Quantum

User's Guide

Quantum DXi V-Series

with DXi 2.2.1 Software

Quantum DXi V-Series User's Guide, 6-67612-03 Rev A, July 2013, Product of USA.

This document is for DXi 2.2.1 Software.

Quantum Corporation provides this publication "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Quantum Corporation may revise this publication from time to time without notice.

Contents

Chapter 4	DXi V-Series Home Page	57

Chapter 5	DXi V-Series Replication	69

Chapter 6　　　　**DXi V-Series Status**　　　　　　　　　　　　　**103**

Chapter 7　　　　**DXi V-Series Alerts**　　　　　　　　　　　　　　**115**

Chapter 8　　　　**DXi V-Series Configuration**　　　　　　　　　**127**

Appendix A   **Troubleshooting**   **273**

Glossary   **279**

Figures

Tables

Tables

Preface

This manual introduces the Quantum DXi V-Series virtual disk backup solution and discusses:

- System operations
- Configuration
- Web interface
- Basic troubleshooting

Audience

This manual is written for DXi V-Series operators and administrators.

> **Note:** It is useful for the audience to have a basic understanding of Windows, Linux, and UNIX® as well as backup/recovery systems.

Document Organization

Following is a brief description of chapter contents.

- Chapter 1, DXi V-Series System Description provides an overview of the DXi V-Series.
- Chapter 2, DXi V-Series Remote Management discusses using the DXi V-Series remote management console to control the system remotely.

- Chapter 3, DXi V-Series Configuration Wizards discusses the wizards that provide guidance for setting up the DXi V-Series.

- Chapter 4, DXi V-Series Home Page discusses the information that appears on the **Home** page of the remote management console.

- Chapter 5, DXi V-Series Replication discusses the remote replication capabilities of the DXi V-Series.

- Chapter 6, DXi V-Series Status discusses DXi V-Series status information.

- Chapter 7, DXi V-Series Alerts discusses DXi V-Series alert information and service tickets.

- Chapter 8, DXi V-Series Configuration discusses configuration of the DXi V-Series.

- Chapter 9, DXi V-Series Utilities discusses DXi V-Series utilities such as diagnostic tools and rebooting the system.

- Appendix A, Troubleshooting discusses problems you may encounter during the setup and operation of the DXi V-Series.

- Glossary provides definitions of terms used in this guide.

Notational Conventions

This manual uses the following conventions:

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.

- 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 system, safety, and regulatory guide.

警告　在使用本产品之前，请先阅读本文档及系统、安全和法规信息指南中所有的说明和警告信息。

警告　操作本產品前，請先閱讀本文件及系統、安全與法規資訊指南中的指示與警告說明。

ADVERSAL　Læs alle instruktioner og advarsler i dette dokument og i *Vejledning om system-sikkerheds- og lovgivningsoplysninger*, før produktet betjenes.

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

HINWEIS　Lesen Sie vor der Verwendung dieses Produkts alle Anweisungen und Warnhinweise in diesem Dokument und im System, Safety, and Regulatory Information Guide (Info-Handbuch: System, Sicherheit und Richtlinien).

אזהרה　לפני ההפעלה של מוצר זה, קרא את כל ההוראות והאזהרות הכלולות במסמך זה וכן *במדריך מידע בנושאי מערכת, בטיחות ותקינה*

警告 この製品を使用する前に、本文書、および『システム、安全、規制に関する情報ガイド』に記載しているすべての警告と指示をお読みください。

경고 이 제품을 작동하기 전에 이 문서 및 시스템, 안전, 및 규제 정보 안내서에 수록된 모든 지침과 경고 표지를 숙지하십시오.

ПРЕДУПРЕЖДЕНИЕ Перед началом эксплуатации данного устройства ознакомьтесь во всеми инструкциями и предупреждениями, приведенными в данном документе и в *Справочном руководстве по устройству, технике безопасности и действующим нормативам*.

ADVERTENCIA Antes de utilizar este producto, lea todas las instrucciones y advertencias en este documento y en la Guia informativa sobre sistema, seguridad y normas.

VARNING Läs alla anvisningar och varningar i detta dokument och i *System, säkerhet och krav från myndigheter - Informationshandbok* innan denna produkt tas i bruk.

Related Documents

The following Quantum documents are also available for the DXi V-Series:

Document No.	Document Title	Document Description
6-00618	*System Safety and Regulatory Information - Quantum Products*	Lists all safety and regulatory information for all Quantum products.

Document No.	Document Title	Document Description
6-67079	*DXi-Series NetBackup and Backup Exec OST Configuration Guide*	Provides information for setting up the DXi V-Series for OST operation with NetBackup and Backup Exec.
6-67081	*DXi-Series Command Line Interface (CLI) Guide*	Provides information on the DXi V-Series command line interface.
6-67353	*DXi Advanced Reporting User's Guide*	Provides information about using DXi Advanced Reporting features.

For the most up-to-date documentation for the DXi V-Series, go to:

http://www.quantum.com/dxi-vseriesdocs

> **Note:** For DXi V1000 Standard Edition users, documentation, community support, and other resources are available through Forum V (http://www.quantum.com/forumv), Quantum's online support forum for virtualization products.

Contacts

Quantum company contacts are listed below.

Quantum Corporate Headquarters

To order documentation on the DXi V-Series or other products contact:

Quantum Corporation *(Corporate Headquarters)*
1650 Technology Drive, Suite 700
San Jose, CA 95110-1382

Quantum Home Page

Visit the Quantum home page at:

http://www.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:

**Quantum.
Global Services**

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

  http://www.quantum.com/ServiceandSupport/Index.aspx

- **eSupport** - Submit online service requests, update contact information, add attachments, and receive status updates via e-mail. 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. Sign up today at:

  http://www.quantum.com/osr

Note: For DXi V1000 Standard Edition users, documentation, community support, and other resources are available through Forum V (http://www.quantum.com/forumv), Quantum's online support forum for virtualization products. Quantum customer support options are available for DXi V-Series Enterprise Edition users. To learn more about upgrading to Enterprise Edition, contact your Quantum Sales Representative.

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

United States	1-800-284-5101 (toll free)
	+1-720-249-5700
EMEA	+800-7826-8888 (toll free)
	+49-6131-3241-1164
APAC	+800-7826-8887 (toll free)
	+603-7953-3010

For worldwide support:

http://www.quantum.com/ServiceandSupport/Index.aspx

Worldwide End-User Product Warranty

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

http://www.quantum.com/pdf/QuantumWarranty.pdf

Chapter 1
DXi V-Series System Description

This chapter describes the DXi V-Series system and its components and includes the following sections:

- Overview
- Features and Benefits
- What's New in DXi 2.2.1 Software
- Data Reduction
- Space Reclamation
- Remote Replication
- Storage Presentation
- DXi Advanced Reporting
- Network Configuration

Overview

Quantum DXi V-Series provides an entry point for Quantum customers who want to implement a virtual infrastructure. The Quantum DXi V-Series is a flexible virtual appliance backup solution that integrates data deduplication and replication technology to connect

backup and DR (disaster recovery) protection across distributed corporate environments. DXi V-Series uses Quantum's patented data deduplication technology to increase disk capacities by 10 to 50 times and makes WAN replication a practical and effective part of disaster recovery planning. Quantum DXi V-Series is designed for customers who need to protect up to 24 TB of deduplicated data and who do not wish to deploy a physical DXi system.

Advanced Data Deduplication Increasing Disk Retention for Backup Data

The DXi V-Series leverages Quantum's patented data deduplication technology (U.S. Pat. No. 5,990,810) to dramatically increase the role that disk can play in the protection of critical data. With the DXi V-Series solution, users can retain 10 to 50 times more backup data on fast recovery disk than with conventional arrays.

