from the list of active rules. After you delete a rule, Vision no longer uses it to generate notifications.

Both administrators and users can manage alert rules, although, users can manage rules only for the devices to which they have access.

Add an alert rule

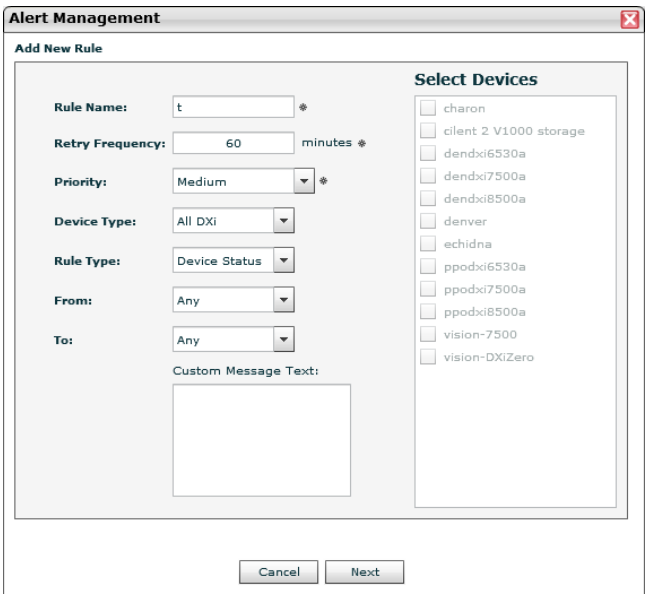
1. On the **Management** menu, click **Alert Management** to display the **Alert Management** dialog box.

Figure 49: Alert Management Dialog Box



2. Click **Add** to display the **Add New Rule** dialog box.

Figure 50: Add New Rule Dialog Box



3. In the **Rule Name** field, enter a name to use in identifying the rule.

   You can enter a rule name that is up to 64 characters in length.

4. In the **Retry Frequency** field, enter the number of minutes in between alert notifications. If an alert notification is not acknowledged after this amount of time, Vision resends the alert notification.

5. In the **Priority** field, click on the drop-down list and select whether the alert should be **Low**, **Medium**, or **High** priority.

6. In the **Device Type** field, select an option from the drop-down list to indicate to which devices the rule applies.

   All <device type>

   The rule applies to all discovered sources of the selected device type.

   Custom <device type>

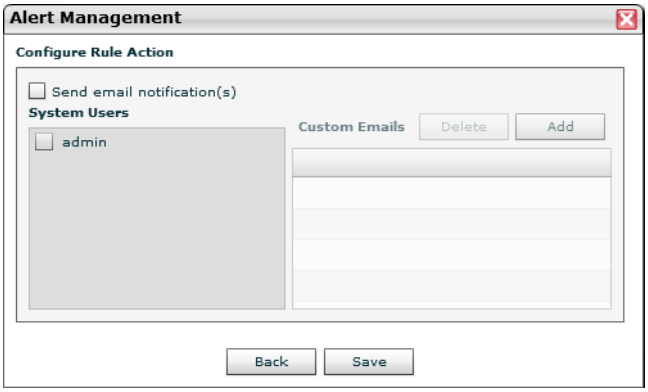
   The rule applies to selected devices within the selected device type.

   To select devices, select the check box next to each device in the **Select Devices** pane to which to apply the rule.

7. In the **Rule Type** field, select an alert rule type from the drop-down list, and then define parameters for the rule. See Types of Vision Alert Rules on page 62.

8. In the **From** and **To** fields, select a color status from each drop-down list to trigger an alert if a device's status changes from one to another.
9. In the **Custom Message Text** box, enter a message to send with the alert, as needed.
10. Click **Next** to display the **Configure Rule Action** dialog box.

Figure 51: Configure Rule Action Dialog Box



11. Set up email notifications, as needed.

Send email notifications when the alert is generated

a. Select the **Send email notification(s)** check box.
b. In the **System Users** box, select each predefined system user to whom to send email notifications.
c. To add custom recipients, click **Add** and in the **New Email** field, enter the email address of the recipient.

   To delete a custom recipient, select the recipient and click **Delete**.

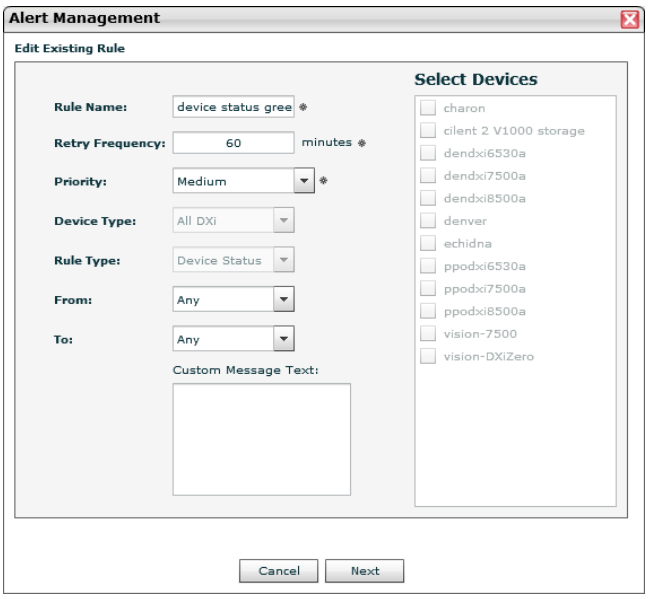
12. Click **Save** to add the rule to the **Alert Management** dialog box.
13. Select the rule and click **Test** to verify that the rule is working correctly.
14. The rule now appears in the list of alert rules and is used to send notifications.

Edit an alert rule

1. On the **Management** menu, click **Alert Management** to display the **Alert Management** dialog box.

2. Select the rule to edit, and click **Edit** to display the **Edit Existing Rule** dialog box.

Figure 52: Edit Existing Rule Dialog Box



3. Edit the alert rules settings, as needed. See Add an alert rule on page 59.

   When editing a rule, you cannot change the **Device Type** or **Rule Type** settings.To make changes to these settings, first delete the rule, and then create a new rule with the correct settings.

4. When you have finished editing the rule, click **Save** and close the **Alert Management** dialog box to apply all updates to the alert rule.

Delete an alert rule

1. On the **Management** menu, click **Alert Management** to display the **Alert Management** dialog box.
2. Select the rule to delete, and click **Delete**.
3. Click **Yes** to confirm the deletion.

   The rule is removed from the **Alert Management** dialog box.

Types of Vision Alert Rules

When you define alert rules in Vision, you must select the type of rule to define. When you select the type of rule, you need to set up specific parameters to apply to the rule.

Rule types vary depending on the device.

Rule Type	Alert Trigger	Parameters
Device Status	An alert is sent when the device status changes, for example, from green to red.	Use the **From** and **To** lists to specify the change in status that triggers the alert.
Replication Status	(DXi devices only) An alert is sent when the replication status of the device changes, for example, from success to failure.	Use the **From** and **To** lists to specify the change in status that triggers the alert.
Disk Threshold	(DXi devices only) An alert is sent when used disk capacity rises above or falls below the specified percentage.	In the **Threshold** list, select **Above** or **Below**, and then enter a threshold percentage in the box. **Example** To send an alert when the used disk capacity level rises above 80%, select **Above** in the list and enter **80** in the box.
After Reduction	(DXi devices only) An alert is sent when the size of all deduplicated, compressed data stored on the DXi rises above the specified threshold value.	In the **Above** box, specify the threshold value in GB.
Total Reduction Ratio	(DXi devices only) An alert is sent when the total reduction ratio on the DXi falls below the specified threshold value.	In the **Below** box, specify the threshold value as a multiple.
Space Reclamation Duration	(DXi devices only) An alert is sent when the duration of space reclamation activity on the DXi exceeds the specified threshold value.	In the **Above** box, specify the threshold value in **Minutes**, **Hours**, or **Days**.
SNMP Trap	An alert is sent when an SNMP trap is received from the device.	(Optional) In the **OID** box, enter the object identifier (OID) for the trap. Enter an OID to filter traps for a specific component. (Optional) In the **Trap Value** box, enter a value to filter traps for a specific trap value.

Manage Devices in Vision

Use Vision's Device Management to do the following:

- View a list of all monitored devices, the current number of monitored devices, and the maximum number of monitored devices authorized by the installed licenses.
- Edit a device to change its properties, or to define user-access to the device.
- Remove a device from the list of monitored devices. After you delete a device, Vision no longer monitors it.

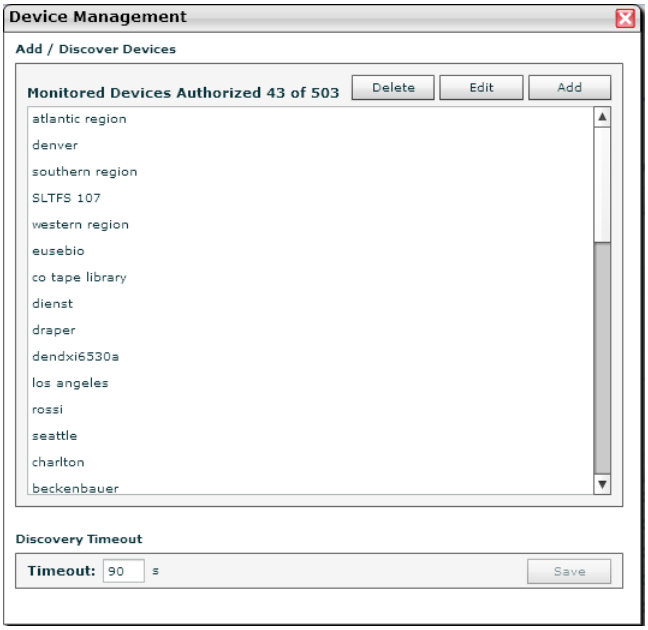
Prerequisites

- You must be an administrator to edit or delete a device.
- Your Vision system must discover devices before they appear in your Vision GUI. See Discover a Device in Vision on page 66.

View information about monitored devices

1. On the **Management** menu, click **Device Management** to display the **Device Management** dialog box.

Figure 53: Device Management Dialog Box



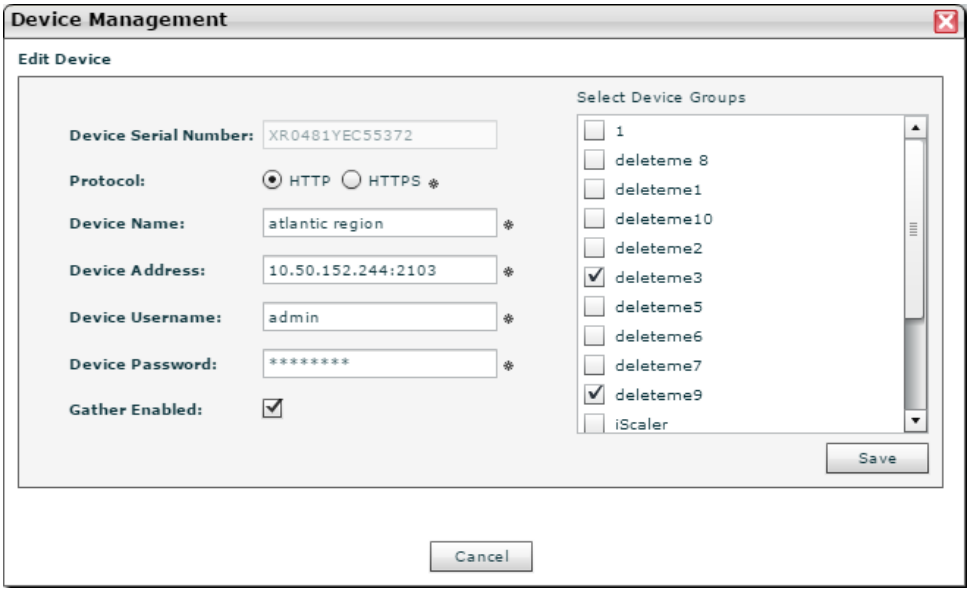
2. Review the following information.

Field	Description
Monitored Devices Authorized x of x	• The first number indicates the number of devices that Vision is currently monitoring, and the second number indicates the maximum number of monitored devices authorized by your installed licenses. • A scrolling list of the devices currently being monitored by Vision.
Discovery Timeout	The amount of time in seconds that a discovery process stops after a device is not discovered. **Change this amount of time** a. Highlight the number in the **Timeout** field. b. Enter a new time in seconds. c. Click **Save**.

Edit a device

1. On the **Management** menu, click **Device Management** to display the **Device Management** dialog box.
2. Select the device to which to make changes and click **Edit** to display the **Edit Device** dialog box.

Figure 54: Edit Device Dialog Box



3. In the **Protocol** field, edit whether the data collection path to the device is encrypted, as needed:
   - **HTTP** – Data collection path is not encrypted.
   - **HTTPS** – Data collection path is encrypted.

   Note: vmPRO appliances always use an encrypted protocol.
4. Edit additional information about the device, as needed. See Discover a Device in Vision below for more information.
5. Select the **Gather Enabled** check box to enable the gathering of status and configuration data from the device, as needed.
6. Click **Save** to save changes to the device, and to return to the **Device Management** dialog box.

Delete a device

1. On the **Management** menu, click **Device Management** to display the **Device Management** dialog box.
2. Select the device and click **Delete**.
3. Click **Yes** to confirm the deletion.
4. Click **OK** to remove the device from the **Device Management** dialog box.

Discover a Device in Vision

Before you can use Vision to monitor your devices, you must first run a process in which Vision discovers your supported Quantum devices: DXi devices, Q-Cloud Protect appliances, Scalar libraries, Scalar LTFS, and vmPRO. After the discovery process is complete, Vision begins to monitor the discovered devices.

Requirements

Make sure that the following requirements are met before discovering devices in Vision.

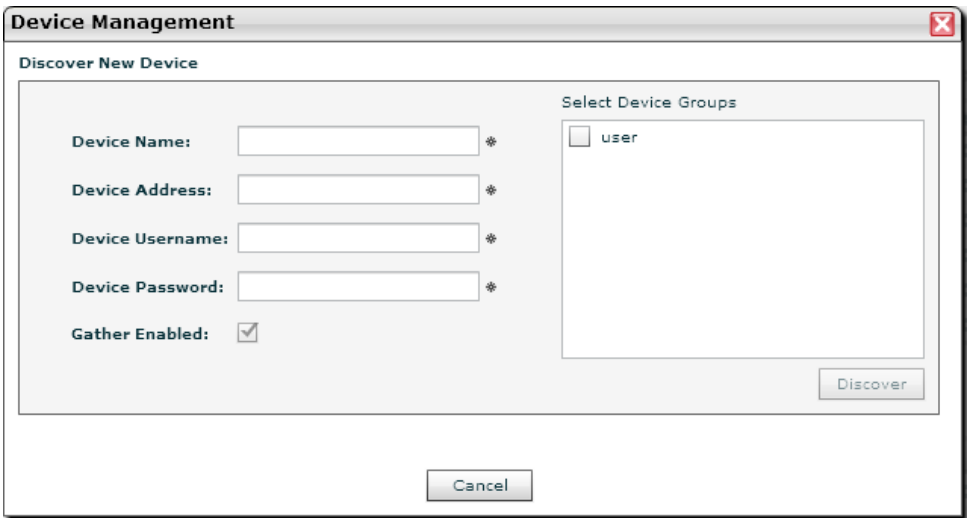
- Vision must be able to access devices over the network. Make sure to properly configure devices for Vision's access.
- Vision cannot discover devices if you are running Internet Explorer 8 on the same server where the Vision software is installed.

Discover a device

1. On the **Management** menu, click **Device Management** to display the **Device Management** dialog box.

2. Click **Add** to display the **Discover New Device** dialog box.

Figure 55: Discover New Device Dialog Box



3. In the **Device Name** field, enter a name with which to identify the device. This name displays on all status and report consoles.

   You can enter a device name that is up to 64 characters in length.

4. In the **Device Address** field, enter the device's IP address in IPv4 or IPv6 format.

> **Important**
>
> We strongly recommend using the device's IP address rather than its hostname. If you are entering a hostname, the Vision server must be running a name service that will resolve the hostname to an IP address.

5. In the **Device Username** and **Device Password** fields, enter the device's admin user name and password.

> **Important**
>
> When discovering Scalar tape libraries, you *must* enter **admin** as the Scalar library's admin user name.

6. Select the **Gather Enabled** check box to enable gathering of status and configuration data from the device.

   The **Gather Enabled** check box cannot be cleared during the discovery process.

7. In the **Select Device Groups** box, select the check box for each user group to which to assign the device.

   Users have access to devices to which their groups have been assigned. If the list is empty, user groups have not been defined. You can define user groups in Group Management, and then assign devices to groups. To define a user group, see Manage Groups in Vision below.

8. Click **Discover**, and then click **OK**.

   When the device is discovered, Vision adds it to the **Device Management** dialog box. It may take a few minutes for information about the new device to display in the **Devices** console.

Manage Groups in Vision

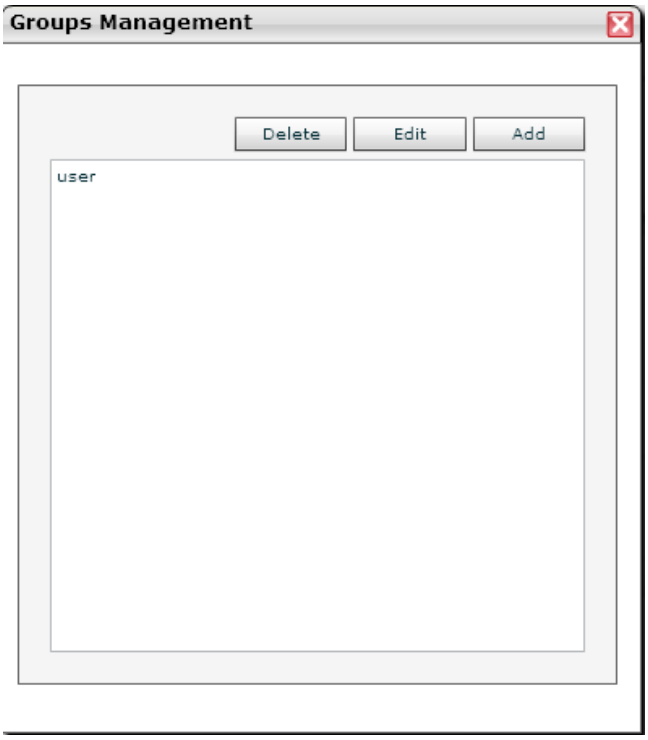
Use Vision Groups Management to define the devices that users can access. When you add a new group to Vision, you assign users and devices to that group. Users who are assigned to the group can access all devices that are also assigned to the group.

You must be an administrator to add, edit, or delete a group.

Add a group

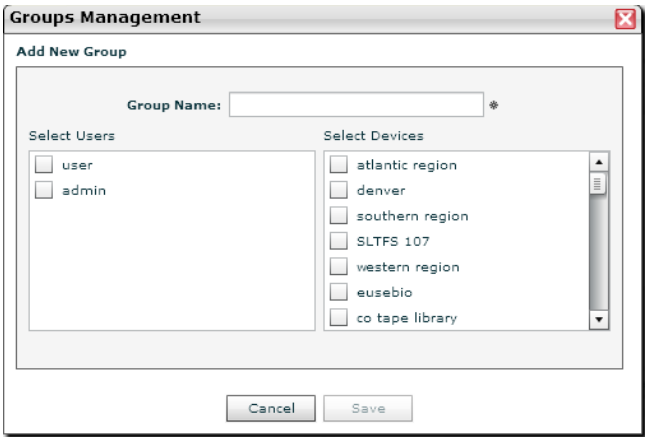
1. On the **Management** menu, click **Groups Management** to display the **Groups Management** dialog box.

Figure 56: Groups Management Dialog Box



2. Click **Add** to display the **Add New Group** dialog box.

Figure 57: Add New Group Dialog Box



3. In the **Group Name** field, enter a unique name to give the group.

   You can enter a group name that is up to 64 characters in length. Name the group carefully. After you create a group, you cannot change its name.

4. In the **Select Users** box, select the check box for each user to assign to the group, as needed.
5. In the **Select Devices** box, select the check box for each device to assign to the group, as needed.
6. Click **Save** to add the group to the **Groups Management** dialog box.

Edit Groups

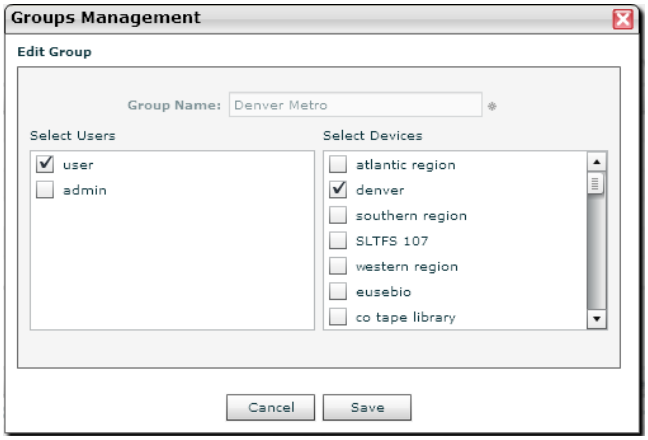
Edit existing groups to change user and device assignments.

When editing a group, keep in mind that you cannot change the group's name. If you need to change the group's name, you must first delete the group, and then re-add the group with the correct name.

Edit a group

1. On the **Management** menu, select **Groups Management** to display the **Groups Management** dialog box.
2. Select the group to edit, and click **Edit** to display the **Edit Group** dialog box.

Figure 58: Edit Group Dialog Box



3. In the **Select Users** box, edit the users assigned to the group, as needed.
4. In the **Select Devices** box, edit the devices assigned to the group, as needed.
5. Click **Save** to save changes to the group, and to return to the **Groups Management** dialog box.

Delete Groups

Delete a group to remove it from the **Groups Management** dialog box.

When you delete a group, users are no longer able to access the devices assigned to that group. Deleting a group does not delete the users or devices assigned to the group.

Delete a group

1. On the **Management** menu, click **Groups Management** to display the **Groups Management** dialog

box.

2. Select the group to edit, and click **Edit** to display the **Edit Group** dialog box.
3. Remove all users from the group, and click **Save** to save changes to the group.
4. Back on the **Groups Management** dialog box, select the group to delete and click **Delete**.
5. Click **Yes** to confirm the deletion and remove the group from the **Groups Management** dialog box.

Manage Users in Vision

To log on to Vision, a user enters their user name and password. The devices and features that are available to a user depend on the user's assigned Vision role.

Vision User Roles

The following user roles can be used in Vision:

Admin

Administrators have access to all devices. They can schedule reports, configure Vision, and manage users, groups, and devices. Multiple administrators can log on to Vision at the same time.

You must be an administrator to add, edit, or delete users.

User

Users have access to devices to which their groups have been assigned. Users can view information in Vision but cannot make changes.

Monitor

Monitors can view information in Vision but cannot make changes. Multiple users can log on as monitor at the same time. However, there is only one Monitor user account. To enable the Monitor user account, see Enable Vision Monitor Access on page 74.

Add Users

When you add users, you can specify the user role and assign the user to one or more groups. After you add the user, the user can log on to Vision with their user name and password.

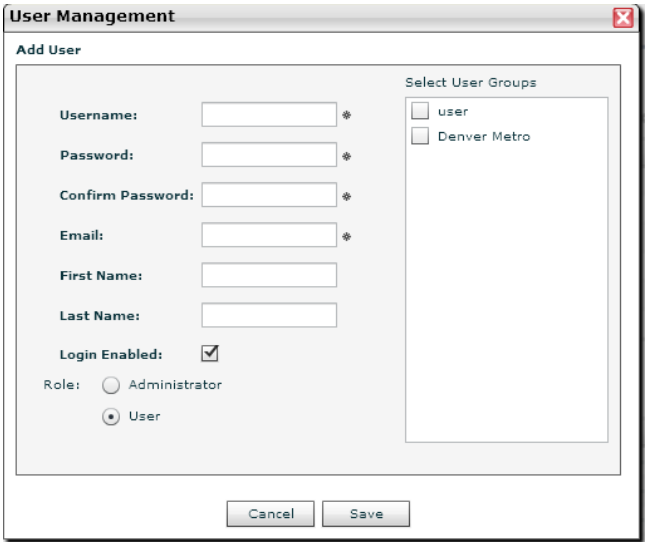
Add a user

1. On the **Management** menu, click **User Management** to display the **User Management** dialog box.

Figure 59: User Management Dialog Box

2. Click **Add** to display the **Add User** dialog box.

Figure 60: Add User Dialog Box



3. Enter information about the user in the following fields:

Field	Description
Username	Enter a unique user name. The user enters this user name to log on to Vision. You can enter a user name that is up to 64 characters in length.
Password	Enter a password for the user name. The user enters this password to log on to Vision.
Confirm Password	Re-enter the password to confirm that you have entered it correctly.
Email	Enter the user's email address. Vision uses this email address to send alerts to the user.
First Name	Enter the user's first name, as needed.
Last Name	Enter the user's last name, as needed.

4. Make sure that the **Login Enabled** check box is selected so enable the user to log on to Vision.
5. In the **Role** field, select the role to assign to the user. See Vision User Roles on page 71.
6. In the **Select User Groups** field, select the check box next to each group to which to assign the user, as needed.
7. Click **Save** to save the new user. The user is added to the **User Management** dialog box.

Edit Users

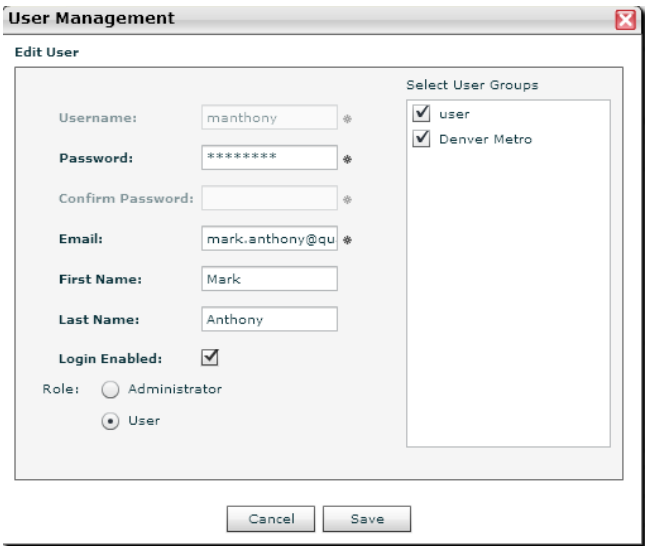
Edit an existing user to change the user's user name, e-mail, name, roles, or groups. You can also enable or disable login access and change the user's password.

Edit a user

1. On the **Management** menu, click **User Management** to display the **User Management** dialog box.

2. Select the user to edit, and click **Edit** to display the **Edit User** dialog box.

Figure 61: Edit User Dialog Box



3. Edit the user's information, as needed. See Add a user on page 71.

   You cannot change the user name when you edit a user. If you need to change the user name, first delete the user and then add a new user with the correct name.

4. Click **Save** to save the updates and return to the **User Management** dialog box.

Delete Users

Remove a user so that they can no longer log on to Vision.

Delete a user

1. On the **Management** menu, click **User Management** to display the **User Management** dialog box.
2. Select the user to delete, and click **Delete**.
3. Click **Yes** to confirm the deletion and remove the user from the **User Management** dialog box.

Enable Vision Monitor Access

Enable Monitor Account Access to allow users to log on to Vision as a monitor. A monitor can view information but cannot make changes. Monitor access is enabled by default.

Note: To log onto Vision as a monitor, enter **monitor** for both the user name and password on the **Login** page.

Enable Monitor account access

1. On the **Vision Configuration** menu, click **Authentication** to display the **Vision Authentication Configuration** dialog box.
2. In the **Monitoring** pane, select the **Enabled Monitor Account Access** check box to enable monitor access to Vision.
3. Click **Save**.

Associate Users with Devices

You can associate users with devices through Groups Management *or* LDAP authentication services.

Associate users and devices with Groups Management

1. In Groups Management, create a group to use in associating users and devices. See Manage Groups in Vision on page 68.
2. Assign the users and devices to associate with each other to the new group.

Associate users with devices using LDAP

1. Define the LDAP group to which a user belongs.
   a. In User Management, assign a Vision role to the user. See Manage Users in Vision on page 71.
   b. in Vision Authentication Configuration, assign the same Vision role to the LDAP group. See Configure LDAP Directory Services for Vision on the next page.

      Because the user belongs to the Vision role assigned to the LDAP group, the user now has all authorizations associated with the LDAP group.
2. Associate devices with the LDAP group to which the user is assigned.
   a. In Groups Management, create a group that uses the same name as the LDAP group, but use all upper-case characters. See Manage Groups in Vision on page 68.

      Example

      If LDAP assigns a group name of **SysAdmin**, you need to create a group in Group Maintenance with a name of **SYSADMIN**.

   b. Assign devices to the new group. See Manage Groups in Vision on page 68.

      The user and devices are now associated because the devices and user are assigned to the same LDAP group.

Vision Authentication Configuration

You can configure Vision to authenticate users with a Lightweight Directory Access Protocol (LDAP) directory service, such as Microsoft Active Directory (AD) or OpenLDAP.

By configuring Vision authentication, you accomplish the following:

- Authenticate user access to Vision.

  When users log into Vision, user authentication validates the login credentials with LDAP directory services.

- Assign Vision roles to users.

  Vision roles determine both the applications that users can access and the actions that users can perform within the applications. You can assign either Administrator or User roles. See Vision User Roles on page 71.

For help with configuring Vision authentication, see Configure LDAP Directory Services for Vision below

Vision Limitations with AD

Due to implementation limitations, an AD user's Primary Group as specified by the user's PrimaryGroupID is NOT consulted for Vision privileges.

Configure LDAP Directory Services for Vision

To configure LDAP directory services for Vision, do the following:

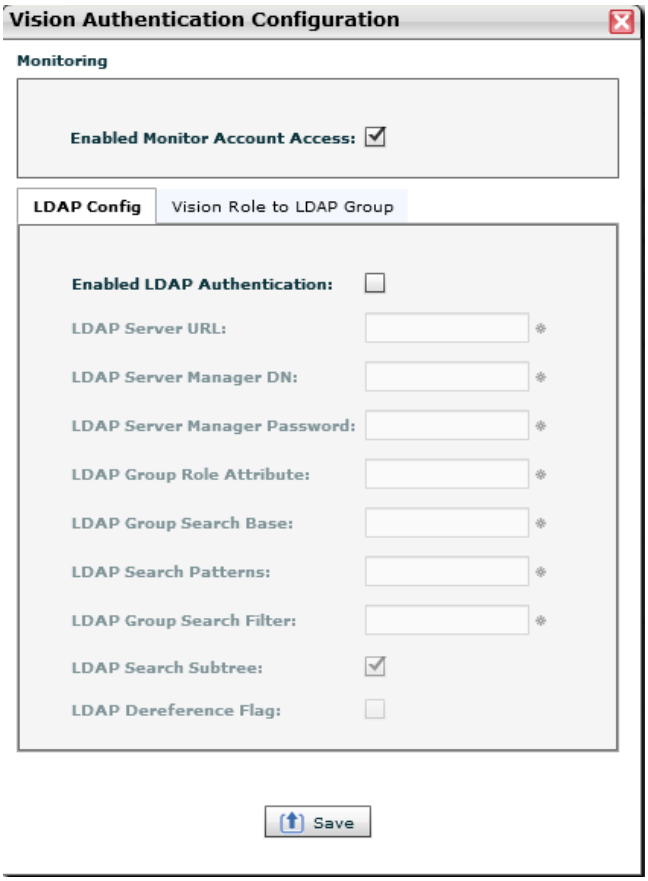
- Enable Vision to access the LDAP server.
- Define attributes with which to authenticate users.
- Associate LDAP groups with Vision user roles.

  You can remove these associations, as needed.

Enable LDAP authentication

1. On the **Vision Configuration** menu, select **Authentication** to display the **Vision Authentication Configuration** dialog box.

Figure 62: Vision Authentication Configuration Dialog Box



2. On the **LDAP Configuration** tab, select the **Enabled LDAP Authentication** check box to enable LDAP authentication.
3. Populate the following fields:

Field	Description
LDAP Server URL	Enter the URL of the LDAP server in the following format: **ldap://<server_ip | hostname>:<port>** **Example** ldap://10.10.10:389

Field	Description
LDAP Server Manager DN	Enter the distinguished name (DN) of a user with LDAP read access, such as your LDAP server administrator. **Example** cn=manager,dc=vision,dc=com
LDAP Server Manager Password	Enter the password that the LDAP server manager uses to access the LDAP authentication services.
LDAP Group Role Attribute	Enter the group role attribute of the LDAP server manager, typically **cn**.
LDAP Group Search Base	Enter the DN in the LDAP directory that contains the Vision group records with which to authenticate users. **Example** ou=groups,dc=vision,dc=com
LDAP Search Patterns	Enter the DN in the LDAP directory that contains the Vision user records with which to authenticate users. **Example** uid={0}, ou=user,dc=vision,dc=com
LDAP Group Search Filter	Enter the group organizational unit (OU) attribute that defines the groups of which the user is a member. **Example** memberUid={0}

4. Leave the **LDAP Search Subtree** check box selected to search for groups in all subtrees under the OU specified by the **LDAP Group Search Base** value.

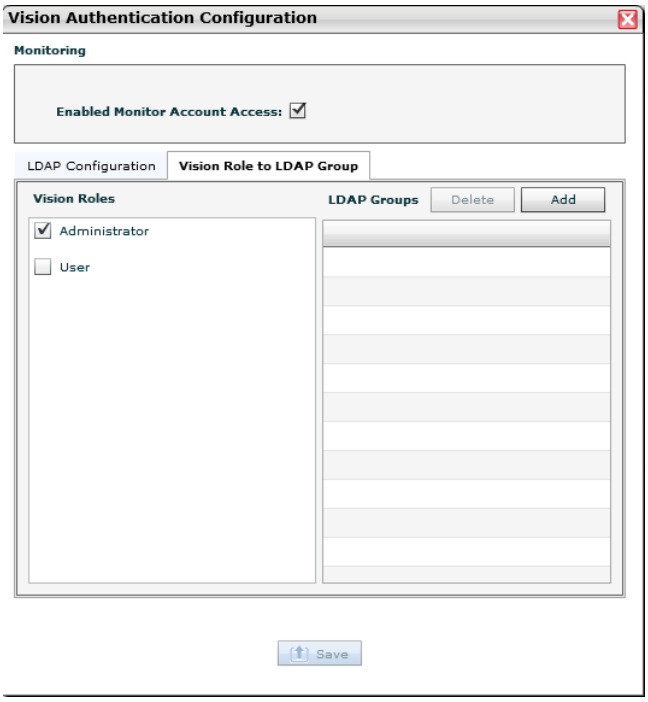
Note: The **LDAP DereferenceFlag** is not used at this time.

5. Click **Save** to save the authentication settings.

Associate an LDAP group with a Vision user role

1. On the **Vision Authentication Configuration** dialog box, select the **Vision Role to LDAP Group** tab.

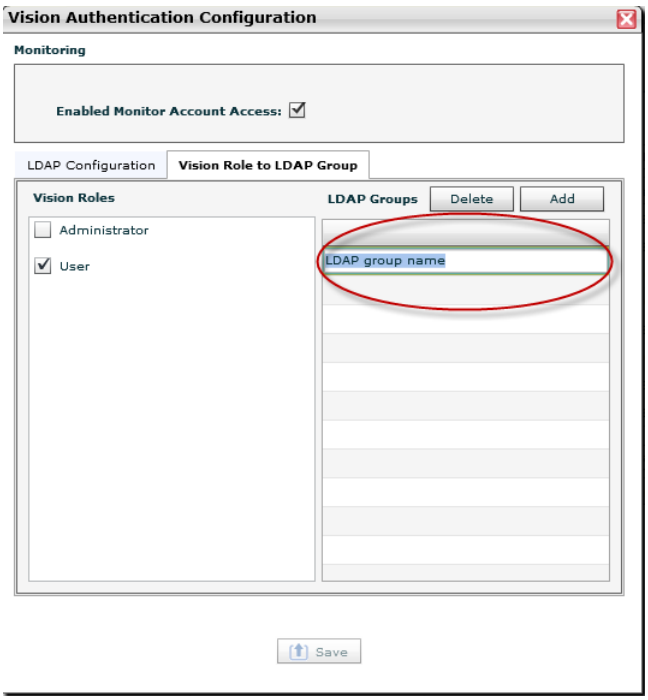
Figure 63: Vision Role to LDAP Group Tab



2. In the **Vision Roles** pane, select the appropriate role, either **Administrator** or **User**, to associate with the LDAP group.

3. In the **LDAP Groups** pane, select **Add** to display a text box in which to enter the LDAP group.

Figure 64: LDAP Groups Pane



4. In the **LDAP Group Name** text box, enter the name of the LDAP group to associate with the selected Vision role.
5. Click **Save** to save the settings and return to the **LDAP Configuration** tab of the dialog box.

Delete an LDAP group association

1. In the **Vision Authentication Configuration** dialog box, select the **Vision Role to LDAP Group** tab.
2. In the **LDAP Groups** pane, select the LDAP group association to delete.
3. Click **Delete** and then click **Yes** to delete the association.

Configure Data Collection in Vision

Use Data Collection Configuration to define the frequency at which Vision collects status and reporting data from monitored devices, and to configure maintenance settings for your Vision database, as needed.

Note: You must be an administrator to configure data collection settings.

Default Vision Database Maintenance Settings

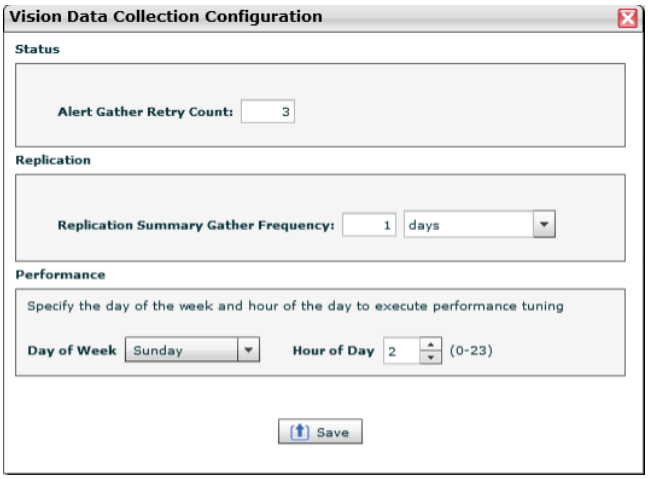
Default Vision database maintenance runs each day at 2:00 a.m. server time. This default maintenance typically takes less than 5 minutes to run.

If you have upgraded to Vision 4.2 and have old data in your database, it can take up to 4 hours for the database maintenance to complete. When the old data expires, the database maintenance will take 5 minutes or less each week.

Configure data collection settings

1. On the **Vision Configuration** menu, select **Data Collection** to display the **Vision Data Collection Configuration** dialog box.

   Figure 65: Vision Data Collection Configuration dialog box

2. In the **Alert Gather Retry Count** field, enter the number of consecutive connection failures before Vision determines a device to be in *connection failed* status.
3. In the **Replication Summary Gather Frequency** field, enter the frequency at which you want Vision to collect DXi replication data:
   a. In the box, enter the number of hours or days to define the frequency that collection occurs.
   b. From the drop-down list, select either **hours** or **days**.

   Note: Replication data includes statistics for namespace, source, and target replication. Access this information in replication reports. See Replication and Chargeback Usage Reports on page 128.

4. In the **Performance** pane, define performance tuning (database maintenance) settings:
   a. In the Day of Week field, enter the day of the week on which to perform database maintenance.
   b. Hour of Day, enter the time of day to begin database maintenance based on a 24-hour configuration.

Example

To begin database maintenance at 12:00 AM, enter **0**. To begin database maintenance at 11:00 PM, enter **23**.

Caution: During this time frame, all Vision features will be unavailable. We recommend setting your Performance Tuning schedule to be during off-hours to avoid negatively impacting work schedules.

5. Click **Save** to save your settings.

Configure Data Expiration Settings in Vision

Use Data Expiration Configuration to define the amount of time that Vision retains data collected from monitored devices. Any data that is older than a specified age is expired and removed from the Vision database, and this information is no longer available for reporting.

When configuring data-retention time periods, keep in mind that aggregated values are retained in the Vision database for a predefined time:

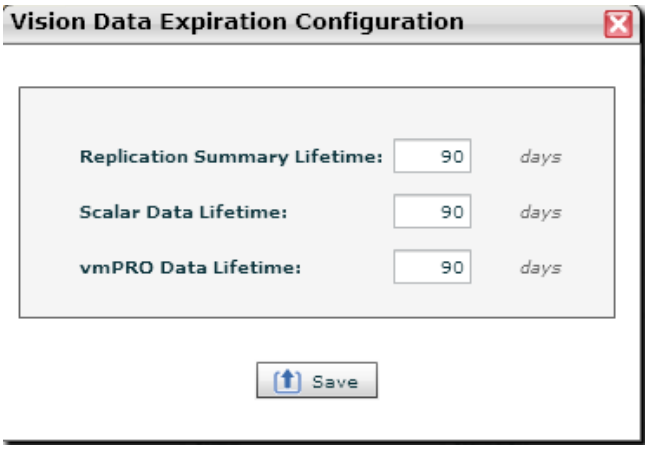
- 15 minute values are retained for 6 months
- 1 hour values are retained for 12 months
- 1 day values are retained for 18 months

Note: You must be an administrator to configure data expiration settings.

Configure data expiration settings

1. On the **Vision Configuration** menu, click **Data Expiration** to display the **Vision Data Expiration Configuration** dialog box.

Figure 66: Vision Data Expiration Configuration Dialog Box



2. Define data expiration values for the following, as needed:
   - In the **Replication Summary Lifetime** field, enter the number of days to retain replication summary values.
   - In the **Scalar Data Lifetime** field, enter the number of days to retain Scalar library data.
   - In the **vmPRO Value Lifetime** field, enter the number of days to retain vmPRO values.
3. Click **Save** to save the settings.

Configure Email Server Settings in Vision

For the Vision server to send email notifications and reports, you must first configure the following settings:

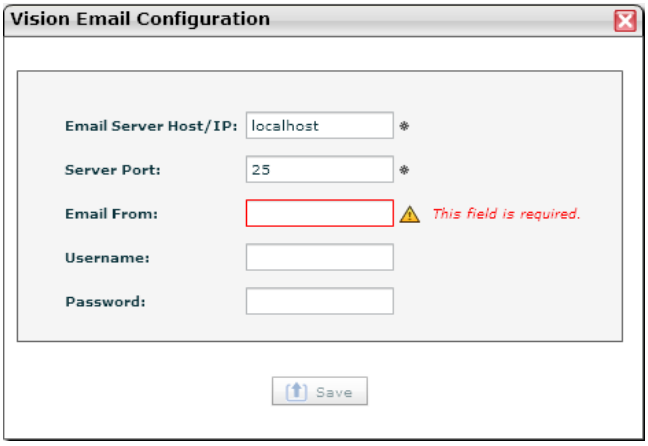
- Email server IP address or hostname
- Email server TCP port numbers
- Email server user name and password
- Vision server email address

Note: You must be an administrator to configure email server settings.

Configure email server settings

1. On the **Vision Configuration** menu, click **Email** to display the **Vision Email Configuration** dialog box.

Figure 67: Vision Email Configuration Dialog Box



2. In the **Email Server Host/IP** field, enter the hostname or IP address of the email server.
3. In the **Server Port** field, enter the TCP port number of the email server. The default value is **25**.
4. In the **Email From** field, enter the email address that appears in the **From** field of emails sent by Vision.
5. In the **Username** field, enter the server user name if the email server uses authentication.
6. In the **Password** field, enter the server password if the email server uses authentication.
7. Click **Save** to save settings.

Add a New Vision License

The temporary license installed with Vision authorizes you to monitor up to 3 devices for up to 60 days. To monitor more devices, or to use Vision for more than 60 days, you must add a permanent license.

To add a license to Vision, contact your Quantum Sales representative for information about purchasing a license. After you receive the License Certificate, perform the following tasks to obtain a license key — required to monitor additional devices — and add it to Vision.

Prerequisites

Before obtaining a license key, make sure you have the following items:

- Vision serial number
- Vision authorization code
- Vision Media Access Control (MAC) address

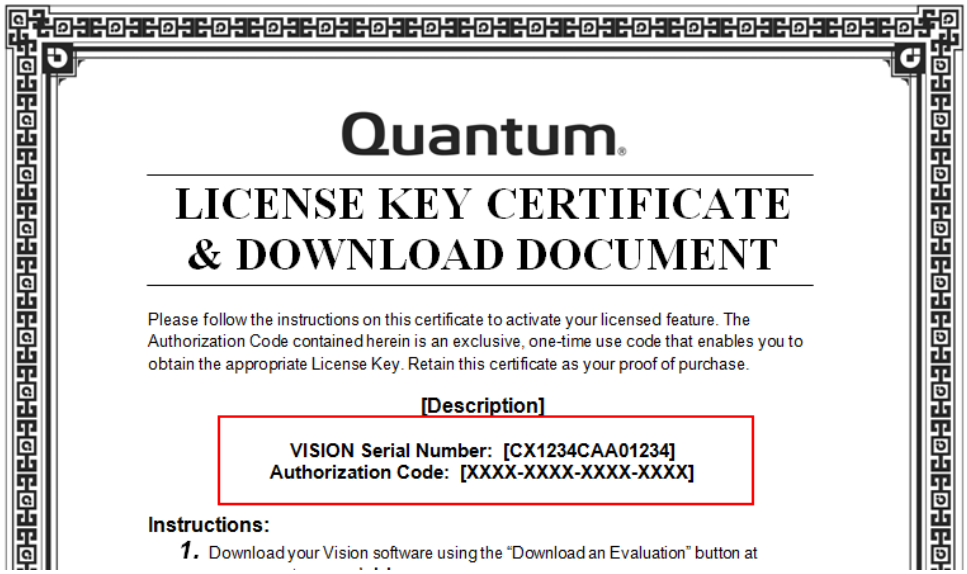
Gather required information

1. Locate your Vision software serial number and authorization code by doing one of the following:

If you download your Vision software

A copy of your *License Key Certificate & Download Document* is emailed to you. Your Vision software serial number and authorization code are located in this document.

Figure 68: License Key Certificate and Download Document


Quantum.

LICENSE KEY CERTIFICATE
& DOWNLOAD DOCUMENT

Please follow the instructions on this certificate to activate your licensed feature. The Authorization Code contained herein is an exclusive, one-time use code that enables you to obtain the appropriate License Key. Retain this certificate as your proof of purchase.

[Description]

VISION Serial Number: [CX1234CAA01234]
Authorization Code: [XXXX-XXXX-XXXX-XXXX]

Instructions:

1. Download your Vision software using the "Download an Evaluation" button at

If you requested a Vision Media Kit

The serial number is located on the back of the Vision installation disk sleeve. The authorization code is located on the License Key Certificate that is included in your media kit.

Figure 69: Vision Installation Disk Sleeve

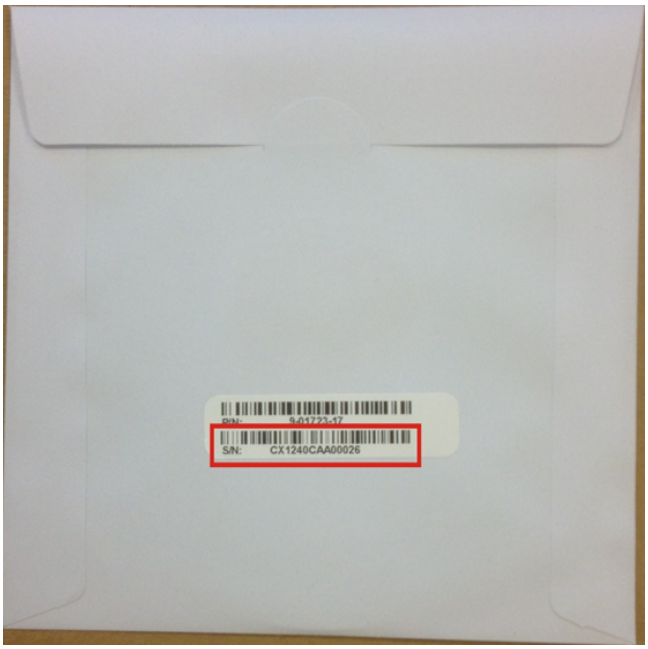
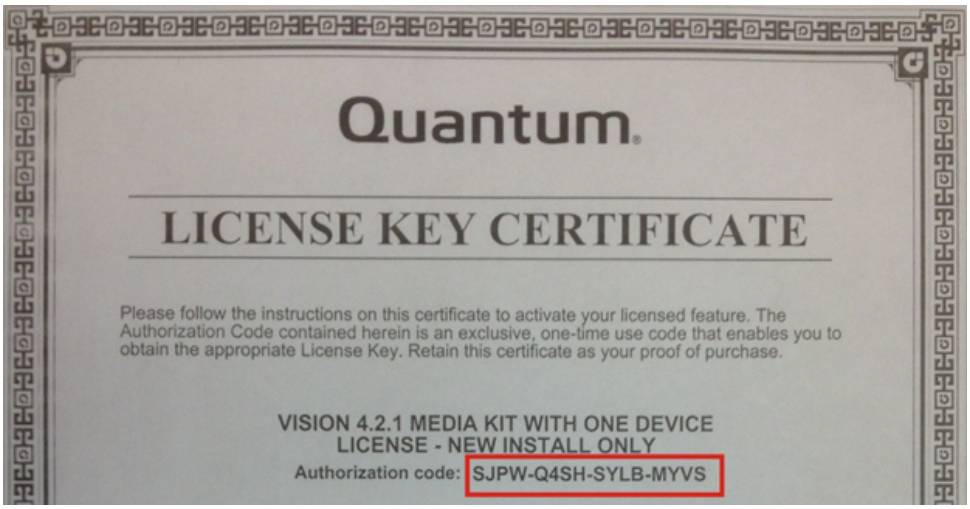


Figure 70: License Key Certificate



Note: Be sure to record/keep your serial number for future use and upgrades.

2. Locate the MAC address of the Vision server.

Steps

a. On the **Vision Configuration** menu, click **Licensing** to display the **Vision License**

Configuration dialog box.
The MAC address appears in the **Mac** field.

b. Click (located at the upper left of the table), and then click **Text** to export the MAC address to a text file.

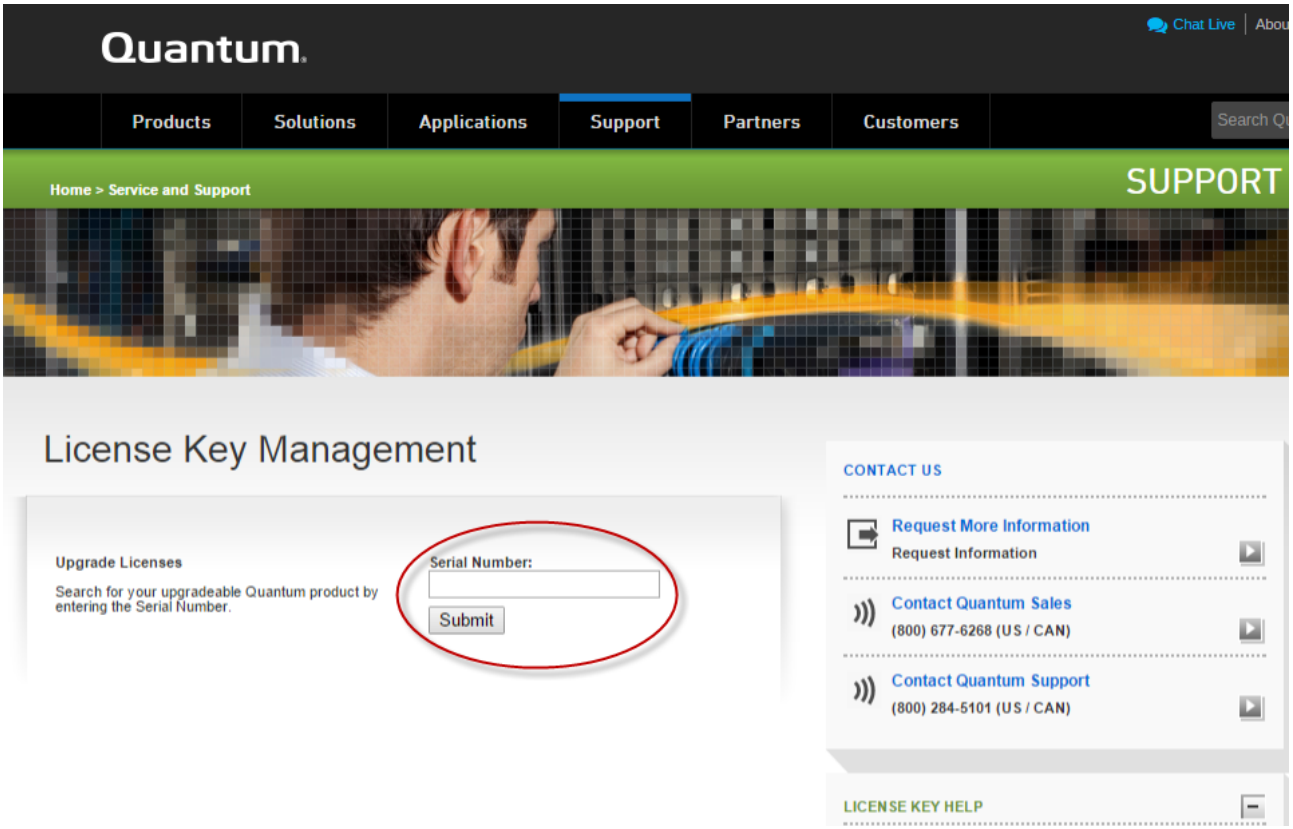
c. Select a location to save the file, enter a name for the file, and click **Save**.

When you perform the following task, you can copy and paste the MAC address from this text file instead of typing it.

Obtain a license key

1. From a Web browser with Internet access, navigate to http://www.quantum.com/licensekeys to display the **License Key Management** page.

Figure 71: License Key Management Page



2. In the **Serial Number** field, enter your Vision software serial number and click **Submit** to display the **Enter MAC Address** page.
3. Enter the MAC address of the Vision server and click **Submit** to display the **Licensed Feature** page.

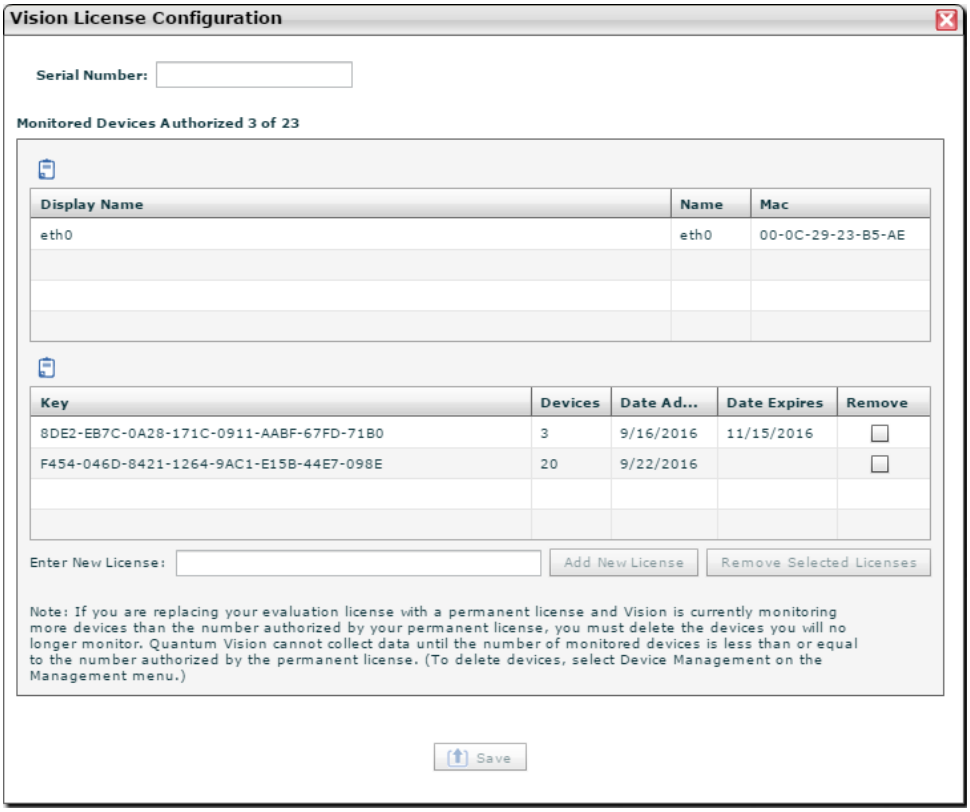
The serial number is now associated with the MAC address of your Vision server. In the future, you will only need to enter the serial number when adding additional licenses.

4. Enter the authorization code and click **Get License Key**. The **License Feature** page returns a license key.
5. Record or save the license key to a text file.
6. If you are adding multiple licenses, repeat steps 4-5 for each license certificate.

Enter the license key in Vision

1. On the Vision GUI's **Configuration** menu, click **Licensing** to display the **Vision License Configuration** dialog box.

Figure 72: Vision License Configuration Dialog Box



2. In the (optional) **Serial Number** field, enter your Vision serial number for future reference.
3. In the **Enter New License** field, enter the license key.
4. Click **Add New License** to add the license to your Vision server.
5. Repeat steps 2-3 if you are adding multiple licenses.

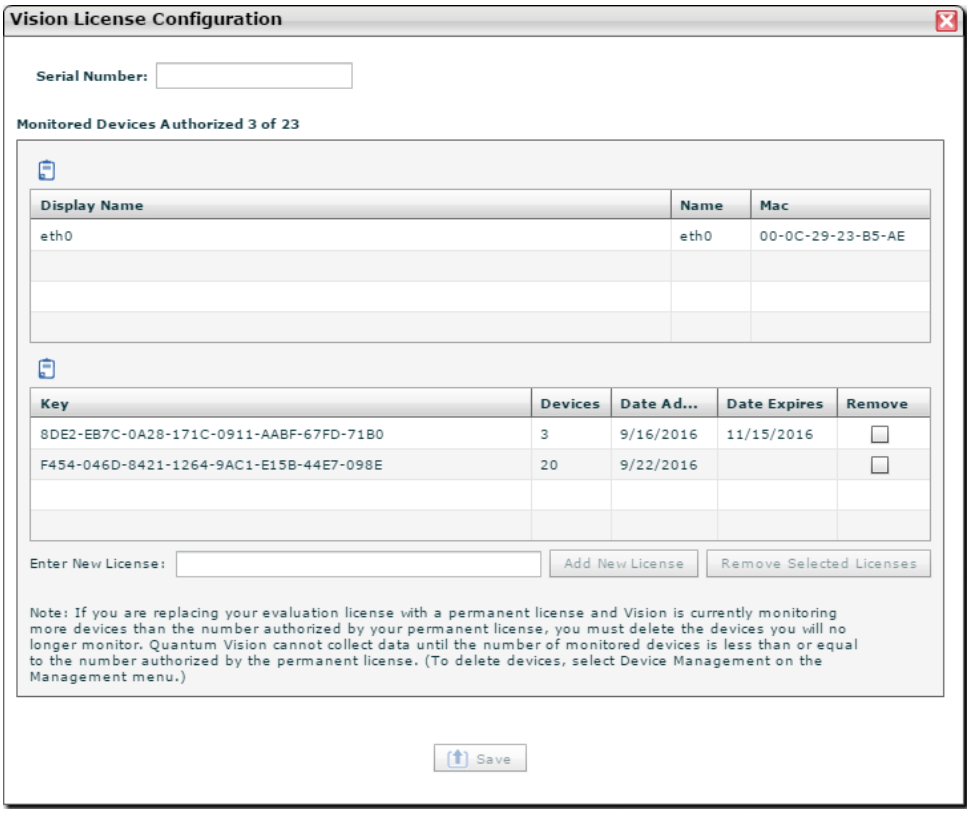
View Licenses Already Installed in Your Vision Server

Use the **Vision License Configuration** dialog box to view information about your licenses installed on the Vision server.

View installed Vision licenses

1. On the **Vision Configuration** menu, click **Licensing** to display the **Vision License Configuration** dialog box.

Figure 73: Vision License Configuration Dialog Box



2. Review the following information:

Field	Description
Monitored Devices Authorized X of Y	The current and maximum amount of monitored devices. The maximum number of devices Vision can monitor is based on all currently added licenses. If the current number of monitored devices equals the maximum number of devices, delete an existing device before adding a new device.

Field	Description
Display Name	The display name of the network interface card (NIC) on the Vision Enterprise Server.
Name	The name of the NIC on the Vision Enterprise Server.
Mac	The Media Access Control (MAC) address of the NIC on the Vision Enterprise Server.
Key	The license key.
Devices	The number of monitored devices allowed by the license.
Date Added	The date the license was added to the Vision server.
Date Expires	The date the license expires.
Remove	If selected, the license will be removed from the Vision server when the **Remove Selected Licenses** button is clicked. Only administrators can remove licenses from the Vision server.

Delete a License from the Vision Server

If you purchase a permanent license, you can delete the evaluation license to stop the server from warning you that the evaluation license will expire.

Important

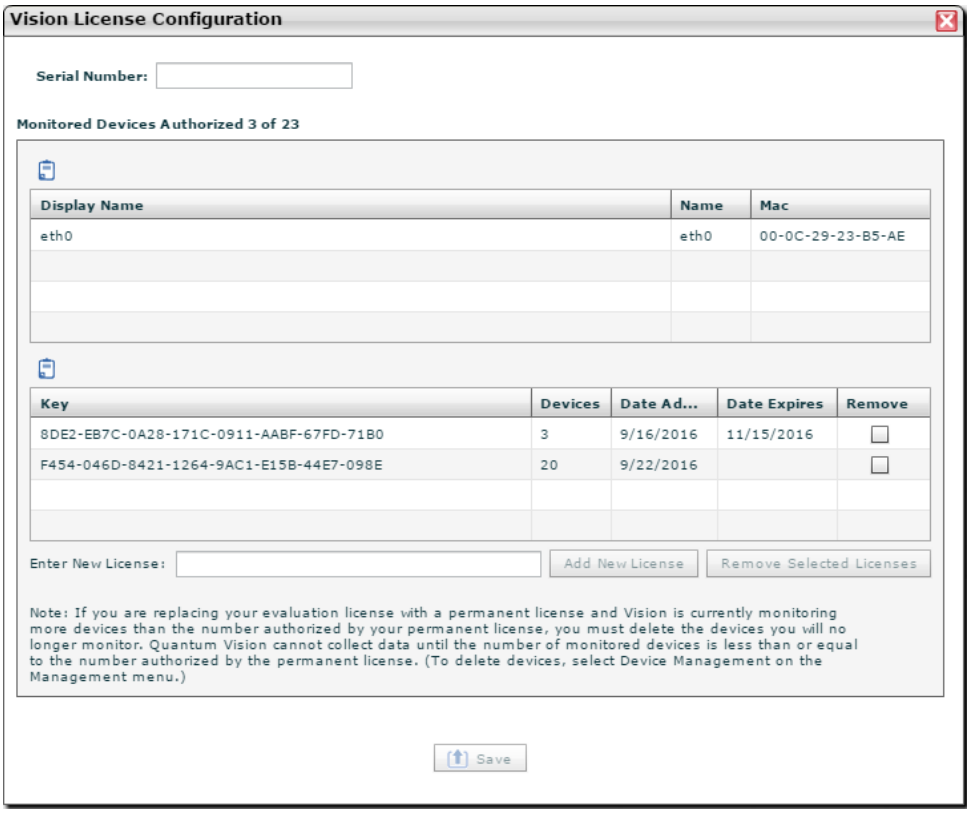
If you delete an evaluation license, you cannot re-enter it. Make sure that you have a permanent license for your Vision server before deleting an evaluation license.

If you inadvertently delete a permanent license, you can re-enter it in the **Vision License Configuration** dialog box.

Delete a license from the Vision server

1. On the **Vision Configuration** menu, click **Licensing** to display the **Vision License Configuration** dialog box.

Figure 74: Vision License Configuration Dialog Box



2. Select the **Remove** check box next to each license to delete.
3. Click the **Remove Selected Licenses** button to delete the selected licenses from the Vision server.

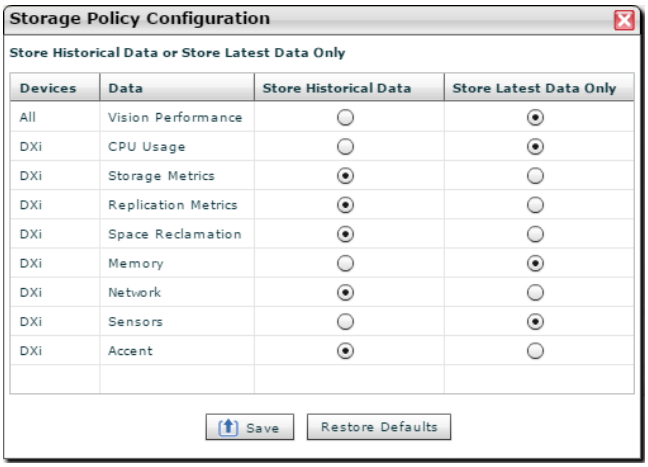
Configure Storage Policies in Vision

Use Vision's Storage Policy Configuration to improve performance and increase scalability by reducing the amount of data stored in the Vision database. With this application, you can define the type of data to include in Vision reporting and analytic results for devices and their specified data groups. The type of data can be either current and historical data, or current data only.

Configure Storage Policies

1. On the **Vision Configuration** menu, click **Storage Policy** to display the **Storage Policy Configuration** dialog box with Vision's default configuration.

Figure 75: Storage Policy Dialog Box



2. For each device and its associated data group, select one of the following data types to use in generating Vision reporting and analytic results:

   Store Historical Data

   Vision stores the latest data value with history for the device's specified data group.

   Store Latest Data Only

   Vision stores the latest data value only (without history) for the device's specified data group.

   Analytic results cannot be generated from the **Store Latest Data Only** selection.

3. Click **Save** to store the new configuration.

Additional Actions

- To return to the previous configuration, click **Cancel**.
- To return to Vision's default configuration, click **Restore Defaults**.

Storage Types for Data Groups

Vision's historical reports show changes in values over time. You can use this data to gain insight into trends or events, which in turn helps with capacity planning and overall troubleshooting.

Examples

- The DXi Percent Full history shows that the rate of disk usage on the DXi has increased, indicating the need to more closely monitor the amount of data being sent to the DXi.

- The Ethernet or Fibre Channel history shows a regular backup period when no data was coming into the DXi, indicating potential problems with the network or with the source of the expected data stream.

Data Types

Using Vision's Storage Policy Configuration, you can specify the type of data to store for a device's specified data groups, which in turn defines the types of reports that can be run for the device's data group.

Historical Data

Vision stores the latest data value with history for the device's specified data group, and runs historical reports for the data group.

Vision saves historical data in 15 minute, 1 hour, and 1 day aggregations for 6, 12, and 18 months, respectively.

Note: Aggregations contain minimum, maximum, and average values for the aggregation period.

Historical data is also used in the graphs in Vision's Analytics view.

Important

Historical reports require that the data group providing the report information is configured to **Store Historical Data**. If a data group is set to **Store Latest Data Only**, and a user attempts to generate a historical report on the data, Vision informs the user that it does not have sufficient data to generate the report.

Latest-only Data

Vision stores the latest data value only (without history) for the device's specified data group, and runs Latest-only Data reports for the data group.

Vision's Default Storage Configuration

The following default data storage policies should be optimal for most users. They provide improved performance and increased scalability by reducing the amount of data stored in the Vision database.

Storage Type	Data Type
Historical	Disk Usage (storage) Network Usage Replication Accent Deduplication

Storage Type	Data Type
Latest (Snapshot)	CPU Usage Memory Usage Internal sensors

Vision Historical Reports

The following table lists Vision Historical reports or Analytics graphs, and their data groups.

Historical Report/Analytics Graph	Data Group
All Percent Full History	DXi Storage Metrics for DXi 25/55 Storage Metrics
DXi Capacity Growth History	DXi Storage Metrics
DXi Ethernet Received History	DXi Network
DXi Ethernet Transmitted History	DXi Network
DXi Fibre Channel Transmitted History	DXi Network
DXi Space Reclamation History	DXi Space Reclamation
DXi CPU Usage History	DXi CPU Usage
DXi Deduplication History	DXi Storage Metrics
DXi Disk Usage History	DXi Storage Metrics
DXi Percent Full History	DXi Storage Metrics
DXi 35/55 Usage History	DXi 35/55 Storage Metrics
DXi 35/55 Replication History	DXi 35/55 Replication Metrics
DXi 35/55 Fans History	DXi 35/55 Sensors
DXi 35/55 Sensors History	DXi 35/55 Sensors
DXi 35/55 Percent Full History	DXi 35/55 Storage Metrics
Space Reclamation	DXi Space Reclamation
Disk Used by Reduced Data	DXi Storage Metrics

Configure Security Settings for Vision

Use the Vision's Security Configuration to define security and access settings for your Vision server.

Security Settings

HTTP and HTTPS Ports

Define HTTP and HTTPS ports for Windows and Linux installed Vision servers.

Important

- Do not configure ports for a Vision appliance on the **Network Ports** dialog box. Instead, log on to the Vision Console Command Line and run the **net ports** command. The **`net ports`** command opens the firewall and updates the ports. See Issue Network Commands on page 10.
- When changing your network ports, be sure to check your existing firewall configuration and make sure the appropriate firewall ports are open.

Access Control

For Vision to gather replication data for Q-Cloud Protect appliances or DXi devices running software versions 3.2 or later, it needs to identify itself through an SSH key pair.

Vision generates this key pair. The private key is Vision's secure identifier. The public key is shared with the Q-Cloud Protect appliance or DXi device. Vision has authorization to gather replication data only when the private and public keys match.

For more information about SSH key pair authentication, see one of the following:

- The Security topic in the DXi 6900 Documentation Center
- The Configuring Access Control topic in the Q-Cloud Protect Documentation Center

Important

If the private key is ever exposed, you can generate a new key pair from Vision. Keep in mind, though, that you must then distribute the new public key to all devices that currently use the old public key.

Configure Security Settings

1. On the **Vision Configuration** menu, click **Security** to display the **Security Configuration** dialog box.

Figure 76: Security Configuration Dialog Box

2. In the **HTTP** and **HTTPS** fields, enter the appropriate port numbers.

   The default ports are 80 for HTTP and 443 for HTTPS.

3. In the **Public Key** area, copy the text and paste it into the UI of the device from which Vision will gather replication data.

   For detailed instructions on pasting the public key in the device's UI, see the Security topic in the DXi 6900 Documentation Center or the Configuring Access Control topic in the Q-Cloud Protect Documentation Center.

   Important

   You can generate a new key pair by clicking **Generate New Key**, but you must then distribute the new public key to all devices that currently use the old public key.

4. Click **Save** to save your settings.
5. Restart the Vision service to apply the security settings.

Chapter 4: Device Consoles

This chapter contains the following topics:

Vision Device Consoles

Use the following Vision device console components to monitor your devices.

Devices Console

The Devices console displays all monitored Quantum devices. Use this console to do the following:

View the overall health and status of all monitored Quantum devices

The following color-coded icons display the status of a device:

- Indicates that all devices are operating correctly.
- Indicates that there is a problem with one or more devices.
- Indicates that there is a major problem with one of more devices.
- Indicates that Vision's connection with the device has failed.
- Indicates that the device is discovered but no data has been collected yet, or the status is unknown.

View and acknowledge alert notifications for devices

Alerts are notifications regarding the status of a device. Vision generates alert notifications based on alert rules defined in Alert Management. See Manage Alert Rules in Vision on page 59.

Schedule a Devices Inventory Report

The Devices Inventory report shows the information displayed on the Devices console and the Consolidated console. You can schedule this report to be generated and emailed to designated recipients.

Consolidated Consoles

The Consolidated consoles display all monitored Quantum devices organized by device families, along with information specific to the device family.

Example

The **DXi Devices Consolidated** console displays capacity usage data for the DXi devices and Q-Cloud Protect appliances.

Console Device Families

- DXi devices and Q-Cloud Protect appliances
- DXi 35/55 devices
- Scalar libraries
- vmPRO
- Scalar LTFS

Individual Device Consoles

Individual Device consoles display information for an individual device.

Example

The **DXi 6900 Device**console calculates and displays information about when the next capacity upgrade is required for the DXi device.

Note: To change the size of a pane on individual device consoles, drag the resize handle on the edge or the pane. When you log off and back onto Vision, the panes are reset to their default sizes.

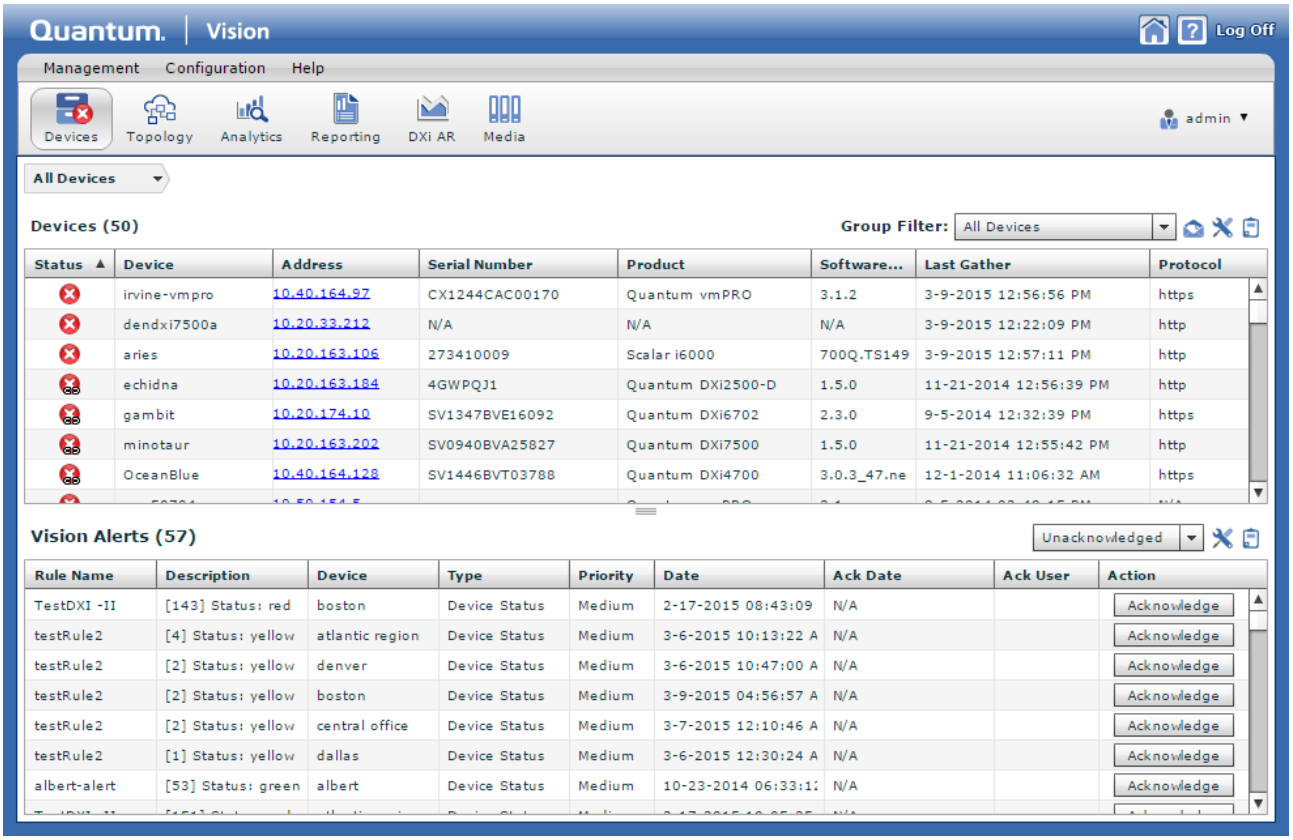
Navigate the Vision Devices Console

Use the Devices Console to monitor Quantum devices, manage alert notifications, and schedule a Devices Inventory report.

Navigate the Devices Console

1. Display the **Devices** console by doing one of the following:
   - On the Vision toolbar, click **Devices**.
   - At the top of the Vision window, click  .

Figure 77: Devices Console



2. In the **Group Filter** list, select a group for which to view information in the **Device Status** pane, as needed. The default is **All Devices**.
3. View the following information for each displayed device:

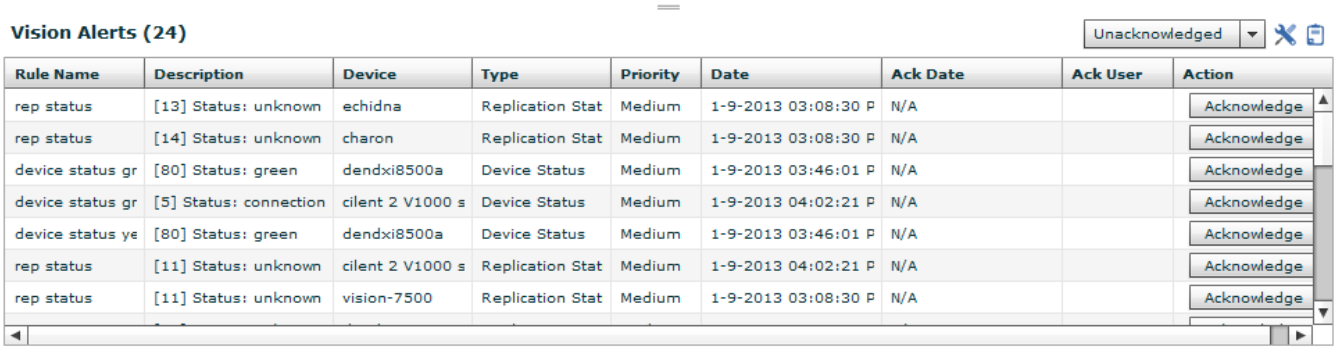
Column	Description
Status	The color-coded icon indicating the device's status.
Device	The name assigned to the device when it was discovered in Vision.
Address	The device's IP address or host name. Click the IP address or host name to launch the native management interface for the device.
Serial Number	The device's serial number.
Product	The Quantum product model name for the device.

Column	Description
Software Version	The current software version of the device.
Last Gather	The last time Vision communicated with the device.
Protocol	**The device's encryption protocol** • **http** – The data collection path to the device uses an unencrypted connection. • **https** – The data collection path to the device uses an encrypted connection. **Note:** The data collection path to vmPRO appliances is always encrypted.

Manage Vision Alert Notifications

Use the Alerts pane on Vision's Device and Consolidated consoles to view and acknowledge alert notifications. Vision generates alert notifications based on alert rules defined in Alert Management. See Manage Alert Rules in Vision on page 59.

Figure 78: Alert Pane on the Devices Console



View alert notifications for devices

1. On the **Device** or **Consolidated** console, review the following information in the **Vision Alerts** pane:

Column	Description
Rule Name	The alert rule defined in Alert Management for which the alert was generated. See Manage Alert Rules in Vision on page 59.
Description	The description of the alert rule.
Device	The device to which the alert notification applies.
Type	The type of alert rule.
Priority	The priority assigned to the alert rule.
Date	The date on which the alert notification was issued.
Ack Date	The date on which the alert was acknowledged. If the alert notification has not been acknowledged, **N/A** displays.
Ack User	The ID of the user who acknowledged the alert notification. If the alert notification has not been acknowledged, this column is left blank.
Action	The action taken to address the alert. If the alert notification has not been addressed, this column is left blank.

2. Perform the following actions, as needed:

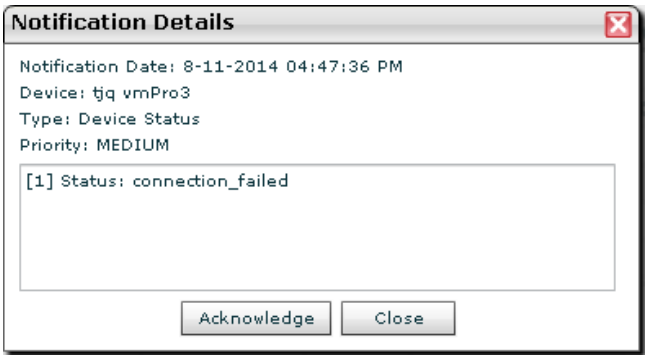
Select the type of notifications to display

From the drop-down list to the right of the **Vision Alerts** heading, select **Acknowledged**, **Unacknowledged**, or**ALL**.

Display the Notification Details dialog box

Double-click an alert to display information about the alert in the **Notification Details** dialog box.

Figure 79: Notification Details Dialog Box



Acknowledge alert notifications for devices

1. Select the alert notification to acknowledge.
2. Do one of the following:
   - Click **Acknowledge** in the **Action** column.
   - Double-click the alert notification to display the **Notification Details** dialog box, and then click **Acknowledge**.

   Vision marks the alert notification as acknowledged.

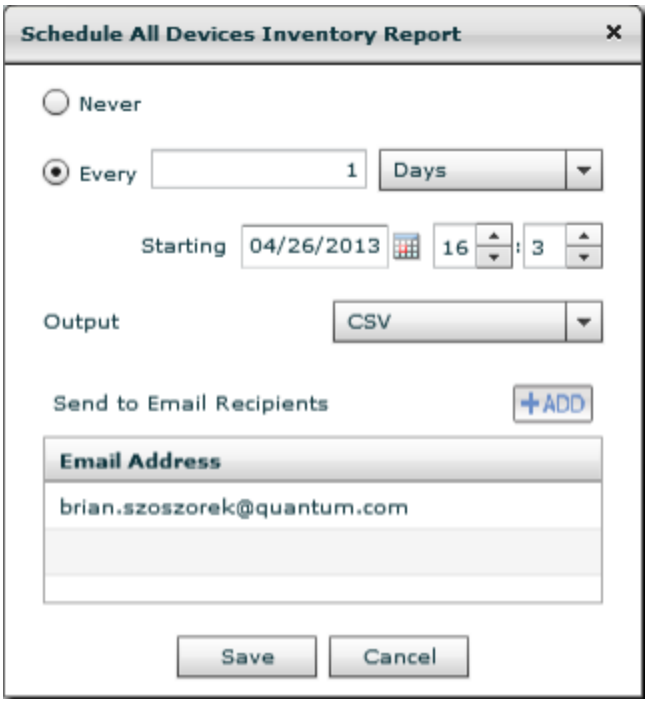
Schedule a Devices Inventory Report

The Devices Inventory report depicts the information displayed on the Device and Consolidated consoles. You can schedule this report to be generated and emailed to designated recipients.

Schedule a Devices Inventory Report

1. From the **Devices** or **Consolidated** console, click  to display the **Schedule <x> Inventory Report** dialog box.

Figure 80: Schedule <x> Inventory Report Dialog Box



2. Select the radio button next to the **Every** field.
3. In the **Every** field, enter the frequency for which to generate and email a report.
4. From the drop-down list, select the time interval to for which to generate and email the report: **Minutes**, **Hours**, **Days**, or **Months**.

Example

a. In the **Every** field, enter **3**.

b. From the drop-down list, select **Days**.

Vision generates and emails the report every three days.

5. In the **Starting** field, do the following:
   a. Click to select the date on which to generate and email the report.
   b. in the 9 : 56 6 fields, enter the time on which to generate and email the report.
6. In the **Output** field, enter the format in which to generate the report, either **XML**, **CSV**, or **Text**.
7. In the **Send to Email Recipients** field, click **Add** to display a **New Email** field in the **Email Address** box.

8. In the **New Email** field, enter the email address for the recipient to whom to email the report.
9. Repeat steps 7-8 for each email recipient.
10. Click **Save** to save the report schedule and exit the dialog box.

Device Configuration Files

You can access a device's current configuration files from the device console.

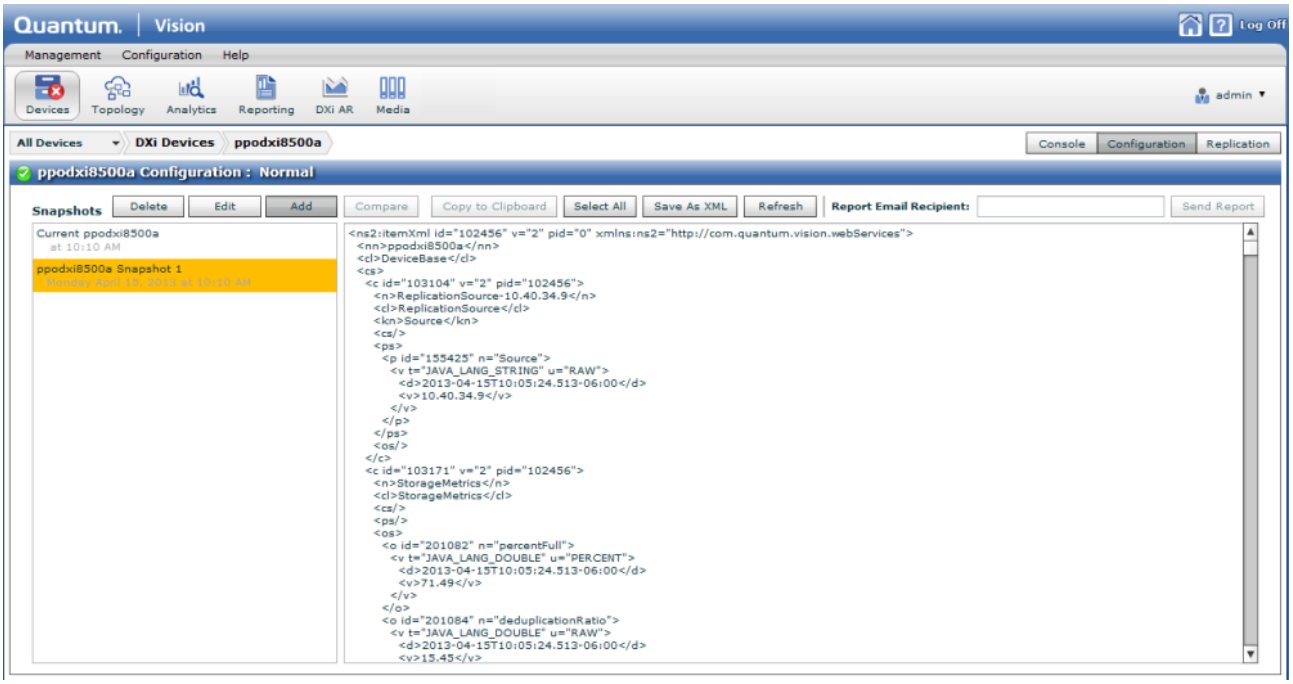
Use these files to capture snapshots of a device's configuration settings at a specific point in time. You can then use these snapshots to compare the device's current configuration settings with past configuration settings to potentially troubleshoot issues with a device.

Access a device's configuration settings

1. From a device's individual console, click the **Configuration** tab to display the **<Device> Configuration** console.
2. In the **Snapshots** pane, double-click a snapshot for which to view configuration settings.
   - To see the device's current configuration settings, double-click the snapshot at the top of the list.
   - To view the most up-to-date version of the configuration settings, click **Refresh**.

3. Review the configuration settings in the right pane of the console.

Figure 81: <Device> Configuration Console



Create a snapshot of a device's current configuration

1. In the **Snapshots** pane, select the current configuration snapshot.
2. Click **Add** to display the **Confirm Add Snapshot** dialog box.

Figure 82: Confirm Add Snapshot Dialog Box

3. In the **Snapshot Name** field, edit the name of the snapshot, as needed.
4. Click **Yes** to create the snapshot. The newly created snapshot displays in the **Snapshot** pane.

Compare snapshots

1. In the **Snapshot** pane, click the first snapshot to use in the comparison.
2. While holding down the **<Ctrl>** key (Windows or Linux) or the **<Command>** key (Mac), click a second snapshot to compare with the first snapshot.
3. Click **Compare** to display the comparison in the right pane.

   If there are not any differences between the two snapshots, the following message displays in the right pane:
   `There are no differences between these snapshots`
4. Expand the **Add**, **Changes**, and **Removes** folders in the displayed folder tree to view the differences between the snapshots.

Additional Functionality

The following table provides information about additional functionality available on the **<Device> Configuration Console**:

Button	Procedure
Delete	**Delete a snapshot** 1. Click the snapshot to delete. 2. Click **Delete**. 3. Click **Yes** to confirm the deletion of the snapshot.
Edit	**Edit the name of a snapshot** 1. Click the snapshot to edit. 2. Click **Edit** to display the **Confirm Edit Snapshot** dialog box. 3. In the **Snapshot Name** field, edit the name of the snapshot, as needed. 4. Click **Yes** to update the snapshot.
Copy to Clipboard	**Copy the configuration settings to another location** 1. Click the snapshot to copy. 2. Click **Select All** to select the configuration settings text. 3. Click **Copy to Clipboard** to copy the configuration settings text. 4. Paste the copied text into another document.

Button	Procedure
Save As XML	**Save the configuration XML as an XML-formatted file** 1. Click the snapshot to save. 2. Click **Save As XML** to display the **Save As** window. 3. In the **Save As** window, browse to the location in which to save the XML-formatted file. 4. In the **File name** field, enter a name for the XML-formatted file. 5. Click **Save** to save the XML-formatted file.
Send Report	**Send a copy of the configuration settings in an email** 1. Click the snapshot to email. 2. In the **Report Email Recipient** field, enter the email address of the recipient of the email. 3. Click **Send Report**.

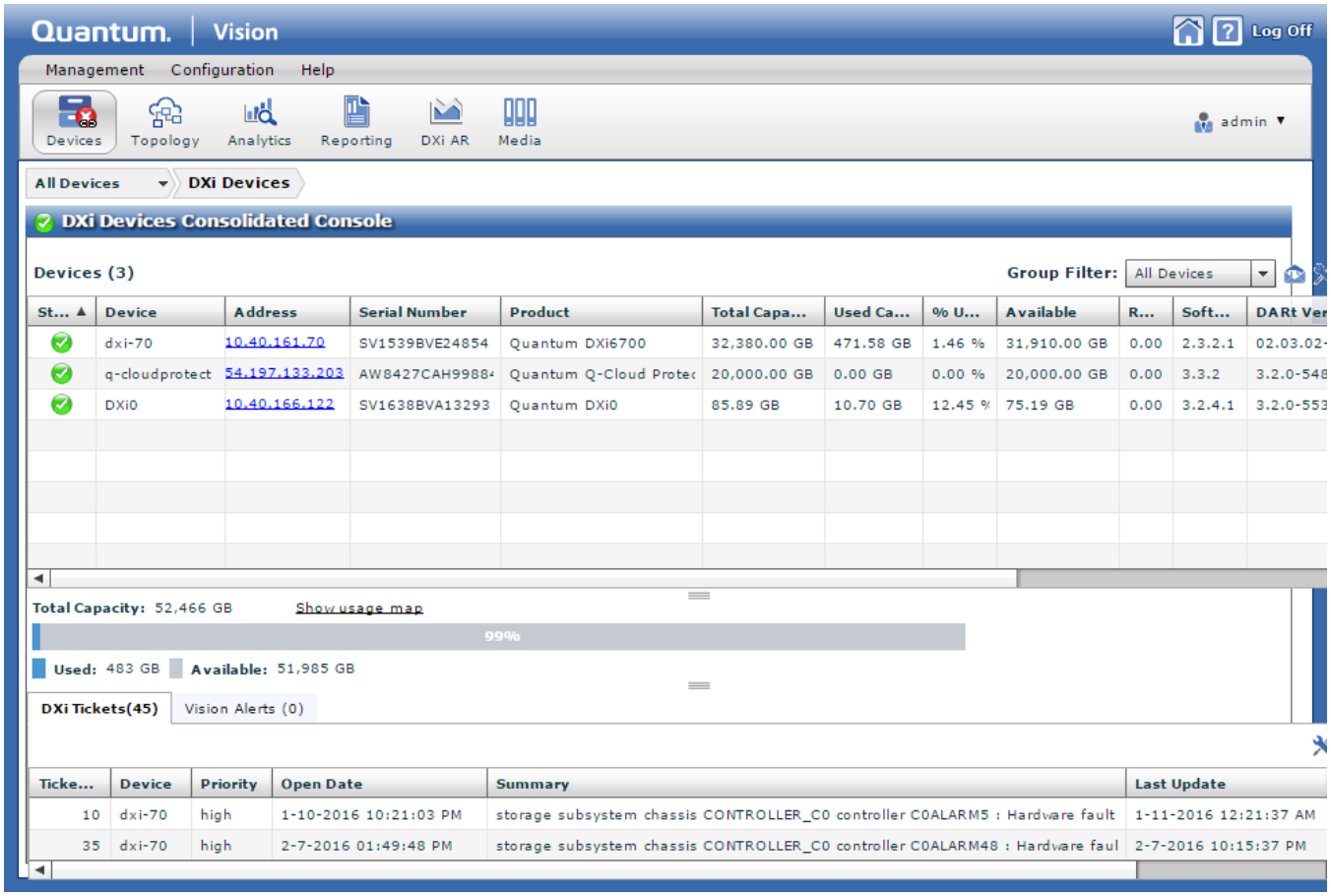
DXi Device Consoles

To monitor DXi devices or Q-Cloud Protect appliances in Vision, you can use the following consoles in addition to the main Vision Device console. From these consoles, you can view information, manage alerts, and calculate capacity upgrade estimates for your DXi devices and Q-Cloud Protect appliances. You can also view replication reports and chargeback data.