Remote Replication of Backup Data Providing Automated Disaster Recovery Protection

With the DXi V-Series, users can transmit backup data from a remote site to a central, secure location to reduce or eliminate media handling. DXi™-Series replication is asynchronous, automated, and operates as a background process.

Enterprise Features Provide Secure Repository

The DXi V-Series presents storage as NAS shares (CIFS and NFS) or OST storage servers.

- **DXi V1000** - Features 1–2 TB of usable deduplication capacity.
- **DXi V4000** - Features 4–24 TB of usable deduplication capacity.

DXi Accent distributes deduplication between the DXi V-Series and the backup server to accelerate backups over bandwidth-constrained networks. Compatibility with Quantum's vmPRO software provides consolidated support for backup of physical and virtual servers.

Features and Benefits

The DXi V-Series system provides the following features and benefits:

- Inline data flow provides leading deduplication with an optimal combination of total system performance, manageability, and value.

- NAS or OST (OpenStorage) presentation layer.

- LAN/WAN replication compatible with the vmPRO virtual backup system, DXi V1000, DXi V4000, DXi2500-D, DXi4000 family, DXi6000 family, DXi7500, and DXi8500 models.

    - **DXi V1000** - Supports one source to one target replication.

    - **DXi V4000** - Supports ten sources to one target replication.

- OST Optimized Duplication support with Symantec Backup Exec and Symantec NetBackup.

- Supported by every major backup software vendor.

What's New in DXi 2.2.1 Software

DXi 2.2.1 Software for DXi V-Series introduces the following significant enhancements:

- **Guided Setup** - The Getting Started Wizard has been streamlined to help you to quickly set up the DXi V-Series after installation. After you complete the wizard, there is no need to restart the system, and you can begin configuring and using it immediately (see DXi V-Series Configuration Wizards on page 25).

- **Site Map** - The **User Interface Site Map** displays a visual map of all management pages in the DXi remote management console. Use the map to quickly locate and jump to any page (see DXi V-Series Management Pages on page 23).

- **Administrative Activity Log** - Use the **Activity Log** to view a record of all activities performed by administrative and service users in the past 90 days. You can view the user who performed the activity, the time the activity was performed, and other information. You can

also download the activity log to an XML file (see <u>Activity Log</u> on page 111).

- **OST Automatic Image Replication (AIR)** - If you are using Symantec NetBackup 7.1 or higher, you can configure an LSU for Automatic Image Replication. If enabled, data on an LSU is automatically replicated to a remote LSU that resides on a DXi in a different NetBackup domain (see <u>Replicating OST Data</u> on page 152).

- **Concurrent Optimized Duplication** - With Concurrent Optimized Duplication, as data is written to the storage server, it is simultaneously replicated to the target DXi. When optimized duplication or Automatic Image Replication subsequently occurs, the operation is more efficient because a portion of the required data has already been replicated to the target storage server (see <u>Replicating OST Data</u> on page 152).

- **DXi Accent Improvements** - DXi Accent supports Windows based media servers running Symantec Backup Exec or NetBackup. In addition, data sent from the media server to the DXi can be encrypted using AES (Advanced Encryption Standard) encryption methods (see <u>DXi Accent</u> on page 179).

- **Consolidated Job Scheduler** - All scheduled functions of the DXi are now managed on the **Scheduler** page, including the scheduling of replication, replication throttling, e-mail reports, healthchecks, and space reclamation (see <u>Scheduler</u> on page 181).

- **DHCP Support** - The DXi V-Series virtual Ethernet devices can be optionally configured using Dynamic Host Configuration Protocol (DHCP), allowing the DXi V-Series to automatically obtain an IP address from a DHCP server (see <u>Network</u> on page 193).

- **VLAN Tagging** - You can enable VLAN tagging and Jumbo Frames for any configured network interface on the DXi (see <u>Network</u> on page 193).

- **Space Reclamation Improvements** - Scheduled and on demand space reclamation has been tuned for increased performance, while automatic space reclamation during low space conditions provides maximum free space recovery. Also, the blockpool automatically reuses free bytes when ingesting data (see <u>Space Reclamation</u> on page 256).

- **Secure File Shred** - With Secure Shred, you can securely and permanently erase sensitive data stored on the DXi. To securely

erase data, first delete files on NAS shares or storage servers, then start secure shred. During secure shred, all residual data associated with the deleted files is securely erased from the disk drives and is overwritten with random patterns. Note that certain limitations apply when running secure shred on a virtual machine (see Secure Shred on page 263).

- **Automatic Licensing** - The correct licenses are automatically retrieved from the licensing server based on your product serial number. In most cases, there is no need to manually enter a license key (see License Keys on page 260

Enhancements in Previous Releases

The following enhancements were introduced in DXi 2.1.x Software:

- **Additional OpenStorage (OST) Improvements** - Enhancements include support for optimized synthetic full backups, and support for HP-UX 11i v3 IA-64 platforms (NetBackup only).

- **Replication Throttling and Scheduler** - With replication throttling, you can configure the DXi to limit its outgoing data replication bandwidth to a specified maximum in order to avoid network contention. Use the new **Scheduler** page to set up a recurring schedule for replication throttle, and to manage schedules for space reclamation and healthchecks.

- **AES 256-bit Encryption** - When sending replicated data to a target system, the DXi can take advantage of 256-bit encryption for stronger security.

- **New CLI Functionality** - The command line interface (CLI) supports new and updated functionality for enabling symlinks and hard links on NAS shares, enabling SMB server signing for NAS shares, mapping OST IP addresses, scheduling replication throttling, and performing advanced configuration of network interfaces.

- **Improved Space Reclamation Process** - The space reclamation process now better adjusts its use of system resources, consuming fewer resources during data ingest and performing space reclamation more quickly when more system resources are available.

The following enhancements were introduced in DXi 2.0.x software:

- **Inline Data Flow** - The new, inline data flow enabled by the DXi 2.x Software deduplicates data as it is ingested into the DXi appliance.

Optimized for the new generation of purpose-built DXi hardware platforms, it provides enhanced performance and more efficient dynamic use of system resources (see Data Reduction on page 7).

- **OpenStorage (OST) Improvements** - Enhancements include increased total performance, including writes, reads, and replication; simplified deployment (see Manage Users on page 169); and dynamically sized LSUs with no hard size limit (see LSU on page 163).

- **Automatic Replication Trigger** - In the Directory/File Based Replication, a file is automatically replicated after it is closed (CIFS shares) or after several minutes of inactivity (NFS shares) (see Directory/File Based Replication on page 71). There is no need for scripting to execute this function. This action makes files at the target available for access without a local recovery operation.

- **Enhanced Usability** - The user interface of the remote management console has been updated and improved to make it easier to see important information at a glance and perform the most common tasks (see DXi V-Series Remote Management on page 15).

  Note: For a list of all menus and pages in the remote management console, see DXi V-Series Management Pages on page 23. Use this list to help find the new location of features in the remote manage console.

- **Custom Network Configuration** - You can now create a custom network configuration using the remote management console as well as through the CLI (command line interface). The custom network option allows you to configure the DXi V-Series with individual IP subnet information for each physical interface (see Network on page 193).

- **Configuration Wizards** - New wizards provide guided assistance to help users configure key features of the DXi V-Series, such as storage presentation and data replication. Each wizard leads you step-by-step through the configuration process (see DXi V-Series Configuration Wizards on page 25).

Data Reduction

Data reduction is the process of reducing the amount of storage capacity required to store your data. The DXi V-Series systems provide two techniques to optimize the storage space required on your system:

- Data Deduplication
- Compression

Data Deduplication

The DXi-Series disk backup and replication systems use Quantum's patented data deduplication technology to dramatically increase the role that disk can play in data protection. With DXi-Series solutions, users can retain 10 to 50 times more backup data on fast recovery disk than with conventional arrays. This advantage allows IT departments to cost-effectively retain months of backup data on disk for faster, more reliable restores and more data recovery points. Quantum's innovative implementation of this core technology means that users do not have to compromise on performance to take advantage of extended retention capability. The new, inline data flow in the DXi 2.x Software provides streamlined deduplication that offers a maximum combination of total system performance, manageability, and value.

Quantum's deduplication technology uses a sub-file, variable-length approach to identify redundant blocks in a data stream—blocks that have appeared before in the same dataset or in datasets processed at an earlier time. When a block appears that has already been stored, the DXi system inserts a reference pointer to the earlier instance of the data segment instead of storing another copy. The result is a dramatic reduction in the storage capacity needed to store the data set, and a similar reduction in the bandwidth needed to replicate deduplicated data sets over a network. For more information on enabling data deduplication, see NAS Summary on page 128.

Compression

The DXi V-Series systems use compression technology after duplicate blocks have been identified and replaced as part of the deduplication process. With compression, unique data that has been through the data deduplication process can be compressed at a typical ratio of approximately 2:1. This enables you to maximize the storage capacity of your system.

Space Reclamation

The space reclamation process performs multiple functions on the DXi V-Series.

When data is deduplicated it is stored in a block pool—a pool of all unique data blocks that were captured during the data deduplication cycle. When subsequent backup jobs occur, the data deduplication engine searches for new data entering the DXi and uses a variable length compression algorithm to compare new data to existing data in the block pool. Unique blocks are added to the block pool and known blocks are indexed.

The space reclamation function searches the blockpool for data blocks that are not referenced by any pointers (that is, the files associated with the block have been expired and removed). Once such a data block is identified, the block is removed to make the space reusable.

For correct system operation, space reclamation *must* be run at regular intervals (at least once a week). Quantum recommends creating a schedule to automatically run space reclamation (see Scheduling Space Reclamation on page 190).

It may be beneficial to schedule space reclamation for a time when other operations are not normally being carried out. Therefore it is important to know when to schedule the space reclamation process. As best practice it is recommended that this process commences at least two hours after your backup job has completed on a daily basis. It is far more efficient to process a day's worth of new data than a week's worth.

Remote Replication

Today most backup occurs on isolated devices, making it difficult to deploy disk backup when disaster recovery protection is required. DXi-Series solutions use data deduplication and replication to decrease by up to 50 times the bandwidth required to move backup data over networks and between sites. This dramatic gain makes it practical and cost-effective for users to replicate backup data over WANs for secure, network-based disaster recovery protection, and it lets users combine rapid, local restores with sound disaster recovery protection.

With DXi-Series replication, users can transmit data from a single site or multiple sites to a central location using any DXi model. DXi-Series replication is an asynchronous, automated background process that includes encryption of data in transit. This model for protecting the distributed enterprise allows users to combine disk, replication, and tape for an optimal combination of performance, simplicity, and security.

For more information on implementing a replication plan, see Chapter 5, DXi V-Series Replication.

Storage Presentation

The DXi V-Series storage area is presented as NAS shares or OST LSUs (Logical Storage Units) (see Network Attached Storage (NAS) on page 10 andOpenStorage (OST) on page 11).

DXi Usage Scenarios

DXi storage presentations are optimized for backup usage rather than file sharing. Backup application usage is typically characterized by:

- Aggregated name spaces and file contents.
- Limited direct, active file access.
- Limited browsing, scanning, or metadata listing (stat).

- Limited metadata manipulation (including rename).

Usage diverging from these characteristics must be qualified to ensure acceptable behavior with respect to functionality, performance, replication, and recovery.

Network Attached Storage (NAS)

The DXi V-Series system has the ability to serve as a NAS backup system (see Figure 1) where the following protocols are supported:

- CIFS Protocol
- NFS Protocol

Note: In the DXi V-Series, NAS shares are optimized for backup rather than file sharing.

CIFS Protocol

The CIFS (Common Internet File System) protocol defines a standard for remote file access from many computers at a time in Windows environments. This protocol allows users with different platforms to share files without installing additional software.

Active Directory Support

The DXi V-Series supports ADS (Active Directory Services) as well as ACLs (Access Control Lists). This provides the following benefits:

- **Compatibility with CIFS domains** - NAS shares are able to join CIFS domains and use domain authentication.
- **Precise control of file system permissions** - Administrators can specify which users and groups can perform what actions.
- **Robust administrative support** - Administrators have the same implicit permissions as they do in Windows operating systems.

Note: Windows 2003, Windows 2003 R2, Windows 2008, and Windows 2008 R2 are supported for Active Directory domain membership.

> **Note:** When you create a CIFS share, the initial permissions are the same as the default permissions for a Windows 2003 share with the addition of an ACE (Access Control Entry) that permits full access to the share for all authenticated users. Administrators can choose to remove this full access ACE, set up custom permissions, or leave the ACL (Access Control List) as is if the server is set up in a fully trusted environment.

NFS Protocol

The NFS (Network File System) protocol was originally designed by Sun™ Microsystems and allows all network users to access shared files stored on computers of different types. NFS provides access to shared files through an interface called the Virtual File System (VFS) that runs on top of TCP/IP. Users can manipulate shared files as if they were stored locally on the user's own hard disk. With NFS, computers connected to a network operate as clients while accessing remote files, and as servers while providing remote users access to local shared files. This protocol is used with UNIX and Linux networks. It can also be used with Windows networks.

Figure 1 NAS Backup using CIFS and NFS

Linux / Unix Clients — NFS — **DXi V1000** — CIFS — **Windows Clients**
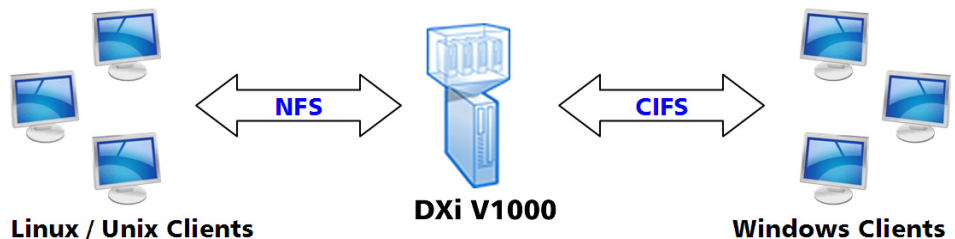
OpenStorage (OST)

With the OST presentation, the DXi system presents storage servers to a Symantec NetBackup or Backup Exec media server through a specific Symantec protocol. A storage server consists of logical storage units (LSUs), which are similar to directories in a NAS file system.

The OST presentation requires the Symantec NetBackup 7.x or later, or Backup Exec 2010 or later host application, and the OST Plug-in client

installation on the media server. Plug-in clients are host-OS dependent and are supplied by Quantum. To use the DXi in OST mode, you must configure an OST storage server and LSUs on the DXi. You must also map the LSUs on the NetBackup server so that NetBackup can perform backups and restore from them. Additionally, policies for optimized duplication (OST replication) may need to be set on the NetBackup server.