DXi Devices Consolidated Console

Use to monitor devices with the DXi Devices group, which includes Q-Cloud Protect appliances. See Navigate the DXi Devices Consolidated Console on page 111.

Figure 83: DXi Devices Consolidated Console



DXi Device Console

Use to monitor and manage an individual DXi device or Q-Cloud Protect appliance. From this console you can also calculate capacity upgrade estimates, and view replication reports and chargeback data. See Navigate an Individual DXi Device Console on page 114.

Figure 84: DXi Device Console – DXi

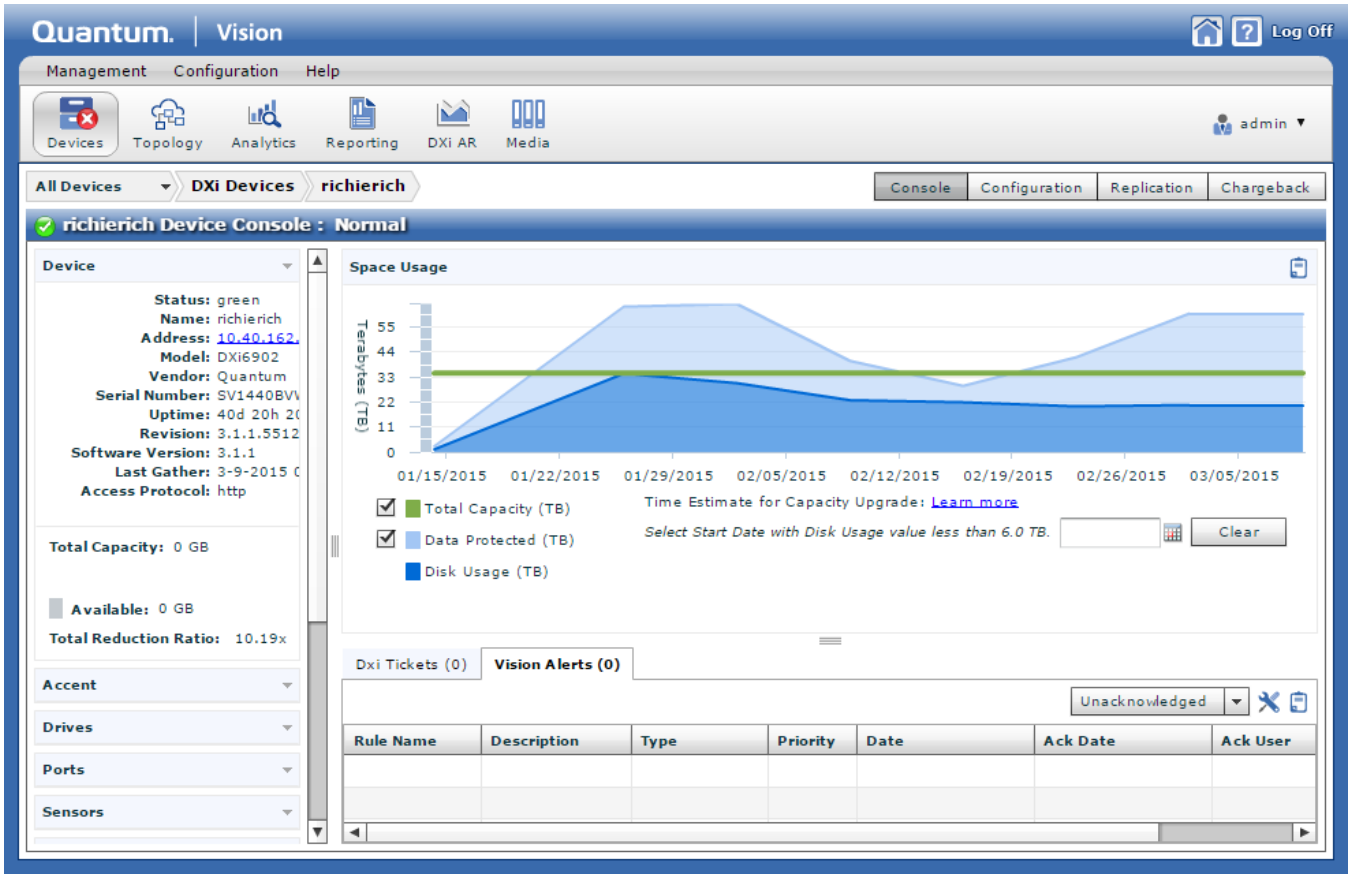
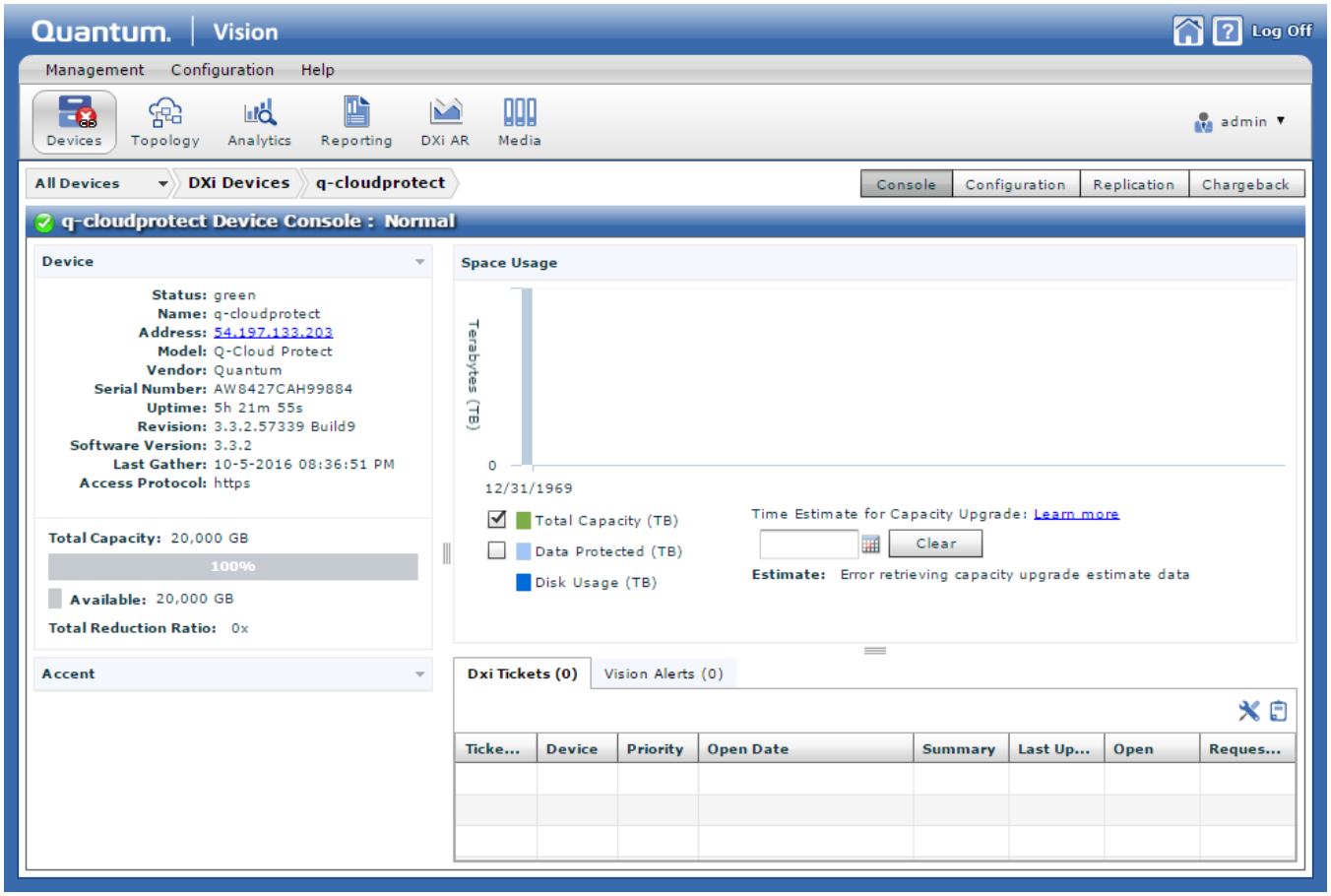


Figure 85: DXi Device Console – Q-Cloud Protect



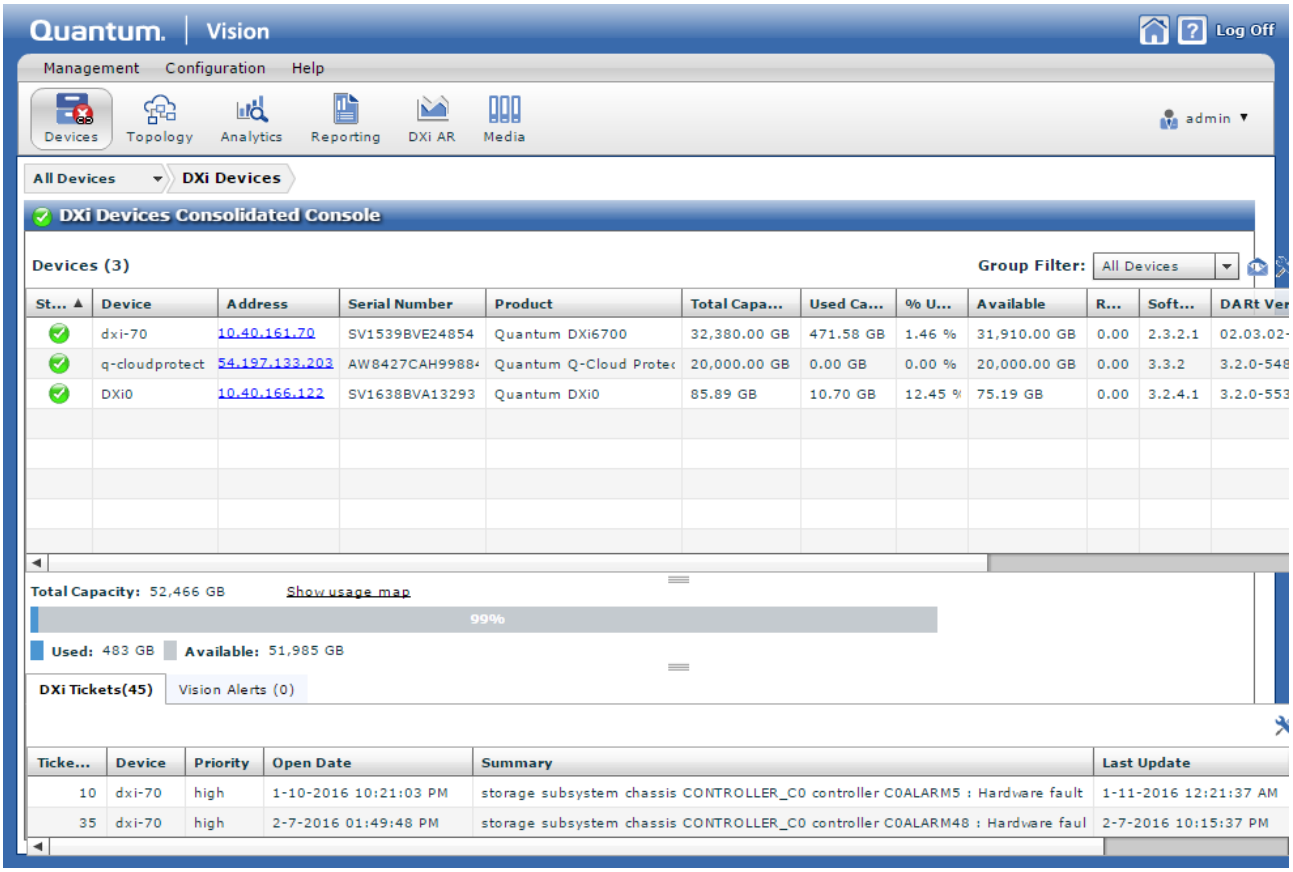
Navigate the DXi Devices Consolidated Console

Use the DXi Devices Consolidated console to monitor DXi devices and Q-Cloud Protect appliances.

Navigate the DXi Devices Consolidated Console

1. From the **All Devices** drop-down list on the **Device** console, select **DXi Devices** to display the **DXi Devices Consolidated** console.

Figure 86: DXi Devices Consolidated Console



2. In the **Devices** pane, view the following information:

Column	Definition
Status	The color-coded icon indicating the device's status.
Device	The name assigned to the device when it was discovered in Vision.
Address	The device's IP address or host name. Click the IP address or host name to launch the native management interface for the device.
Serial Number	The device's serial number.
Product	The Quantum product model name for the device.
Total Capacity	The device's total storage capacity

Column	Definition
Used Capacity	The amount of storage being used on the device.
% Used	The percentage of storage being used on the device.
Available	The amount of storage that is available on the device.
Reduction Ratio	The amount of data on the device that has been deduplicated and compressed.
Software Version	The current software version of the device.
DARt Version	The current Advanced Reporting version attached to the device.
Uptime	The amount of time that the device has been communicating with the Vision server.
Last Gather	The last time status data was received from the device.
Protocol	**The device's encryption protocol** • **http** – The data collection path to the device uses an unencrypted connection. • **https** – The data collection path to the device uses an encrypted connection.

3. In the **Total Capacity**pane, view the following information:

   Total Capacity

   Total disk space of the DXi devices and Q-Cloud Protect appliances.

   Usage Bar

   Used (blue) and **Available** (light gray) disk space for the DXi devices and Q-Cloud Protect appliances, shown in percentages in the bar graph and numbers in the legend under the bar graph.

   - Click **Show usage map** to view the capacity information in a larger bar graph.
   - Click **Show capacity information** to return to the **Total Capacity** pane.

4. In the **Device Alerts** pane, view the following information on the **DXi Tickets** tab:

Column	Description
Ticket #	The service ticket number for a DXi device or Q-Cloud Protect appliances.

Column	Description
Priority	The priority assigned to the service ticket.
Open Date	The date on which the service ticket was opened.
Summary	A summary of the issue on the service ticket.
Last Update	The date and time on which the last update to the ticket was made.
Open	The open status for the ticket.
RequestId	The ID of the request from which the ticket was generated.

5. In the **Device Alerts** pane, view and acknowledge alert notifications, as needed. See Manage Vision Alert Notifications on page 101.

Navigate an Individual DXi Device Console

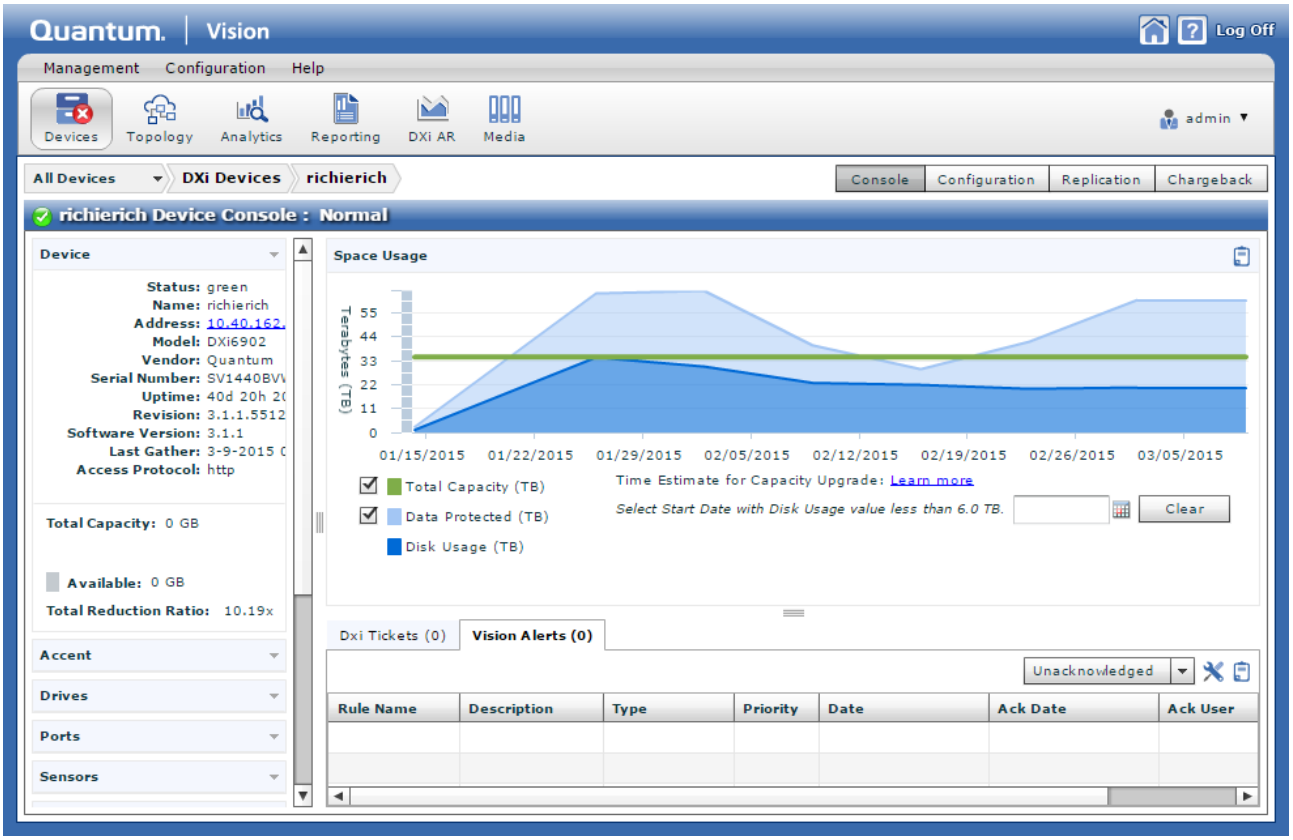
Use the **DXi Device** console to view information about an individual DXi device, including device component status, disk space usage, and tickets and alerts.

For information about tickets and alerts, see Navigate the DXi Devices Consolidated Console on page 111.

Navigate the Device Status pane

1. From the **Devices** console, double-click the DXi device for which to display the **DXi Device** console.

Figure 87: DXi Device Console – DXi



2. In the **Device Status** pane, view the following status information about the components within a DXi system:

Note: Not all components display for each DXi device. The displayed components depend upon the DXi device's configuration. Click the arrow next to a component to show or hide a list of sub-components.

Component	Description
Device	Overall DXi system status, indicated by a status color. **Device-specific data** • **Name** – The device's name. • **Address** – The device's IP address/hostname. Click to launch the native management interface for the DXi system. • **Model** – The device's model. • **Vendor** – The vendor from whom the device was purchased. • **Serial Number** – The device's serial number. • **Uptime** – The amount of time that the device has been communicating with the Vision server. • **Revision** – The revision number of the DXi software. • **Software Version** – The version number of the DXi software. • **Last Gather** – The last time status data was received from the device. • **Access Protocol** – The device's encryption protocol.
Total Capacity	**Capacity data** • **Total Capacity** – Total disk space of the DXi device. • **Usage Bar** – **Used** (blue) and **Available** (light gray) disk space for the DXi devices, shown in percentages in the bar graph and numbers in the fields under the bar graph. • **Dedupe** – The amount of disk space that contains deduplicated data. • **Non Dedupe** – The amount of disk space that contains non-deduplicated data. • **System Metadata** – The amount of disk space that contains system metadata. • **Total Reduction Ratio** – The amount of data that has been deduplicated and compressed. **Additional Information** On DXi systems that predate version 2.3, **Used** + **Available** disk space might be greater than **Total Capacity**. This mismatch in calculations is caused by reclaimable space being counted in both the **Used** and **Available** categories. As of version 2.3, reclaimable space is only being included in **Available** disk space. All reported numbers and sums are now correct.
Accent	Total bandwidth savings achieved for the device when Accent is enabled.

Component	Description
Drives	**Disk drive data** • Name of the drive. • Status of the drive, such as **Normal**. • Location of the drive. • Total storage capacity of the drive. Double-click a row to view this same information, along with the drive's enable property, index, model, and alert severity in a table format on the **Drive Details** dialog box.
Ports	**Fibre Channel and Ethernet ports data** • Name of the port. • Type of port. Double-click a row to view this same information, along with the port's index, alert severity, status, value, WWPN assignment, and received and transmitted values in a table format on the **Port Details** dialog box.
Sensors	**Sensor data** • Name of the sensor. • Type of sensor, either **Voltage**, **Temperature**, or **IPMI**. Double-click a row to view this same information, along with the sensor's index, alert severity, status, and observation values in a table format on the **Sensor Details** dialog box.
Switches	**Fibre Channel and Ethernet switch data** • Name of the switch. • Vendor from whom you purchased the switch. • Type of switch, either **Ethernet** or **FiberChannel**. Double-click a row to view this same information, along with the switch's index, alert severity, and status in a table format on the **Switch Details** dialog box.

Component	Description
VTL Partitions	**Virtual tape library (VTL) partition data** • Name of the partition. • Whether deduplication is enabled for the partition, either **true** or **false**. • Whether replication is enabled for the partition, either **true** or **false**. • Average throughput for the partition. Double-click a row to view this same information, along with the partition's backup window values, index, mode, and number of tape cartridges and drives in a table format on the **VTL Details** dialog box.
PTT Devices	**Path-to-tape (PTT) library and drive data** • Serial number for the device. • Vendor from whom you purchased the device. • Product type of the device. Double-click a row to view this same information, along with the device's alias, revision number, and type in a table format on the **PTT Details** dialog box.
NAS Shares	**NAS share data** • Name of the NAS share. • Type of share, either **NFS** or **CIFS**. • Whether deduplication is enabled for the partition, either **true** or **false**. • Whether replication is enabled for the partition, either **true** or **false**. Double-click a row to view this same information, along with the NAS share's node, backup window values, description, hidden or displayed status, permission value, and signature value in a table format on the **NAS Share Details** dialog box.
Adapters	**Installed hardware adapter data** • Name of the adapter. • Type of adapter, either a compression card, Fibre Channel controller, or network interface cards (NICs). Double-click a row to view this same information, along with the adapter's model revision value and vendor name in a table format on the **HBA Details** dialog box.

Component	Description
Fans	Device's cooling fans. Double-click a row to view the **Fan Details** dialog box. **Fan Details** • Index for the fan. • Alert severity assigned to the fan, such as **Normal**. • Status of the fan, such as **Normal**. • Observed values for the fan.
Batteries	**RAID controller backup battery data** • Name of the battery. • Location of the battery. Double-click a row to view this same information, along with the battery's enabled value, index, alert severity, and status in a table format on the **Battery Details** dialog box.
Power Supplies	Device's power supplies. Double-click a row to view information about the power supplies in the **Power Supply Details** dialog box. **Power Supply Details** • Index for the power supply. • Alert severity assigned to the power supply, such as **Normal**. • Status of the power supply, such as **Normal**.
Licenses	**Installed feature license data** • Name of the license. • Current number of the license being used. • Maximum number of allocated licenses. Double-click a row to view this same information, along with the license's description, product to which the license applies, and that product's vendor in a table format on the **License Details** dialog box.

Navigate the Space Usage pane

1. From the **Devices** console, double-click the DXi device for which to display the **DXi Device** console.
2. Using the line graph and legend, view the following space usage information for the device:

Line	Description
Total Capacity (green)	Total amount of disk space on the device, in terabytes (TBs).
Data Protected (light blue)	Amount of protected data on the device, in TBs.
Disk Usage (dark blue)	Amount of disk space currently being used on the device, in TBs.

3. Use the **Time Estimate for Capacity Upgrade** field to calculate the capacity upgrade estimate. See Capacity Upgrade Estimate in Vision on page 124.

Additional Information

- Maximum values are used for the before and after reduction rates
- A maximum of 12 months of data can be displayed.

Navigate an Individual Q-Cloud Protect Appliance Console

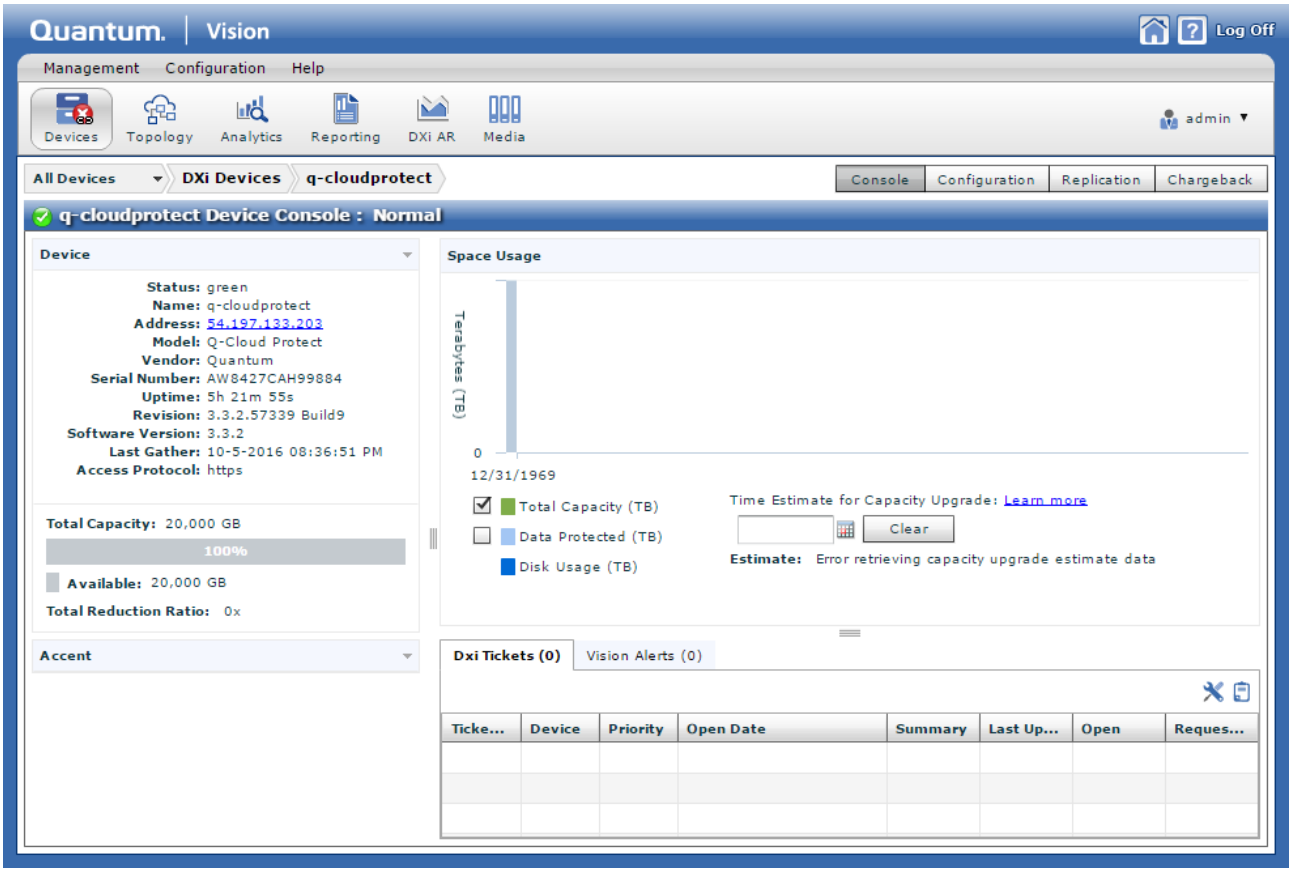
Use the **Q-Cloud Protect Appliance** console to view information about an individual Q-Cloud Protect appliance, including the cloud appliance's component status, disk space usage, and tickets and alerts.

For information about tickets and alerts, see Navigate the DXi Devices Consolidated Console on page 111.

Navigate the Device Status pane

1. From the **Devices** console, double-click the Q-Cloud Protect appliance for which to display the **Q-Cloud Protect Device** console.

Figure 88: DXi Device Console – Q-Cloud Protect



2. In the **Device Status** pane, view the following status information about the cloud appliance's components:

Note: Not all components display for each DXi device. The displayed components depend upon the DXi device's configuration. Click the arrow next to a component to show or hide a list of sub-components.

Component	Description
Device	Overall Q-Cloud Protect system status, indicated by a status color. **Device-specific data** • **Name** – The cloud appliance's name. • **Address** – The cloud appliance's IP address/hostname. Click to launch the native management interface for the Q-Cloud Protect appliance. • **Model** – The cloud appliance's model. • **Vendor** – The vendor from whom the cloud appliance was purchased. • **Serial Number** – The cloud appliance's serial number. • **Uptime** – The amount of time that the cloud appliance has been communicating with the Vision server. • **Revision** – The build number of the Q-Cloud Protect software. • **Software Version** – The version number of the Q-Cloud Protect software. • **Last Gather** – The last time status data was received from the cloud appliance. • **Access Protocol** – The cloud appliance's encryption protocol.
Total Capacity	**Capacity data** • **Total Capacity** – Total disk space of the cloud appliance. • **Usage Bar** – **Used** (blue) and **Available** (light gray) disk space for the cloud appliance, shown in percentages in the bar graph and numbers in the fields under the bar graph. • **Dedupe** – The amount of disk space that contains deduplicated data. • **Non Dedupe** – The amount of disk space that contains non-deduplicated data. • **System Metadata** – The amount of disk space that contains system metadata. • **Total Reduction Ratio** – The amount of data that has been deduplicated and compressed.
Accent	Total bandwidth savings achieved for the cloud appliance when Accent is enabled.

Component	Description
VTL Partitions	**Virtual tape library (VTL) partition data** To present the storage capacity of the Q-Cloud Protect appliance as a VTL partition that is compatible with standard backup applications, you must add partitions. When you add a partition, you must specify the type of physical library to emulate, as well as configure virtual tape drives and storage slots. • Name of the partition. • Whether deduplication is enabled for the partition, either **true** or **false**. • Whether replication is enabled for the partition, either **true** or **false**. • Average throughput for the partition. Double-click a row to view this same information, along with the partition's backup window values, index, mode, and number of tape cartridges and drives in a table format on the **VTL Details** dialog box.
NAS Shares	**NAS share data** To present the storage capacity of the Q-Cloud Protect appliance as a NAS share that is compatible with standard backup applications, you must first add shares. When you add a share, you must specify whether it uses the NFS protocol (for Linux networks) or the CIFS protocol (for Windows networks). • Name of the NAS share. • Type of share, either **NFS** or **CIFS**. • Whether deduplication is enabled for the partition, either **true** or **false**. • Whether replication is enabled for the partition, either **true** or **false**. Double-click a row to view this same information, along with the NAS share's node, backup window values, description, hidden or displayed status, permission value, and signature value in a table format on the **NAS Share Details** dialog box.

Component	Description
Licenses	**Installed feature license data** • Name of the license. • Current number of the license being used. • Maximum number of allocated licenses. Double-click a row to view this same information, along with the license's description, product to which the license applies, and that product's vendor in a table format on the **License Details** dialog box.

Navigate the Space Usage pane

1. From the **Devices** console, double-click the Q-Cloud Protect appliance for which to display the **Q-Cloud Protect Device** console.
2. Using the line graph and legend, view the following space usage information for the cloud appliance:

Line	Description
Total Capacity (green)	Total amount of disk space on the cloud appliance, in terabytes (TBs).
Data Protected (light blue)	Amount of protected data on the cloud appliance, in TBs.
Disk Usage (dark blue)	Amount of disk space currently being used on the cloud appliance, in TBs.

3. Use the **Time Estimate for Capacity Upgrade** field to calculate the capacity upgrade estimate. See Capacity Upgrade Estimate in Vision below.

Additional Information

- Maximum values are used for the before and after reduction rates
- A maximum of 12 months of data can be displayed.

Capacity Upgrade Estimate in Vision

Use the capacity upgrade estimate to determine when capacity might be completely consumed on a DXi device or Q-Cloud Protect appliance.

The capacity upgrade estimate is calculated as compound growth between a beginning and ending point in time. The result displays the number of weeks until a capacity upgrade is mostly likely required.

See Navigate an Individual DXi Device Console on page 114 and Navigate an Individual Q-Cloud Protect Appliance Console on page 120.

Tips for Calculating a Capacity Upgrade Estimate

Review the following tips to obtain the most reliable capacity upgrade estimate by identifying a period of time that reflects regular growth:

Steady-State Period

We recommend using a period of time that represents stable growth. Such a steady-state period occurs after the initial loading of data onto your DXi device or cloud appliance, when you have a backup expiring for each new backup stored, and when the increase in capacity reflects annual growth of data.

Do not include time periods when you first populate your DXi or cloud appliance or add a new data source. If you include such time periods, the reported compound growth will be much higher than normal growth, and your capacity upgrade estimate will be lower than it should be.

Examples

- Initial backups are retained for 30 days. So for the first month of use, data appears to be growing rapidly. That apparent rapid growth is due to data not being deleted, rather than actual data growth.
- A new email group's data is sent to the DXi device for backup. Much like with your initial backup operations, data growth appears more rapid than normal. This apparent rapid growth continues until the new data backups begin to expire and the new email group's data reaches a steady state.

Data Points

We recommend that you use more than 5 data points to calculate the compound growth rate for capacity. Data points reflect the amount of data backed up after reduction. Vision uses the highest data point from each week to calculate the compound growth rate for a period of x weeks, as shown in the following equation:

sum of highest data points from each week / number of weeks = compound growth rate

Using the compound growth rate, Vision estimates the number of weeks before a capacity upgrade is required. You need more than 5 data points – or 5 weeks of backups to the DXi or cloud appliance – for a reliable compound growth rate.

Vision cannot calculate the capacity upgrade estimate if the data point value is beyond the point for which the capacity is already considered full. If the DXi or cloud appliance is already at maximum capacity, it requires a capacity upgrade.

Incline vs. Decline Periods

We recommend running the capacity upgrade estimate during an **incline period**, which is a period of time when the amount of data at the beginning point is lower than the amount of data at the ending point.

If you run the capacity upgrade estimate during a **decline period** — when the amount of data at the beginning point is higher than the amount of data at the ending point — Vision cannot accurately estimate when a capacity upgrade is needed because the length of the decline period is unknown.

If you run a capacity upgrade estimate during a decline period, Vision displays the capacity upgrade estimate as a broken red line.

Recommended Actions for Low Capacity

When the capacity upgrade estimate shows that a DXi device or cloud appliance is approaching capacity, use the following recommendations to extend the time before upgrading capacity on the device.

- Run reclamation more often.

  We recommend running reclamation weekly or after a known network disruption has occurred.

- Reduce the number of excess scratch tapes.

  The percentage of scratch tapes should not be much greater than the anticipated year-over-year growth rate.

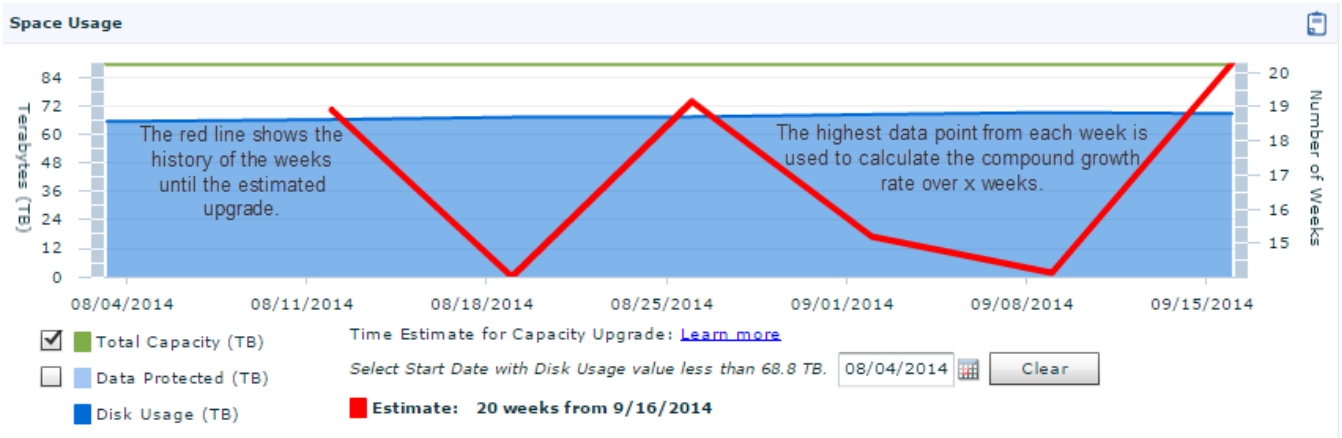
- Re-label scratch tapes using your backup application, and run DXi reclamation to free up space.
- Reduce the number of Name Space snapshot versions that are retained, if applicable.
- Shorten retention policies, if appropriate.
- Make sure that compressed, encrypted, and multiplexed jobs are not being sent.
- Verify that the size of your cartridges is not too large.

  The cartridge size should be the same size as your average backup job.

- If your DXi's software version predates 2.2 and you are running Trigger Based Replication, run synchronizations weekly or after a known network disruption.
- Request a HealthCheck assessment through your Quantum account team.

Understanding the Capacity Upgrade Estimate

Review the following information to understand how the capacity upgrade estimate is displayed on the **Space Usage** graph.



Line Slope	Indication
Positive (sloping up from left to right)	The current capacity upgrade estimate is greater than the previous estimate. Positive slopes usually indicate that a DXi device or cloud appliance currently has both low amounts of stored data and a slow growth rate.
Flat or Negative (level or sloping down from left to right)	The current estimate is the same as or lower than the previous estimate, showing that the DXi device or cloud appliance is in a steady state. Any net increase in data is the result of natural data growth, rather than growth caused by adding new backup sources where reclamation policies have not yet reached their maximum retention period.
Mix of Positive and Negative	Any of the following: • New data sources have been added, where reclamation policies have not yet reached their maximum retention period. • Interruptions to retention policies or introductions of new replications into a target have occurred. • Changes in retention policies have occurred, such as an indefinite legal hold or reduction in the number of required backups.

Calculate the Capacity Upgrade Estimate

Use the capacity upgrade estimate to determine when current capacity for a DXi device or Q-Cloud Protect appliance will be consumed.

For detailed information regarding how to obtain the most accurate estimate, how to handle low capacity, and how to read the information presented in the **Space Usage** graph, seeCapacity Upgrade Estimate in Vision on page 124.

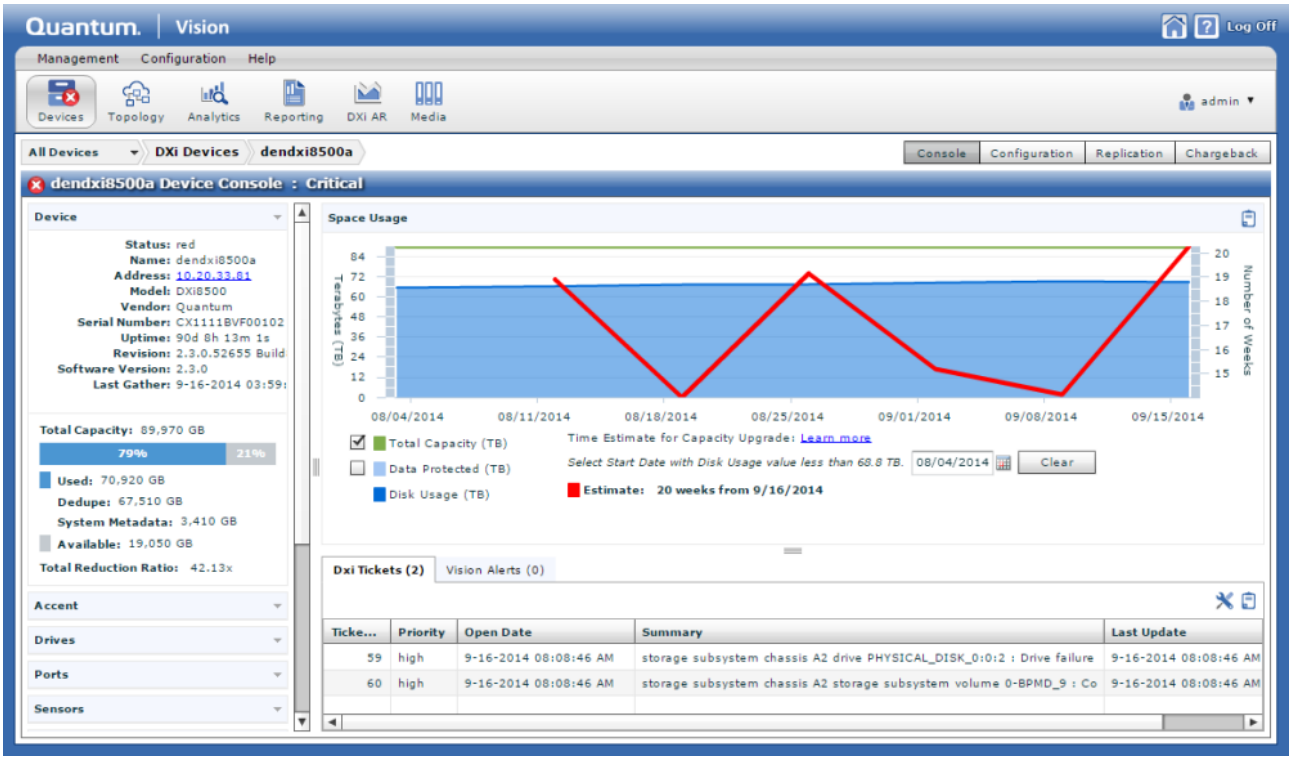
Calculate the capacity upgrade estimate

1. From the **Devices** console, double-click the DXi device or cloud appliance for which to display the **<Individual> Device** console.
2. In the **Space Usage** pane, select the **Total Capacity** or **Data Protected** check box to display that information on the graph, as needed.
3. Under the **Time Estimate for Capacity Upgrade** field, click the calendar button to select a date on which to begin the calculation for the upgrade estimate.

   Note: Vision can take up to 1 week to collect 12 months' worth of data for existing DXi installations.

   Vision plots the capacity upgrade estimate in the **Space Usage** graph and displays the **Estimate** field with the estimated capacity upgrade date.

Figure 89: DXi Device Console – Capacity Upgrade Estimate



4. Move the cursor to various points in time on the graph to see the estimated number of weeks until a capacity upgrade is needed.

Replication and Chargeback Usage Reports

From DXi or Q-Cloud Protect Device consoles, you can access the Device Replication report and the Chargeback Usage report.

Important

Vision uses the DXi and Q-Cloud Protect IP addresses — rather than hostnames — to determine replication relationships. It does not recognize replication relationships if the DXi or Q-Cloud Protect IP address is not supplied.

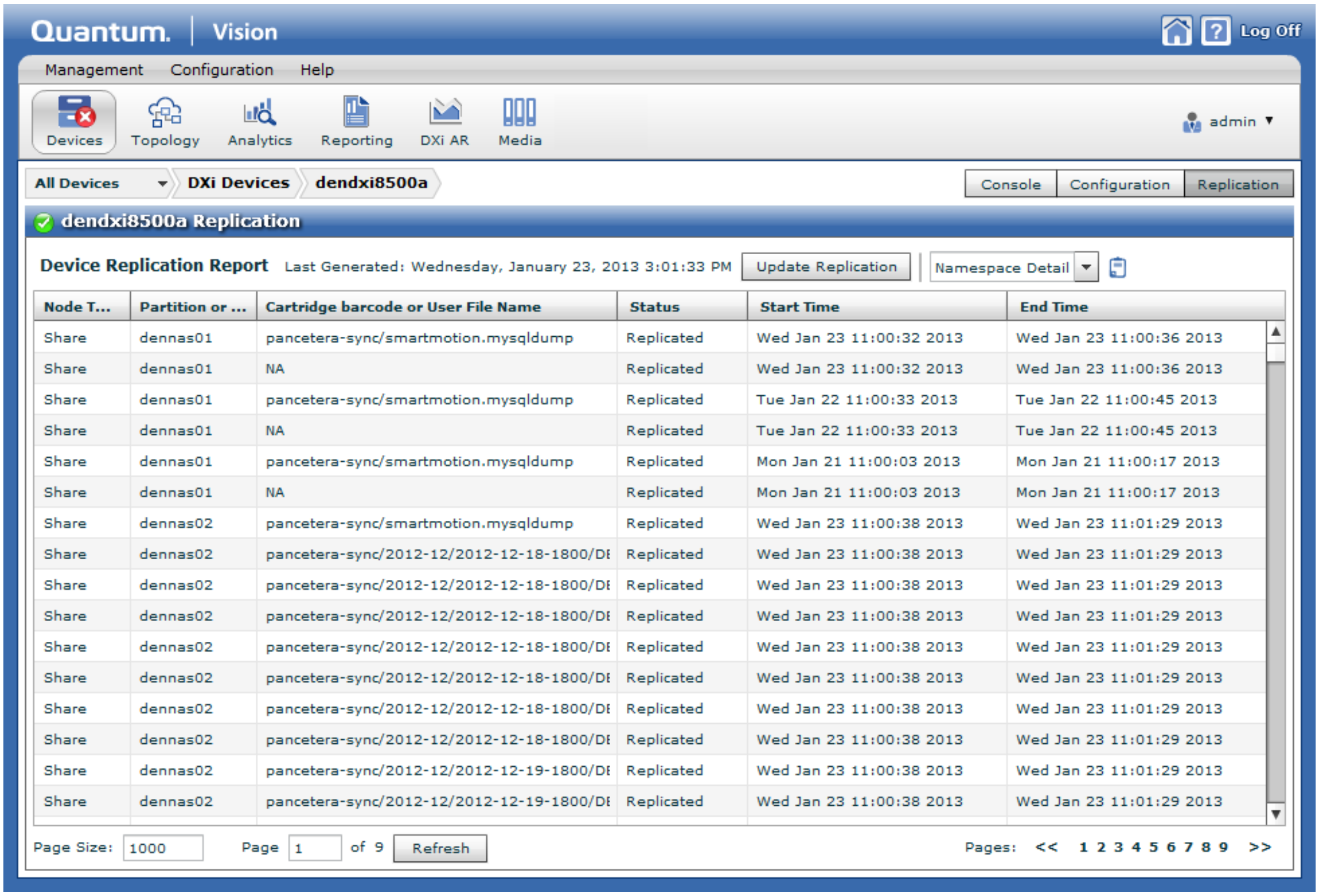
Device Replication Report

Use the Device Replication report to view both detailed and summary information for namespace file replication, source replication, and target replication.

Replication reports are accessible for the following: DXi V-Series virtual appliances, DXi4500, DXi4700, DXi6500, DXi6700, DXi6800, DXi6900, DXi6900-S, DXi7500, DXi8500, and Q-Cloud Protect.

See View Replication Reports on the next page.

Figure 90: Device Replication Report



Access Control

For Vision to gather replication data for Q-Cloud Protect appliances or DXi devices running software versions 3.2 or later, it needs to identify itself through an SSH key pair.

Vision generates this key pair. The private key is Vision's secure identifier. The public key is shared with the Q-Cloud Protect appliance or DXi device. Vision has authorization to gather replication data only when the private and public keys match. For more information, see Configure Security Settings for Vision on page 95.

Chargeback Usage Report

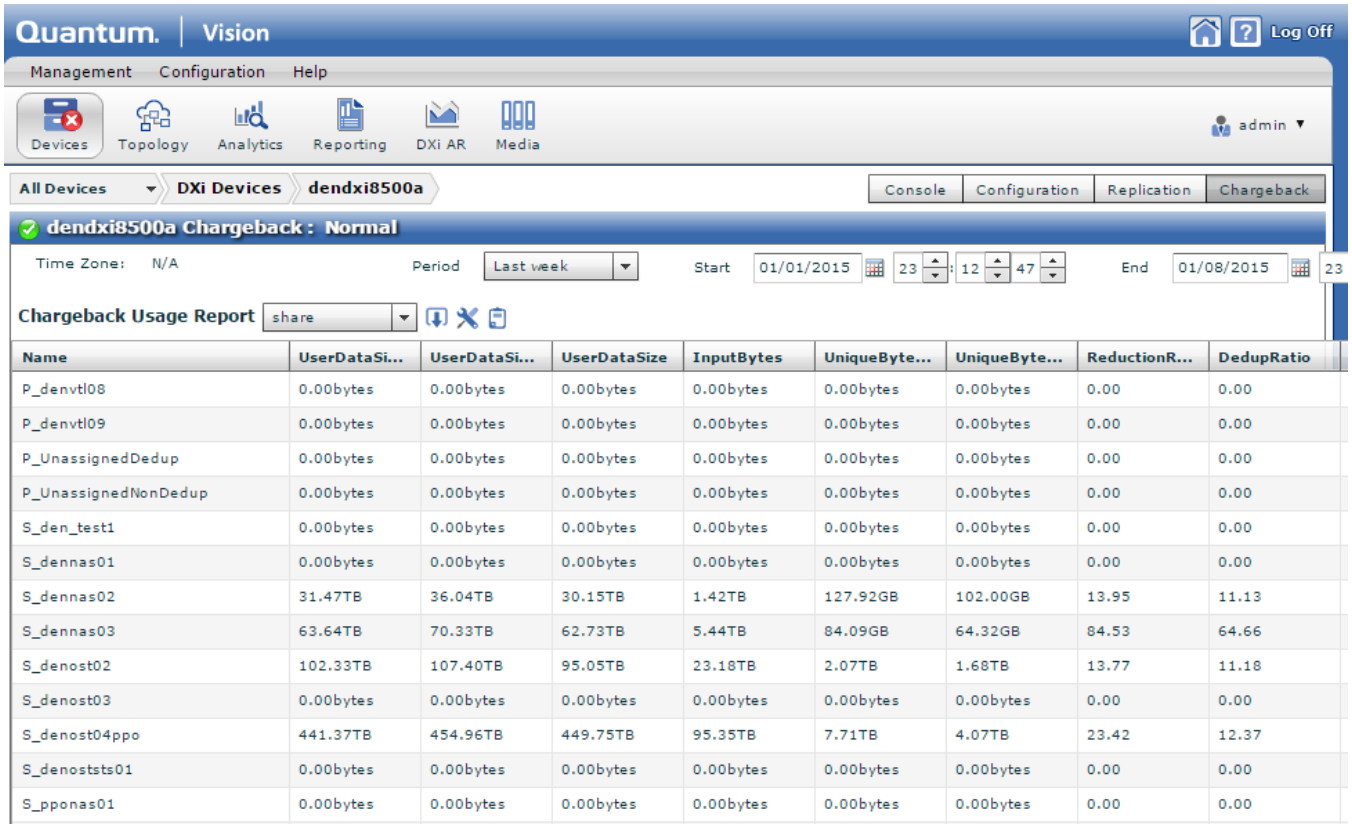
Use the Chargeback Usage report to view ingest and capacity information for both shares and partitions

configured on a DXi device or Q-Cloud Protect appliance.

You can view Chargeback Usage reports for DXi devices with a software version of 2.3 or newer and Q-Cloud Protect appliances.

See View Chargeback Usage Reports on page 134.

Figure 91: Chargeback Usage Report



Name	UserDataSi...	UserDataSi...	UserDataSize	InputBytes	UniqueByte...	UniqueByte...	ReductionR...	DedupRatio
P_denvtl08	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
P_denvtl09	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
P_UnassignedDedup	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
P_UnassignedNonDedup	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_den_test1	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_dennas01	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_dennas02	31.47TB	36.04TB	30.15TB	1.42TB	127.92GB	102.00GB	13.95	11.13
S_dennas03	63.64TB	70.33TB	62.73TB	5.44TB	84.09GB	64.32GB	84.53	64.66
S_denost02	102.33TB	107.40TB	95.05TB	23.18TB	2.07TB	1.68TB	13.77	11.18
S_denost03	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_denost04ppo	441.37TB	454.96TB	449.75TB	95.35TB	7.71TB	4.07TB	23.42	12.37
S_denoststs01	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_pponas01	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00

View Replication Reports

Use the Device Replication report to view both detailed and summary information for namespace file replication, source replication, and target replication.

Replication reports are accessible for Q-Cloud Protect appliances and the following DXi devices: DXi V-Series virtual appliances, DXi4500, DXi4700, DXi6500, DXi6700, DXi6800, DXi6900, DXi6900-S, DXi7500, and DXi8500.

Access Control

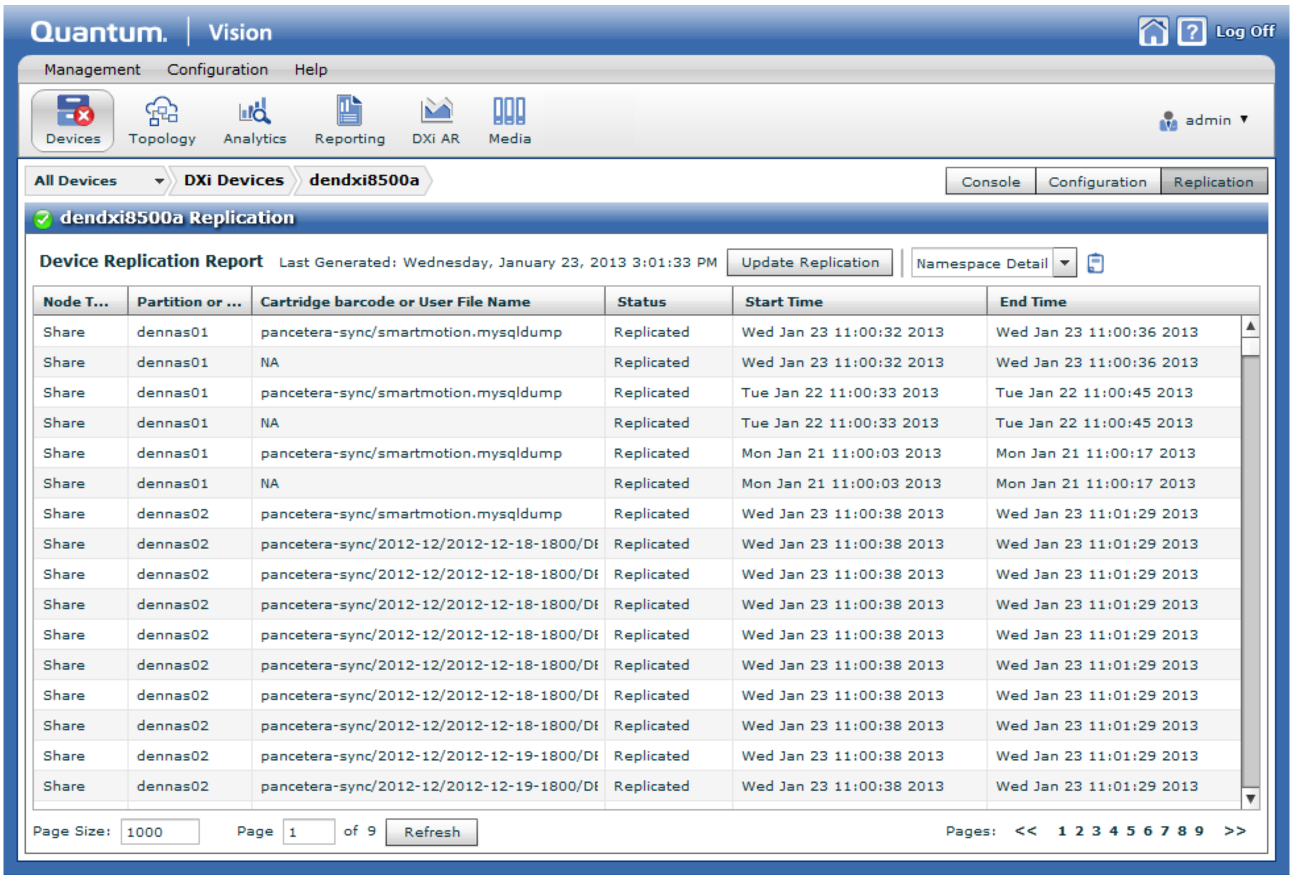
For Vision to gather replication data for Q-Cloud Protect appliances or DXi devices running software versions 3.2 or later, it needs to identify itself through an SSH key pair.

Vision generates this key pair. The private key is Vision's secure identifier. The public key is shared with the Q-Cloud Protect appliance or DXi device. Vision has authorization to gather replication data only when the private and public keys match. For more information, see Configure Security Settings for Vision on page 95.

View replication reports

1. From the **<individual> Device** console, click the **Replication** tab to display the **Replication** console.

Figure 92: Replication Console



2. In the report type drop-down list (next to the **Updated Replication** button), select the type of report to display:

Report	Description
Namespace Detail	**Detailed namespace file replication data** • The type of node from which data was replicated, such as **Share**. • The name of the partition or share from which the data was replicated. • The name of the cartridge or user file from which data was replicated. • The status of the replication, such as **Success**. • The time at which the replication began and completed. • The ID assigned to the replicated bundle. • The IP address or hostname of the target system.
Namespace Summary	**Summary namespace file replication data** • The type of node from which data was replicated, such as **Share**. • The name of the partition or share from which the data was replicated. • The status of the replication, such as **Success**. • The time at which the replication began and completed. • The total number of data bytes replicated. • The amount of time it took for the replication to complete in MB/second. • The ID assigned to the replicated bundle. • The IP address or hostname of the target system.
Source Detail	**Detailed source system data** • The type of node from which data was replicated, such as **Share**. • The name of the partition or share from which the data was replicated. • The target system to which the data was replicated. • The barcode or path of the target system. • The status of the replication, such as **Success**, and any other information associated with the replication status. • The time at which the replication began and completed. • The rate at which the replication completed. • If the replication has not completed, the estimated time until completion. • The trigger ID assigned to the replication.

Report	Description
Source Summary	**Summary source system data** • The type of node from which data was replicated, such as **Share**. • The name of the partition or share from which the data was replicated. • The target system to which the data was replicated. • The number of replication tasks currently in the queue. • The number of replication tasks currently running. • The number of successful replication tasks. • The number of failed replication tasks.
Target Detail	**Detailed target system data** • The type of node from which data was replicated, such as **Share**. • The name of the partition or share from which the data was replicated. • The source system from which the data was replicated. • The barcode or path of the source system. • The status of the replication, such as **Success**, and any other information associated with the replication status. • The time at which the replication began and completed. • The rate at which the replication completed. • If the replication has not completed, the estimated time until completion. • The AUD ID assigned to the replication.
Target Summary	**Summary target system data** • The type of node from which data was replicated, such as **Share**. • The name of the partition or share from which the data was replicated. • The source system from which the data was replicated. • The most severe status allowed before an alert is triggered. • The last time at which a replication began and completed. • The AUD ID assigned to the replication.

3. Manage the displayed information by doing any of the following:

Update the displayed data

Click **Update Replication** and select the type of report to display from the report type drop-down list. Updating the displayed data can take up to 30 minutes.

Specify the number of rows displayed on a page

Enter a value in the **Page Size** field and click **Refresh**.

Navigate between pages of the report

- Use the controls in the lower right of the report.
- To navigate to a specific page, enter the page number in the **Page** box and click **Refresh**.

View Chargeback Usage Reports

Use the Chargeback Usage report to view ingest and capacity information for both shares and partitions configured on a DXi device or Q-Cloud Protect appliance.

You can only view Chargeback Usage reports for DXi devices with a software version of 2.3 or newer.

Tips for Using the Chargeback Usage Report

Keep the following tips in mind when using the Chargeback Usage report:

Reported Intervals

The DXi device or Q-Cloud Protect appliance reports chargeback in 1 or 5 minute intervals, so the display always lags by at least 1 to 5 minutes. In addition, if a replication starts and completes in a single reporting interval, ingest data is not displayed on the graph or legend.

Rounding and Granularity

Changes in rounding and granularity can cause small differences in the values displayed in the GUI, graph summaries, and file outputs. There may also be small differences in graph summary values when the time granularity is changed.

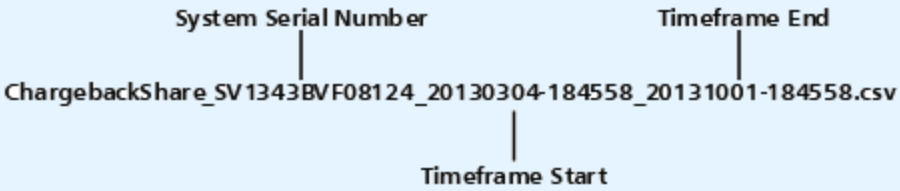
Time Frame

Because of the way the statistics are estimated, chargeback yields the best results when the selected time frame is greater than 7 days.

File Name

When you download a Chargeback Usage report using the **Download Chargeback** icon, Vision provides the report with a file name that is an aggregate of the report type, the system's serial number, and the start and end times of the selected time frame.

Example



View a Chargeback Usage Report

1. From the **< individual> Device** console, click the **Chargeback** tab to display the **Chargeback** console.
2. Select the time period on which to report by doing one of the following:

   Select a pre-defined time period

   In the **Period** drop-down list, select **Last Week**, **Last Month**, or **Last Quarter** to report on the corresponding time period.

   Define a custom time period

   a. In the **Period** drop-down list, select **Custom** to define a custom time period on which to report.

   b. In the **Start** and **End** fields, define the custom time period.

3. In the **Chargeback Usage Report** drop-down list, select one of the following to define the type of report to generate:

   share

   Generates data for all shares configured on the DXi device or cloud appliance.

   replication

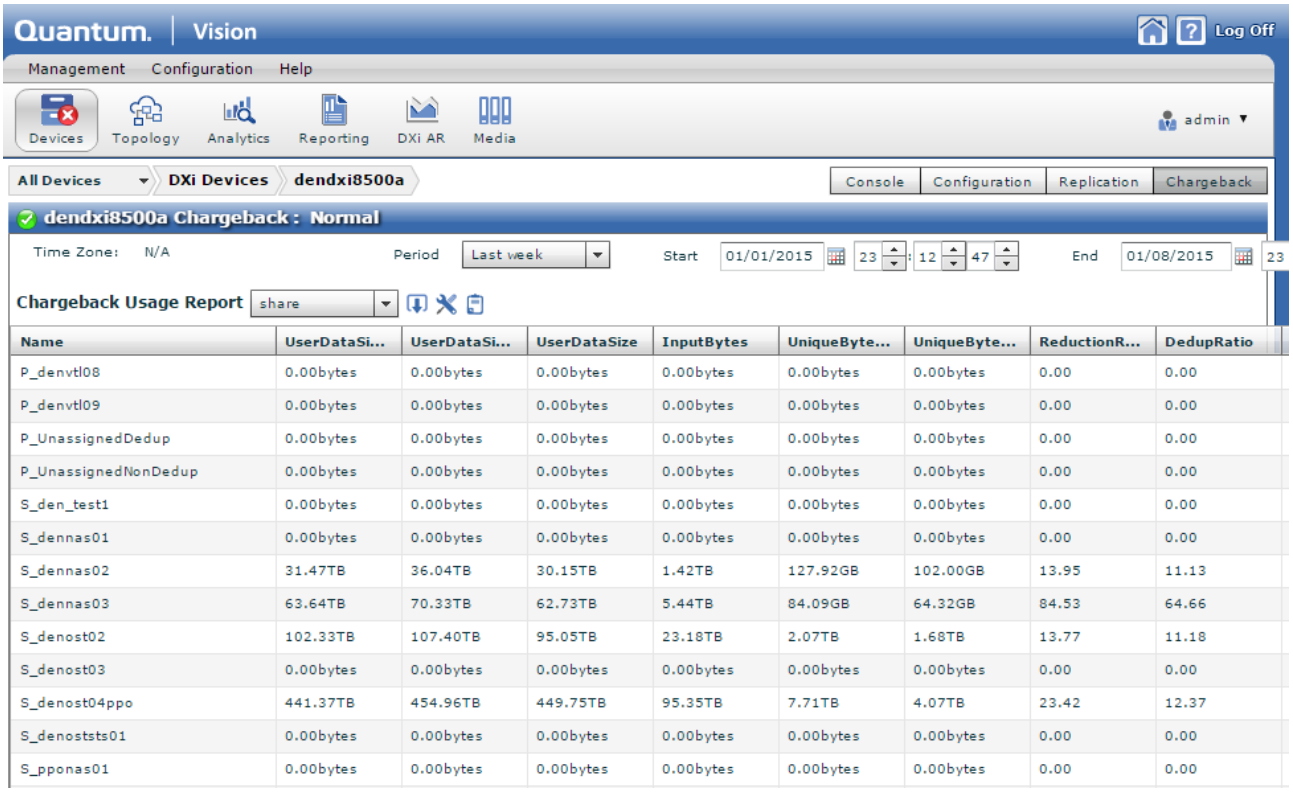
   Generates data for all shares or partitions replicated to the target system.

   partition

   Generates data for all partitions configured on the DXi device or cloud appliance.

   Vision displays the Chargeback Usage report for the defined criteria. See Chargeback Report Results on the next page for a description of each column in the report.

Figure 93: Chargeback Usage Report



Name	UserDataSi...	UserDataSi...	UserDataSize	InputBytes	UniqueByte...	UniqueByte...	ReductionR...	DedupRatio
P_denvtl08	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
P_denvtl09	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
P_UnassignedDedup	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
P_UnassignedNonDedup	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_den_test1	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_dennas01	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_dennas02	31.47TB	36.04TB	30.15TB	1.42TB	127.92GB	102.00GB	13.95	11.13
S_dennas03	63.64TB	70.33TB	62.73TB	5.44TB	84.09GB	64.32GB	84.53	64.66
S_denost02	102.33TB	107.40TB	95.05TB	23.18TB	2.07TB	1.68TB	13.77	11.18
S_denost03	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_denost04ppo	441.37TB	454.96TB	449.75TB	95.35TB	7.71TB	4.07TB	23.42	12.37
S_denoststs01	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00
S_pponas01	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00bytes	0.00	0.00

4. Click on a row in the report to display both the **Ingest** and **Capacity** graphs for the selected share or partition. See Chargeback Report Results below for a description of each graph.

Chargeback Report Results

This topic provides detailed information about Chargeback Usage report results.

Chargeback Usage Report Content

The following table defines each column within the Chargeback Usage report, whether being viewed from the **Chargeback** console or from a downloaded Chargeback Usage report file.

Column	Description
Hostname*	The system's IP address or host name for the device.
SystemSerialNumber*	The system's serial number for the device.
Start*	The beginning date and time for which the data is being reported.

Column	Description
End*	The ending data and time for which the data is being reported.
Name	For either the source or target system, the name of the partition (**P**) or share (**S**), as configured on the DXi or cloud appliance and as shown in the DXi or cloud appliance GUI for the ingest CSV.
UserDataSize	One of the following: • For backup, the amount of user data stored in the partition or share at the end of the selected time period. This value represents the sum of the file sizes in the partition or share prior to data reduction. • For replication, the size of the replicated partitions or shares sent to the DXi or cloud appliance at the end of the selected time period. This value includes the size of the ingested replication copies.
UserDataSizeAvg	The sum of all observed values in the **UserDataSize** column, divided by the number of observations for the selected period of time.
UserDataSizeMax	The maximum **UserDataSize** value observed for the selected period of time.
InputBytes	The total size of data as it arrives at the DXi or cloud appliance during the selected time frame. This value represents only ingested data — it does not include deleted data.
UniqueBytesPreCompression	The total amount of ingested data after deduplication for the selected time frame. This value represents only ingested data — it does not include deleted data.
UniqueBytesPostCompression	The total amount of ingested data after total reduction (both compression and deduplication) for the selected time range. This value represents only ingested data — it does not include deleted data.
ReductionRatio	The sum of all observed values in the **UserDataSize** column, divided by the sum of all values in the **UniqueBytesPostCompression** column.
DedupRatio	The sum of all observed values in the **UserDataSize** column, divided by the sum of all values in the **UniqueBytesPreCompression** column.
CompressionRatio	The value in the **ReductionRatio** column, divided by the value in the **DedupRatio** column.
OnDisk	The effective disk usage for the DXi or cloud appliance's share or partition at the end of the selected period of time.

Column	Description
OnDiskAvg	The sum of all observed values in the **OnDiskAvg** column, divided by the number of observations for the selected period of time.
PercentOfTotalCapacity	The percent of the total capacity of disk space being used for the selected time period.

* These values display only in the downloaded Chargeback Usage Report file.

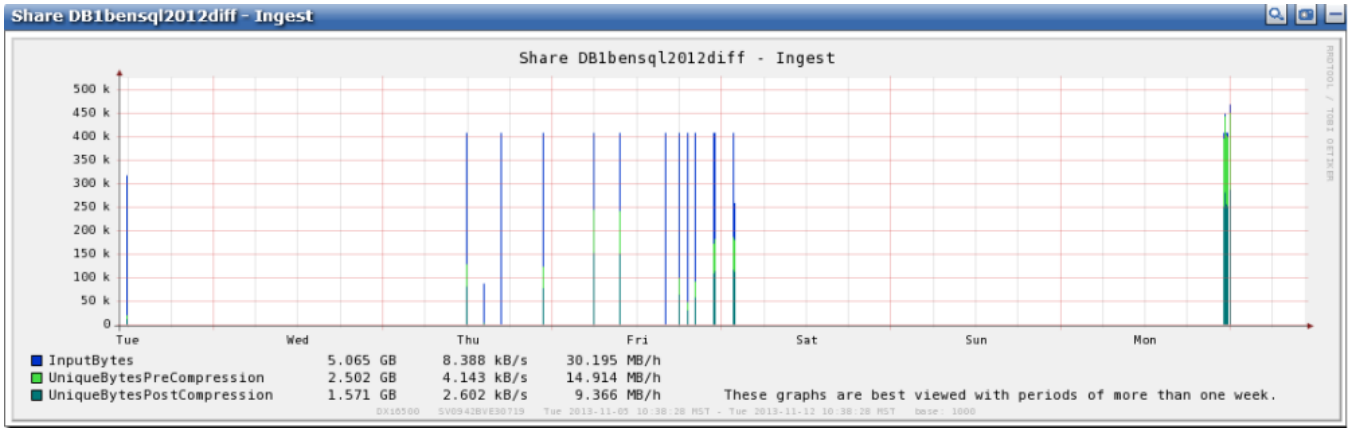
Ingest and Capacity Graphs

The **Ingest** and **Capacity** graphs display information about the selected share or partition within the Chargeback Usage report.

Ingest Graph Data

The Ingest Graph displays the following data:

Figure 94: Ingest Graph

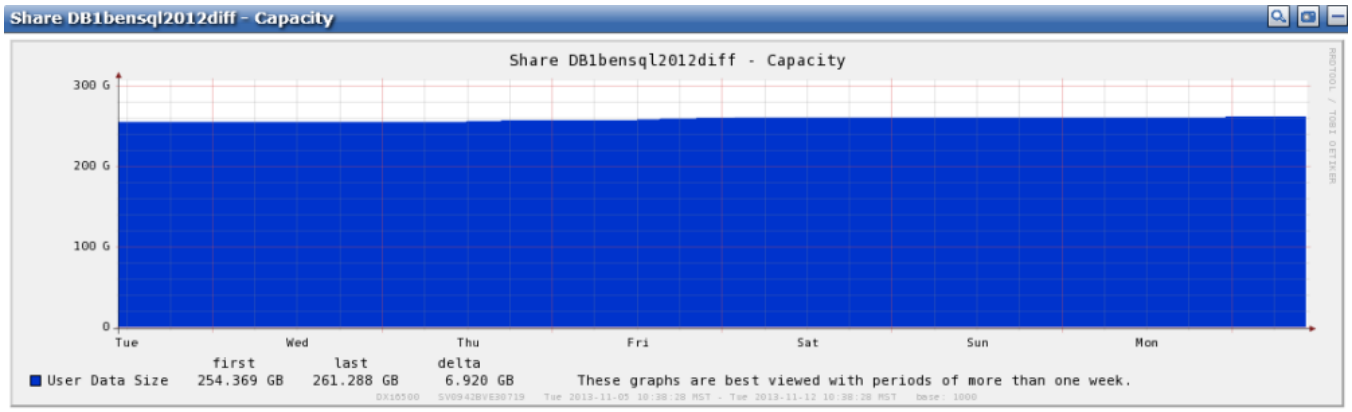


InputBytes	The data ingested prior to reduction or compression.
UniqueBytesPreCompression	The data ingested after deduplication.
UniqueBytesPostCompression	The data ingested after compression and deduplication.

Capacity Graph Data

The Capacity Graph displays the following data. When reviewing the data, keep in mind that the last minute of the graph corresponds to the value in the **UserDataSize** column of the **Chargeback Usage Report**.

Figure 95: Capacity Graph



User Data Size	The amount of data coming into a single partition or share for backup for each minute during the selected time period.
first	The first data point of the User Data Size.
last	The last data point of the User Data Size.
delta	The difference between the first and last data points of the User Data Size.

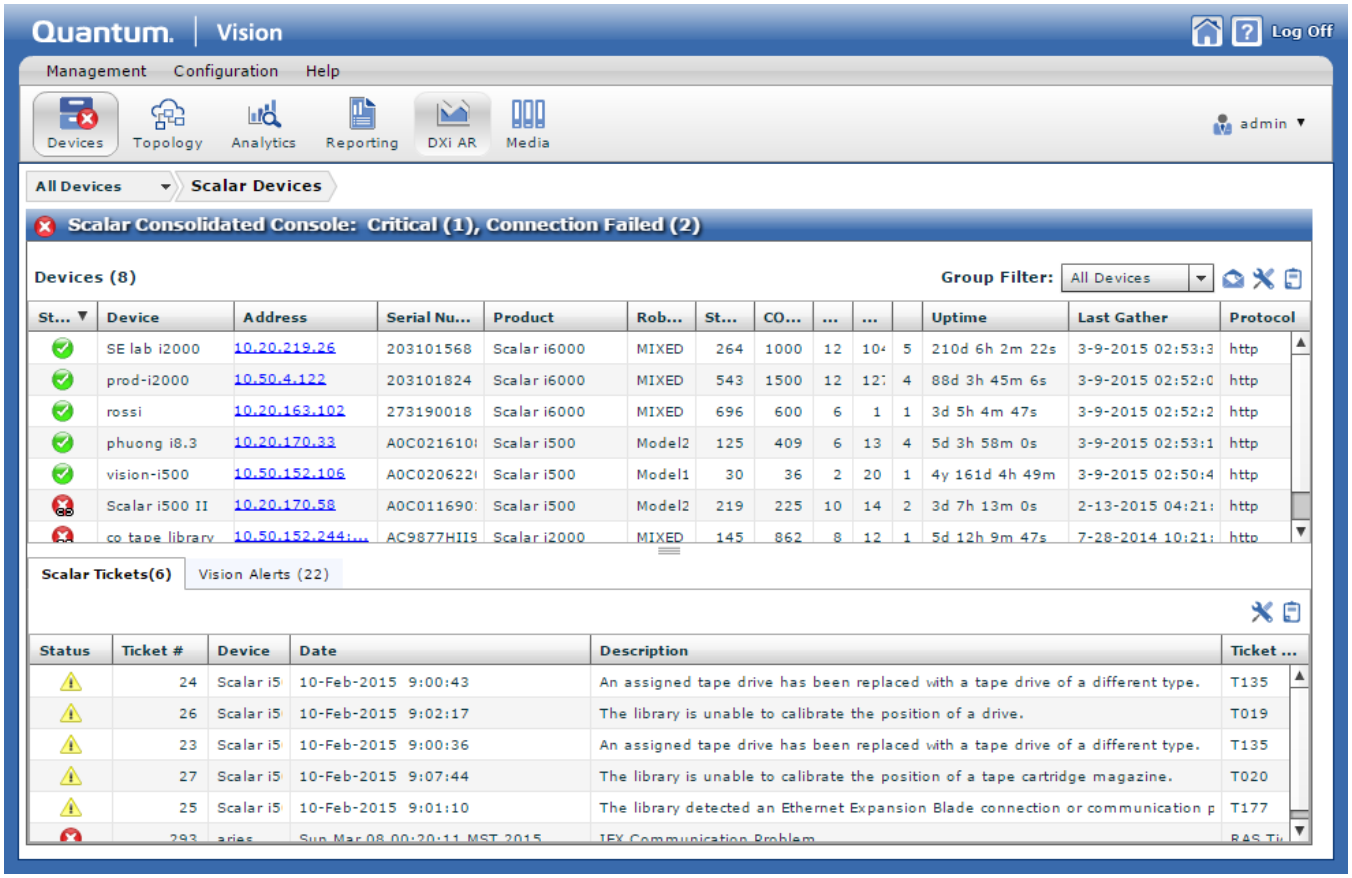
Scalar Device Consoles

To monitor Scalar devices in Vision, you can use the following two consoles in addition to the main Vision Device console. From these consoles, you can view information about tape library components, storage slot usage, partition components, and device alerts.

Scalar Consolidated Console

Use the Scalar Consolidated console to monitor tape libraries within the Scalar Devices Group. From this console, you can also access tickets and alerts for Scalar tape libraries. See Navigate the Scalar Consolidated Console on page 141.

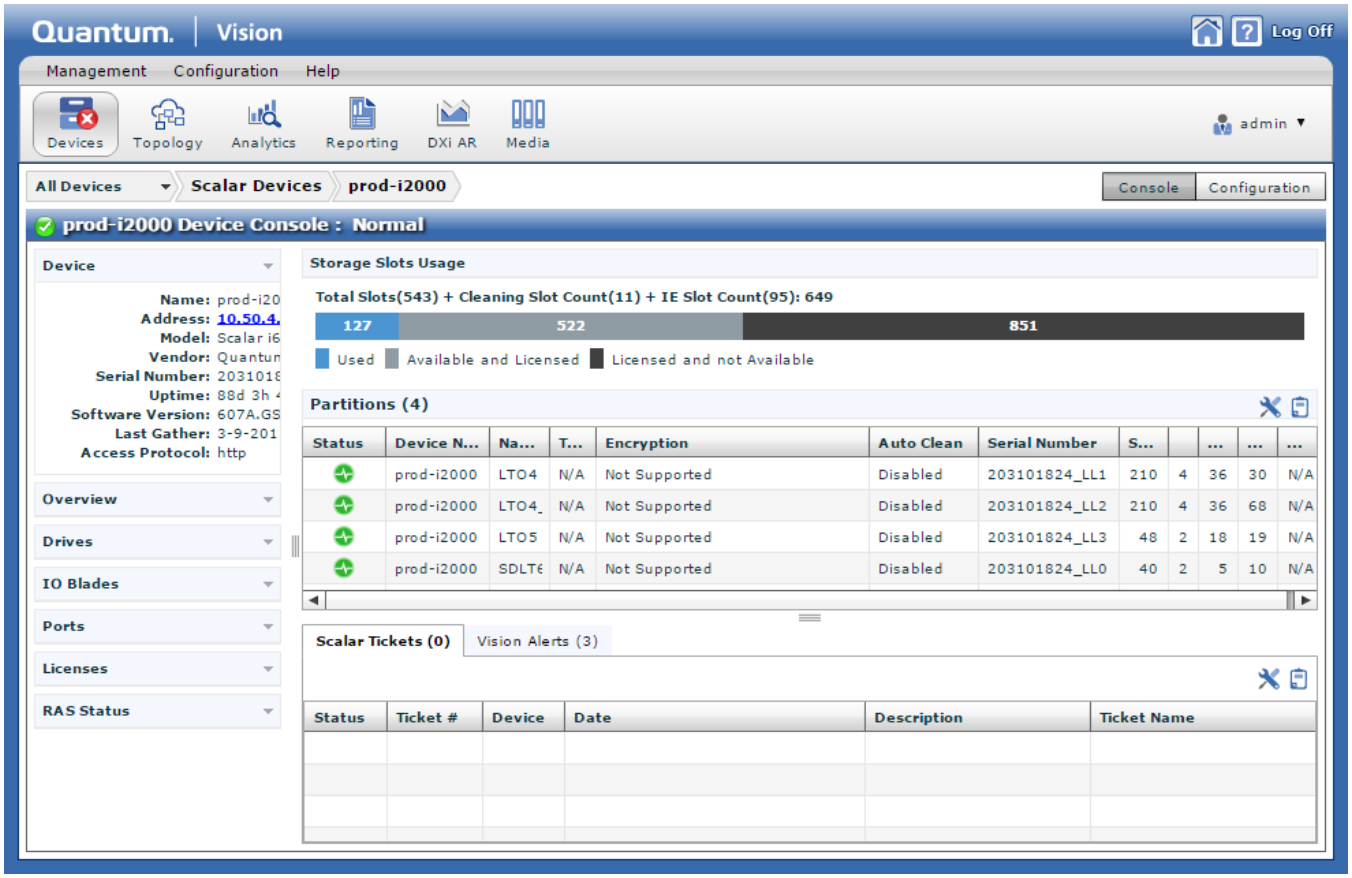
Figure 96: Scalar Consolidated Console



Scalar Device Console

Use the Scalar Device console to view information about an individual Scalar tape library, including device component status, storage slot usage, partition component status, and tickets and alerts. See Navigate an Individual Scalar Device Console on page 143.

Figure 97: Scalar Device Console



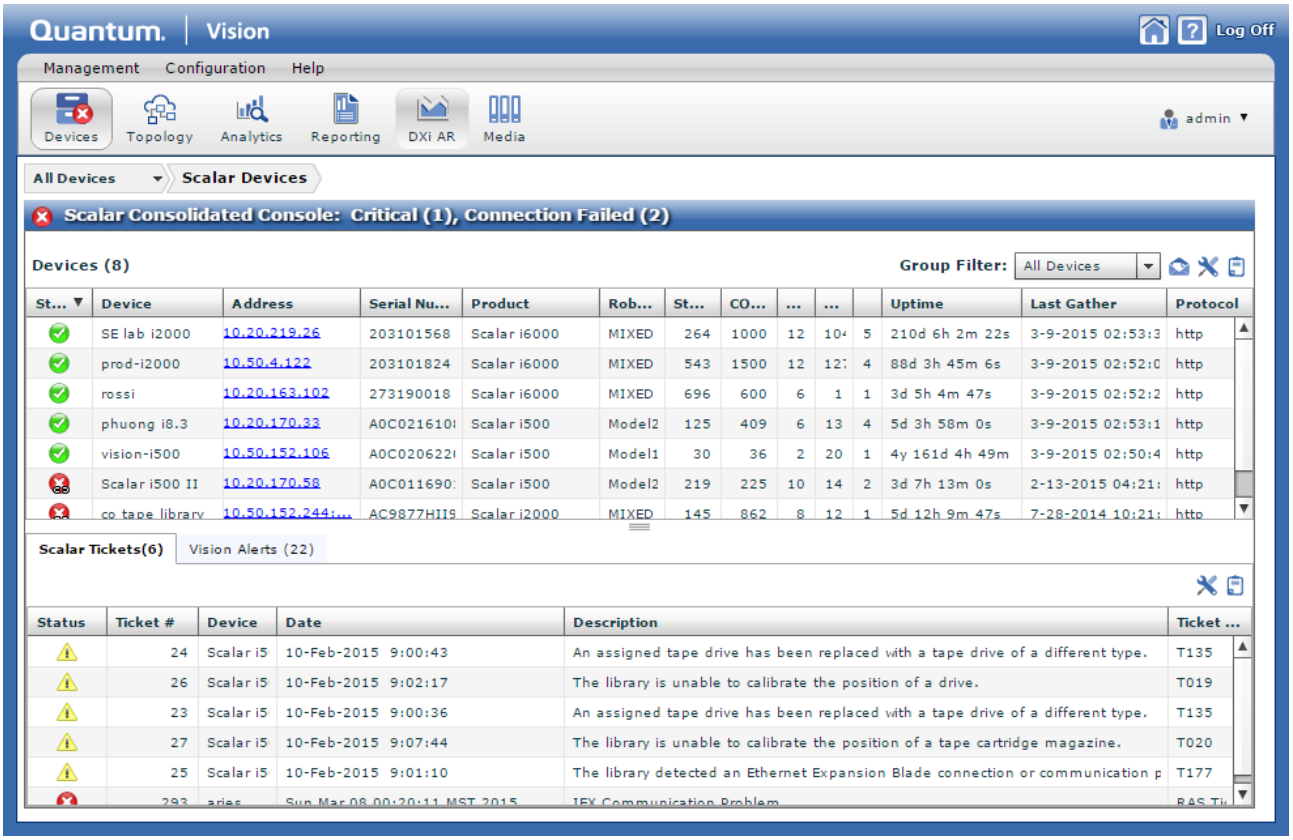
Navigate the Scalar Consolidated Console

Use the Scalar Consolidated console to monitor tape libraries within the Scalar Devices Group.

Navigate the Scalar Consolidated Console

1. From the **All Devices** drop-down list on the **Device** console, select **Scalar Devices** to display the **Scalar Consolidated** console.

Figure 98: Scalar Consolidated Console



2. In the **Devices** pane, view the following information:

Column	Definition
Status	The color-coded icon indicating the tape library's status.
Device	The name assigned to the tape library when it was discovered in Vision.
Address	The tape library's IP address or host name. Click the IP address or host name to launch the native management interface for the tape library.
Serial Number	The tape library's serial number.
Product	The Quantum product name for the tape library.
Robotics Model	The type of robotics model used for the tape library.

Column	Definition
Storage Slots	The number of storage slots within the tape library.
COD Licensed Slots	The number of COD licensed slots within the tape library.
Drives	The number of tape drives installed in the tape library.
Media	The number of media drives installed in the tape library.
Partitions	The number of configured partitions within the tape library.
Uptime	The amount of time that the tape library has been communicating with the Vision server.
Last Gather	The last time status data was received from the tape library.
Protocol	**The device's encryption protocol** • **http** – The data collection path to the device uses an unencrypted connection. • **https** – The data collection path to the device uses an encrypted connection.

3. In the **Device Alerts** pane, view the following information on the **Scalar Tickets** tab:

Column	Description
Status	The color-coded icon indicating the tape library's status.
Ticket #	The service ticket number for the tape library.
Device	The tape library for which the ticket has been generated.
Date	The date on which the service ticket was opened.
Description	A brief description of the issue on the service ticket.
Ticket Name	The type of ticket, such as **RAS Ticket**.

4. In the **Device Alerts** pane, view and acknowledge alert notifications, as needed. See Manage Vision Alert Notifications on page 101.

Navigate an Individual Scalar Device Console

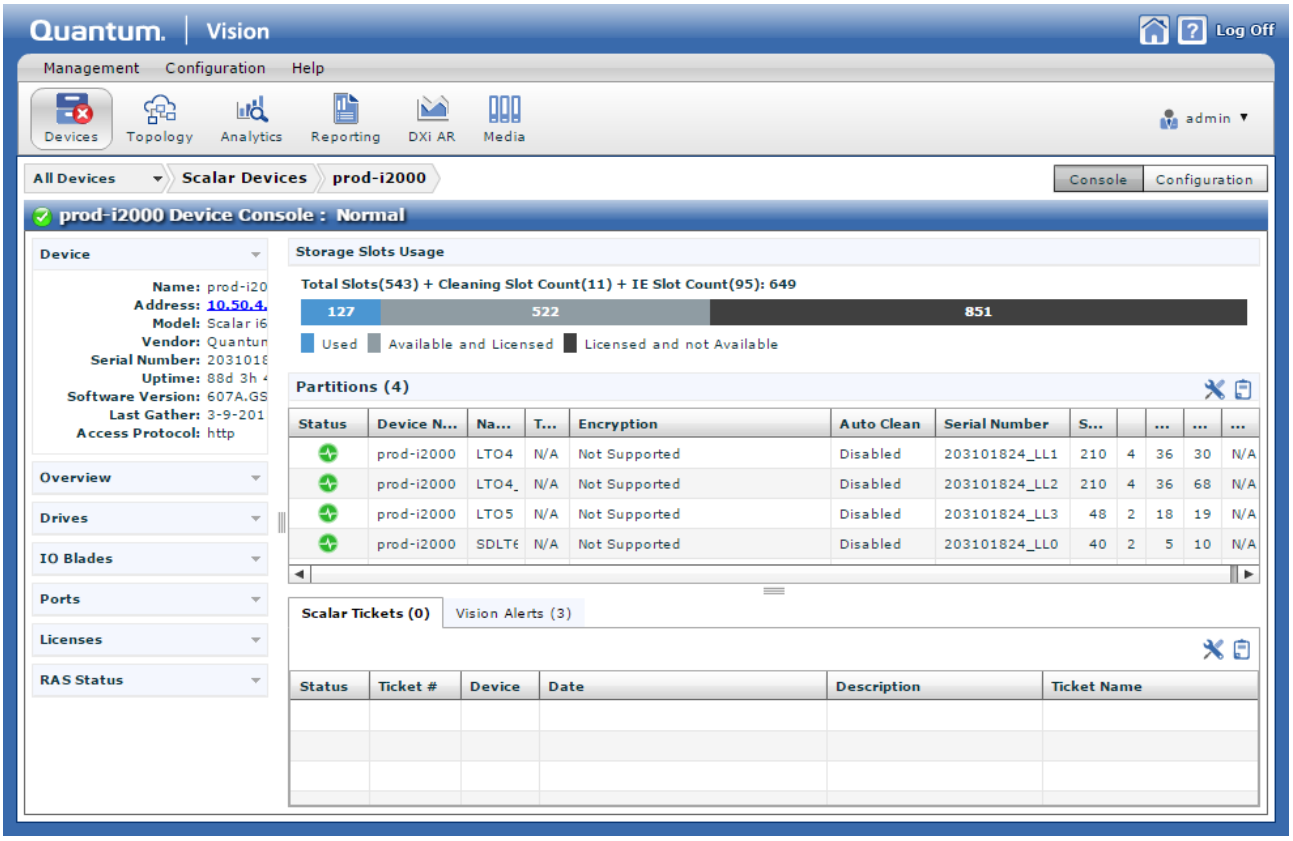
Use the Scalar Device console to view information about an individual Scalar tape library, including device component status, storage slot usage, partition component status, and tickets and alerts.

For information about Scalar tickets and alerts, see Navigate the Scalar Consolidated Console on page 141.

Navigate through the Device pane on the Scalar Device Console

1. From the **Devices** console, double-click the Scalar tape library for which to display the **Scalar Device** console.

Figure 99: Scalar Device Console



2. In the **Device** pane, view the following information about the components within the Scalar tape library.

Note: Not all components display for each Scalar tape library. The displayed components depend upon the tape library's configuration. Click the arrow next to a component to show or hide a list of sub-components.

Component	Description
Device	**Device-specific information** • **Name** – The tape library's name. • **Address** – The tape library's IP address/hostname. Click to launch the native management interface for the Scalar tape library. • **Model** – The tape library's model. • **Vendor** – The vendor from whom the tape library was purchased. • **Serial Number** – The tape library's serial number. • **Uptime** – The amount of time that the tape library has been communicating with the Vision server. • **Software Version** – The current software version of the tape library. • **Last Gather** – The last time status data was received from the tape library. • **Access Protocol** – The device's encryption protocol.
Overview	Total number of each type of component within the tape library.
Drives	**Tape drive information** • Status of the drive, whether **Varied On** or **Varied Off**. • Partition in which the drive exists. • The type of drive, such as **LT06**. • The number assigned to the drive. • The drive's reported serial number. • The drive's interface type, such as **FIBRE**. • The drive's encryption status, such as **Application Managed**. • The drive's mount status, such as **Empty**. Double-click a row to view this same information in a table format on the **Drives Details** dialog box.
IO Blades	**I/O Blade information** • The type of I/O Blade, such as **Quantum FC IOB/7404**. • The HPF, such as **Disabled**. • The I/O Blade's serial number. Double-click a row to view this same information, along with the I/O Blade's location, software version, and status in a table format on the **IO Blade Details** dialog box.

Component	Description
LTFS Blades	**LTFS Blade information** • The type of LTFS Blade, such as LTFS-1. • The LTFS Blade's IP address. • The LTFS Blade's serial number. Double-click a row to view this same information, along with the LTFS Blade's location, offline or online status (mode), partition, software version, and status in a table format on the **LTFS Blade Details** dialog box.
Ports	**Fibre Channel port information** • The type of I/O blade, such as **Quantum FC IOB/7404**. • The port's number. • The WWPN assigned to the port. • The type of port, such as **Initiator** or **Target**. Double-click a row to view this same information, along with the port's connection speed and type, index number, loop ID, and status in a table format on the **Port Details** dialog box.
Licenses	**Tape library licensing information** • Tape library's licensed features. • The number of licenses for each feature. Double-click a license to view this same information in a table format on the **License Details** dialog box.
RAS Status	Tape library's subsystem components. Double-click a component to view its status on the **RAS Status Details** dialog box.

Navigate the Storage Slots Usage pane

1. From the **Devices** console, double-click the Scalar tape library for which to display the **Scalar Device** console.
2. In the **Storage Slot Usage** pane above the bar graph, view the number of available, cleaning, IE, and total slots for the tape library.