Figure 2   OpenStorage (OST) Example

OST (Open Storage)
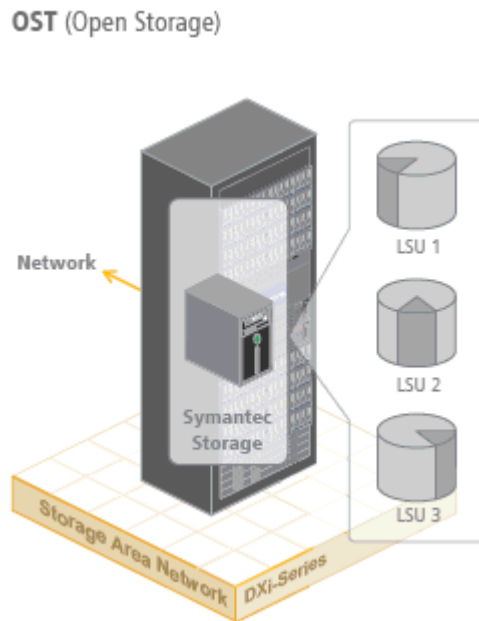
DXi Advanced Reporting

Quantum DXi Advanced Reporting works with all DXi-Series disk backup systems. DXi Advanced Reporting combines comprehensive performance data logging with powerful visual reporting and analysis tools to help you identify potential problems and optimize system operation. For more information, refer to the *DXi Advanced Reporting* section of your *DXi V-Series User's Guide*.

Network Configuration

During network configuration, each individual interface on the DXi V-Series can be configured as a subnet with its own network settings. The DXi V-Series utilizes four VMware VMXNET3 virtual Ethernet ports. The virtual Ethernet ports are not bonded into a single interface. Bonding would provide a benefit only if the ESXi server has network connectivity over multiple 1GbE or 10GbE physical Ethernet ports. Similarly, there is no benefit in routing different traffic types (management, replication, or data) on different interfaces unless the ESXi server hardware is configured to utilize such a configuration.

The DXi V-Series supports DHCP for automatic configuration of IP addresses. You can also manually specify IP addresses as required by your network.

For more information about configuration network settings, see Network on page 193.

> **Note:** Each configured network interface requires its own set of network settings (IP address, network mask, and gateway).

The Quantum DXi V-Series provides a powerful Web-based user interface that allows you to configure and manage the system from a remote workstation on the same network as the DXi V-Series.

> **Note:** The illustrations in this document show the DXi V1000 user interface. The functionality of DXi V4000 systems is identical unless otherwise noted.

Use the DXi V-Series remote management console to perform the following tasks:

- Set up the DXi V-Series using guided procedures (see DXi V-Series Configuration Wizards on page 25).

- View important system information at a glance (see DXi V-Series Home Page on page 57).

- Manage data replication activities (see DXi V-Series Replication on page 69).

- Monitor system performance (see DXi V-Series Status on page 103).

- View administration alerts and resolve service tickets (see DXi V-Series Alerts on page 115).

- Configure storage presentation, data replication, and system settings (see DXi V-Series Configuration on page 127).

- Run diagnostic tools and maintain the system (see DXi V-Series Utilities on page 247).

Accessing Remote Management

Access the remote management console using a Web browser on a workstation that is on the same network as the DXi V-Series.

See the following sections for more information about accessing DXi V-Series remote management:

- Supported Browsers
- Logging On to the DXi V-Series
- Logging Off of the DXi V-Series

Supported Browsers

Web browser software is not included with the DXi V-Series. You must obtain and install it separately. The DXi V-Series remote management console supports the following Web browsers:

- **Windows** - Microsoft Internet Explorer 8.x or higher, Mozilla Firefox 7.x or higher
- **Linux** - Mozilla Firefox 7.x or higher

Note: For correct operation of the remote management console, disable any pop-up blockers and enable JavaScript in your Web browser.

Note: Buttons, borders, and other graphic elements may display differently in Internet Explorer 7 and 8. These differences are cosmetic only and do not affect functionality in any way.

Logging On to the DXi V-Series

To log on to the DXi V-Series remote management console:

1 Launch a supported Web browser on a workstation that has network access to the DXi V-Series.

2 In the browser address box, type the IP address of the DXi V-Series, and then press **<Enter>**.

The **Login** window displays (see Figure 3).

Figure 3 Login Window
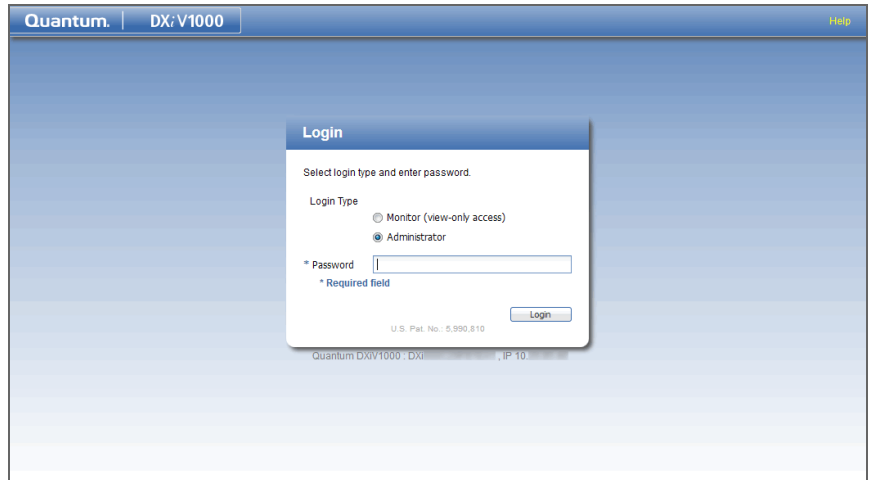
If the **Login** window does not display, verify that the IP address is correct and that the network path to the DXi V-Series is valid. Also verify that you are using a supported Web browser. Then try again. If you are still unable to access the Login window, contact your DXi V-Series administrator.

> **Note:** The default IP address is **10.1.1.1**. The IP address can be changed during installation using the **Getting Started Wizard** or at a later time on the **Network** page (see Network on page 193).

3 Select the login type and enter the corresponding password.

- **Monitor** - Allowed to view information on the DXi V-Series remote management console but cannot make changes. (The default password is **password**.)

- **Administrator** - Allowed to view and change information on the DXi V-Series remote management console. (The default password is **password**.)

> **Note:** Passwords are limited to 15 characters. All alphanumeric characters are allowed, as well as underscores (**_**) and hyphens (**-**). Passwords can be changed on the **Web & CLI Passwords** page (see Web & CLI Passwords on page 213).

4 Click **Login**.

5   If a security banner message has been specified for the DXi V-Series, click **Accept**.

Note:	For information about specifying a security banner message, see Security Notice on page 220.

The **Home** page displays (see Figure 4).

Figure 4 Home Page
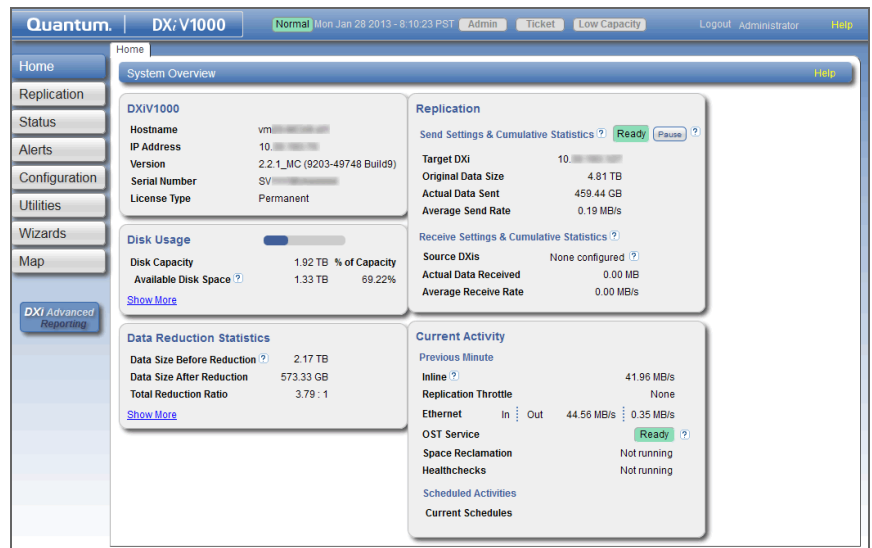
If you are unable to log on, verify that the password is correct, then try again. If you are still unable to log on, contact your DXi V-Series administrator.