3. In the bar graph, view the following information:

Bar Graph Block	Description
Used (blue)	The number of slots within the tape library that are currently being used.
Available and Licensed (gray)	The number of slots within the tape library that are currently available and licensed.
Available and not Licensed (light gray)	The number of slots within the tape library that are currently not licensed but would be available.
Licensed and not Available (dark gray)	The number of slots within the tape library that are currently licensed but not available.

Additional Information

- If the number of available slots equals the number of licensed slots, neither **Licensed and not Available** nor **Available and not Licensed** displays.
- If the number of available slots is less than the number of license slots, **Licensed and not Available** displays.
- If the number of available slots is greater than the number of licensed slots, **Available and not Licensed** displays.

Navigate the Partitions pane

1. From the **Devices** console, double-click the Scalar tape library for which to display the **Scalar Device** console.
2. In the **Partitions** pane, view the following information:

Column	Description
Status	The color-coded icon indicating the status of the partition.
Device Name	The name of the device within the partition.
Name	The name of the partition.
Type	The type of partition, such as **Standard**.
Encryption	The partition's encryption status, such as **Application Managed**.
Auto Clean	The partition's auto clean status, such as **Disabled**.

Column	Description
Serial Number	The partition's serial number.
Storage Slots	The number of storage slots within the partition.
Drives	The number of drives within the partition.
IE Slots	The number of IE slots within the partition.
Media	The number of media drives within the partition.
Protocol	**The device's encryption protocol** • **http** – The data collection path to the device uses an unencrypted connection. • **https** – The data collection path to the device uses an encrypted connection.

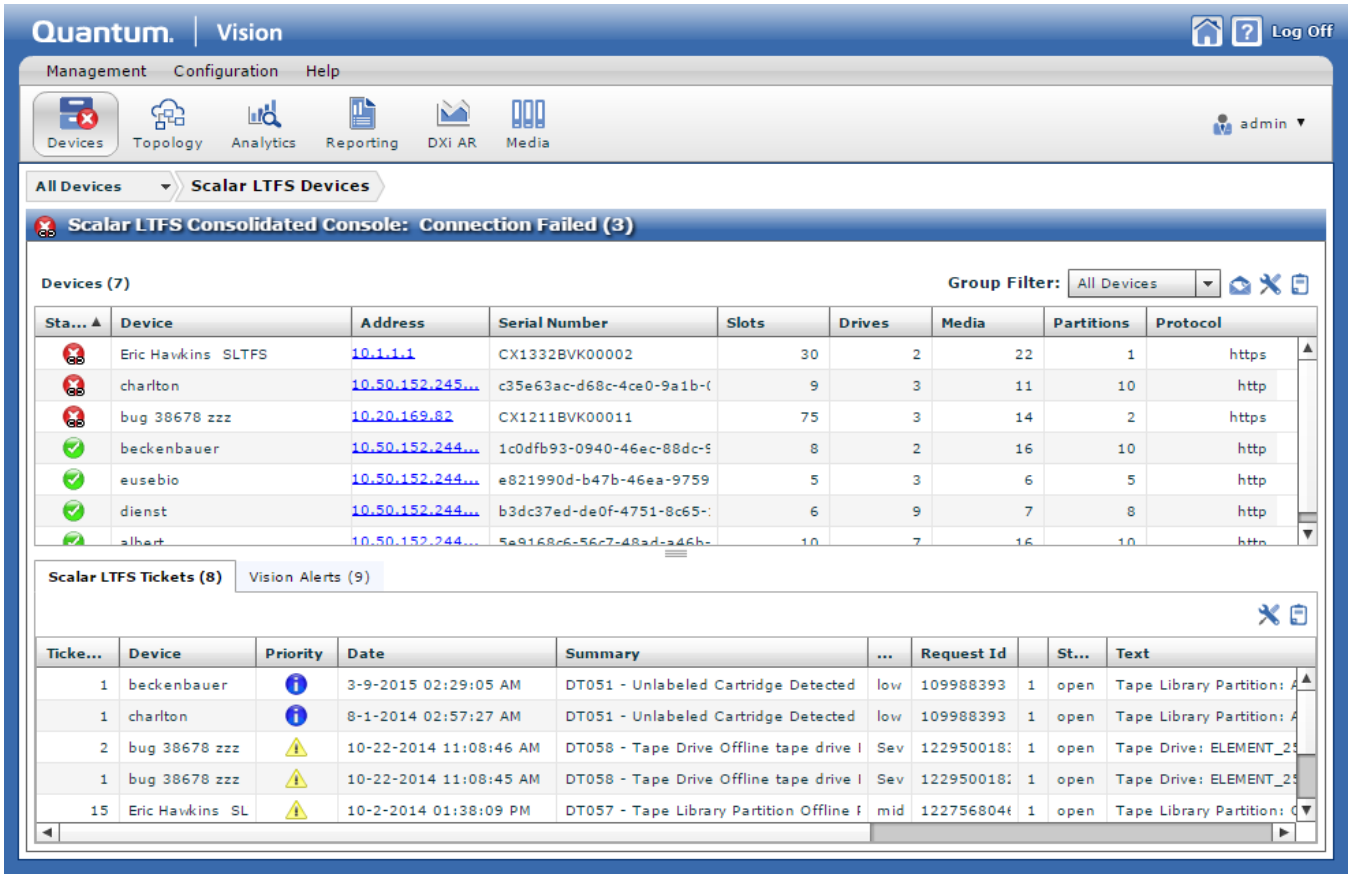
Scalar LTFS Device Consoles

To monitor Scalar LTFS devices in Vision, you can use the following two consoles, in addition to the main Vision Device console. From these consoles, you can view information about Scalar LTFS device components, partition components, and device alerts.

Scalar LTFS Consolidated Console

Use the Scalar LTFS Consolidated console to monitor systems within the Scalar LTFS Devices Group. From this console, you can also access tickets and alerts for Scalar LTFS systems. See Navigate the Scalar LTFS Consolidated Console on page 150.

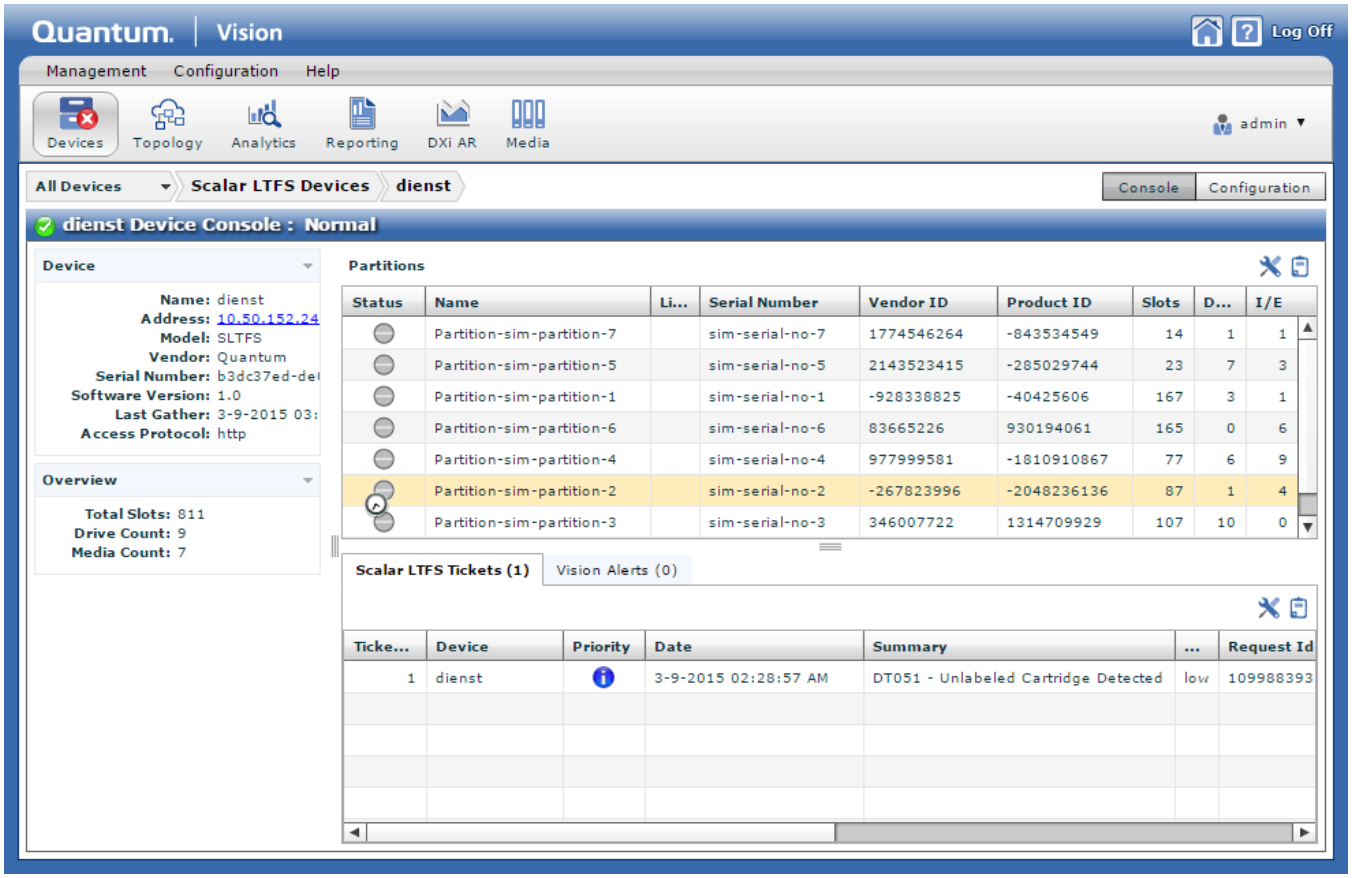
Figure 100: Scalar LTFS Consolidated Console



Scalar LTFS Devices Console

Use the Scalar LTFS Devices console to view information about an individual Scalar LTFS system, including component status, partition component status, and tickets and alerts. See Navigate an Individual Scalar LTFS Device Console on page 152.

Figure 101: Scalar LTFS Devices Console



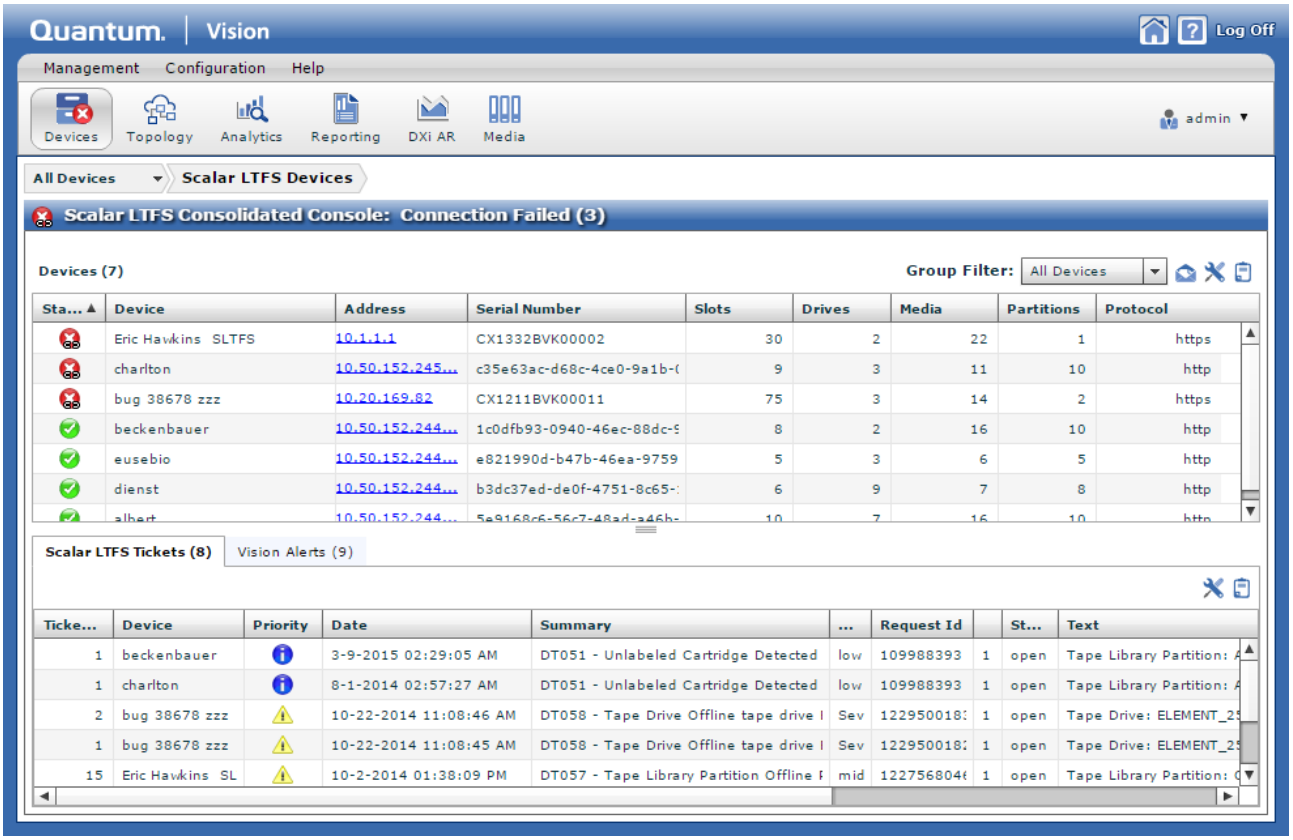
Navigate the Scalar LTFS Consolidated Console

Use the Scalar LTFS Consolidated console to monitor systems within the Scalar LTFS Group.

Navigate the Scalar LTFS Consolidated Console

1. From the **All Devices** drop-down list on the **Device** console, select **Scalar LTFS Devices** to display the **Scalar LTFS Consolidated** console.

Figure 102: Scalar LTFS Consolidated Console



2. In the **Devices** pane, view the following information:

Column	Definition
Status	The color-coded icon indicating the device's status.
Device	The name assigned to the device when it was discovered in Vision.
Address	The device's IP address or host name. Click the IP address or host name to launch the native management interface for the device.
Serial Number	The device's serial number.
Slots	The number of slots within the device.
Drives	The number of tape drives installed in the device.

Column	Definition
Media	The number of media drives installed in the device.
Partitions	The number of configured partitions within the device.
Protocol	**The device's encryption protocol** • **http** – The data collection path to the device uses an unencrypted connection. • **https** – The data collection path to the device uses an encrypted connection.

3. In the **Device Alerts** pane, view the following information on the **Scalar LTFS Tickets** tab:

Column	Description
Ticket	The service ticket number for the device.
Device	The Scalar LTFS device for which the ticket has been generated.
Priority	The color-coded icon indicating the priority of the service ticket.
Date	The date on which the service ticket was opened.
Summary	A brief summary of the issue on the service ticket.
Alert Text	The alert status associated with the service ticket, such as **Severity 2**.
Request Id	The ID of the request from which the ticket was generated.
Status Type	A numeric value indicating the status of the service ticket, such as **1** for an open-status ticket.
Status Text	The status of the service ticket, such as **open**.
Text	A description of the issue being addressed by the service ticket.
Time	The time at which the service ticket was opened.

4. Click the **Vision Alerts** tab to view and acknowledge alert notifications, as needed. See Manage Vision Alert Notifications on page 101.

Navigate an Individual Scalar LTFS Device Console

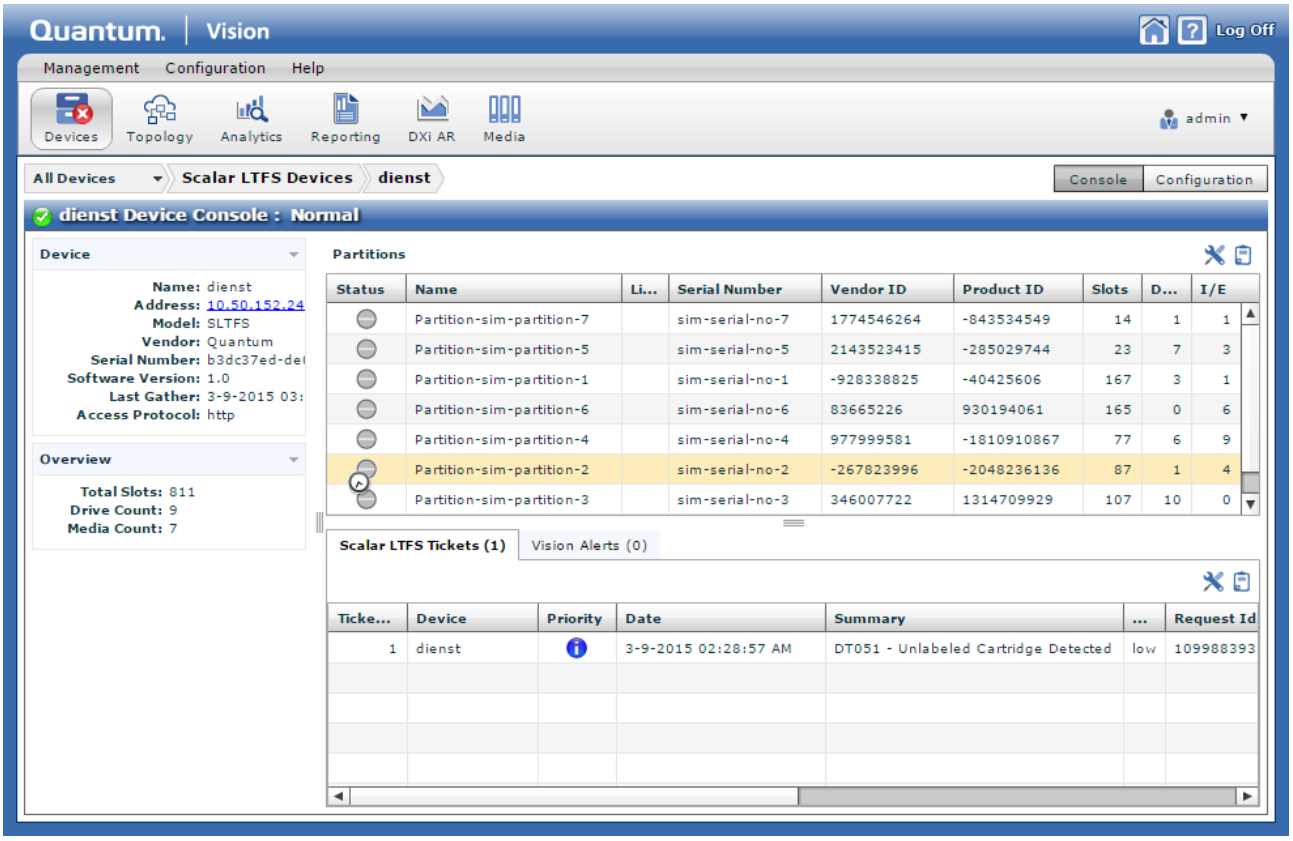
Use the Scalar LTFS Device console to view information about an individual Scalar LTFS device, including device component status, partition component status, and tickets and alerts.

For information about the Device Alert pane, see Navigate the Scalar LTFS Consolidated Console on page 150.

Navigate the Scalar LTFS Device Console

1. From the **Devices** console, double-click the Scalar LTFS device for which to display the **Scalar LTFS Device** console.

Figure 103: Scalar LTFS Device Console



2. In the **Device** pane, view the following information about the components within the Scalar LTFS device:

Note: Click the arrow next to a component to show or hide a list of sub-components.

Component	Description
Device	**Device-specific information** • **Name** – The device's name. • **Address** – The device's IP address/hostname. Click to launch the native management interface for the device. • **Model** – The device's model. • **Vendor** – The vendor from whom the device was purchased. • **Serial Number** – The device's serial number. • **Software Version** – The current software version of the device. • **Last Gather** – The last time status data was received from the device. • **Access Protocol** – The device's encryption protocol.
Overview	Total number of slots, drives, and media within the Scalar LTFS device.

3. In the **Partitions** pane, view the following information about the partitions within the Scalar LTFS device:

Column	Description
Status	The color-coded icon indicating the status of the partition.
Name	The name of the partition.
Library	The library with which the partition is associated, if any.
Serial Number	The partition's serial number.
Vendor ID	The ID of the vendor from whom you purchased the product.
Product ID	The ID of the product associated with the partition.
Slots	The number of storage slots within the partition.
I/E	The number of IE slots within the partition.

vmPRO Device Consoles

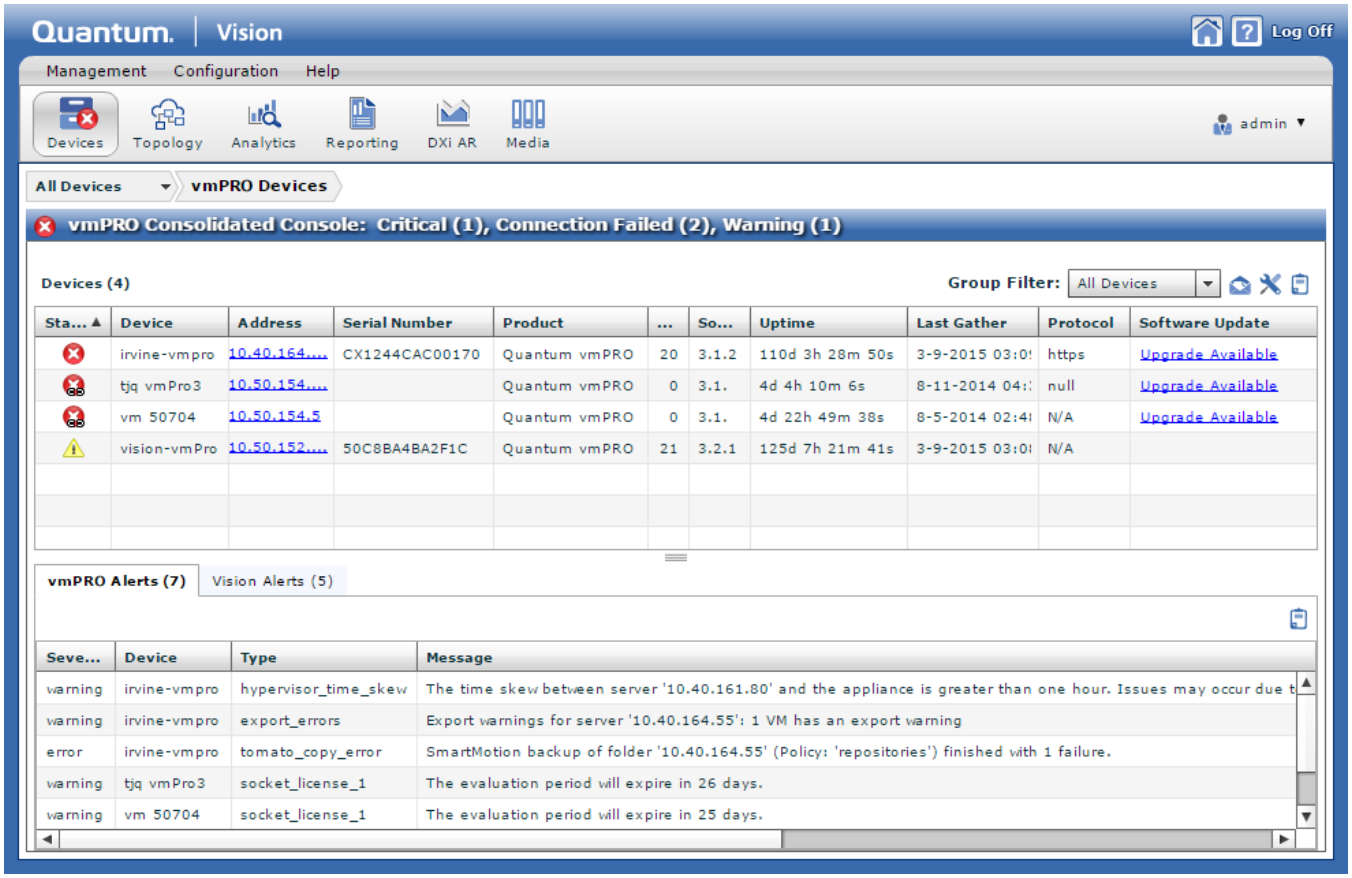
To monitor vmPRO appliances in Vision, you can use the following two consoles, in addition to the main Vision Device console. From these consoles, you can view information about vmPRO appliance components, virtual machines (VMs), and appliance alerts.

vmPRO Consolidated Console

Use the vmPRO Consolidated console to monitor vmPRO appliances within the vmPRO Devices Group. From this console, you can also access vmPRO-specific alerts and Vision alerts for vmPRO appliances. See Navigate the vmPRO Consolidated Console on page 158.

In addition, if a vmPRO software update is available for an appliance, you can update the software directly from this console. See Update vmPRO Software from Vision on the next page.

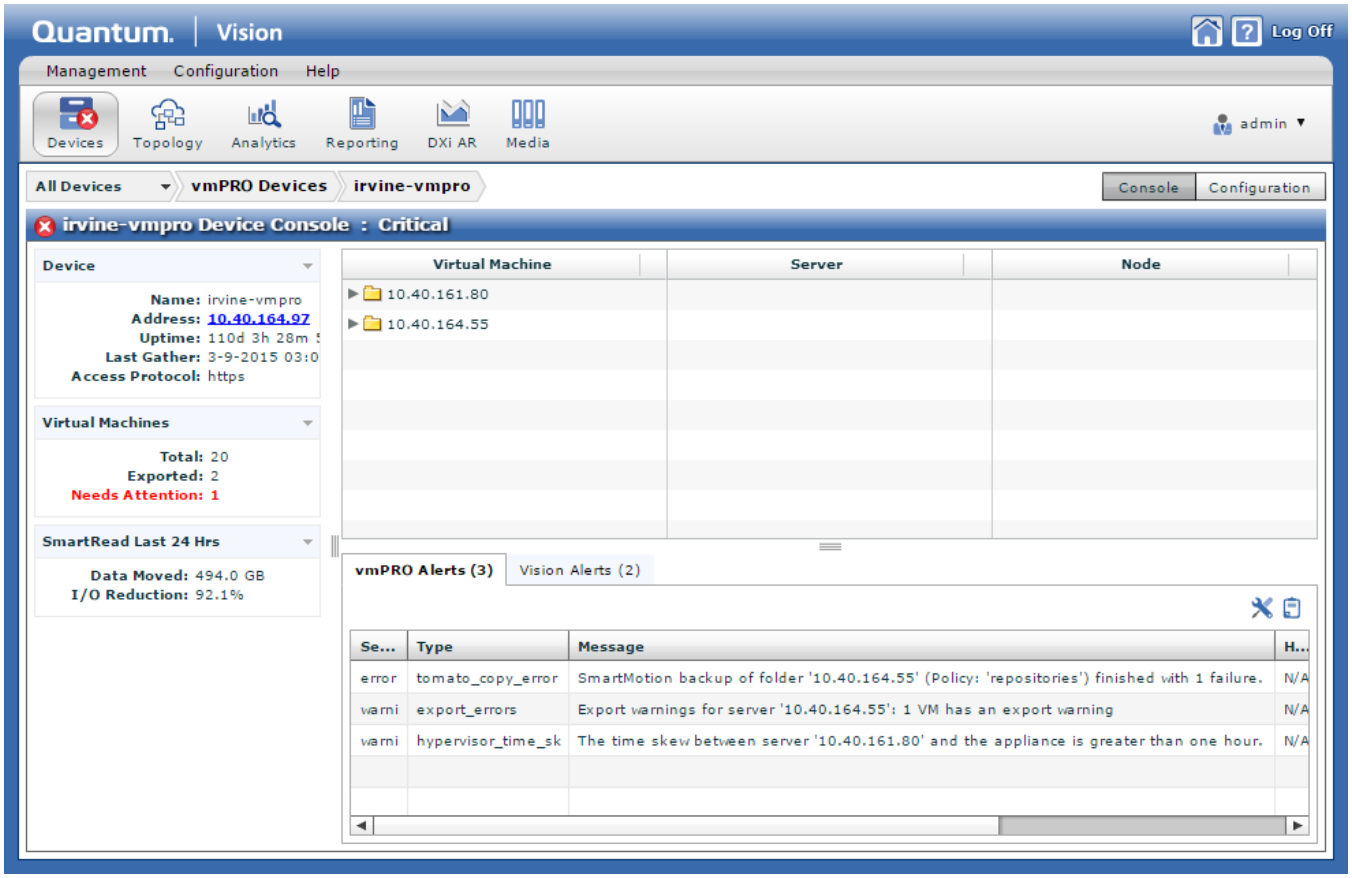
Figure 104: vmPRO Consolidated Console



vmPRO Device Console

Use the vmPRO Device console to view information about an individual vmPRO appliance, including device component status, VM data, and alert notifications. See Navigate an Individual vmPRO Device Console on page 160.

Figure 105: vmPRO Device Console



Update vmPRO Software from Vision

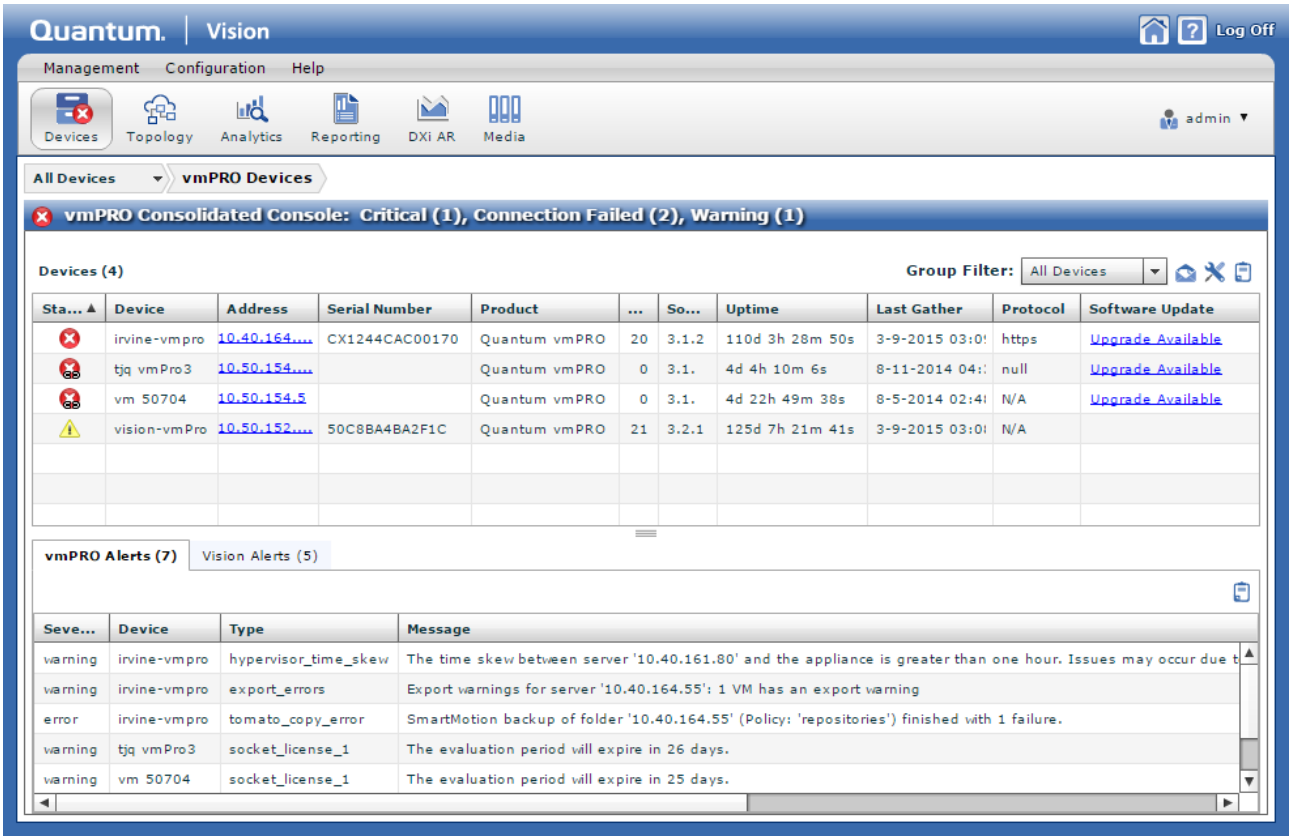
Use the vmPRO Consolidated console to see if a newer version of Quantum vmPRO is available for the appliance. If an update is available, you can access that update right from the vmPRO Consolidated console.

The vmPRO Software Update feature is only available for vmPRO versions 3.1 and newer.

Update vmPRO software from Vision

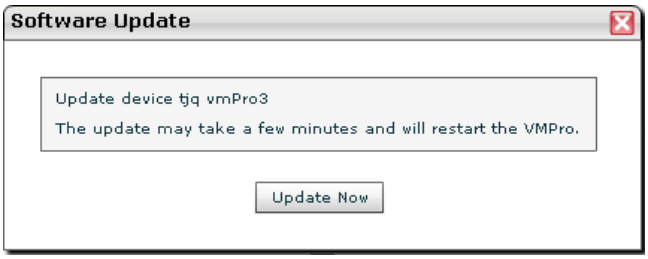
1. From the **All Devices** drop-down list on the **Device** console, select **vmPRO Devices** to display the **vmPRO Consolidated** console.

Figure 106: vmPRO Consolidated Console



2. View the **Software Update** column of the **Devices** pane. If an **Upgrade Available** link is in the column, a newer version of Quantum vmPRO exists for the appliance.
3. Click the **Upgrade Available** link to display the **Soft Update** dialog box.

Figure 107: vmPRO Software Update Dialog Box



4. In the **Software Update** dialog box, click **Update Now** to begin the software update.

   After the software update has finished, **`Upgrade has finished`** displays in the **Software Update** column.

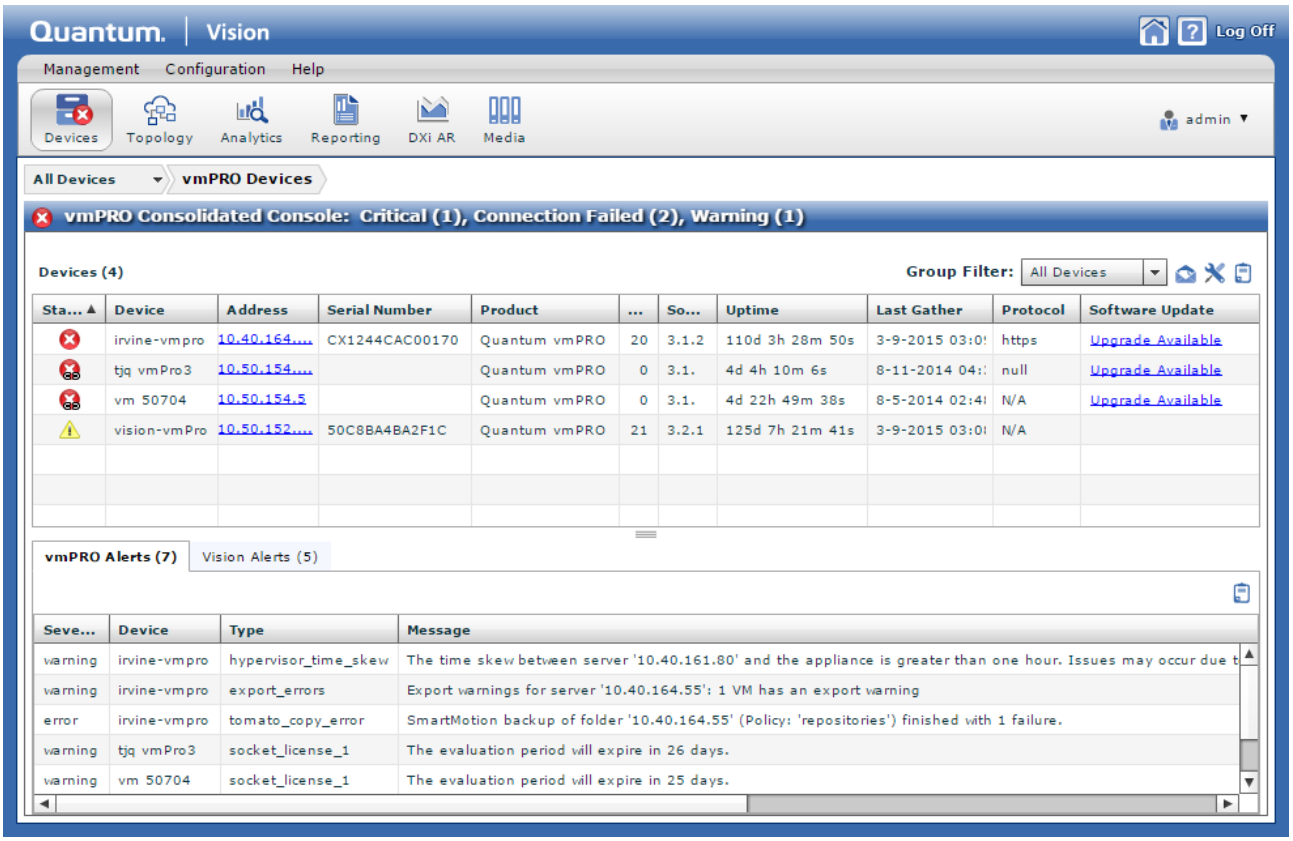
Navigate the vmPRO Consolidated Console

Use the vmPRO Consolidated console to monitor appliances within the vmPRO device group, and to access both vmPRO-specific alerts and Vision alerts for vmPRO appliances.

Navigate the vmPRO Consolidated Console

1. From the **All Devices** drop-down list on the **Device** console, select **vmPRO Devices** to display the **vmPRO Consolidated** console.

Figure 108: vmPRO Consolidated Console



2. In the **Devices** pane, view the following information:

Column	Definition
Status	The color-coded icon indicating the appliance's status.
Device	The name assigned to the appliance when it was discovered in Vision.

Column	Definition
Address	The appliance's IP address or host name. Click the IP address or host name to launch the native management interface for the appliance.
Serial Number	The appliance's serial number.
Product	The Quantum product name for the appliance.
VMs	The number of virtual machines (VMs) that are being backed up by the appliance.
Software Version	The current software version for the appliance.
Uptime	The amount of time that the appliance has been communicating with the Vision server.
Last Gather	The last time status data was received from the appliance.
Protocol	**The device's encryption protocol** • **http** – The data collection path to the device uses an unencrypted connection. • **https** – The data collection path to the device uses an encrypted connection. **Note:** The data collection path to vmPRO appliances is always encrypted.
Software Update	Displays **Upgrade Available** when a newer version of Quantum vmPRO software is available for the appliance. See Update vmPRO Software from Vision on page 156.

3. In the **Device Alerts**pane, view the following vmPRO-specific alert information on the **vmPRO Alerts** tab:

Column	Description
Severity	The severity of the alert, such as **warning**.
Device	The appliance to which the alert applies.
Type	The type of alert, such as **socket_license_1**.
Message	An explanation of the alert, such as **The evaluation period will expire in <x> days**.

4. In the **Device Alerts** pane, view and acknowledge alert notifications on the **Vision Alerts** tab, as needed. See Manage Vision Alert Notifications on page 101.

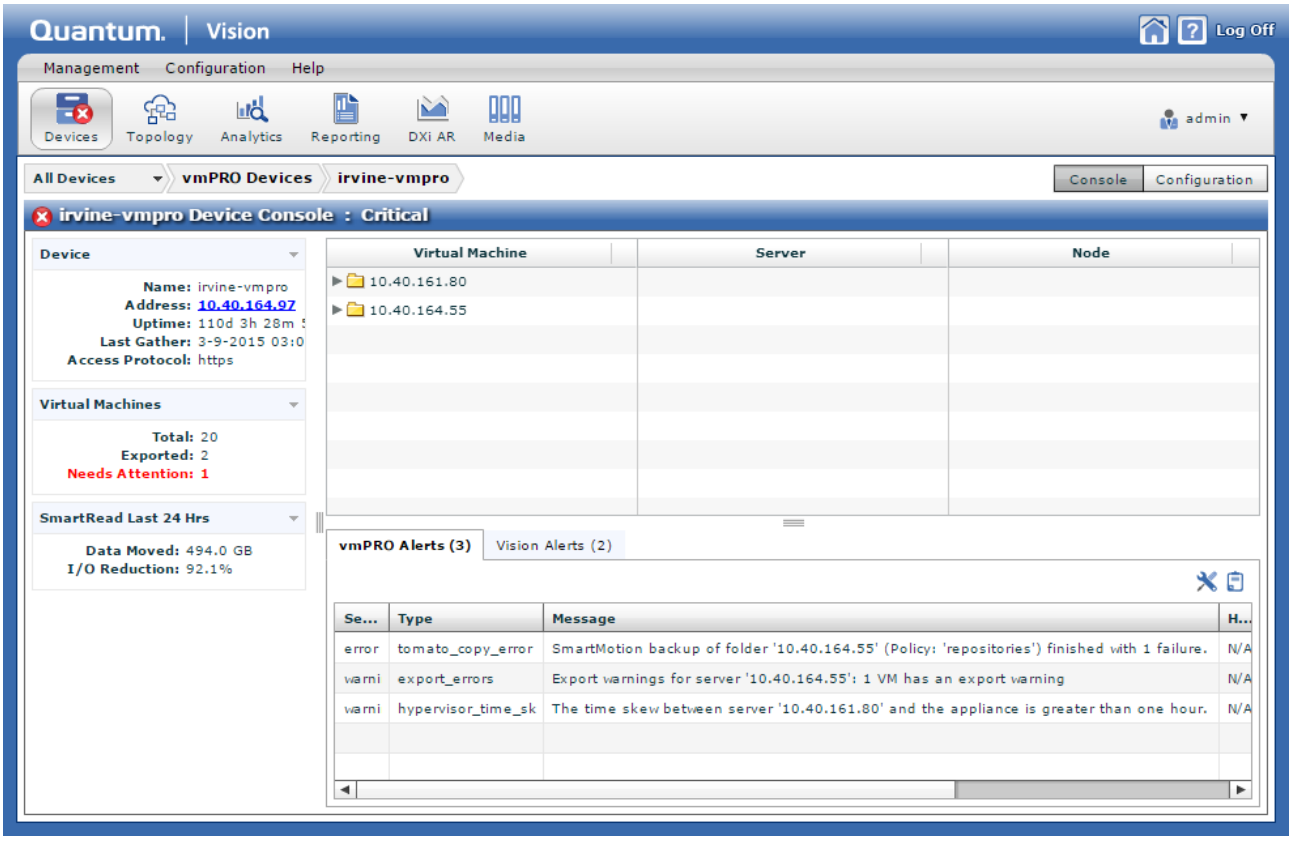
Navigate an Individual vmPRO Device Console

Use the vmPRO Device console to view information about an individual vmPRO appliance, including appliance component status, virtual machine (VM) data, and alert notifications.

Navigate an individual vmPRO Device Console

1. From the **Devices** console, double-click the vmPRO appliance for which to display the **vmPRO Device** console.

Figure 109: vmPRO Device Console



2. In the **Device** pane, view the following information:

Note: Click the arrow next to a component to show or hide a list of sub-components.

Component	Description
Device	**vmPRO appliance-specific information** • **Name** – The appliance's name. • **Address** – The appliance's IP address/hostname. Click to launch the native management interface for the vmPRO appliance. • **Uptime** – The amount of time that the appliance has been communicating with the Vision server. • **Last Gather** – The last time status data was received from the appliance. • **Access Protocol** – The device's encryption protocol, which is always encrypted for vmPRO appliances.
Virtual Machines	**Summary information about the VMs being backed up by the vmPRO appliance** • Total number of VMs backed up to the appliance. • Number of VMs that have been exported from the appliance. • Number of VMs requiring attention.
SmartRead Last 24 Hrs	**SmartRead information collected for the past 24 hours** • Amount of data moved on the appliance. • Amount of I/O reduction for the appliance. **Note:** SmartRead applies to vmPRO versions 3.0 and later.

3. In the **Virtual Machine** pane, view the following information:

Column	Description
Virtual Machine	Displays the appliance's hypervisors, and the VMs within each hypervisor. Hypervisors are host systems for the VMs being backed up by vmPRO. Click the arrow next to a hypervisor to view the VMs that have been configured on the hypervisor.
Server	For each VM within a hypervisor, displays the server for the VM.
Node	For each VM within a hypervisor, displays the node for the VM.

4. In the **Device Alerts** pane, view the following vmPRO-specific alert information for an appliance on the **vmPRO Alerts** tab:

Column	Description
Severity	The severity of the alert, such as **warning**.
Type	The type of alert, such as **socket_license_1**.
Message	An explanation of the alert, such as **The evaluation period will expire in <x> days**.
HV Host	The hypervisor to which the alert applies.
V Host	The virtual host to which the alert applies.
Managed Alert	Whether the alert is being managed, either **true** or **false**.
Node	The vmPRO appliance to which the alert applies.
Node UUID	The vmPRO appliance's universally unique identifier (UUID).
Object Id	The object of the alert, such as the name of the license that is expiring.
Posted	Whether the alert has been posted, either **true** or **false**.

Note: See Manage Vision Alert Notifications on page 101 for information about the **Vision Alerts** tab.

Chapter 5: Topology Console

This chapter contains the following topics:

Vision Topology Console

The Vision Topology console displays a topology map for all monitored DXi devices, Q-Cloud Protect appliances, Scalar libraries, Scalar LTFS, and vmPRO.

Presented Topology

The following information is presented on the topology map.

Replication Relationships

Source-to-target replication relationships between DXi devices and Q-Cloud Protect appliances.

Important

Vision uses the DXi and Q-Cloud Protect IP addresses — rather than hostnames — to determine replication relationships. It does not recognize replication relationships if the DXi or Q-Cloud Protect IP address is not supplied.

PTT Connections

Path to tape (PTT) connections between DXi devices and Scalar libraries.

Scalar Connections

Scalar LTFS interface connections with Scalar libraries.

vmPRO Export Connections

vmPRO data export connections with DXi devices.

Unbound Devices

Devices that are not bound to other devices.