Caution:	More than one Administrator can log on to the DXi at a time. If two Administrators attempt to make configuration changes on the same page at the same time, it is possible that one Administrator's changes will overwrite the other's. Always coordinate configuration changes with other Administrator users.

**Logging Off of the
DXi V-Series**

When you are done working in the DXi V-Series remote management
console, click **Logout** on the upper right of the remote management
console to end your session.

Note: If the DXi V-Series remote management console is idle for more
than 30 minutes (default setting), the system logs off the user.
The inactivity timeout can be changed on the **Login Session**
page (see Login Session on page 219).

The Remote Management Console

After you log on to the DXi V-Series, the remote management console
displays. The remote management console includes the following
features:

- System Banner

- Main Menu

- DXi V-Series Management Pages

System Banner

The system banner displays at the top of the remote management
console (see Figure 5). Use the system banner to see overall system
status and alert information at a glance, and to quickly access additional
information. The system banner also displays the time and date as well
as the login type (administrator or monitor).

Figure 5 System Banner
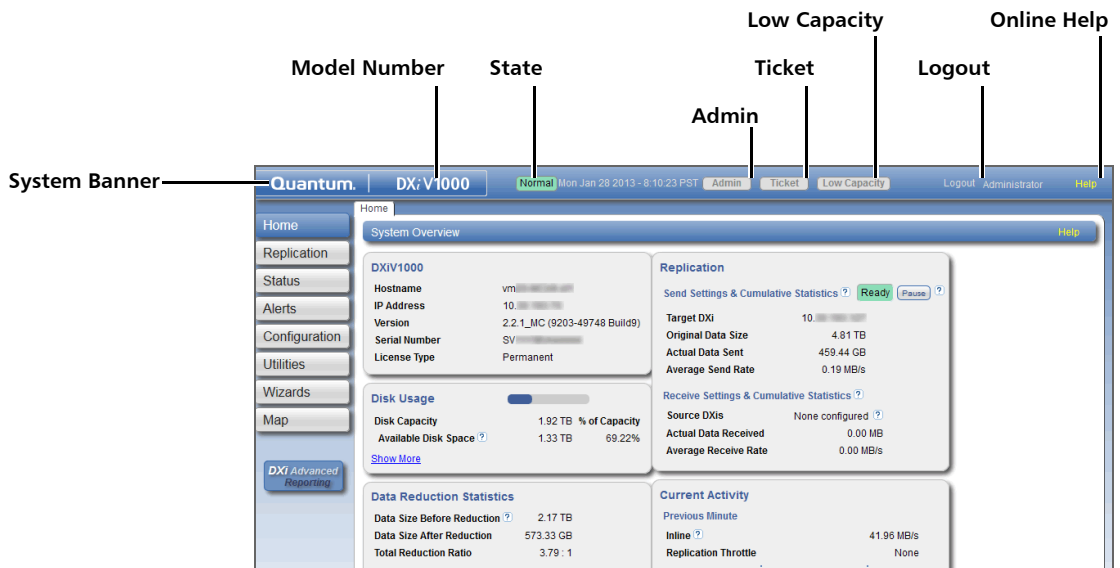
The following items display on the system banner:

- **Model Number** - The model number of the DXi V-Series.

- **State** - Displays the operating state of the DXi V-Series:

    - **Normal** - (Green) The system is operating correctly.

    - **Attention** - (Yellow) There is a problem with the system.

    - **I/O Write Low Threshold** - (Yellow) Ingest continues and space reclamation starts.

    - **Verify Failure** - (Red) The blockpool verify process has failed.

    - **Low Space** - (Red) Available disk space has fallen to a low level. Ingest is stopped.

    - **No Space** - (Red) Available disk space has fallen to a critical level. All I/O is stopped.

    Click the **Status** button to display detailed status information the system.

- **Admin** - The **Admin** button turns yellow when an administration alert occurs. Click the **Admin** button to manage administration alerts (see Admin Alerts on page 115).

- **Ticket** - The **Ticket** button turns yellow when open service tickets are present. Click the **Ticket** button to manage service tickets (see Service Tickets on page 117).

- **Low Capacity** - The **Low Capacity** button turns yellow when available disk space falls to a low level (see Low Capacity Management on page 21). Click the **Low Capacity** button to view the administration alerts related to low disk capacity (see Admin Alerts on page 115).

  > **Note:** When disk capacity is low, target replication to the system is paused (see Replication Service on page 98). In addition, space reclamation is automatically started to free up disk space (see Space Reclamation on page 256).

- **Logout** - Click to end your remote management session.

- **Help** - Click to display the online help.

Low Capacity Management

As disk capacity is used and free disk space approaches low levels, the DXi V-Series automatically responds in the following ways:

- The **Low Capacity** condition is activated when the amount of free disk space is less than 50 GB (DXi V1000) or 500 GB (DXi V4000).

  The **Low Capacity** condition indicator turns off when free disk space is larger than this threshold.

- An administrative alert and a service ticket are generated each time free disk space drops below one of the following threshold values:

  - **50 GB (DXi V1000) or 500 GB (DXi V4000)** - The system banner displays **Attention** and the system enters the **Low Threshold** state. Ingest continues and space reclamation starts.

  - **10 GB (DXi V1000) or 250 GB (DXi V4000)** - The system banner displays **Low Space**. Ingest stops and replication is paused, but data can still be read.

  - **5 GB (DXi V1000) or 10 GB (DXi V4000)** - The system banner displays **No Space**. All data read/write is stopped.

- When the DXi V-Series enters the **Low Capacity** condition, space reclamation is automatically started to free up disk space.

A space reclamation task is initiated every 10 minutes until space reclamation begins. Space reclamation ends when the DXi V-Series exits the **Low Capacity** condition. (Any space reclamation tasks running at that time are allowed to complete.)

- When the DXi V-Series enters the **Low Space** condition, target replication to the system is paused. Target replication resumes when the DXi V-Series exits the **Low Space** condition.

- Ingest of backup data is not throttled during the **Low Capacity** condition unless free disk space falls below the 10 GB (DXi V1000) or 250 GB (DXi V4000) threshold. When this occurs, no write requests are accepted until free disk space rises above 10 GB (DXi V1000) or 250 GB (DXi V4000).

Main Menu

The main menu displays on the left side of the DXi V-Series remote management console (see Figure 6). Click a menu item to display the corresponding management page.

To access **DXi Advanced Reporting**, click the link below the main menu. Quantum DXi Advanced Reporting provides performance data logging and visual reporting and graphing features for Quantum DXi-Series systems. For more information, see the *Quantum DXi Advanced Reporting User's Guide* (6-67353).

> **Note:** Clicking **Wizards** on the main menu replaces the main menu with the wizards menu. Click a menu item to begin a wizard, or click **Exit** to return to the main menu (see DXi V-Series Configuration Wizards on page 25).