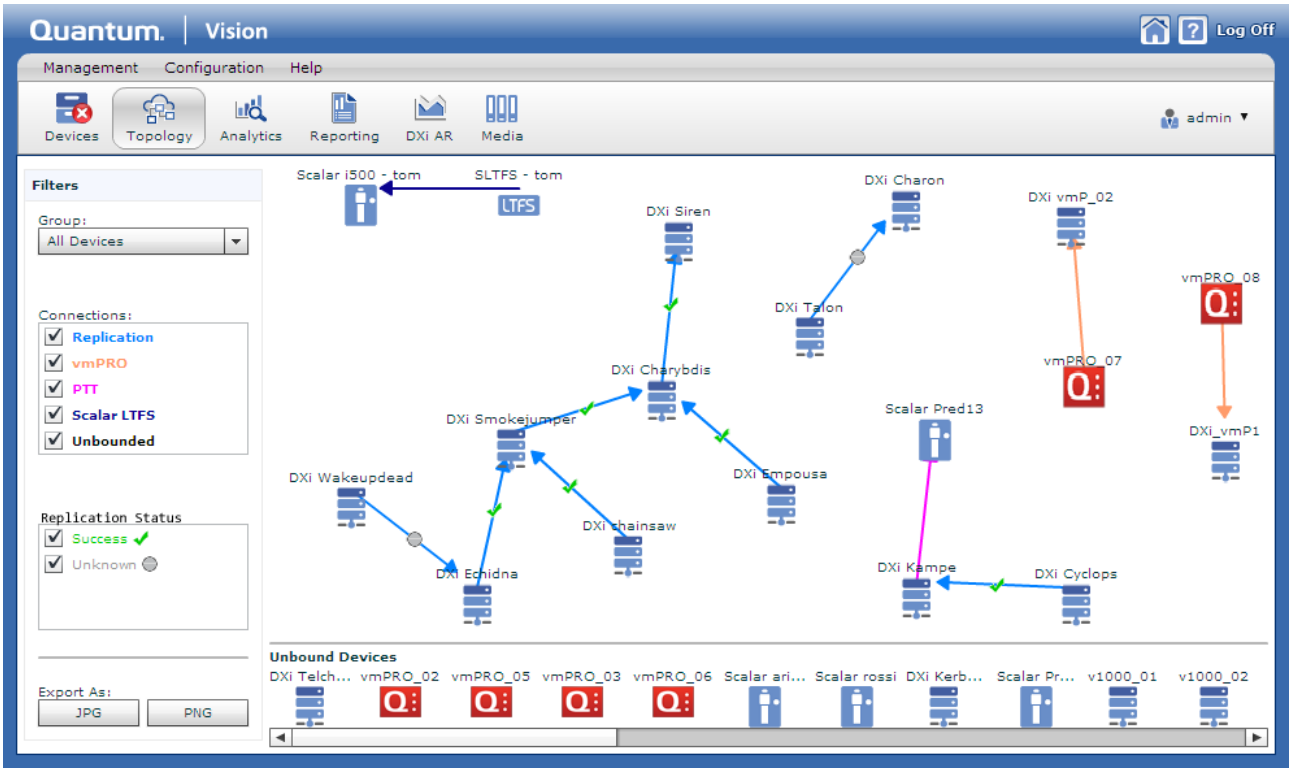
Navigate the Vision Topology Console

Use the Vision Topology console to view a map of connections between all monitored DXi devices, Q-Cloud Protect appliances, Scalar libraries, Scalar LTFS, and vmPRO.

Navigate the Topology Console

1. On the Vision toolbar, click **Topology** to display the **Topology** console.

Figure 110: Topology Console



2. Filter the display as needed:

Group drop-down list

Select the group of devices to display. See Manage Groups in Vision on page 68 for information about creating groups.

Connections area

Select one or more types of connections to display: **Replication**, **vmPRO**, **PTT**, **Scalar LTFS**, and **Unbounded**.

Note: The type of **Connections** check boxes that display depend on the actual connections that exist.

Replication Status area

Select one or more replication statuses to display: **Success, Unknown**, or **Failure**.

Note: The type of **Replication Status** check boxes that display depend on the actual replication statuses that exist.

The Topology console displays the connections between devices, along with additional information about connection status and unbound devices. For further information about reading the map, see Topology Console Icon and Mapping Keys.

3. View further details about connections, statuses, and devices by doing any of the following:

Click a device icon

A tooltip displays the device's product model, serial number, and amount of available disk space, as well as a link to the device's console.

Additional Information

For DXi devices and Q-Cloud Protect appliances, keep the following in mind:

- Free disk space is unallocated space.
- Reclaimable disk space is space that is allocated, but that can be reclaimed after Space Reclamation is run.
- Available disk space is free + reclaimable space.

Click a DXi device or Q-Cloud Protect appliance icon

A tooltip displays additional replication information for the DXi device or Q-Cloud Protect appliance.

Important

Vision uses the DXi and Q-Cloud Protect IP addresses — rather than hostnames — to determine replication relationships. It does not recognize replication relationships if the DXi or Q-Cloud Protect IP address is not supplied.

Click a Scalar library icon

A tooltip displays the number of slots, drives, media, and partitions within the library.

Click a Scalar LTFS icon

A tooltip displays information about the slot fill rate for the device.

Click the color-coded status icon

Select **Go To Replication Report** to view the most recent replication report for a DXi device or Q-Cloud Protect appliance.

Click the color-coded status mark

A tooltip displays additional PTT information.

Export the topology map as a graphic file

1. In the **Export As** area, click either **JPG** or **PNG** to export the topology as either a .jpg or .png file.
2. In the **Save As** dialog box, browse to the location to save the file.
3. In the **File name** field, enter a file name for the topology map.
4. Click **Save**.

Topology Console Icon and Mapping Keys

Use the following keys to interpret the Topology console.

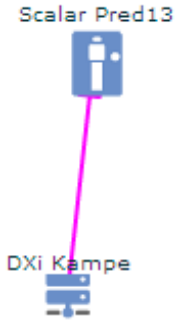
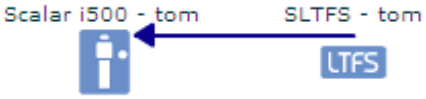
Icon Key

The **Topology Console** represents devices using different icons:

Icon	Description
	**DXi** **Q-Cloud Protect**
	**Scalar Library**
	**Scalar LTFS**
	**vmPRO**

Mapping Key

The **Topology Console** maps relationships between devices using color-coded lines and symbols:

Topology Mapping Symbols	Description
	**Source-To-Target Replication** Source-to-target replication allows source systems to replicate backed-up data to a target system **Example** A DXi6900 system can replicate its data to a Q-Cloud Protect appliance to provide enhanced data security and disaster protection. • A blue line connecting two systems indicates that they are configured for source-to-target replication. The arrow indicates the direction of replication from source to target system. • The color-coded icon on the line indicates the status of the most recent replication: green (success), red (failure), or gray (unknown). **Important** Vision uses the DXi and Q-Cloud Protect IP addresses — rather than hostnames — to determine replication relationships. It does not recognize replication relationships if the DXi or Q-Cloud Protect IP address is not supplied.
	**PTT** Path to tape (PTT) allows you to move data from a DXi system to physical tape cartridges in an attached physical tape library using a Network Data Management Protocol (NDMP) connection. A magenta line connecting two systems indicates that the corresponding systems are configured for PTT.
	**Scalar LTFS Interface** A dark blue line connecting a Scalar LTFS server to a Scalar library indicates that the Scalar LTFS server provides an LTFS interface for the Scalar library.

Topology Mapping Symbols	Description
	**vmPRO Data Export** An orange line connecting a vmPRO system (versions 3.0 and newer) to a DXi system indicates that data is being exported from the vmPRO system to the DXi device.
	**Unbound Devices** Icons in the **Unbound Devices** pane represent DXi devices, Q-Cloud Protect appliances, Scalar libraries, Scalar LTFS servers, and vmPRO systems that do not have any relationships with discovered devices.

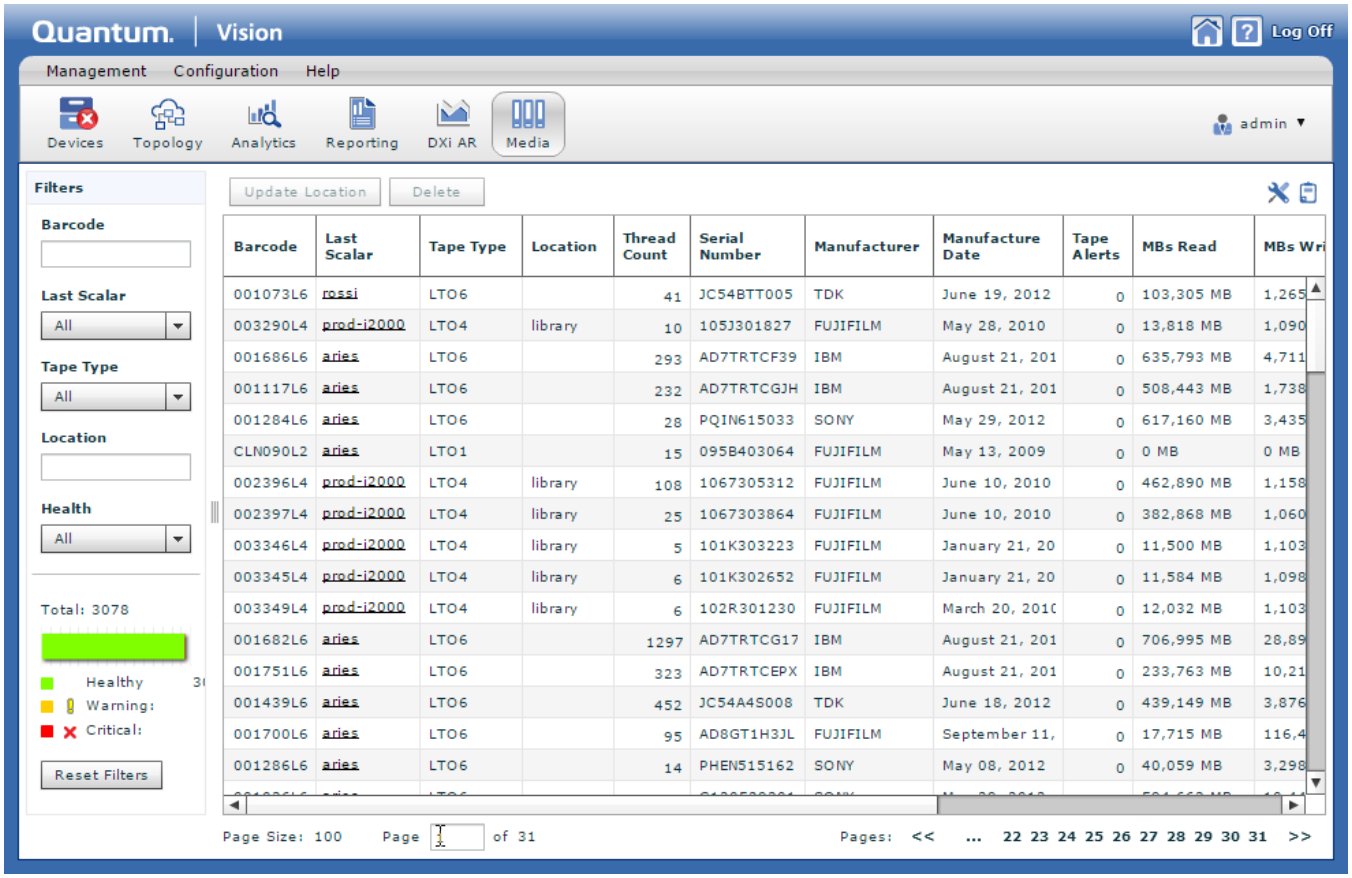
Chapter 6: Media Console

This chapter contains the following topics:

Vision Media Console

The Vision Media console displays information for tape media within Scalar libraries. Use this console to monitor Scalar libraries, update media locations, and delete obsolete media.

Figure 111: Media Console



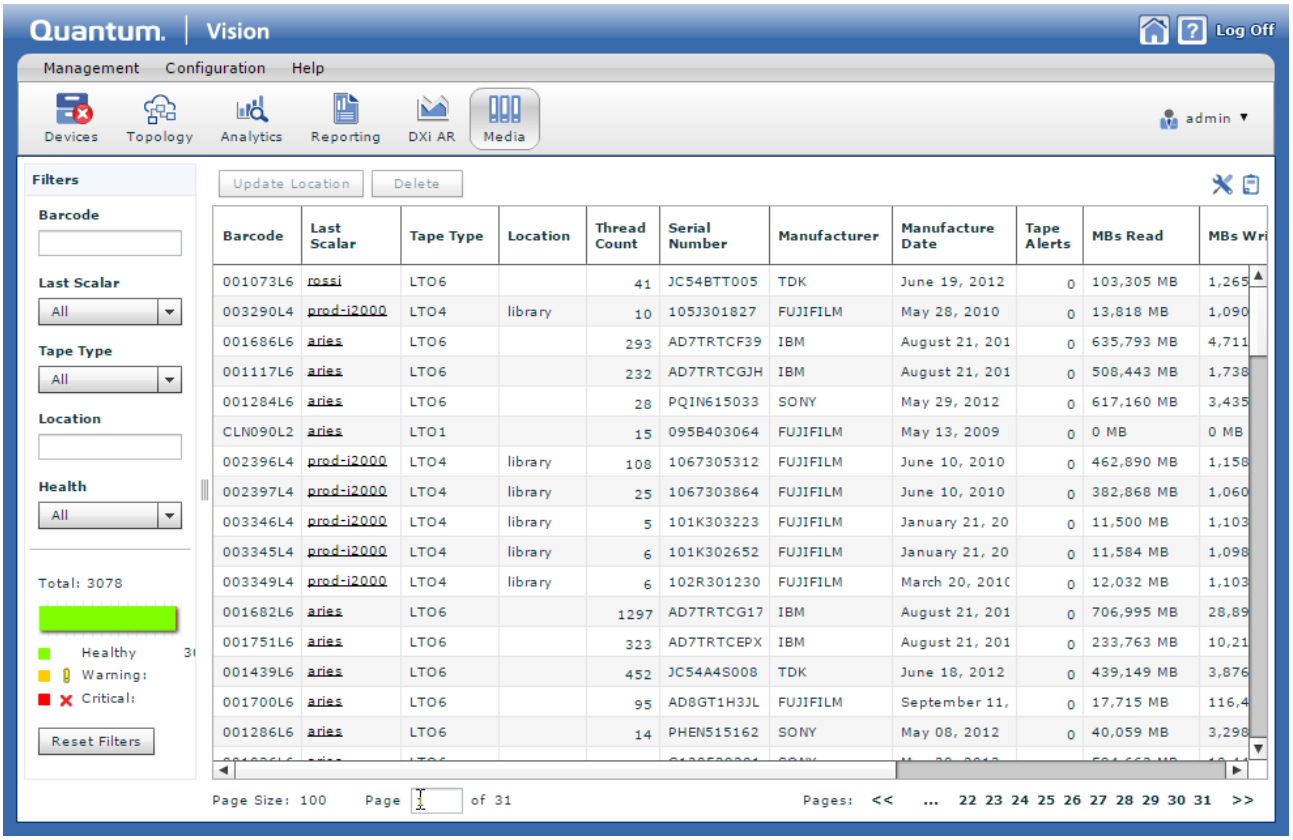
Navigate the Vision Media Console

Use the Vision Media console to monitor information for tape media within Scalar libraries.

Select information to display in the Media table

1. On the Vision toolbar, click **Media** to display the **Media** console.

Figure 112: Media Console



2. In the **Filters** pane, filter the information that displays in the **Media** table, as needed:

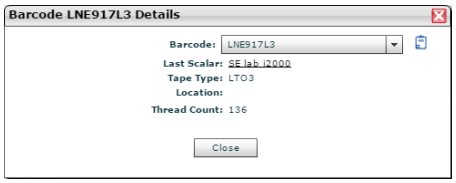
Filter	Description
Barcode	Use to display only the media with the defined barcode. Enter the barcode of the media for which to view information. You can use wild card searches in this field by entering either the percent sign (**%**) or an asterisk (*****).
Last Scalar	Use to display the last physical device from which Vision received media status. From the drop-down list, select one or more Scalar libraries for which to view information.
Tape Type	Use to display only the selected tape types. From the drop-down list, select one or more types of tapes for which to view information.
Location	Use to display only media residing in the selected location. Enter a specific Scalar library location for which to view information.

Filter	Description
Health	Use to display only Scalar libraries with the selected health status. From the drop-down list, select one or more health statuses for which to view information. **Additional Information** The health status is a roll up of a Scalar library's thread count, tape alert, and Extended Data Life Management (EDLM) status. The total number of Scalar libraries and the total number of libraries for each health status are displayed underneath the **Health** field. Hold the cursor over the status bar to see a tooltip with the health status, number and percentage of libraries with the associated health status, and total number of libraries.

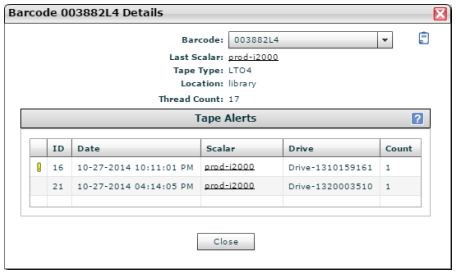
Click **Reset Filters** to clear the selection criteria and reset the **Media** table to its default state, as needed.

Media Table Columns

The following provides descriptions of the Media table's columns.

Column	Description
Barcode	The barcode of the media. Double-click a row to display the **Barcode Details** dialog box. **Figure 113:** Barcode Details Dialog Box 
Last Scalar	The last physical device from which Vision received status for the media. Click the device to display the **Scalar Device Console** for that device. See Navigate an Individual Scalar Device Console on page 143.
Tape Type	The type of tape for the media.

Column	Description
Location	The current location of the media, either **library**, **exported**, or a custom location. The location value can be configured on the Scalar library or manually set through Vision. See Update Media Locations from Vision on page 176. **Additional Information** The location for media can display as **unknown** in the following scenarios: • The **Last Scalar** is listed and the media is located in the library I/E station or in a drive. • The **Last Scalar** is **N/A** and the media has been removed from the library. **Track Exported Media** To track exported media, you must enable Media Security Notifications on the Scalar i2000/i6000 library. a. Access the LMC client for the library and select **Setup > Notifications > Media Security**. b. Select the notifications to track in Vision, and then click **OK**.
Thread Count	The number of times the media has been threaded onto a tape drive. Use the thread count to help determine the health of the media (media health is also determined by tape alerts and EDLM status). Different thread counts indicate the following: • <8000 – The media's status is **Healthy**. • 8,000 – 10,000 – The media's status is **Warning**. • >10,000 – The media's status is **Critical**.
Serial Number	The Media's serial number.
Manufacturer	The manufacturer of the media.
Manufacture Date	The date on which the media was manufactured.

Column	Description
Tape Alerts	The number and type of alerts associated with the tape. The following icons indicate the type of alert: – Warning – Critical Double-click a row to display the **Barcode Details Tape Alert** dialog box. **Figure 114:** Barcode Details Tape Alert Dialog Box  For additional information about tape alerts, see http://www.tapealert.org/specifications.
MBs Read	The amount of data in megabytes (MBs) read from the media.
MBs Written	The amount of data in MBs written to the media.
Last Scalar LTFS	The last Scalar LTFS device that was using the media as an LTFS. Click the link to launch the native management interface for the device.
EDLM Type	The type of EDLM scan that was performed.
EDLM Status	The EDLM status for the device's media. A status of **N/A** indicates that Vision could not determine the device's status.
EDLM Date	The date that the last EDLM scan was completed.
Encryption	The encryption type for the media.
Attribute	The media's attribute: • Write Once Read Many (**WORM**) • Write Many Read Many (**WMRM**) • **Cleaning**

Column	Description
Recovered Read Errors	The number of recovered read errors for the media.
Unrecovered Read Errors	The number of unrecovered read errors for the media.
Recovered Write Errors	The number of recovered write errors for the media.
Unrecovered Write Errors	The number of unrecovered write errors for the media.

Navigate Through Multiple Pages on the Media Table

The Media table displays information for the selected tape media. If there are more than 100 rows of information, Vision displays the information on multiple pages.

Navigate between pages on the Media table

- In the **Page** field, enter the page to navigate to and press **Enter** to view another page of information.
- Click **<<** or **>>** to move backward or forward through pages.

Update Media Locations from Vision

By default, the Media console displays media's location as one of the following:

- **library** if the media is located in a library (all Scalar libraries)
- **exported** if the media has been exported from the library (Scalar i2000/i6000 libraries only).

You can enter a custom location for media from the Media console, such as when media is exported to a remote location.

Update the location for media from Vision

1. On the **Media** console, select the media in the table and click **Update Location** to display the **Update Media Location** dialog box.

Figure 115: Update Media Location Dialog Box

2. In the **New Location** field, enter the new location for the media.
3. Click **Submit** to update the media's location.

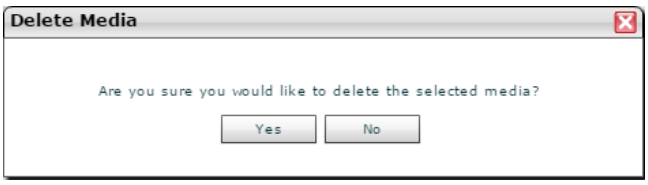
Delete Media from Vision

If media is no longer used, you can delete it from the Vision Media console.

Delete media from the Media Console

1. On the **Media** console, select the media in the table and click **Delete** to display the **Delete Media** dialog box.

Figure 116: Delete Media Dialog Box



2. Click **Yes** to confirm the deletion.

Chapter 7: Analytics

This chapter contains the following topics:

Vision Analytics

Vision includes a set of interactive graphs that allow you to quickly visualize and compare key statistics for DXi devices, Q-Cloud Protect appliances, Scalar libraries, and vmPRO virtual appliances. You can access these graphs at any time from the Vision Analytics Console.

What Kind of Information is Displayed?

Each interactive graph displays information about core device functionality, such as the following:

- Replication status on DXi devices or Q-Cloud Protect appliances
- SmartMotion status for vmPRO virtual appliances

- Tape alerts on Scalar libraries

DXi and Q-Cloud Protect Graphs

Scalar Library Graphs

vmPRO Virtual Appliance Graphs

Interactive Graphs in Vision Analytics

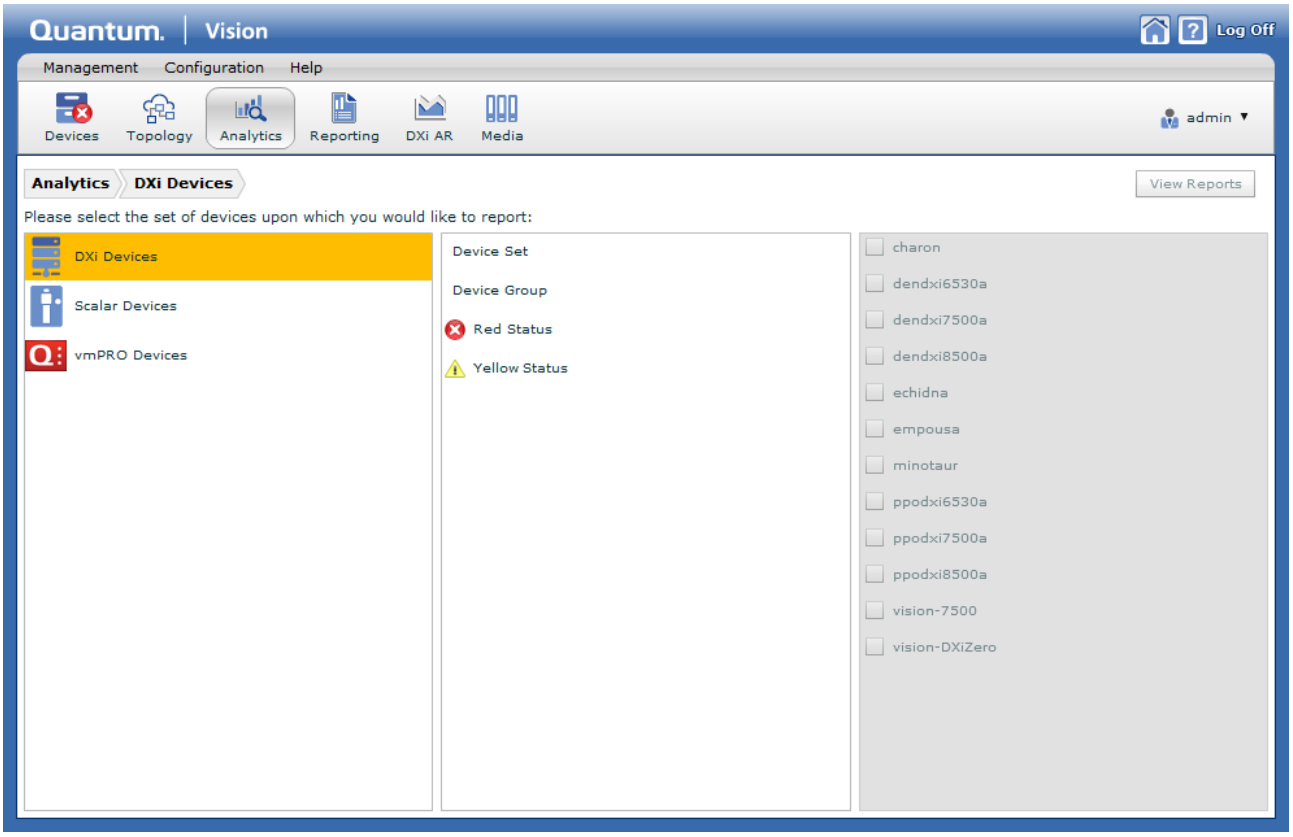
Use the Analytics console and Analytics Device Set console to view interactive graphs for DXi, Q-Cloud Protect, Scalar, and vmPRO.

Keep in mind that analytics cannot be generated for newly discovered devices until one data collection cycle has been completed.

Select devices for which to display interactive graphs

1. On the Vision toolbar, click **Analytics** to display the **Analytics** console.

Figure 117: Analytics Console



2. Select the devices for which to display the interactive graphs by doing one of the following:

Select by device family

a. In the left pane, select the device family for which to display the graphs:

- **DXi Devices**
- **Scalar Devices**
- **vmPRO Devices**

Note: Interactive graphs are not available for DXi 35/55 devices.

b. In the center pane, select **Device Group** to view graphs for all devices within a group.

c. In the right pane, select each device within the family to include in the graphs.

Select by device group

a. In the left pane, select the device family for which to display the graphs:
   - **DXi Devices**
   - **Scalar Devices**
   - **vmPRO Devices**

   Note: Interactive graphs are not available for DXi 35/55 devices.

b. In the center pane, select **Device Group** to view graphs for all devices within a group.

c. In the right pane, select one or more Vision groups to include in the graphs.

Select by alert status

a. In the left pane, select the device family for which to display the graphs:
   - **DXi Devices**
   - **Scalar Devices**
   - **vmPRO Devices**

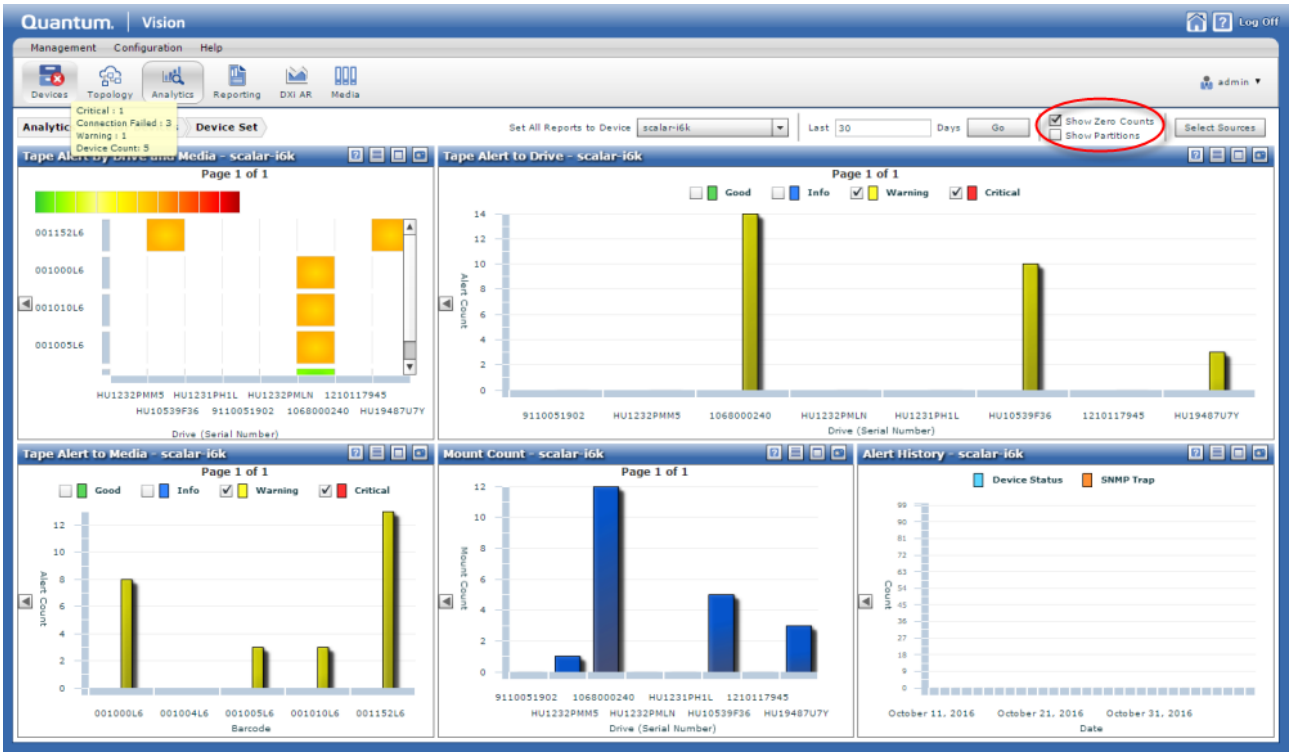
   Note: Interactive graphs are not available for DXi 35/55 devices.

b. In the center pane, select one of the following:
   - **Red Status**
   - **Yellow Status**

c. In the right pane, select each device with the associated alert status to include in the graphs.

3. Click **View Reports** to display the interactive graphs for the selected devices in the **Analytics Device Set** console.

Figure 118: Analytics Device Set Console (for Scalar)



Navigate within an interactive graph

1. Display the **Analytics Device Set** console for the selected devices.
2. Perform the following tasks from the **Analytics Toolbar** as needed:

Task	Steps
View reports for a specific device.	From the **Set All Reports to Device** drop-down list, select the device for which to view reports.
Change the time range displayed in the graph.	a. In the **Last Days** field, enter the number of days for which to view information. b. Click **Go** to update the generated information.

Task	Steps
Display or hide data points with a value of zero on the graphs.	• Select the **Show Zero Counts** check box to display data points with a value of zero • Clear the **Show Zero Counts** check box to hide data points with a value of zero.
Select different devices to include in the graphs.	Click **Select Sources** to return to the **Analytics** console and select different devices to include in the graphs.

3. Use the following icons included on each graph, as needed:

Icon	Function
	Click to display a description of the graph.
	Click to both maximize the graph and to stack graphs vertically or horizontally. • Use the horizontal-stacked view to access statistics for one device at a time. Click the arrows on the sides of the graph to navigate between devices. • Use the vertical-stacked view to compare statistics between multiple devices at once.
	Click to maximize or minimize the graph.
	Click to export the graph. a. Select to **Export As JPEG** or **Export As PNG** to display the **Save As** dialog box. b. In the **File name** field, enter a name for the graph. c. Click **Save**.

DXi and Q-Cloud Protect Analytics

The Analytics DXi Device Set console displays current DXi device or Q-Cloud Protect appliance status. You can use the graphs to identify potential issues with DXi devices or Q-Cloud Protect appliances. With each graph, you can hold the cursor over the graph or click within the graph to access additional information.

Space Reclamation

Displays the progress of space reclamation over time. See Space Reclamation Interactive Graph on

page 185.

Replication Status

Displays a summary of replication statuses over time. See Replication Status Interactive Graph on page 186.

Disk Used by Reduced Data

Displays the amount of unique, compressed data stored over time. Disk Used by Reduced Data Interactive Graph on page 187.

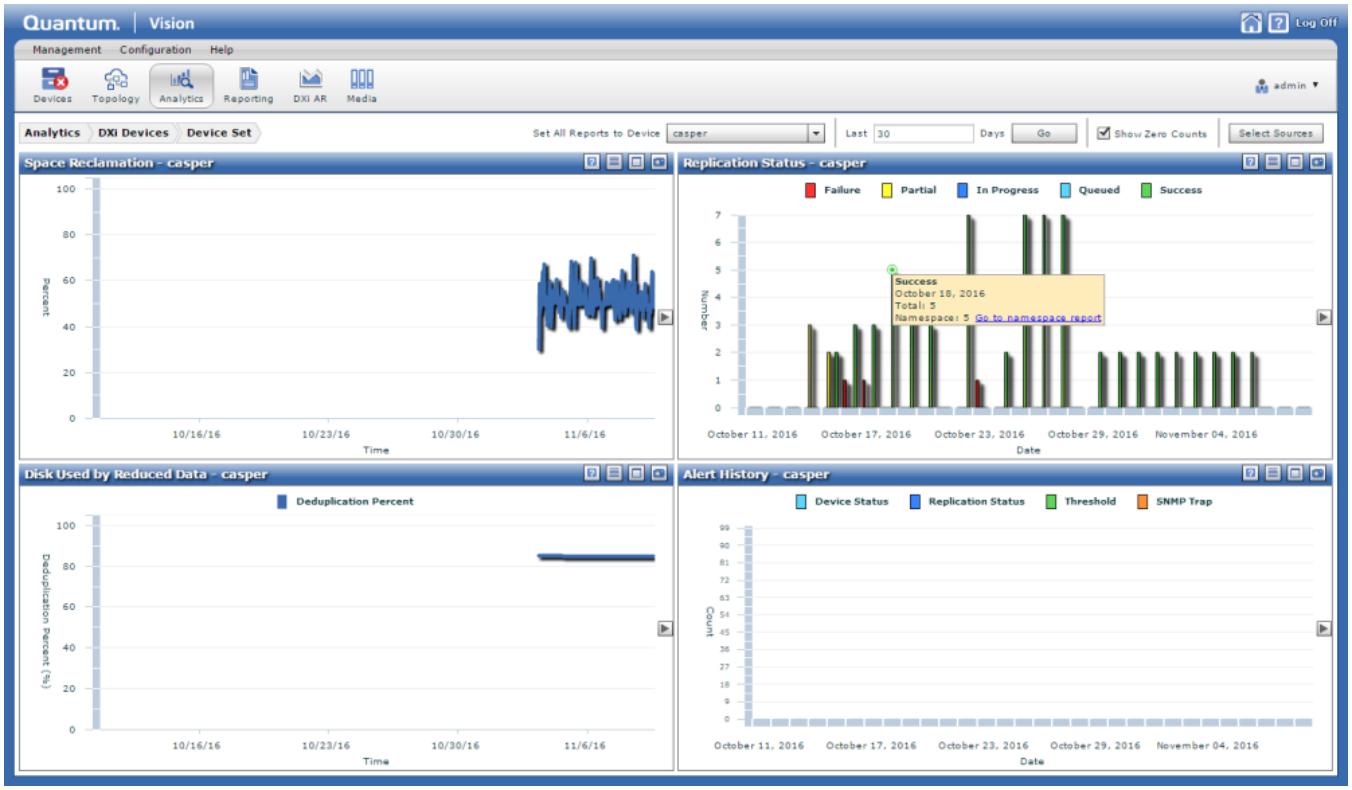
Accent

Displays the amount of data both before and after deduplication with Accent enabled over time. See Accent Interactive Graph on page 188.

Alert History

Displays a summary of alerts over time. See DXi or Q-Cloud Protect Alert History Interactive Graph on page 188.

Figure 119: Analytics DXi Device Set Console



Space Reclamation Interactive Graph

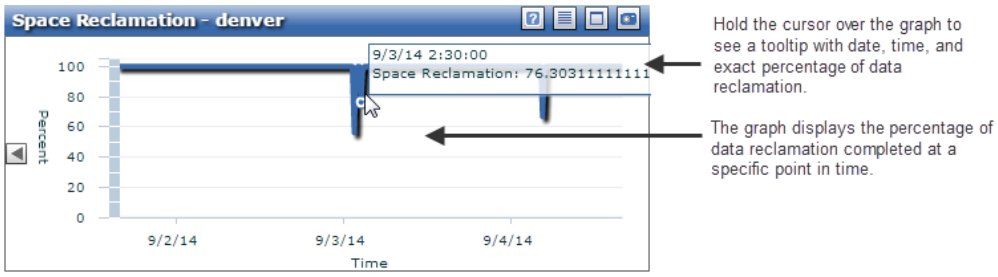
During space reclamation, the DXi or Q-Cloud Protect system searches the blockpool for data tags that are no longer referenced and then deletes the unneeded data tags to free up space. The Space Reclamation interactive graph displays the progress of such space reclamation over time.

Use the information on the graph to determine if space reclamation is performing at optimum levels.

Example

If space reclamation continues to run for long periods of time without completing (reaching 100%), it may indicate that other activities are contending for resources.

Figure 120: Space Reclamation Graph



Replication Status Interactive Graph

The **Replication Status** interactive graph displays a summary of replication statuses for DXi devices or Q-Cloud Protect appliances over time. Use the Replication Status graph to see when replication is occurring and to identify potential problems.

Replication Data

Use this graph to see the following:

Replication status

- Failure – (Red) The replication was not completed.
- Partial – (Yellow) The replication was only partially completed.
- In Progress – (Dark Blue) The replication is in progress.
- Queued – (Light Blue) The replication is queued and will continue when the system is ready.
- Success – (Green) The replication was completed successfully.

Replication count

- Counts display for each status type that occurred on the corresponding date.
- Counts for each type of replication are stacked into one bar for a single day.

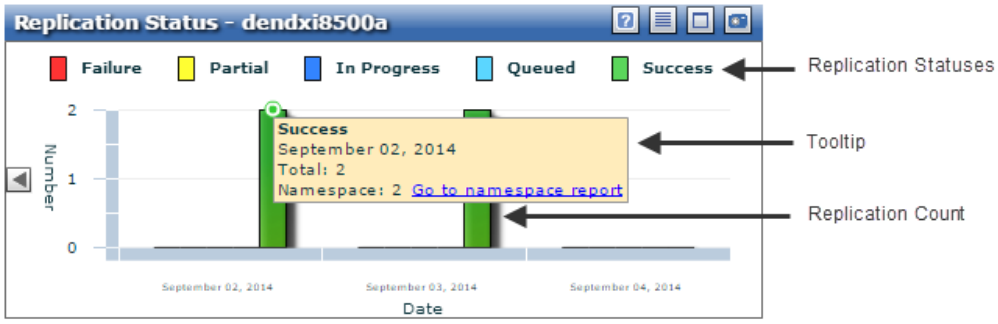
Tooltips

- Status counts are reported for both namespace and target (trigger) replication.

  Note: Target replications are also referred to as trigger, directory/file, or cartridge-based replications.

- Date on which the replication occurred is listed.
- Link to a status report for the associated replication.

Figure 121: Replication Status Graph



Disk Used by Reduced Data Interactive Graph

The Disk Used by Reduced Data interactive graph displays the amount of unique, compressed data (deduplicated data) stored on a DXi device or Q-Cloud Protect appliance.

Deduplication Data

Use this graph to see the following:

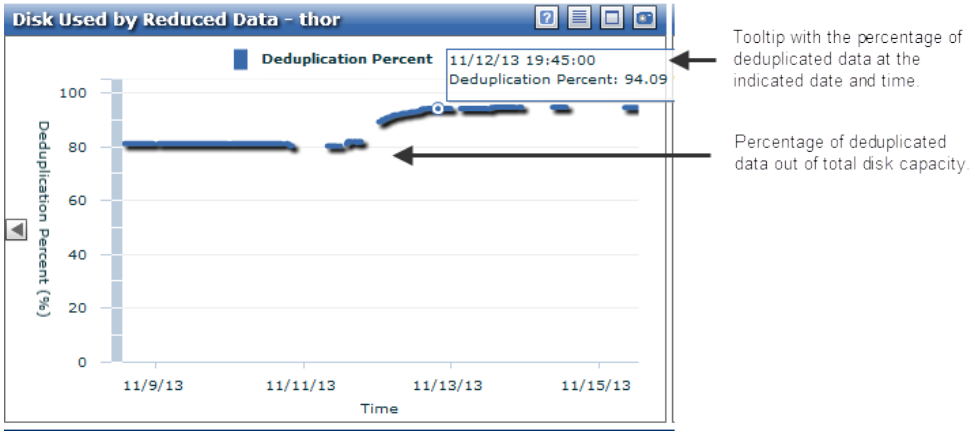
Deduplication Percentage

The percentage of deduplicated data out of the total disk capacity for specific points in time. This information is displayed as a tooltip when you hold the cursor over a point on the graph.

Deduplication Growth

The growth of deduplicated data over time.

Figure 122: Disk Used by Reduced Data Graph



Accent Interactive Graph

The Accent interactive graph displays the amount of data both before and after deduplication on Accent-enabled DXi devices or Q-Cloud Protect appliances.

Note: This graph displays only for systems that are Accent-enabled and configured.

Accent Data

Use this graph to see the following:

Data Amounts

The amount of data in gigabytes on the DXi device or Q-Cloud Protect appliance both before and after deduplication.

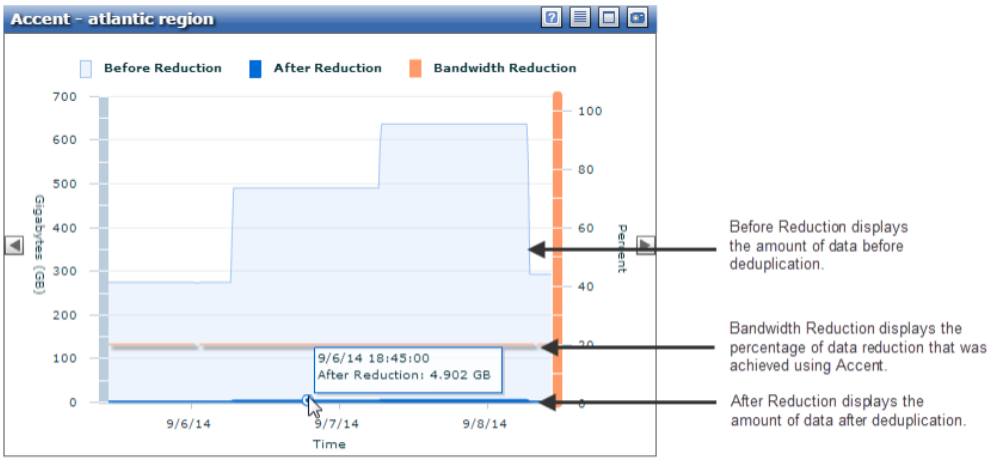
Data Reduction

The percentage of data reduction achieved using Accent.

Tooltip

A tooltip with the date and time on which the information was recorded, along with the exact numbers depicted by the graph, when you hold your cursor over a point on the **Before Reduction**, **After Reduction**, or **Bandwidth Reduction** lines.

Figure 123: Accent Graph



DXi or Q-Cloud Protect Alert History Interactive Graph

Alerts are notifications that Vision sends when conditions defined in Alert Rules have been met. See Manage Alert Rules in Vision on page 59.

The DXi or Q-Cloud Protect Alert History interactive graph displays a summary of alerts over time for DXi devices and Q-Cloud Protect appliances. Use this interactive graph to see when alerts are occurring and to identify potential problems.

DXi Alerts

Use this graph to see the following alerts:

Device Status

Vision sends an alert when the device or appliance status changes, such as from green to red.

Replication Status

Vision sends an alert when the replication status changes, such as from green to red.

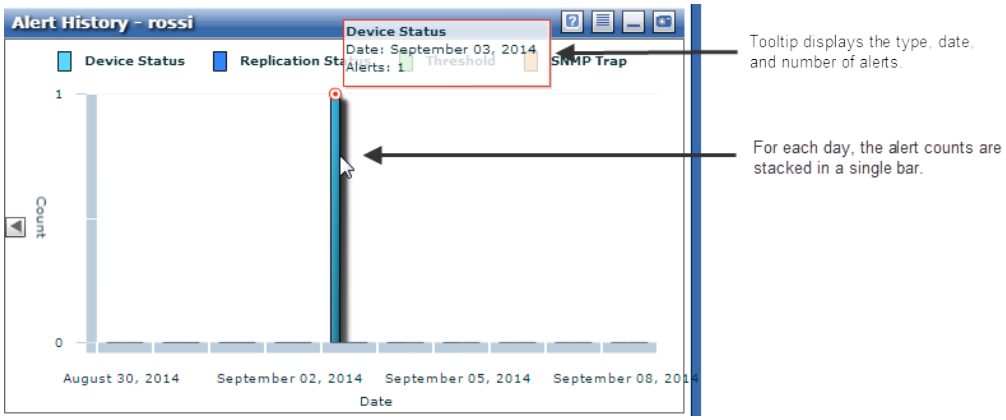
Disk Threshold

Vision sends an alert when used disk capacity rises above or falls below the specified percentage.

SNMP Trap

Vision sends an alert when a Simple Network Management Protocol (SNMP) trap is received from the device or appliance.

Figure 124: DXi or Q-Cloud Protect Alert History Graph



Scalar Analytics

The Analytics Scalar Device Set console displays interactive graphs that you can use to identify potential issues with Scalar libraries. With each graph, you can hold the cursor over the graph or click within the graph

to access additional information.

Tape Alert By Drive and Media

Displays a summary of tape alerts generated by disk or media within a Scalar library. See Tape Alert By Drive and Media Interactive Graph on the next page.

Tape Alert to Drive

Displays a summary of tape alerts generated by disks within a Scalar library. You can also use this graph to view partitions within Scalar libraries. See Tape Alert to Drive Interactive Graph on page 192.

Tape Alert to Media

Displays a summary of tape alerts generated by media within a Scalar library. See Tape Alert to Media Interactive Graph on page 193.