Figure 6 Main Menu
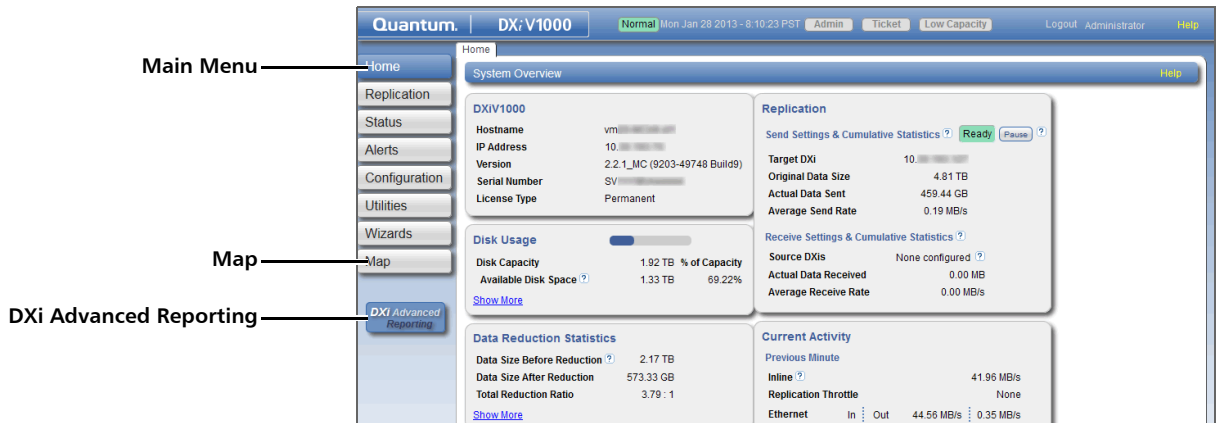
DXi V-Series Management Pages

Use the DXi V-Series management pages to view information as well as configure and manage the system. To navigate to a page, first click a menu item, then click a tab to display the corresponding page. Some pages include sub-tabs that display pages with additional information and options.

To view a graphical map of all remote management pages, click **Map** on the main menu (see Figure 6). On the map, click the name of a page to quickly navigate to that page (see Figure 7).
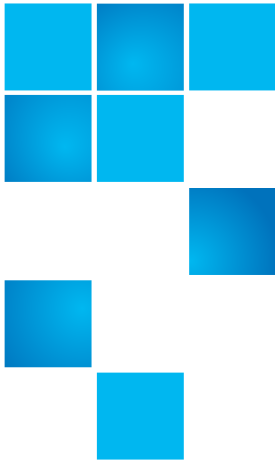
If you need help as you work, click **Help** in the page's title bar to see online help for that page. In addition, Quick Tips are available on many pages. Click the **Quick Tip** icon **[?]** next to a section or field to learn more about that item.

Caution:	Unless directed to do so by the documentation, do not use your Web browser's **Back**, **Forward**, or **Refresh** buttons when navigating in the remote management console. Doing so may have unintended effects. Instead, always use the main menu and tabs to navigate in the remote management console.

Figure 7 Remote Management
Pages Map

Click a page name to navigate to that page
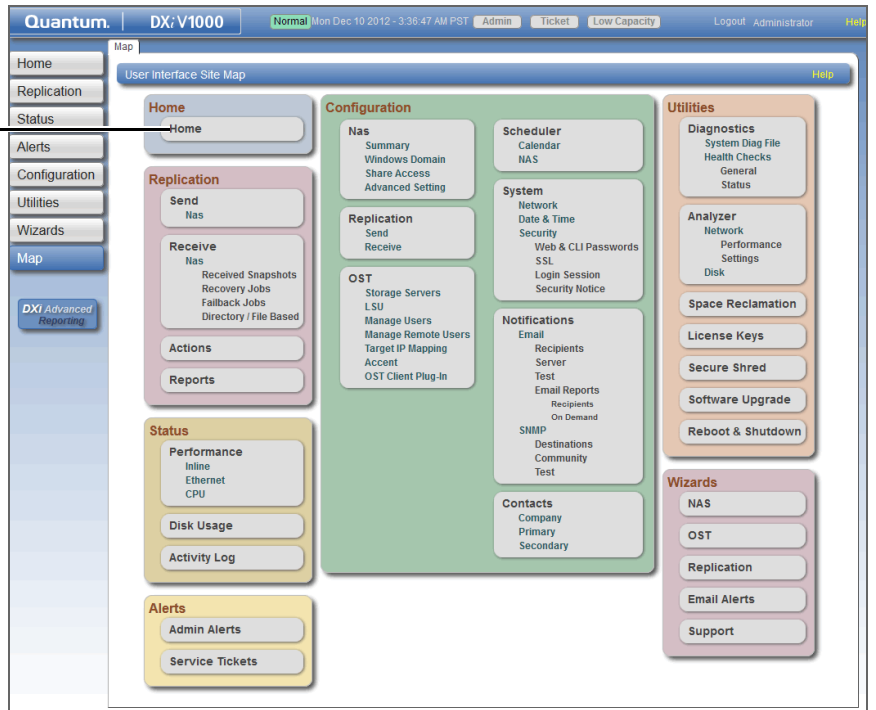
Chapter 3

DXi V-Series Configuration Wizards

The **Configuration Wizards** provide guided assistance for setting up the DXi V-Series. Use the wizards to quickly configure the most important features of the system, including storage presentation and data replication. Each wizard leads you step-by-step through the configuration process.

The **Configuration Wizards** page displays the first time you log on to the remote management console after completing the **Getting Started** wizard. After that, to access the **Configuration Wizards**, click **Wizards** on the main menu. This replaces the main menu with the **Wizards** menu (see Figure 8).

The **Wizards** menu includes the following wizards:

- **NAS** - Helps you configure the DXi V-Series as a NAS (Network Attached Storage) appliance for use on a Windows or UNIX/Linux network (see NAS Wizard on page 26).

- **OST** - Helps you configure the DXi V-Series to present its storage as one or more OST (OpenStorage) storage servers for use with a backup application (see OST Wizard on page 33).

- **Replication** - Helps you configure the DXi V-Series to send replicated data to or receive replicated data from another DXi system (see Replication Wizard on page 40).

- **Email Alerts** - Helps you configure the DXi V-Series to automatically send notifications and reports to selected recipients (see Email Alerts Wizard on page 46).

- **Support** - Helps you enable licensed features on the DXi V-Series, register your system with Quantum, and perform other tasks that will aid Quantum customer support in assisting you (see Support Wizard on page 50).

Click an item on the **Wizards** menu to begin a wizard. After you complete a wizard, a green check mark displays next to its name on the **Wizards** menu. To display the main menu again, click **Exit**.

Figure 8 Wizards Menu
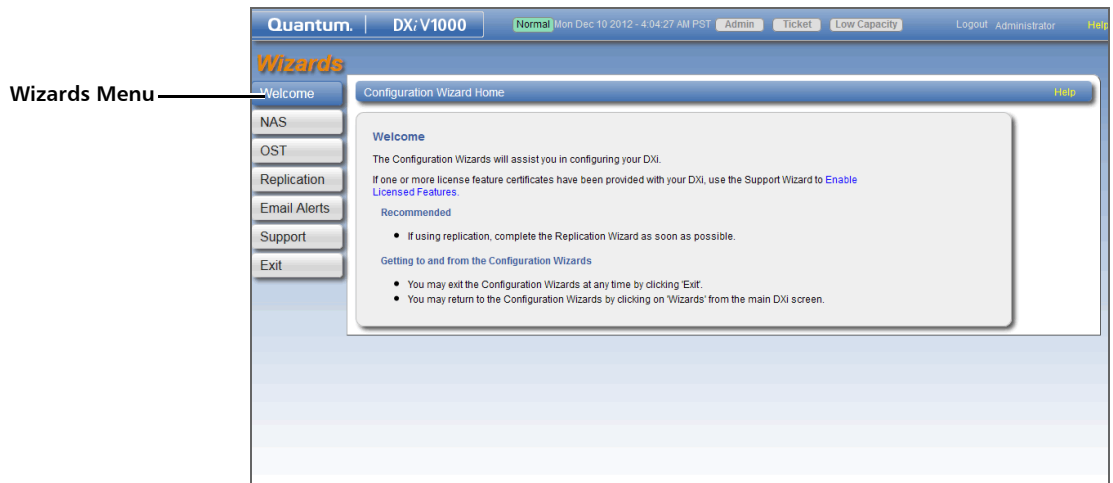
NAS Wizard

The **NAS** wizard provides guided assistance for configuring the DXi V-Series as a NAS (Network Attached Storage) appliance. The wizard helps you determine if the NAS shares will be used on a Windows or UNIX/Linux network, and if necessary helps you join the DXi V-Series to a Windows domain. Then the wizard guides you through the process of adding one or more NAS shares to receive backup data.