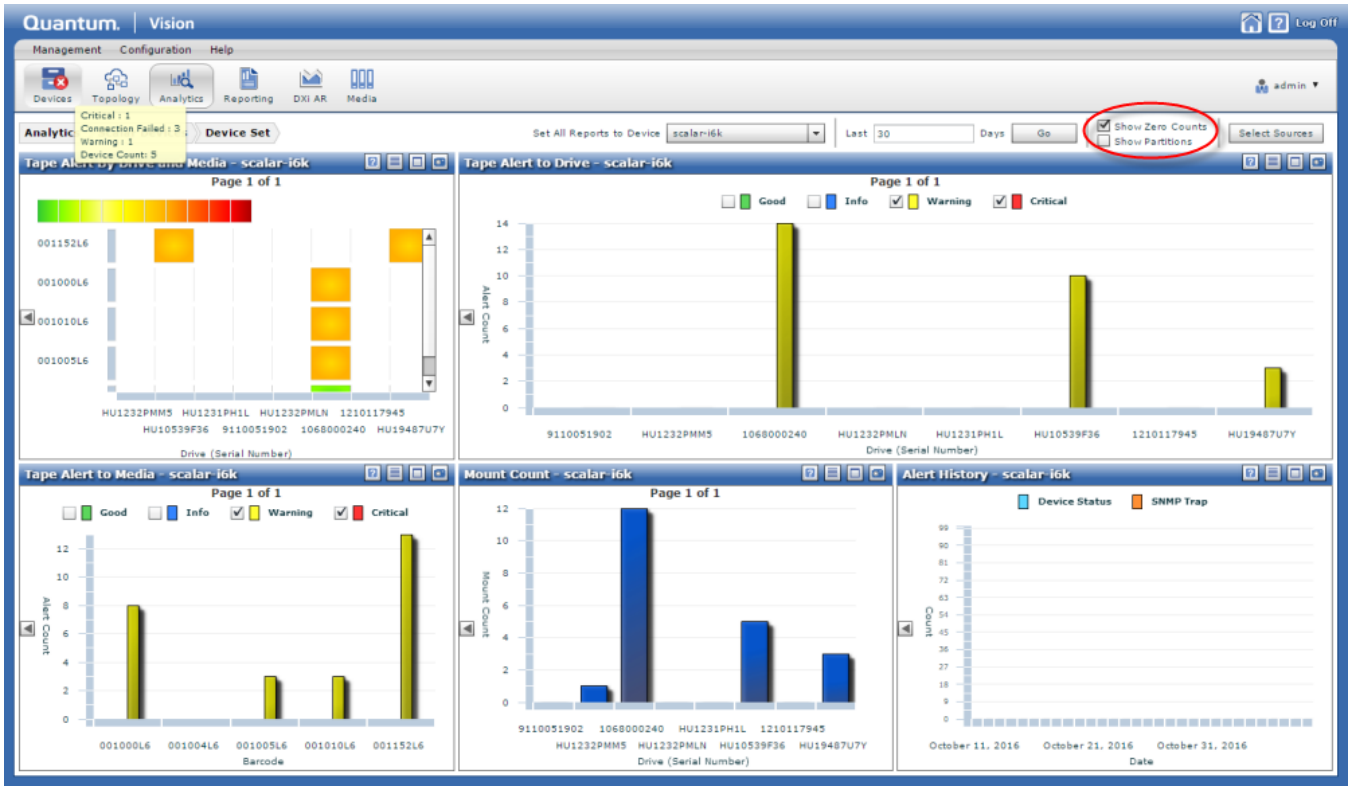
Mount Count

Displays the number of mounted tape cartridges for each drive within a scalar library.You can also use this graph to view partitions within Scalar libraries. . See Mount Count Interactive Graph on page 194.

Scalar Alert History

Displays a summary of alerts for a Scalar library over time. See Scalar Alert History Interactive Graph on page 195.

Figure 125: Scalar Device Set Console



Tape Alert By Drive and Media Interactive Graph

Whenever a problem occurs within a drive or related media (tape cartridges) of a Scalar library, Vision reports the library-generated tape alert. The Tape Alert By Drive and Media interactive graph displays a summary of such tape alerts using a heat map. This heat map indicates the number and severity of tape alerts that have occurred for a specific combination of a tape cartridge and drive.

Color	Severity	Alert Type	Criteria
	1–3	Good (G) or Informational (I)	Any number of good or informational tape alerts
	4	Warning (W)	One warning tape alert
	5	Warning (W)	Two warning tape alerts
	6	Warning (W)	Three or more warning tape alerts

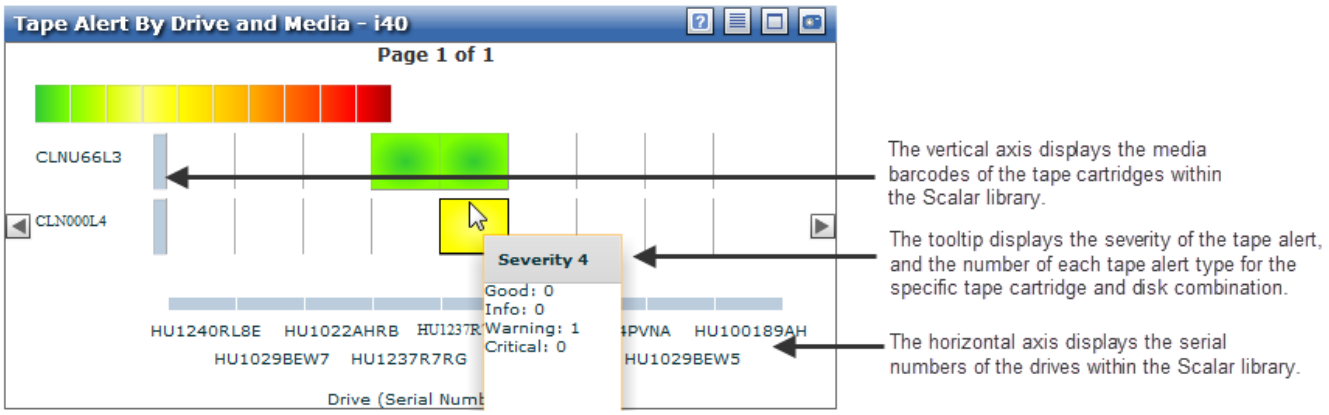
Color	Severity	Alert Type	Criteria
	7	Critical (C)	One critical tape alert
	8	Critical (C)	Two critical tape alerts
	9	Critical (C)	Three critical tape alerts
	10	Critical (C)	Four or more critical tape alerts

Cross-reference the tape alert to a specific tape cartridge and drive combination during the time that the alert was generated. By comparing alerts to specific cartridge and drive combinations, you can better determine where the problem exists.

Typical Alerts

- If a single drive exhibits tape alerts against multiple tape cartridges, the problem exists within the drive.
- If a single tape cartridge exhibits tape alerts against multiple drives, the problem exists within the tape cartridge.

Figure 126: Tape Alert By Drive and Media Interactive Graph



Tape Alert to Drive Interactive Graph

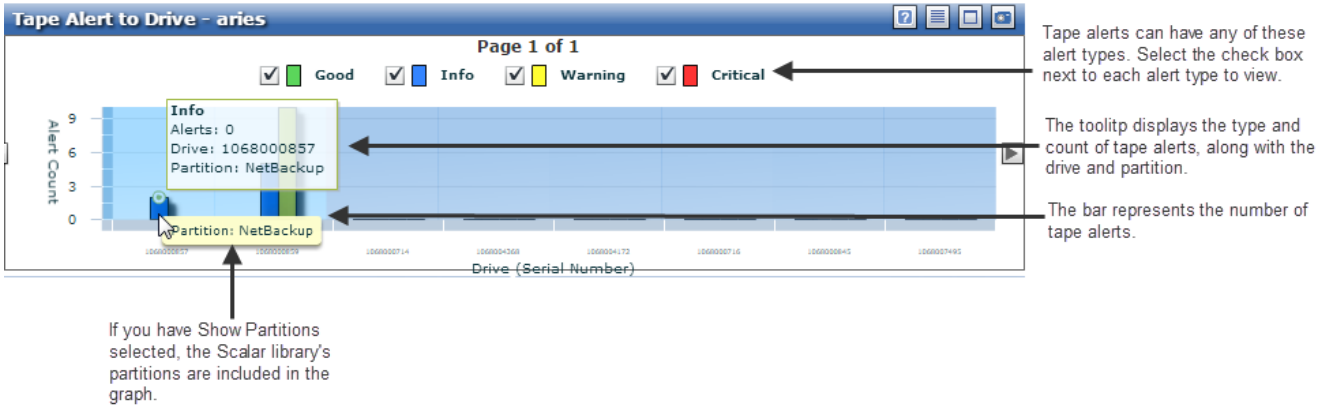
Whenever a problem occurs within a drive or related media (tape cartridges) of a Scalar library, Vision reports the library-generated tape alert.The Tape Alert to Drive interactive graph displays the cumulative number for each type of tape alert generated per tape drive in a Scalar library.

Use this interactive graph to pinpoint problematic drives by identifying the drives generating the most tape alerts. In addition, you can select the **Show Partitions** check box at the top of the console to display the Scalar library's partitions in this graph.

Typical Alert

If a single drive exhibits tape alerts against multiple tape cartridges, a problem exists within the drive.

Figure 127: Tape Alert To Drive Interactive Graph



Tape Alert to Media Interactive Graph

Whenever a problem occurs within a drive or related media (tape cartridges) of a Scalar library, Vision reports the library-generated tape alert. The Tape Alert to Media interactive graph displays the cumulative number for each type of tape alert generated per tape cartridge in a Scalar library.

Use this interactive graph to pinpoint problematic tape cartridges by identifying the cartridges generating the most tape alerts.

Typical Alert

If a single tape cartridge exhibits tape alerts against multiple drives, a problem exists within the tape cartridge.

Figure 128: Tape Alert To Drive Interactive Graph

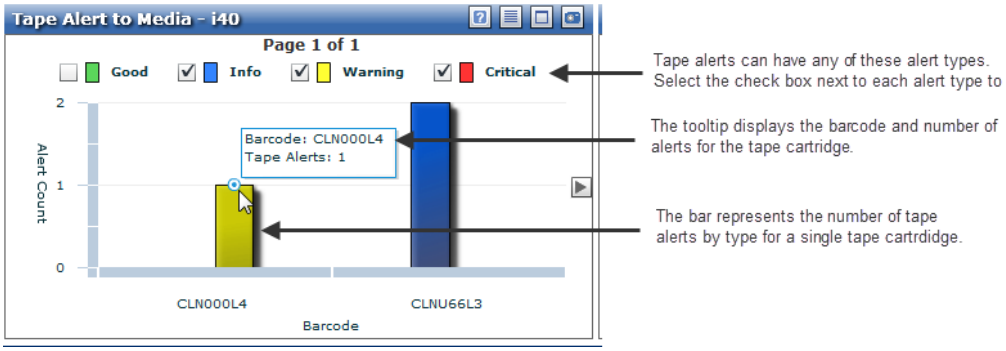
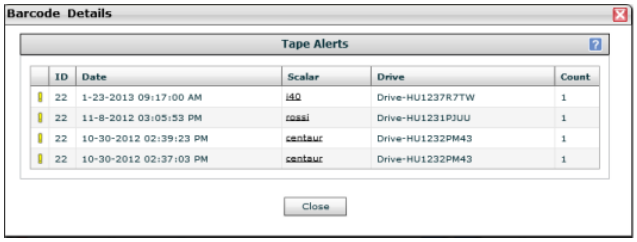


Figure 129: Barcode Details Dialog Box



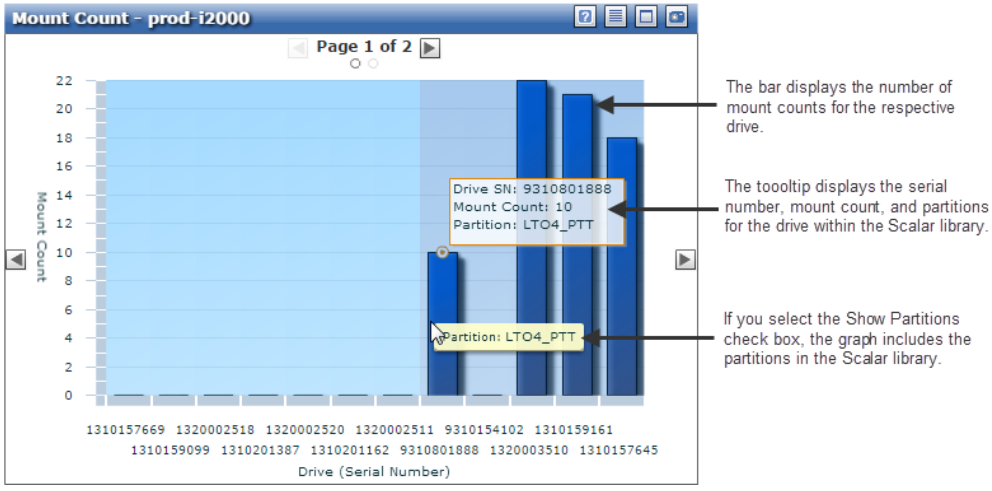
Click a bar in the Tape Alert to Media Interactive Graph to display the Barcode Details dialog box. This dialog box displays tape alerts for all Scalar libraries discovered in Vision.

Mount Count Interactive Graph

The Mount Count interactive graph displays the number of times that a tape cartridge is mounted to a drive within a Scalar library. Each time that a tape cartridge is mounted to a drive, the count increases by one.

Use this graph to see how often tape drives are used within the Scalar library over a specified period of time. In addition, you can select the **Show Partitions** check box at the top of the console to display the Scalar library's partitions in this graph.

Figure 130: Mount Count Interactive Graph



Scalar Alert History Interactive Graph

Alerts are notifications that Vision sends when conditions defined in Alert Rules have been met. See Manage Alert Rules in Vision on page 59.

The Scalar Alert History interactive graph displays a summary of alerts over time for Scalar libraries. Use this interactive graph to see when alerts are occurring and to identify potential problems.

Scalar Alerts

The Scalar Alert History Interactive graph displays the following alerts:

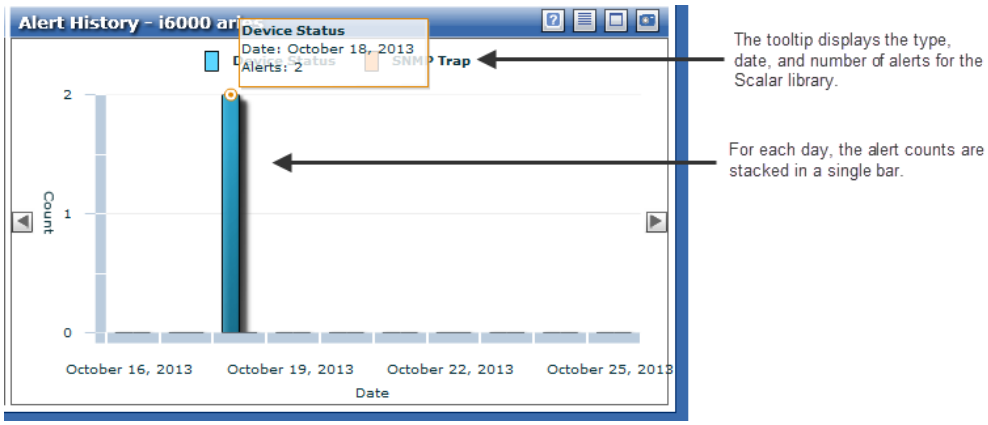
Device Status

Vision sends an alert when the device status changes, such as from green to red.

SNMP Trap

Vision sends an alert when a Simple Network Management Protocol (SNMP) trap is received from the device.

Figure 131: Scalar Alert History Interactive Graph



vmPRO Analytics

The Analytics vmPRO Device Set console displays the following interactive graphs for vmPRO 3.0 and newer. Use these interactive graphs to view current vmPRO device and SmartMotion™ backup status, as well as to identify potential issues with vmPRO devices. With each graph, you can hold the cursor over the graph or click within the graph to access additional information.

SmartRead™ I/O Reduction

Displays the percentage of I/O data reduction over time due to vmPRO's SmartRead feature. See SmartRead I/O Reduction Interactive Graph on the next page.

SmartRead™ Data Move

Displays the amount of changed data versus the amount of unchanged data on a vmPRO device. See SmartRead Data Move Interactive Graph on page 198.

SmartMotion™ Status

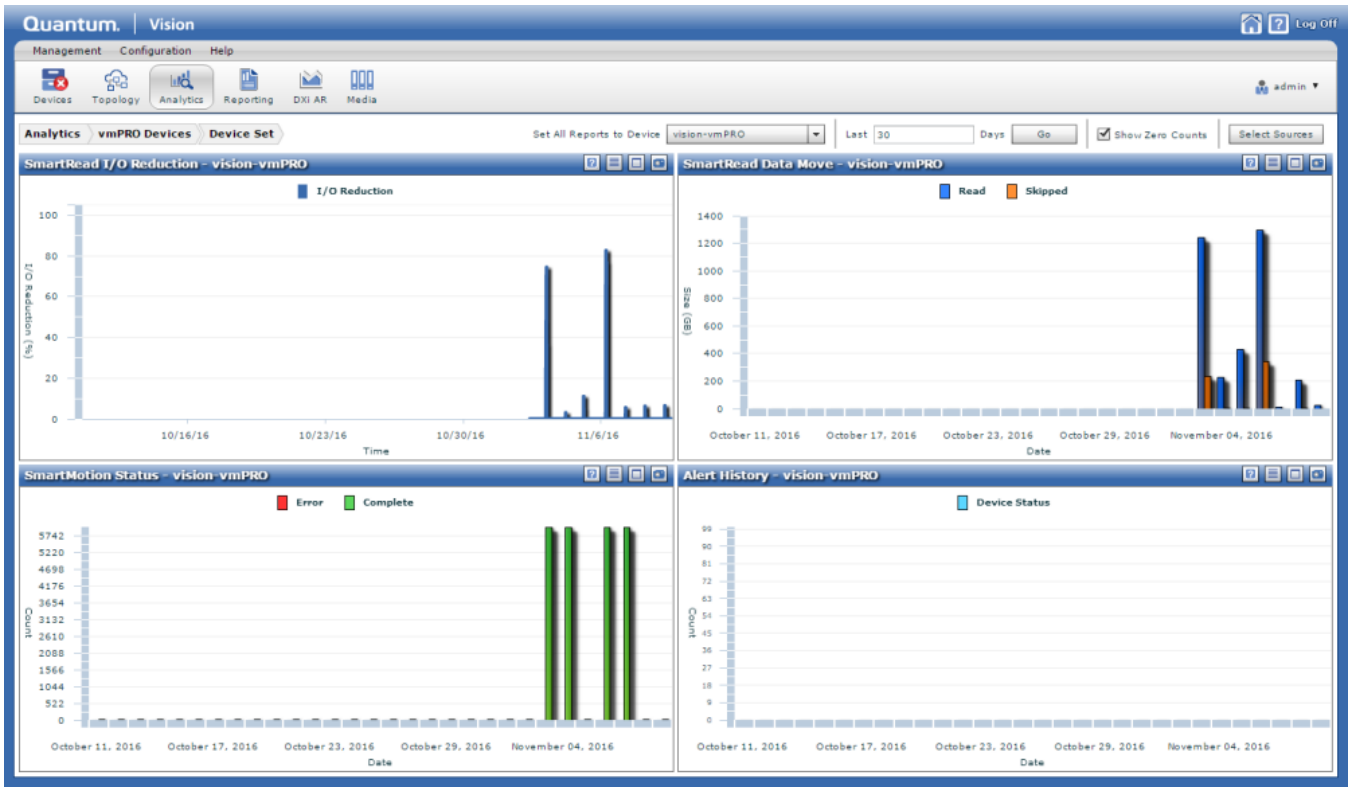
Displays the number of successful and failed SmartMotion backups. See SmartMotion Status Interactive Graph on page 199.

Alert History

Displays a summary of alerts for a vmPRO device over time. See vmPRO Alert History Interactive Graph on

page 199.

Figure 132: vmPRO Device Set Console

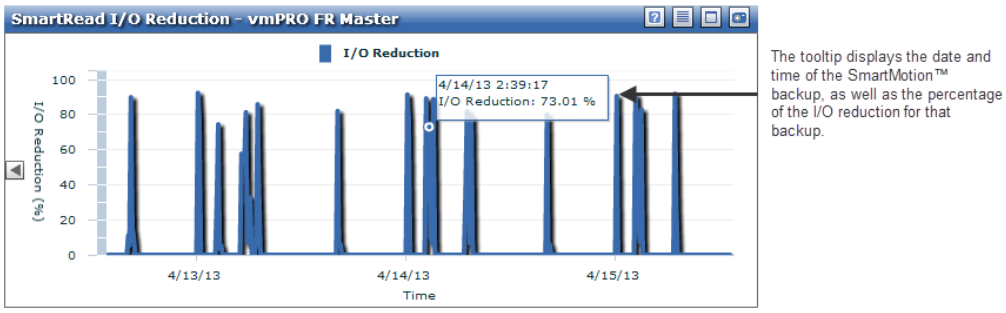


SmartRead I/O Reduction Interactive Graph

The SmartRead™ feature in vmPRO identifies that data that has changed since the last SmartMotion backup. This utility reduces the total network I/O and accelerates backups because only the changed data is backed up.

The SmartRead I/O Reduction interactive graph displays the percentage of I/O data reduction over time due to vmPRO's SmartRead feature.

Figure 133: SmartRead I/O Reduction Interactive Graph



SmartRead Data Move Interactive Graph

The SmartRead™ feature in vmPRO identifies that data that has changed since the last SmartMotion backup. This utility reduces the total network I/O and accelerates backups because only the changed data is backed up.

SmartRead Data

The SmartRead Data Move interactive graph displays the amount of changed data (**Read**) versus the amount of unchanged data (**Skipped**) on the VMs over time:

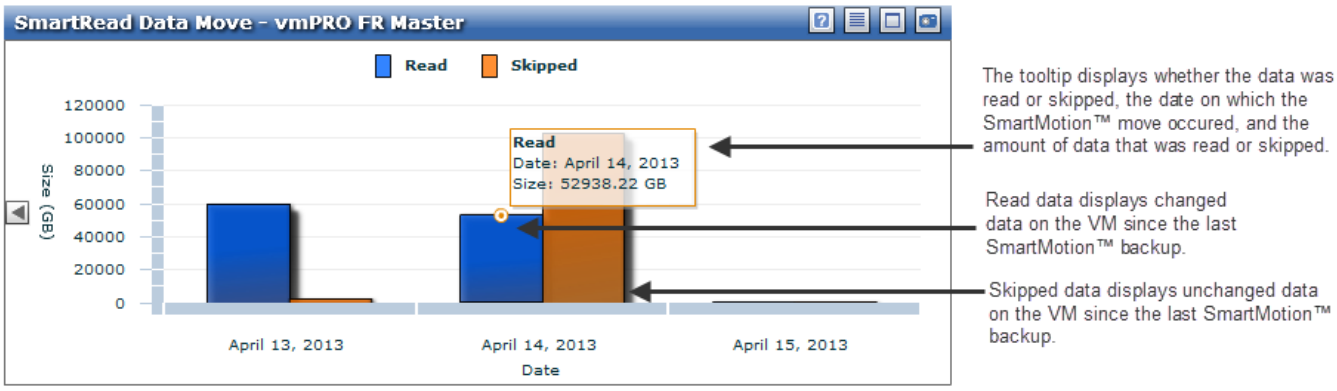
Read Data

The data that SmartMotion backed up for the current data move.

Skipped Data

The data that was previously backed up, and therefore, skipped during the current data move.

Figure 134: SmartRead Data Move Interactive Graph

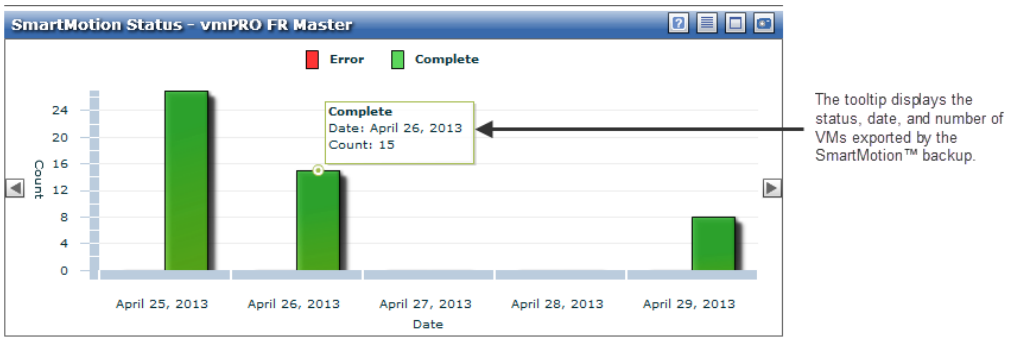


SmartMotion Status Interactive Graph

The SmartMotion™ feature in vmPRO provides backup services by initiating a scheduled backup of specified VMs. The SmartMotion Status interactive graph displays the number of successful SmartMotion backups (**Complete**) and the number of failed SmartMotion backups (**Error**).

Use this graph to troubleshoot issues with SmartMotion backups for vmPRO devices.

Figure 135: SmartMotion Status Interactive Graph



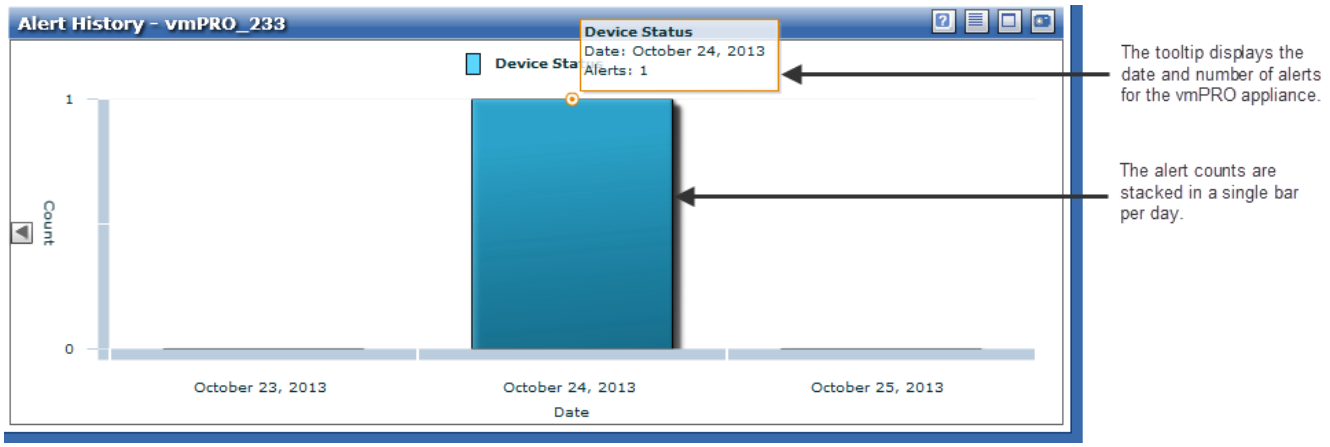
vmPRO Alert History Interactive Graph

Alerts are notifications that Vision sends when conditions defined in Alert Rules have been met. See Manage Alert Rules in Vision on page 59.

The vmPRO Alert History interactive graph displays a summary of Device Status alerts over time for vmPRO devices.

Vision sends a Device Status alert when the vmPRO device status changes, such as from green to red. Use this interactive graph to see when alerts are occurring and to identify potential problems.

Figure 136: vmPRO Alert History Interactive Graph



Chapter 8: Reporting

This chapter contains the following topics:

Vision Reporting

Vision includes a set of standard reports that present configuration, performance, and capacity information for DXi, Q-Cloud Protect, DXi 35/55, and Scalar. Using the Reporting console, you can generate and view reports, set up recurring schedules for automatically generating reports, and send reports to specified recipients.

Standard Vision Reports

Vision provides three types of standard reports in either a chart or table format:

Properties/Status Report

Displays a table of device configuration properties and statuses, such as the type and number of licenses for a Scalar library.

Observable History Report

Displays a chart showing historical performance or capacity data for applicable devices, such as deduplication statistics over time for a DXi device.

Observable Snapshot Report

Displays a chart showing current performance or capacity data for applicable devices, such as a snapshot of current capacity usage for a Q-Cloud Protect appliance.

Unique Vision Reports

The **Alert Acknowledgement History** report and the **DXi Replication** reports are unique and do not report on properties or data series.

Alert Acknowledgement History Report

Displays a history of acknowledged alerts.

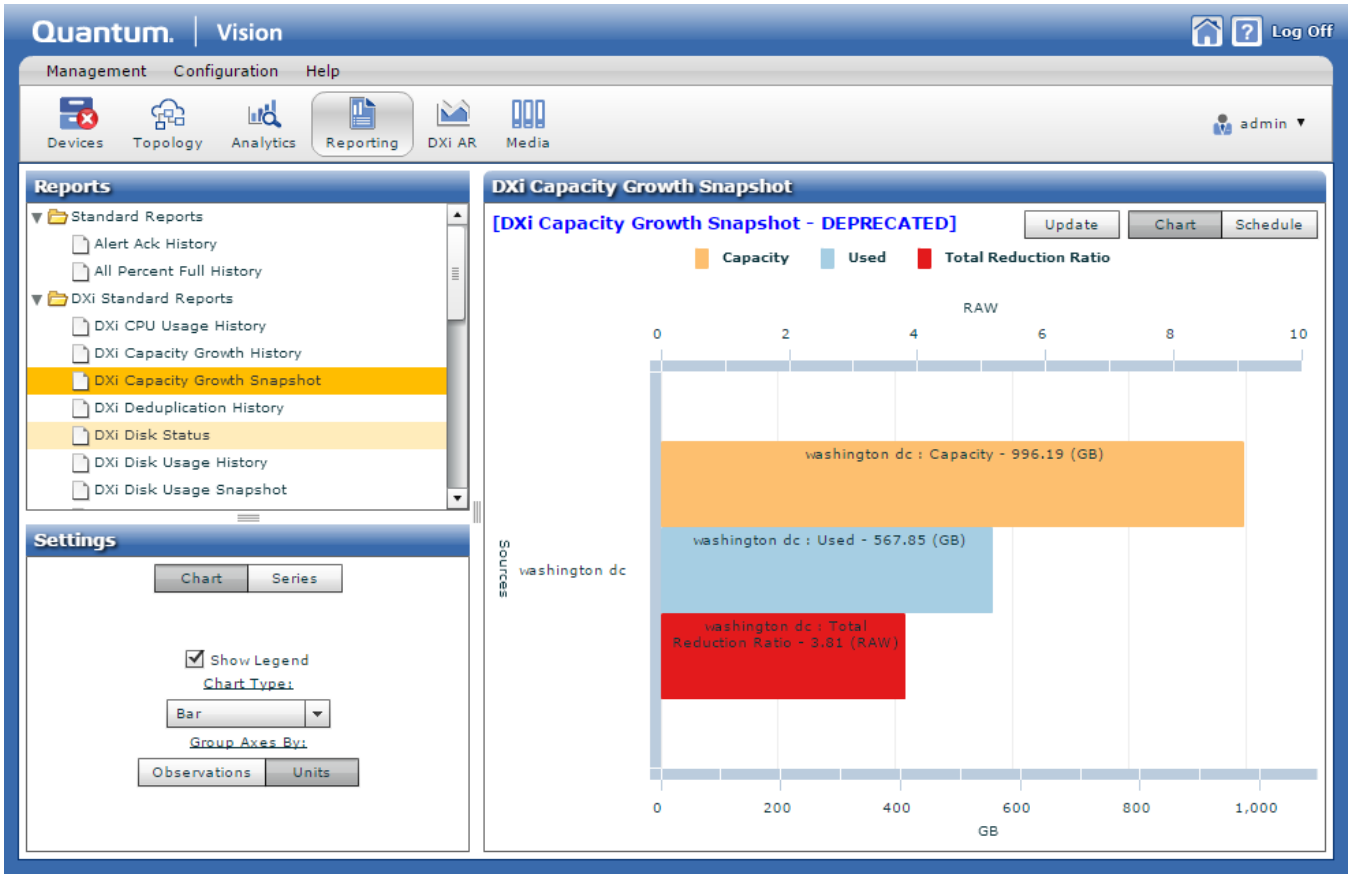
DXi Replication Reports

Display status counts and summary statistics for replication activity.

Additional Information

For DXi devices and Q-Cloud Protect appliances, you can access the Advanced Reporting cosnole in Vision. Use this console to view a wide variety of detailed performance information for your DXi devices and Q-Cloud Protect appliances. See Advanced Reporting in Vision on page 215.

Figure 137: Reporting Console – Observable Snapshot Report (DXi Capacity Growth Snapshot)



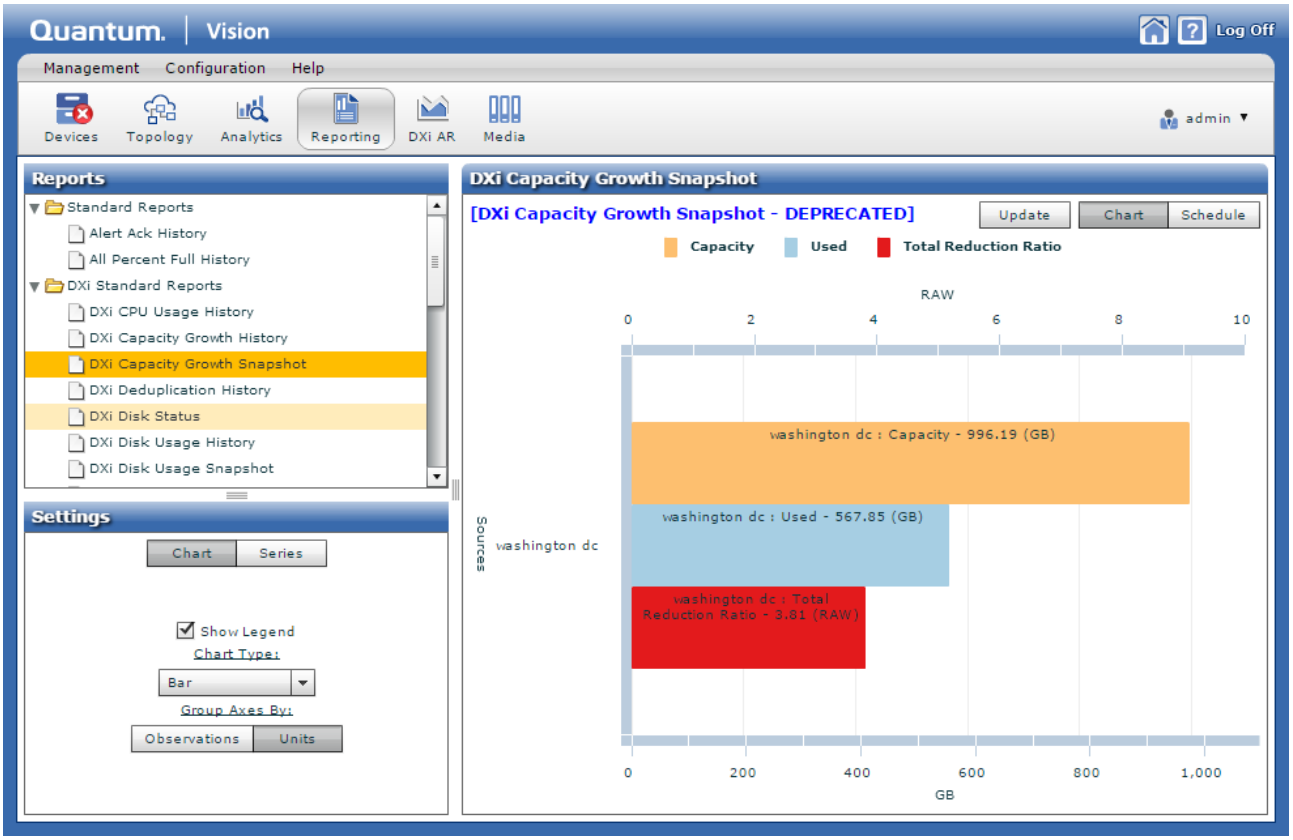
Generate Standard Vision Reports

Use the Vision Reporting console to generate, view, and modify standard Vision reports.

Generate a report

1. On the Vision toolbar, click **Reporting** to display the **Reporting** console.

Figure 138: Reporting Console



2. In the **Reports** pane, select the report to view from the appropriate folder.
3. In the **Settings** pane, select the following settings:

Modify the appearance of a chart

Note: Chart settings are available only for **Observable History** and **Observable Snapshot** reports.

a. Click **Chart**, and select the **Show Legend** check box to display the chart legend.

b. In the **Chart Type** drop-down list, select a type of chart to apply to the report.

- For **Observable History** reports, you can select from **Line**, **Area**, or **Plot** charts.
- For **Observable Snapshot** reports, you can select from **Bar** or **Column** charts.

c. In the **Group Axes By** field, click one of the following to select how to group data on the Y-axis:

- **Observations** – Group data by data series.
- **Unit** – Group data by data unit type.

d. In the **Value Type** drop-down list (for **Observable History** reports only), select a value to indicate how minutely to plot data points:

- **Minutes Summary** – Plot data points by minutes.
- **Hours Summary** – Plot data points by hours.
- **Days Summary** – Plot data points by days.

Select the sources (devices) and data series for which to generate the report

Note: Data series settings are available only for **Observable History** and **Observable Snapshot** reports.

a. Click **Series.**

b. In the left column, select each device to include in the report.

c. In the right column, select each data series to include in the report.

d. Click **All Data** to include all data series in the report.

The available data series are determined by the selected report.

Modify the time frame for which to generate the report

Note: Time frame settings are available only for **Alert Acknowledgment History, Observable History**, and **Replication** reports.

a. Click **Time Frame**, and do one of the following:

- In the **Last** field, enter a numeric value, and in the drop-down list, select **Minutes**, **Hours**, **Days**, or **Months**to indicate the time frame for the report.

  or

- In the drop-down list, select **Custom**. In the **Start** and **End** fields, enter the beginning and ending date and time of the time frame.

b. Click **Update** at the top of the chart to modify the report's time frame.

The report displays with all applicable settings.

Additional Standard Report Options

Use the following options to access additional information from a standard Vision report, or to perform additional functions.

Access tooltips with further details about the data

Move the cursor over an object on the graph.

Update the data to the current point in time or to apply newly defined settings

Click **Update**.

View data points in a table

1. Click **Data** to display the charted data in a table format.

   This button is not available for Properties reports.

2. In the **Data Series** drop-down list, select a different data series for which to display data, as needed.

   A data value reported as **NaN** (not a number) indicates that a value could not be collected for that data point. These values appear as gaps in a chart.

Return to a chart view

Click **Chart** to display data in a chart.

Schedule a report to be generated and emailed

Click **Schedule** to display the **Report Schedule** pane.

See Schedule Standard Vision Reports belowfor steps on how to schedule a report and define a list of recipients to whom to send the report.

Schedule Standard Vision Reports

You can set up a recurring standard Vision reports schedule from the Reporting console. Within the recurring report schedule, you can designate recipients to whom to send the report, along with the information to include in the report.

Important

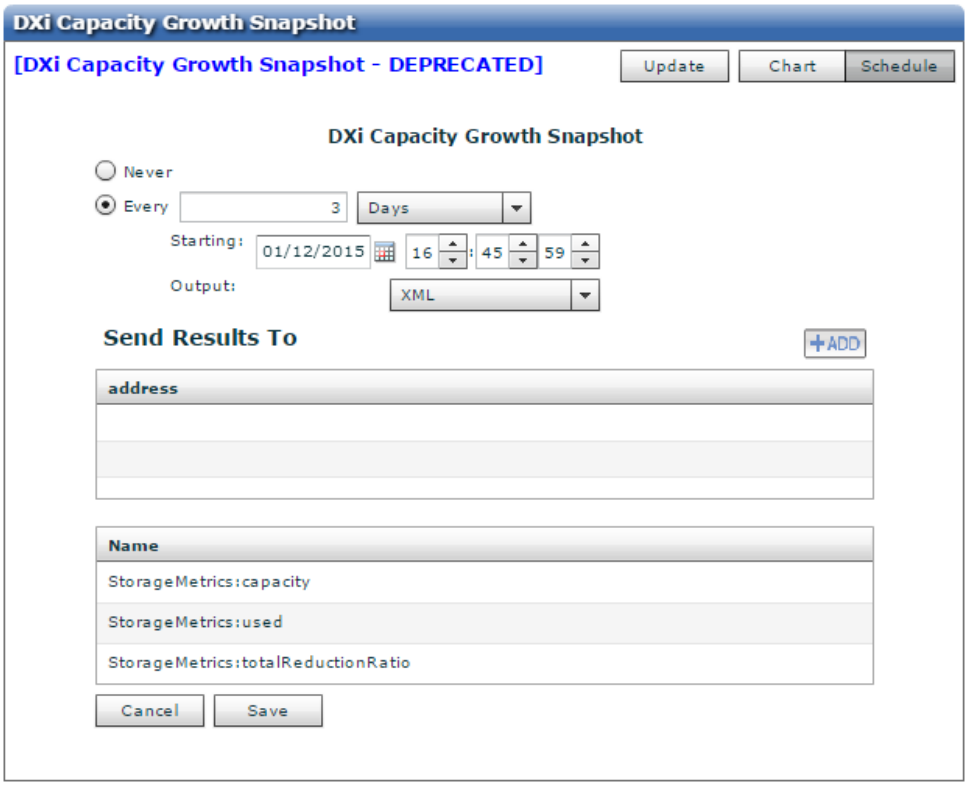
You must configure email server settings in Vision before sending reports. See Configure Email Server Settings in Vision on page 83.

Set up a recurring report schedule

1. On the Vision toolbar, click **Reporting** to display the **Reporting** console.
2. Generate the report for which to set up a recurring schedule. See Generate Standard Vision Reports on page 202.

3. Click **Schedule** to display the **Report Schedule** pane.

Figure 139: Report Schedule Pane



4. Select the radio button next to the **Every** field to enable a recurring schedule.

   To disable a recurring schedule or to send the current report only, select **Never**.

5. In the **Every** field, enter a numeric value, and then select **Minutes**, **Hours**, **Days**, or **Months** in the drop-down list to specify the frequency of recurrence.

6. Configure the following additional report settings, as needed:

Field	Description
Starting	Select the date and time on which to begin the recurring schedule.
Report Time Frame	Enter a numeric value, and then select **Minutes**, **Hours**, **Days**, or **Months** in the drop-down list to specify the time frame from which to select data for the report. **Note:** This setting is available only for **Alert Acknowledgment History** and **Observable History** reports.

Field	Description
Report Values	Select a value to indicate how minutely to plot data points. • **Minutes Summary** – Plot data points by minutes. • **Hours Summary** – Plot data points by hours. • **Days Summary** – Plot data points by days. **Note:** This setting is available only for **Observable History** reports.
Output	Select the output format for the report, either **XML**, **CSV**, **Text**, or **Graph**. **Note:** The **Graph** option is available only for **Observable History** reports.

7. In the **Send Results To** area, click **Add** to display the **New Email** field.
8. In the **New Email** field, enter the recipient's email address.
9. Repeat steps 7–8 for each recipient to whom to send the report.

   To delete a recipient, select the recipient in the list and click **Delete**.
10. In the **Name** box, select the name to assign to the emailed report.
11. Click **Save**.

    Vision generates and sends the report at the specified frequency.

Standard Vision Reports

The following table lists the standard Vision reports, along with the report type and data series included in each report.

When viewing this table, keep in mind that the available data series vary depending on the device for which the report is being generated. In addition, remember that you cannot add or remove data series from the standard Vision reports.