> **Note:** You cannot use the NAS wizard to edit existing shares. For more information about working with NAS shares, see NAS on page 127.

To begin the **NAS** wizard, on the **Wizards** menu, click **NAS**.

Step 1: About

1 Read the information about the wizard (see Figure 9).

2 Click **Next** to continue.

> **Note:** At any time while using the wizard, you can click **Previous** to return to the previous step.

Figure 9 NAS Wizard: About
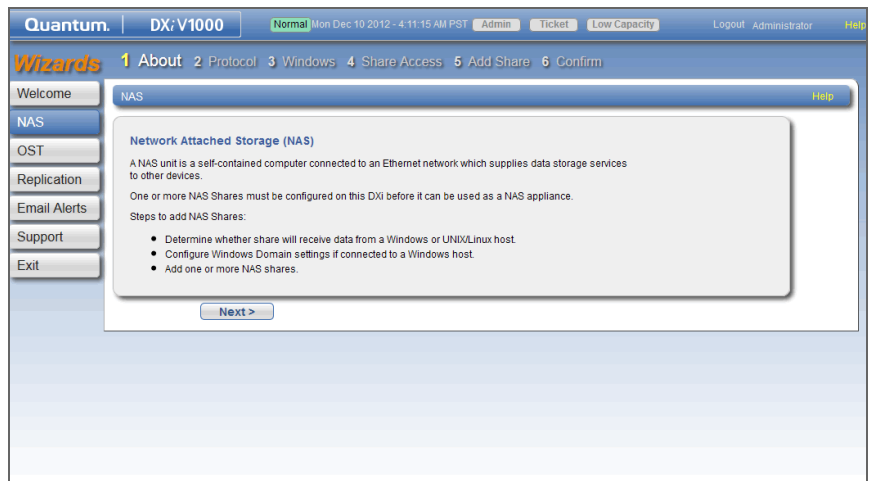
Step 2: Protocol

1 Select the type of host the DXi V-Series will present NAS shares to (see Figure 10):

- **Windows (CIFS)** - All hosts that will interact with the DXi V-Series run Windows.

- **UNIX/Linux (NFS)** - All hosts that will interact with the DXi V-Series run UNIX or Linux.

> • **Both Windows & UNIX/Linux** - Both types of hosts (Windows
> and UNIX/Linux) will interact with the DXi V-Series.

2 Click **Next** to continue.

Figure 10 NAS Wizard:
Protocol
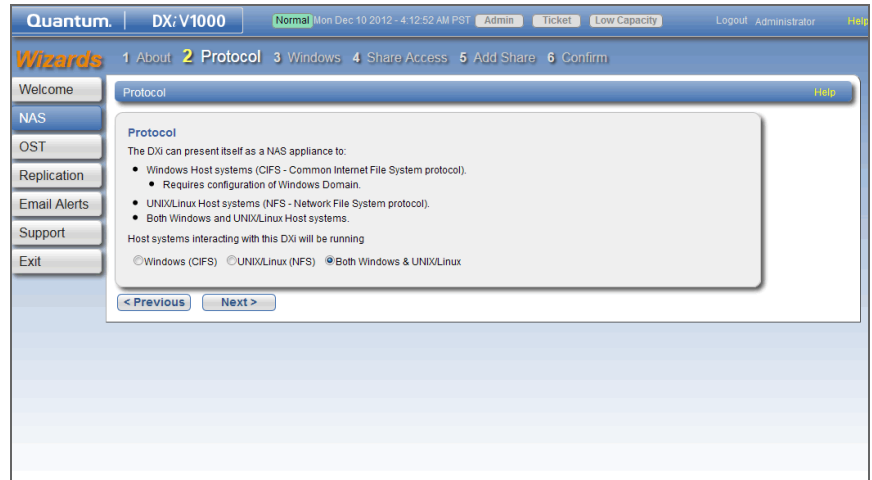
Step 3: Windows

Note: If you selected the **UNIX/Linux (NFS)** option in the previous
step, the wizard automatically skips this step. Continue with
Step 5: Add Share on page 31.

1 Select an option for joining the DXi V-Series to the Windows
network (see Figure 11):

  • **Active Directory** - Add the DXi V-Series to a Windows network
  using Active Directory

  • **Workgroup** - Add the DXi V-Series to a workgroup on a
  Windows network

  Note: To disjoin a domain, see Windows Domain on page 135.

2 In the **Domain/Workgroup Name** box, enter the name of the
domain or workgroup the DXi V-Series is joining.

3 (Active Directory only) Enter information about the primary domain
controller:

- **Primary Domain Controller** - Select an option for the Primary Domain Controller (PDC):

    - **Use DNS Discovery** - Discover the PDC automatically.

    - **Specify Address** - Enter the fully qualified name or the IP address of the PDC.

- **Organization Unit** - (Optional) Enter the name of the organizational unit in the domain.

    The DXi V-Series will become a member of this organization.

- **Administrator Name** - Enter **Administrator** or any user that has the right to join the domain.

    By default, any user belonging to the **Administrators** group or the **Domain Admins** group has the right to join the domain. In addition, any user can join the domain if they are specifically delegated this right by a member of the **Administrators** group.

- **Administrator Password** - Enter the password for the user entered above.

Note: To configure users, see Share Access on page 138.

---

4 Click **Next** to continue.

Figure 11 NAS Wizard: Windows

Step 4: Share Access

1 Do one of the following depending on whether the DXi V-Series is joining a Windows Workgroup or an Active Directory Domain:

- **Windows Workgroup** - Enter information about the workgroup user:

  - **User Name** - Enter the name of the workgroup user.

  - **Password** - Enter the password for the workgroup user.

  - **Confirm Password** - Enter the password again to confirm it.

  - **Description** - (Optional) Enter a brief description of the workgroup user.

  - **Grant Administrator Privileges** - Select the check box to add the workgroup user to the Windows Administrators group.

    This allows the workgroup user to override certain permissions settings and prevents the workgroup user from being locked out of shares or directories.

- **Active Directory Domain** - Enter the **Fully Qualified User or Group Name** of the share administrator.

2 Click **Add**.

3 (Optional) To add additional workgroup users or share administrators, repeat Steps 1–2.

4 Click **Next** to continue.

Figure 12 NAS Wizard: Share Access

Step 5: Add Share

1 Under **Add Share**, enter information about the NAS share (see [Figure 13](#)):

- **Name** - Enter the name of the NAS share.

- **Description** - (Optional) Enter a brief description of the share.

- **Enable deduplication** - Select the check box to enable data deduplication. Quantum recommends that you enable data deduplication to optimize disk usage.

  Note: Data deduplication is enabled by default. You cannot enable or disable data deduplication after the share is added.

- **Hide from network browsing** - (Windows shares only) Select the check box to hide the share from network browsing. If selected, you cannot see the share when browsing the network.

- **Export Protocol** - (Available only if you selected the **Both** option in [Step 2: Protocol](#) on page 27) Select the export protocol for the share:

    - **CIFS** - Select the CIFS option to use the share on a Windows network.

- **NFS** - Select the NFS option to use the share on a UNIX or Linux network.