Standard Reports

Report Name	Report Type	Included Data Series/Displayed Information
Alert Ack History	Alert Acknowledgement	(none)
All Percent Full History	Observable History	Storage Metrics – Percent Full

DXi and Q-Cloud Protect Standard Reports

Report Name	Report Type	Included Data Series/Displayed Information
DXi Capacity Growth History	Observable History	Storage Metrics - Capacity Storage Metrics - Total Reduction Ratio Storage Metrics - Used
DXi Deduplication History	Observable History	Storage Metrics - Compression Ratio Disk Usage Detail - After Reduction Storage Metrics - Deduplication Ratio Storage Metrics - Percent Full Storage Metrics - Total Reduction Ratio
DXi Disk Status	Properties	Source DXi Disk index Disk name Disk Status, such as Online Disk Location
DXi Disk Usage History	Observable History	Disk Usage Detail - After Reduction Disk Usage Detail - Available[a] Disk Usage Detail - Used
DXi Disk Usage Snapshot	Observable Snapshot	Disk Usage Detail - After Reduction Disk Usage Detail - Available[a] Disk Usage Detail - Used
DXi Ethernet Received History	Observable History	Port Group - Port - Received
DXi Ethernet Transmitted History	Observable History	Port Group - Port - Transmitted
DXi FibreChannel Received History	Observable History	Port Group - Port - Received
DXi FibreChannel Transmitted History	Observable History	Port Group - Port - Transmitted

Report Name	Report Type	Included Data Series/Displayed Information
DXi NAS Status	Properties	Source DXi NAS share name NAS share type, such as nfs NAS share replication enabled status, either true or false NAS share deduplication enabled status, either true or false
DXi Port Status	Properties	Source DXi Port name Port type, such as Fibre Channel Port Status
DXi Replication Namespace Status Counts	Observable History	Namespace - Success Namespace - Partial Namespace - Failure
DXi Replication Namespace Summary	Replication	Source DXi Replication date Replication name Replication node type, such as share or partition Replication status Replication start time Replication end time Total bytes replicated mb replicated per second

Report Name	Report Type	Included Data Series/Displayed Information
DXi Replication Namespace Summary Unsuccessful	Replication	Source DXi Replication date Replicationname Replication node type, such as share or partition Replication status Replication start time Replication end time Total bytes replicated mb replicated per second
DXi Replication Source Summary	Replication	Source DXi Replication date Replication name Replication node type, such as share or partition Target's IP address Most severe status Replication last start time Replication last end time
DXi Replication Source Summary Unsuccessful	Replication	Source DXi Replication date Replication name Replication node type, such as share or partition Target's IP address Most severe status Replication last start time Replication last end time

Report Name	Report Type	Included Data Series/Displayed Information
DXi Replication Target Summary	Replication	Target DXi Replication date Replication name Replication node type, such as share or partition Source's IP address Most severe status Replication last start time Replication last end time
DXi Replication Target Summary Unsuccessful	Replication	(none)
DXi Space Reclamation History	Observable History	Data Scanned Space Reclaimed
DXi Virtual Tape Library (VTL) Status	Properties	Source DXi VTL Name VTL Index VTL Status, such as online Deduplication Enabled, either true or false Replication Enabled, either true or false

DXi 35/55 Standard Reports

Report Name	Report Type	Included Data Series/Displayed Information
DXi 35/55 Fans History	Observable History	Fan Groups - Fans - Value
DXi 35/55 Percent Full History	Observable History	Storage metrics - Percent Full

Report Name	Report Type	Included Data Series/Displayed Information
DXi 35/55 Replication History	Observable History	Replication - Source - Average Received Replication - Source - Average Sent Replication - Source - Replications Received Replication - Target - Replications Sent Replication - Target - Total Received Replication - Target - Total Sent
DXi 35/55 Sensors History	Observable History	Sensor Group - Sensor - Value
DXi 35/55 Usage History	Observable History	Library - Capacity Library - Free Library - Throughput Library - Used
DXi 35/55 Usage Snapshot	Observable Snapshot	Library - Capacity Library - Free Library - Throughput Library - Used

Scalar Standard Reports

Report Name	Report Type	Included Data Series/Displayed Information
Scalar Drive Status	Properties	Scalar library Drive serial number Drive status, such as Online or Varied On Drive type, such as LTO-6 Drive interface type, such as Fibre Channel Drive mount status, such as Empty Drive encryption, such as Disabled Drive owner
Scalar IO Blade Ports	Properties	Scalar library IO Blade serial number IO Blade port index IO Blade port status, such as Ready
Scalar IO Blade Status	Properties	Scalar library IO Blade serial number IO Blade status, such as Ready

Report Name	Report Type	Included Data Series/Displayed Information
Scalar LTFS Blade Status	Properties	Scalar library LTFS Blade name LTFS Blade serial number LTFS Blade IP address LTFS Blade location LTFS Blade mode, such as online LTFS Blade state, such as Ready LTFS Blade status, such as Good
Scalar Library Status	Properties	Scalar Library Rollup Status, such as red
Scalar Licensing	Properties	Scalar Library License name License quantity
Scalar Partitions	Properties	Scalar Library Partition name Partition mode, such as online
Scalar RAS Status	Properties	Scalar Library Sub system, such as Library or Media RAS status, such as Degraded

Chapter 9: Advanced Reporting in Vision

This chapter contains the following topics:

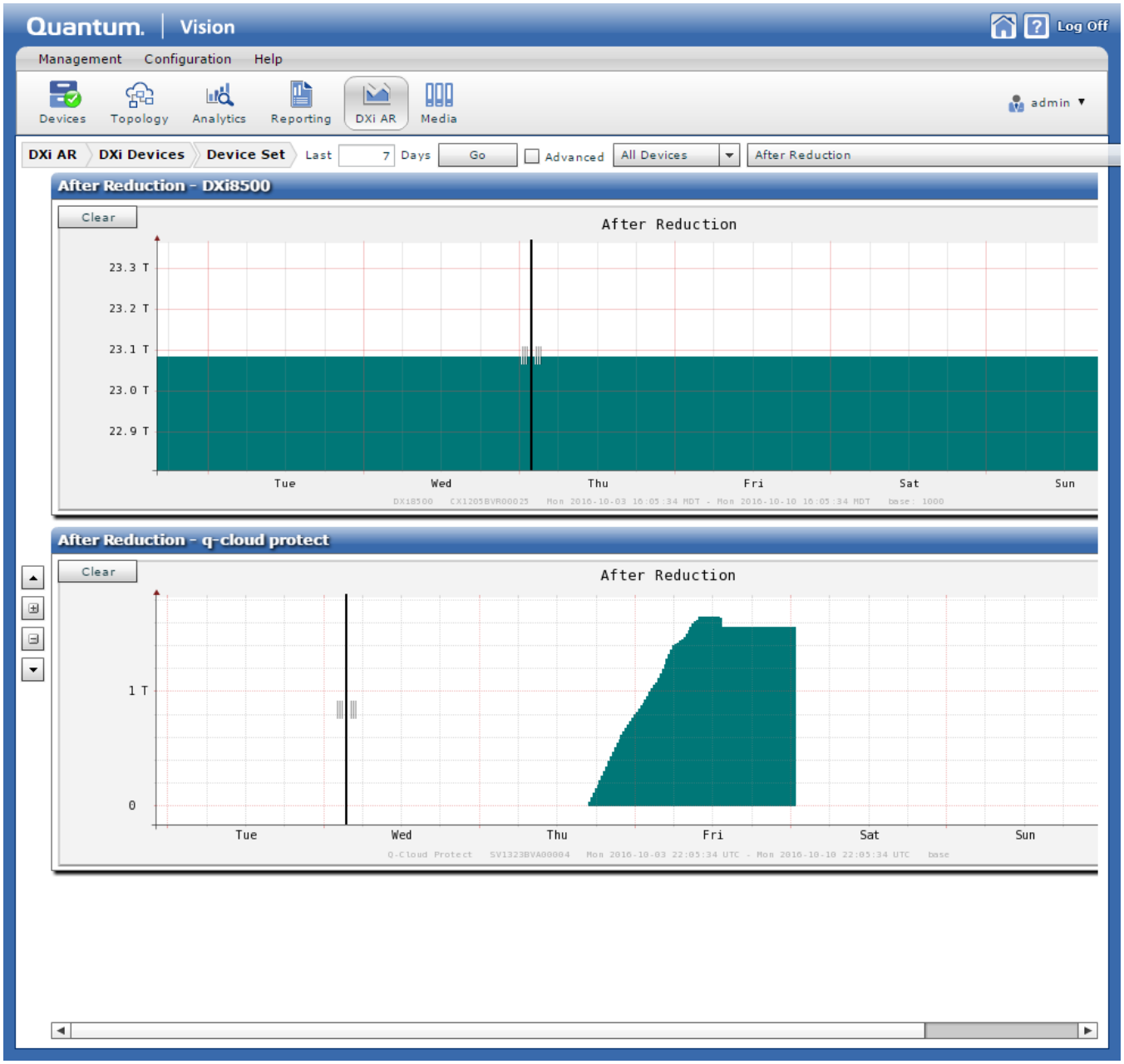
Advanced Reporting in Vision

Advanced Reporting is a powerful visual reporting and analysis tool integrated with DXi and Q-Cloud Protect systems. You can access Advanced Reporting reports from within Vision so you can compare graphs for multiple DXi devices and Q-Cloud Protect appliances.

The reports and graphs that are available on the Advanced Reporting Console differ depending on themodel and the version of software installed on the DXi device or Q-Cloud Protect appliance. For detailed information about each of the available reports and graphs, see the Advanced Reporting Documentation Center.

Note: DXI Advanced Reporting graphs are not available for DXi 35/55 devices.

Figure 140: Advanced Reporting – Graph View



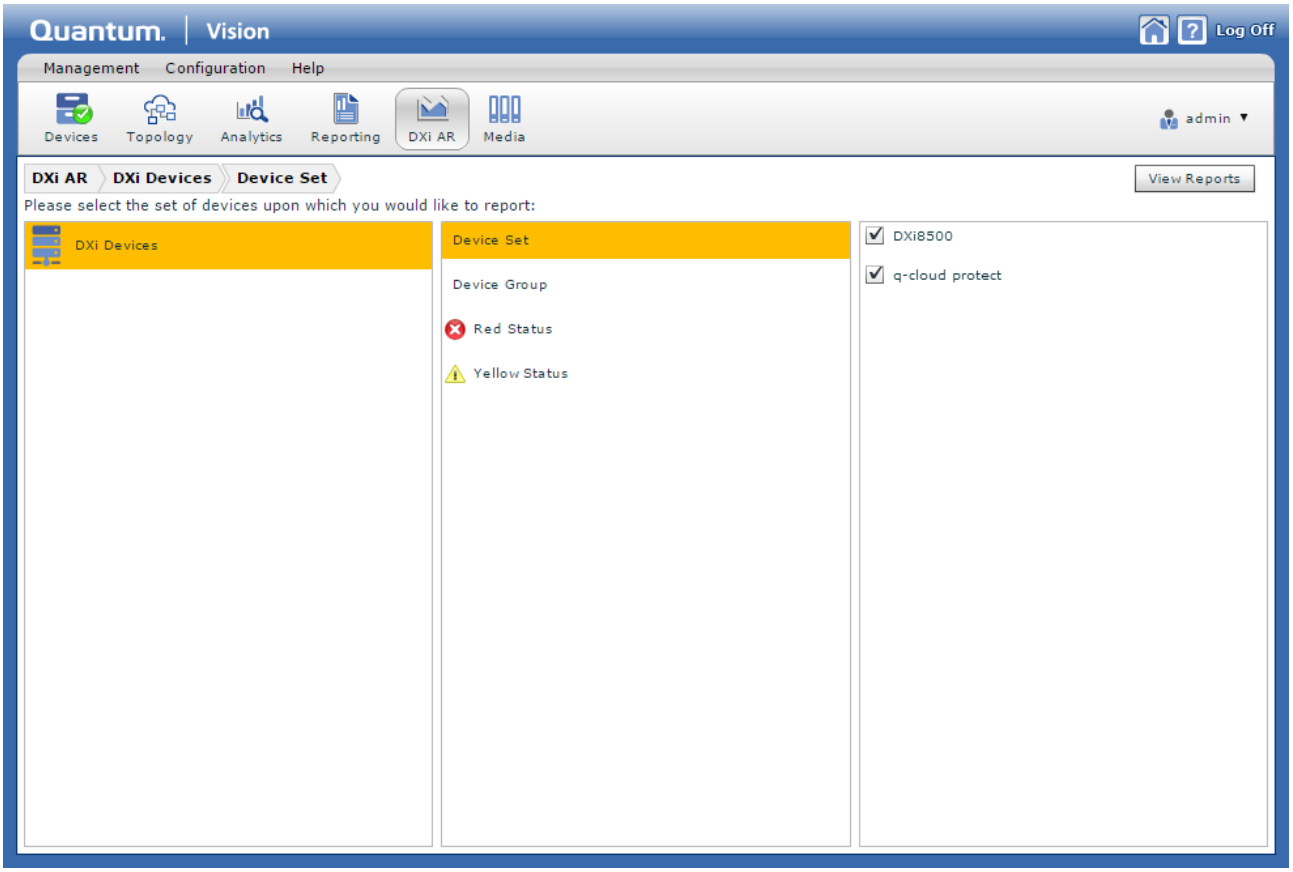
Advanced Reporting Graphs in Vision

Use the DXi Advanced Reporting Console and Graph Console to view advanced reporting graphs for DXi devices and Q-Cloud Protect appliances.

Select the devices for which to display Advanced Report graphs

1. On the Vision toolbar, click **DXi AR** to display the **DXi AR** console.

Figure 141: DXi Advanced Reporting Console – Select Devices



2. Select the devices for which to display data by doing one of the following:

Select by device set

a. In the left pane, select **DXi Devices**.

b. In the center pane, select **Device Set** to view graphs for one or more selected DXi devices or Q-Cloud Protect appliances.

c. In the right pane, select each DXi device or Q-Cloud Protect appliance to include in the graphs.

Select by device group

a. In the left pane, select **DXi Devices**.

b. In the center pane, select **Device Group** to view graphs for all DXi devices or Q-Cloud Protect appliances within a group.

c. In the right pane, select one or more Vision groups to include in the graphs.

Select by alert status

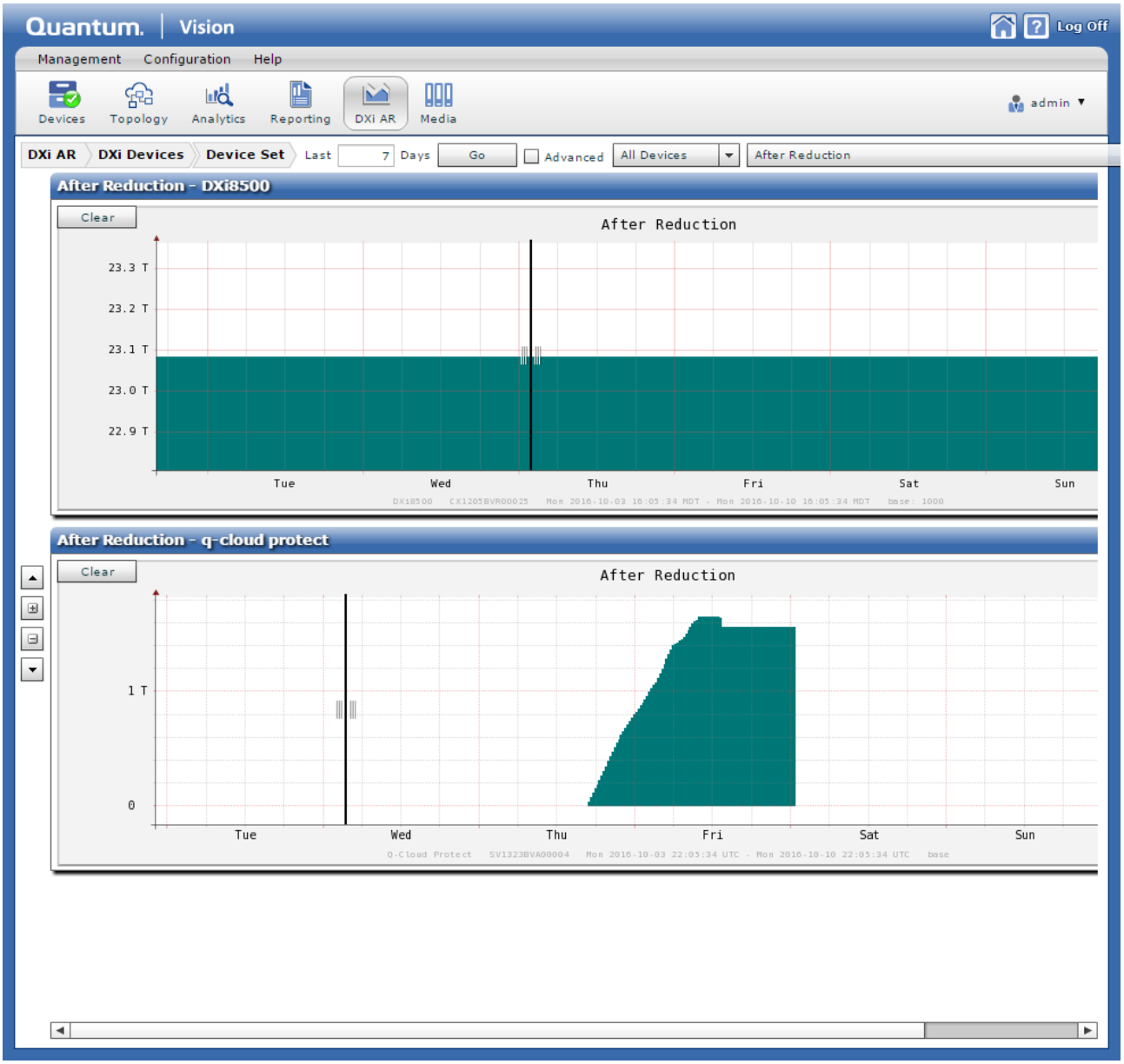
a. In the left pane, select **DXi Devices**.

b. In the center pane, select one of the following:
   - **Red Status** – View graphs for systems with a red status.
   - **Yellow Status** – View graphs for systems with a yellow status.

c. In the right pane, select each DXi device or Q-Cloud appliance with the associated alert status to include in the graphs.

3. Click**View Reports** to display the Advanced Reporting graphs for the selected devices.

Figure 142: Advanced Reporting – Graph View



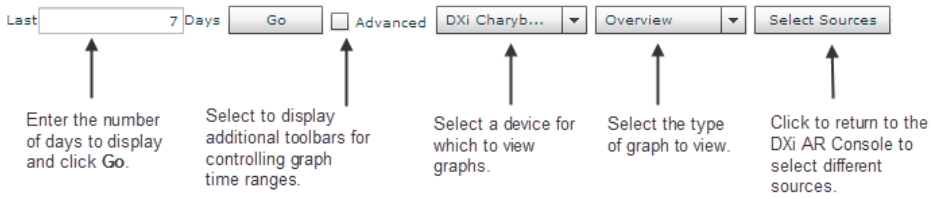
Navigate within an Advanced Reporting graph

1. Display the Advanced Reporting graphs for the selected devices.

2. Use the following options on the toolbar, as needed:

Option	Function
Last Days field / **Go** button	Change the time range displayed in the graph. a. In the **Last Days** field, enter the number of days for which to view information. b. Click **Go** to update the generated information.
Advanced check box	Display a button bar with additional tools for controlling the time range in the graph. See Define Time Ranges in Advanced Reporting on the next page.
Devices drop-down list	Select a different DXi device or Q-Cloud appliance for which to view the generated graphs, or to view graphs for all devices selected on the **DXi Advanced Reporting** console.
Reports drop-down list	Select a different graph to view. The options from which to select differ depending on the model and the version of software installed on the DXi device or Q-Cloud Protect appliance, as well as on whether you are viewing a single device or all selected devices. • If you are viewing a single device, the standard Advanced Reporting reports are displayed with at least two graphs. • If you are viewing multiple devices, only one type of graph is displayed at a time with one instance of the graph for each device. For detailed information about each of the available reports and graphs, see the Advanced Reporting Documentation Center.
Select Sources button	Return to the **DXi Advanced Reporting** console and select different devices to include in the graphs.

Figure 143: Graph Toolbar



3. Use the following icons included with each graph, as needed:

Icon	Function
	Click to hide the graph's legend and title. Click again to display the graph's legend and title.
	Click to export the graph. a. Select to **Export As JPEG** or **Export As PNG** to display the **Save As** dialog box. b. In the **File name** field, enter a name for the graph. c. Click **Save**.
	Click to minimize the graph.
	• Click the upward-pointing arrow to scroll the graph order up by one graph. • Click the plus sign to show all legends and titles for all displayed graphs. • Click the minus sign to hide all legends and titles for all displayed graphs. • Click the downward-pointing arrow to scroll the graph order down by one graph.

Define Time Ranges in Advanced Reporting

To define time ranges for displayed data, use the Advanced Time Range bar or the Dynamic Zoom feature on the Advanced Reporting console.

Viewing Tips

Review the following tips to understand how time-range changes effect your view.

Resolution

When you change the time range, Advanced Reporting automatically adjust the resolution of performance data.

- The resolution is finer — more granular — for shorter time ranges.
- The resolution is coarser — less granular — for longer time ranges.

Preset Ranges

When you apply a preset time range, Advanced Reporting resizes the time range while maintaining the center of the time range.

Example

if you are currently viewing a one-week time range that goes from Sunday to Saturday, applying the **1d** preset displays data for Wednesday.

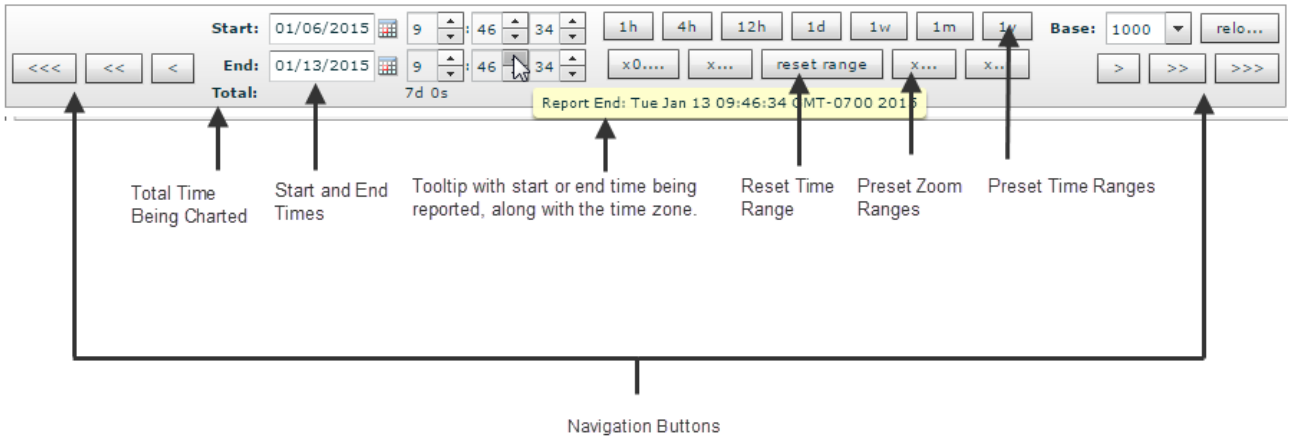
Scale

No matter how long of a time range that you span, Advanced Reporting scales all logged data to use the entire width of each graph.

Define time ranges

1. Display the Advanced Reporting graphs for the selected devices.
2. Select the **Advanced** check box to display the **Advanced Time Range** button bar.

Figure 144: Advanced Time Range Button Bar



3. In the **Base** drop-down list, select the numeric base for the data on which to report:

   1000 Bytes/KBs

   Tape drives, tape cartridges, and disk drives report capacities in units of 1000 bytes per kilobyte.

   1024 Bytes/KBs

   Backup applications typically report summaries in units of 1024 bytes per kilobyte.

4. Adjust the time range by doing any of the following:

   Adjust start and end times

   a. In the **Start** and **End** fields, enter a starting and ending date and time to define the time range to display.

b. Click **reload** to redisplay the graphs with the new time range.

Assign a preset time range

Click any of the following **Preset Time Range** buttons to quickly display data for a different time range:

- **1h** – 1 hour
- **4h** – 4 hours
- **12h** – 12 hours
- **1d** – 1 day
- **1w** – 1 week
- **1m** – 1 month
- **1y** – 1 year

Assign a preset zoom-factor

Click any of the following to zoom in or out on the graphs by a fixed factor:

- **x0.25** – Zooms in by a quarter of the currently displayed time range.
- **x0.5** – Zooms in by half of the currently displayed time range.
- **x2.0** – Zooms out by 2 times the currently displayed time range.
- **x4.0** – Zooms out by 4 times the currently displayed time range.

Adjust the time range forward or backward

Click **Backward** or **Forward Navigation** to move the time range by any of the following amounts:

- **<<<** or **>>>** Moves the time range backward or forward an amount equal to the current time range.
- **<<** or **>>** Moves the time range backward or forward an amount equal to one half of the current time range.
- **<** or **>** Moves the time range backward or forward an amount equal to one quarter of the current time range.

Reset the time range

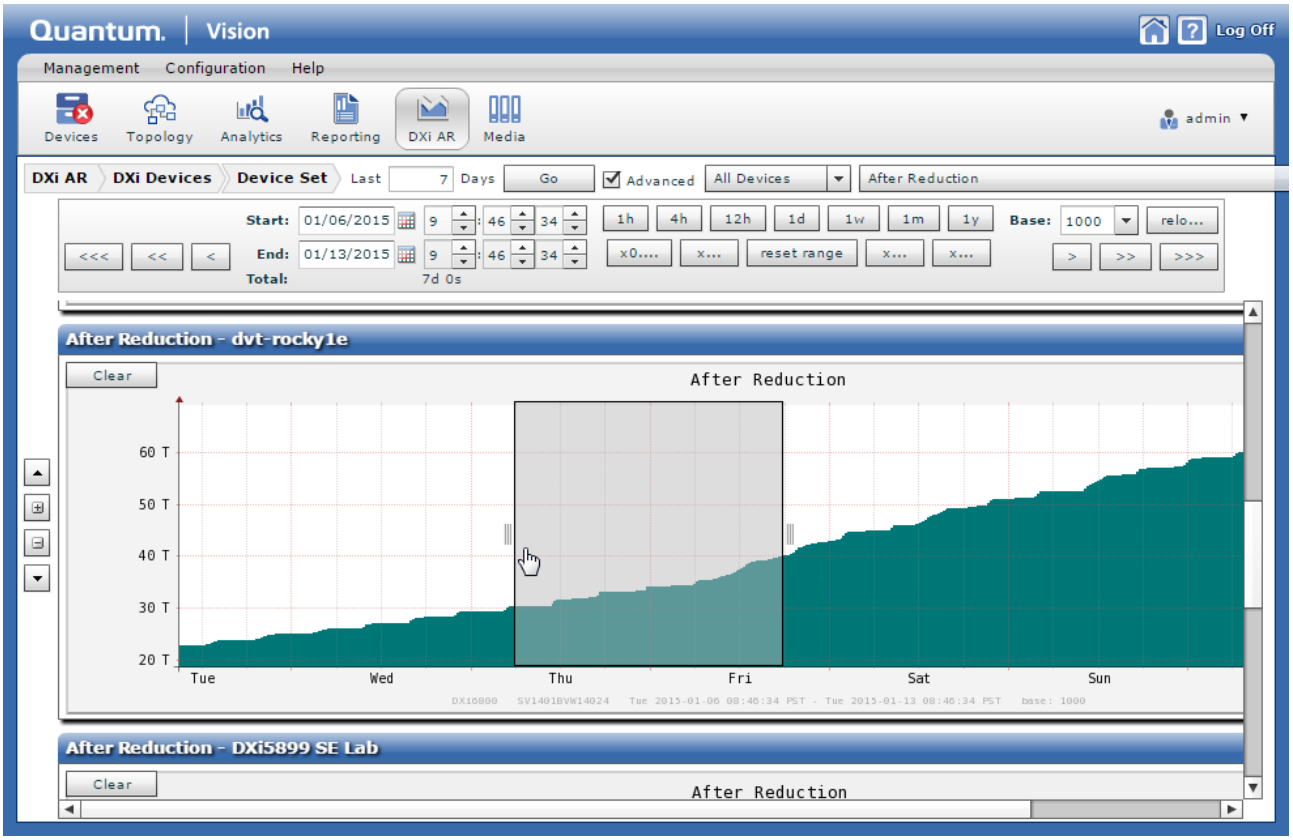
Click **reset range** to adjust the time range to display the most recent seven days of logging.

Use the dynamic zoom feature

1. Display the Advanced Reporting graphs for the selected devices.
2. Click the part of the graph to zoom to display selection handles.
3. Drag the selection handles to adjust the area of the graph to zoom.

4. Double-click the selected area to zoom.

Figure 145: Dynamic Zoom Feature



5. Click **Clear** to reset the graph to its original time range.

Appendix 10: Appendix A

This Appendix addresses how to backup, restore, and migrate your Vision database.

This appendix contains the following topics:

Vision Database Backup, Restore, and Migration

Vision's database consists of two separate storage systems: Relational Database Management System (RDBMS) and Round-Robin Database (RRD).

You should regularly back up your Vision databases to protect against data loss. Back up the RDBMS and the RRD databases together to preserve consistency between the databases in the backup. You can then restore lost Vision data from the backed-up databases.

Note: For Vision 4.2.1 and earlier, the RDBMS is Apache Derby. For Vision 4.3 and newer, the RDBMS is PostgreSQL. This version of help only applies to Vision 4.3 and newer.

Vision Software Migration

In addition to backing up and restoring your Vision database, you might need to move your Vision software from one Vision server to another. To perform a Vision software migration, you will need to back up the Vision database on the current server, restore the database on the new server, and update your Vision licenses on the new server.

For more information, see Migrate Vision to a Different Server on page 230.

Back Up Your Vision Database

You should regularly back up your Vision databases to protect against data loss. Use the following tasks to back up your Vision database running on Windows or Linux, and for both non-appliance and appliance versions of your Vision database.

Additional Information

We recommend that you back up the PostgreSQL RDBM and the RRD together to preserve consistency between the databases in the backup.

Back up your Vision (non-appliance) database on a Windows operating system

1. Stop the Vision services.
   a. Log on to the Vision server as **administrator**.
   b. From the **Services** panel, stop the **Quantum Vision** service.
2. Copy both of your Vision databases.

   RRD

   a. Change your directory location to **c:\Program Files (x86)\Quantum Vision\database**.
   b. In the database folder, select the **rrd** folder.
   c. Right-click on the **rrd** folder, and select **Copy** from the menu.
   d. Paste the **rrd** folder and all of its contents onto another server.

   PostgreSQL RDBMS

   a. Open a command window and run the following command:

```
"C:\Program Files (x86)\Quantum Vision\database\PostgreSQL\8.4\bin\pg_dump"
-U postgres -Fc visiondb > visiondb.pgdump
```

This command creates **visiondb.pgdump**, which is the backup file of the PostgreSQL RDBMS database.

b. Copy and paste **visiondb.pgdump** to the same location to which you copied your **rrd** folder.

3. Restart the Vision services.
   a. Log on to the Vision server as **administrator**.
   b. From the **Services** panel, start the **Quantum Vision** service.

Back up your Vision (non-appliance) database on a Linux operating system

1. Stop the Vision services.
   a. Log on to the Vision server as **root**.
   b. Run the command **`service vision stop`**.
2. Copy both of your Vision databases.

   RRD

   a. Change your directory location to **/opt/quantum-vision/database**.
   b. In the database directory, select the **rrd** subdirectory.
   c. Copy the **rrd** subdirectory and all of its contents.
   d. Paste the **rrd** subdirectory and all of its contents onto another server.

   PostgreSQL RDBMS

   a. Open a terminal window and run the following command:
   `/opt/quantum-vision/database/PostgreSQL/8.4/bin/pg_dump -U postgres -Fc visiondb > visiondb.pgdump`

   This command creates **visiondb.pgdump**, which is the backup file of the PostgreSQL RDBMS database.

   b. Copy and paste **visiondb.pgdump** to the same location to which you copied your **rrd** subdirectory.

3. Restart the Vision services.
   a. Log on to the Vision server as **root**.
   b. Run the command **`service vision start`**.

Back up your Vision (appliance) database

1. Log on to the appliance as the **sysadmin** user.
2. At the prompt, run the command **`admin backup`**.
3. Enter the following information at the appropriate prompts:
   - The IP address of the remote server on which to place the backed-up database.
   - The user name and password for the remote server.
   - The destination directory on the remote server.
   - The SSH port number (default: 22) for the remote server.

Results

- The Vision appliance creates a backup archive and copies the archive to the remote server, using secure copy with the provided credentials.
- The backup process generates a file name for the database backup. You will see a message similar to the following:
  `Database archive successfully saved at /tmp/vision_database.tar on server 12.34.567.890`

  You can rename the backup file after it is exported if you want to save multiple backups.

Restore Your Vision Database

Use the following tasks to restore your Vision database running on both Windows and Linux, and for both non-appliance and appliance versions of your Vision database.

Restore a backed-up Vision (non-appliance) database on a Windows operating system

1. Stop the Vision services.
   a. Log on to the Vision server as **administrator**.
   b. From the **Services** panel, stop the **Quantum Vision** service.
2. Restore the Vision database.
   a. Change your directory location to **c:\Program Files (x86)\Quantum Vision\database**.
   b. In the database folder, select and delete the existing **rrd** folder.
   c. Replace the deleted **rrd** folder with a backed-up **rrd** folder.

3. Open a command window and run the following commands:
   "C:\Program Files (x86)\Quantum Vision\database\PostgreSQL\8.4\bin\dropdb" -U postgres visiondb
   "C:\Program Files (x86)\Quantum Vision\database\PostgreSQL\8.4\bin\createdb" -U postgres visiondb
   "C:\Program Files (x86)\Quantum Vision\database\PostgreSQL\8.4\bin\pg_restore" -U postgres -d visiondb visiondb.pgdump

   Error Message

   When restoring the database, you might encounter the following error message. If so, disregard it.

   ```
   # /opt/quantum-vision/database/PostgreSQL/8.4/bin/pg_restore - U postgres -d
   visiondb visiondb.pgdump
   pg_reste: [archiver (db)] Error while PROCESSING TOC:
   pg_restore: [archiver (db)] Error from TOC entry 578; 2612 16386 PROCEDURAL
   LANGUAGE plpgsql postgres
   pg_restore: [archiver (db)] could not execute query: ERROR: language
   "plpgsql" already exists
   Command was: CREATE PROCEDURAL LANGUAGE plpgsql;
   WARNING: errors ignored on restore: 1
   ```

4. Restart the Vision services.
   a. Log on to the Vision server as **administrator**.
   b. From the **Services** panel, start the **Quantum Vision** service.

Restore a backed-up Vision (non-appliance) database on a Linux operating system

1. Stop the Vision services.
   a. Log on to the Vision server as **root**.
   b. Run the command **service vision stop**.
2. Restore the Vision database.
   a. Change your directory location to **opt/quantum-vision/database**.
   b. In the database directory, select and delete the existing **rrd** subdirectory.
   c. Replace the deleted **rrd** subdirectory with a backed-up **rrd** subdirectory.
3. Open a terminal window and run the following commands:
   /opt/quantum-vision/database/PostgreSQL/8.4/bin/dropdb -U postgres visiondb
   /opt/quantum-vision/database/PostgreSQL/8.4/bin/createdb -U postgres visiondb
   /opt/quantum-vision/database/PostgreSQL/8.4/bin/pg_restore -U postgres -d visiondb visiondb.pgdump

Error Message

When restoring the database, you might encounter the following error message. If so, disregard it.

```
# /opt/quantum-vision/database/PostgreSQL/8.4/bin/pg_restore - U postgres -d
visiondb visiondb.pgdump
pg_reste: [archiver (db)] Error while PROCESSING TOC:
pg_restore: [archiver (db)] Error from TOC entry 578; 2612 16386 PROCEDURAL
LANGUAGE plpgsql postgres
pg_restore: [archiver (db)] could not execute query: ERROR: language
"plpgsql" already exists
Command was: CREATE PROCEDURAL LANGUAGE plpgsql;
WARNING: errors ignored on restore: 1
```

4. Start the Vision services.
   a. Log on to the Vision server as **root**.
   b. Run the command **`service vision start`**.

Restore your Vision (appliance) database

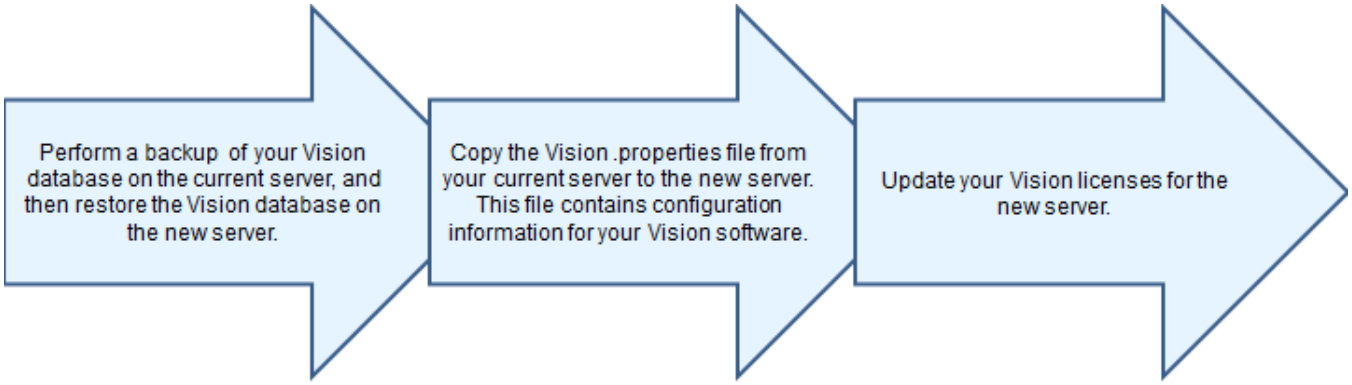
1. Log on to the appliance as the **sysadmin** user.
2. At the prompt, run the command **`admin restore`**.
3. Enter the following information at the appropriate prompts:
   - The IP address of the remote server on which the backed-up database is stored.
   - The user name and password for the remote server.
   - The file name of the database backup that you want to restore.
   - The SSH port number (default: 22) for the remote server.

Result

The Vision appliance retrieves the backup archive using secure copy with the provided credentials, and then restores the database on the appliance.

Migrate Vision to a Different Server

To perform a Vision software migration from one server to another, do the following:



Important

When migrating Vision from one server to another, you must install the same version of Vision on the new server.

Migrate your Vision software to a different server

1. Install the Vision software on the new server.
2. Back up the Vision database on the current server. See Back Up Your Vision Database on page 226.
3. Copy the Vision **.properties** file from the current server to the new server.

   Windows operating systems

   Copy and paste to and from this directory: **C:\Program Files (x86)\Quantum Vision\config\vision.properties**.

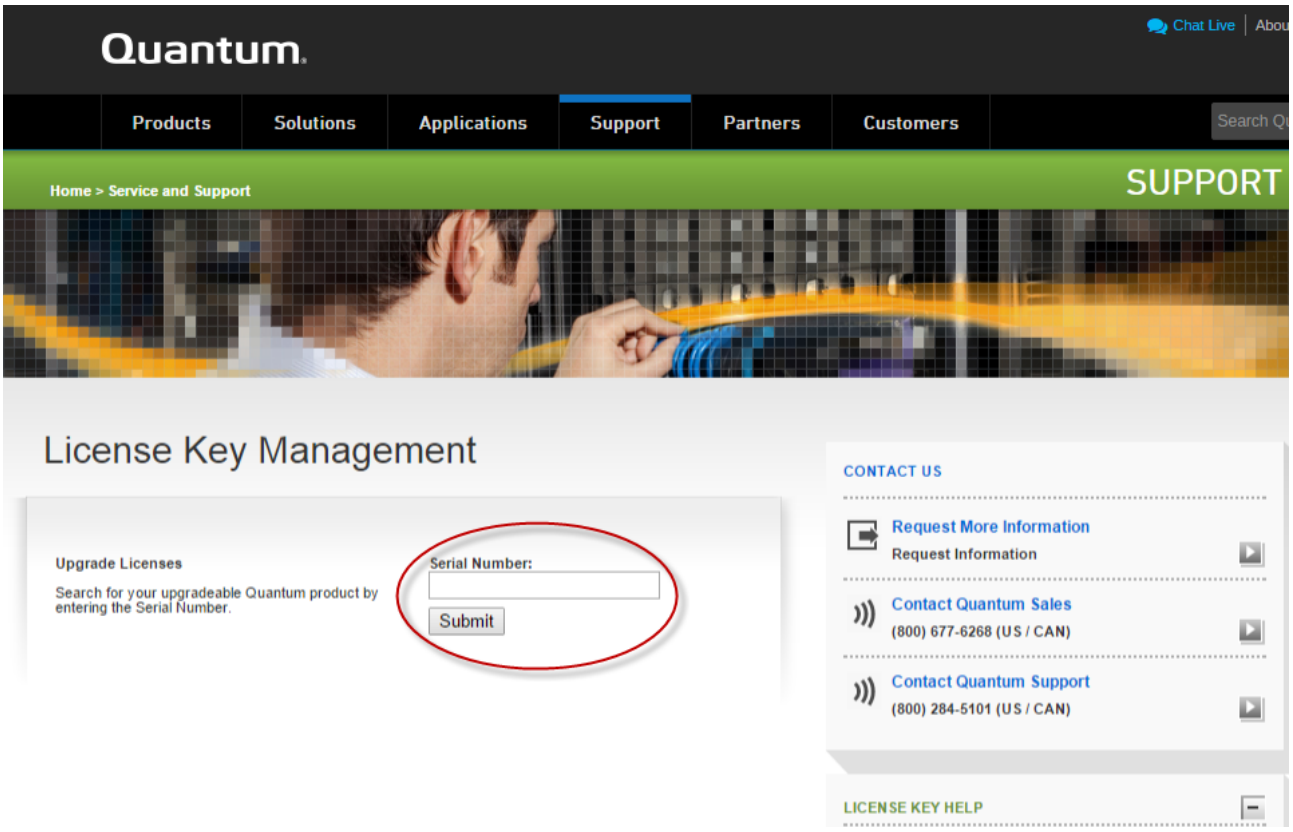
   Linux operating systems

   Copy and paste to and from this directory: **/opt/quantum-vision/config/vision.properties**.
4. Restore the Vision database on the new server. See Restore Your Vision Database on page 228.

Update your Vision license for the new server

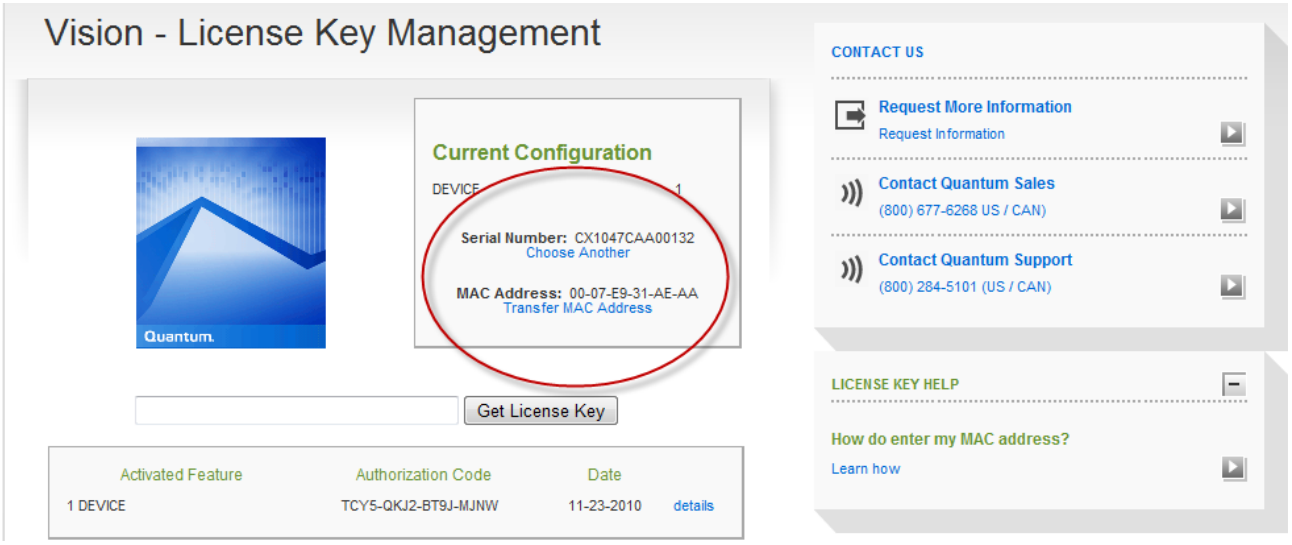
1. Open a Web browser on a computer with Internet access, and navigate to http://www.quantum.com/licensekeys to display the **License Key Management** page.

Figure 146: License Key Management Page



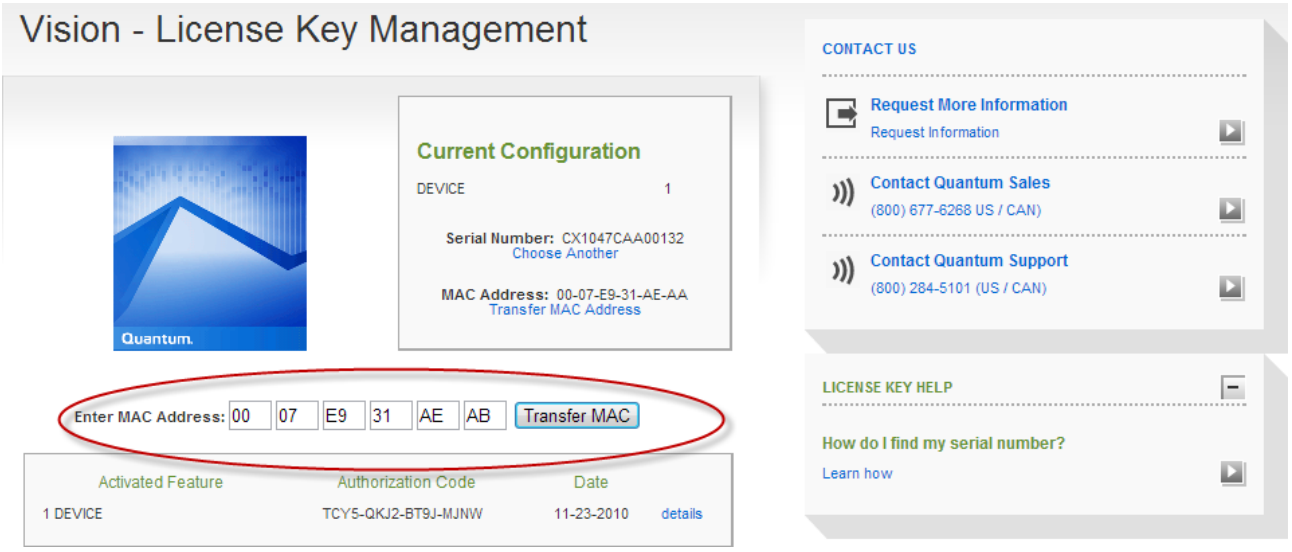
2. In the **Serial Number** field, enter your Vision software serial number and click **Submit** to display your current license configuration.

Figure 147: License Key Management Page - Current Configuration



3. Click on the **Transfer MAC Address** link to display the **Enter MAC Address** field.

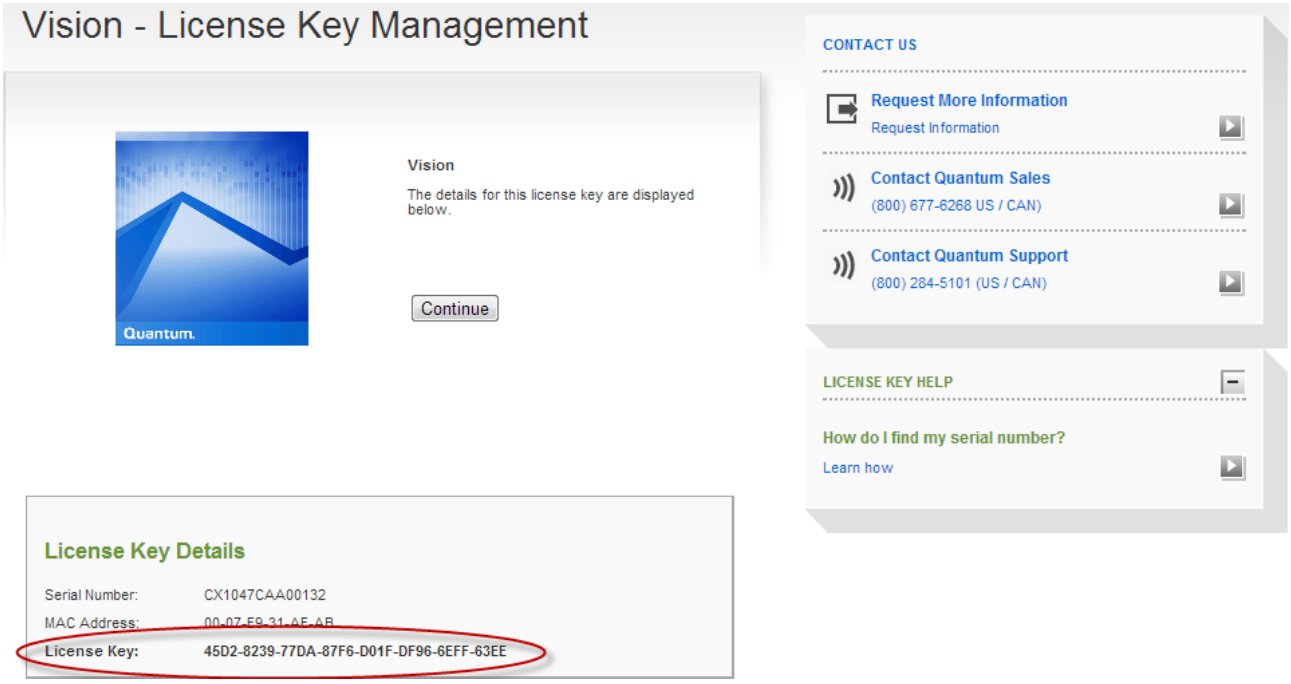
Figure 148: License Key Management Page - Enter MAC Address Field



4. In the **Enter MAC Address** field, enter the MAC address of the new server. See Add a New Vision License on page 84 for information about locating a server's MAC address.

5. Click **Transfer MAC** to display the **License Key Details** box.

Figure 149: License Key Management Page - License Key Details Box



6. Enter the new license key in the **Vision License Configuration** dialog box. See Add a New Vision License on page 84.
7. Repeat steps 1-6 for all current licenses.