2 Click **Add**.

3 (Optional) To add additional shares, repeat Steps 1–2.

4 Click **Next** to continue.

Figure 13 NAS Wizard: Add Share
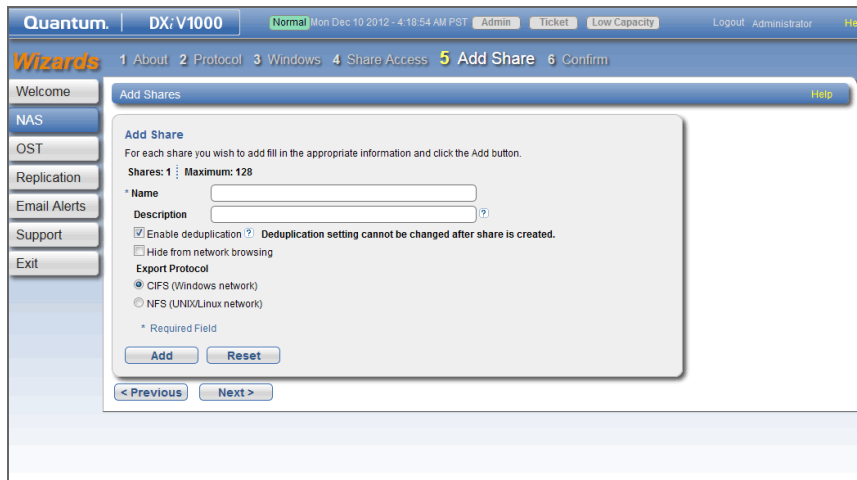
Step 6: Confirm

1 Review the settings you selected to make sure they are correct (see [Figure 14](#)). If necessary, click **Previous** to return to a previous step to make changes.

2 To make changes to a NAS share you added, first select the share and click **Delete** to delete the share. Then click **Previous** to return to the previous step and add a new share.

3 After you have confirmed all settings, click **Finish**. The wizard configures the DXi V-Series with the settings you selected.

Figure 14 NAS Wizard:
Confirm
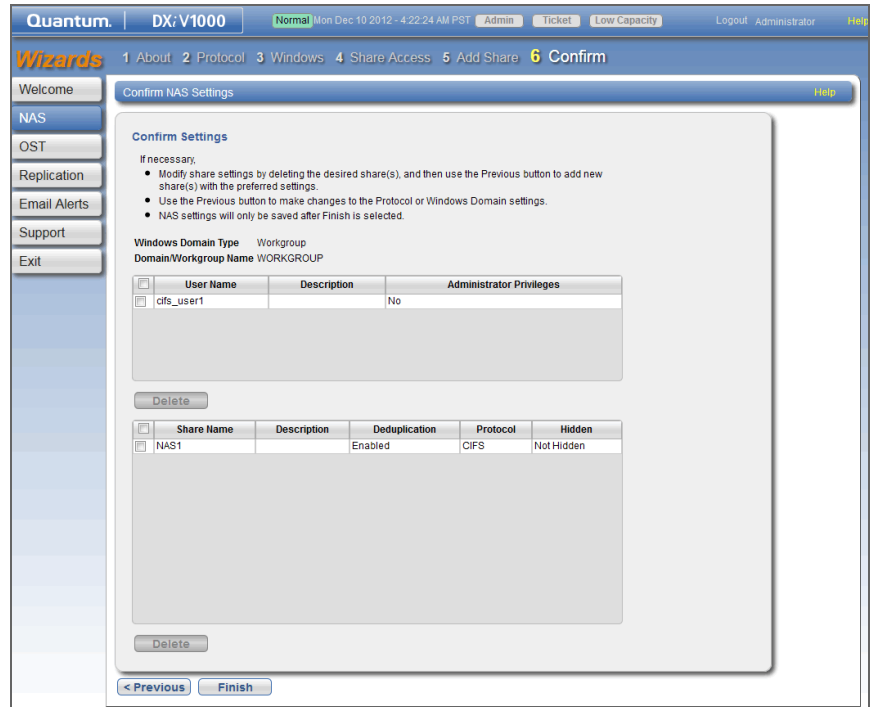
OST Wizard

The **OST** wizard provides guided assistance for configuring the
DXi V-Series to present its storage as one or more OST (OpenStorage)
storage servers for use with a backup application. The wizard guides
you through the process of adding one or more OST storage servers,
configuring LSUs (logical storage units), and adding OST users. The
wizard also provides a link for downloading and installing the OST Plug-
in on your backup host.

Note: You cannot use the OST wizard to edit existing storage servers
or LSUs. For more information about working with OST, see

To begin the **OST** wizard, on the **Wizards** menu, click **OST**.

Step 1: About

1 Read the information about the wizard (see Figure 15).

   The **About** page displays the status of the OST service. OST settings can be configured in **Ready**, **Stopped**, or **Verifying** state. The OST server is available for backup only in **Ready** state.

2 Click **Next** to continue.

Note: At any time while using the wizard, you can click **Previous** to return to the previous step.

Figure 15 OST Wizard: About
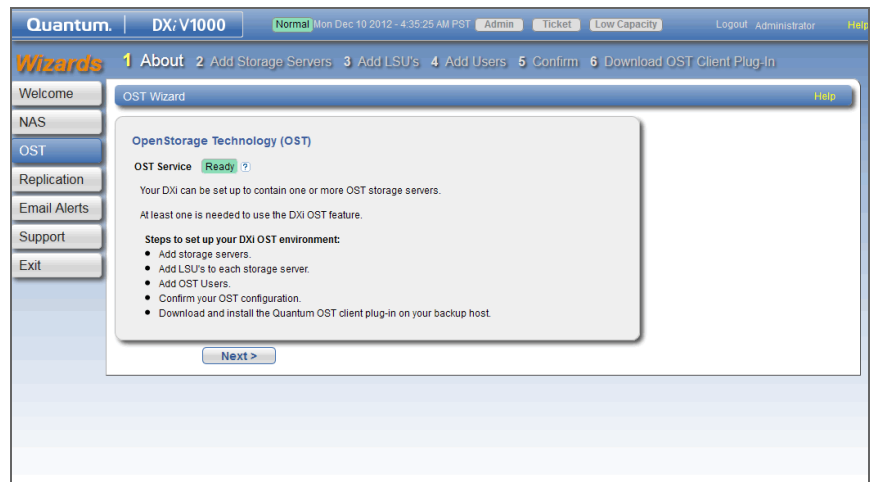
Step 2: Add Storage Servers

1 Under **Add Storage Server**, enter information about the storage server (see Figure 16):

   • **Name** - Enter the name of the storage server.

   Caution: Do not use an underscore (_) in the name of the storage server.

- **Description** - (Optional) Enter a brief description of the storage server.

- **Max Connections** - Enter the maximum number of connections allowed to the storage server (3 to 65536).

   Note: Quantum recommends setting **Max Connections** to 300.

- **Enable Concurrent Optimized Duplication** - Select the check box to enable optimized duplication during OST ingest.

   Concurrent Optimized Duplication is disabled by default. If enabled, as data is written to the storage server, it is simultaneously replicated to the target DXi. When optimized duplication or Automatic Image Replication subsequently occurs, the operation is more efficient because a portion of the required data has already been replicated to the target storage server.

   Note: To configure the target DXi, see Replication Wizard on page 40.

   Note: When Concurrent Optimized Duplication is enabled, all data on the storage server is duplicated, not just the specified images.

2 Click **Add**.

The storage server displays in the **Storage Servers Added** table.

3 (Optional) To add additional storage servers, repeat Steps 1–2.

To remove a storage server, select it in the **Storage Servers Added** table and click **Delete**.

4 Click **Next** to continue.

Figure 16 OST Wizard: Add
Storage Servers
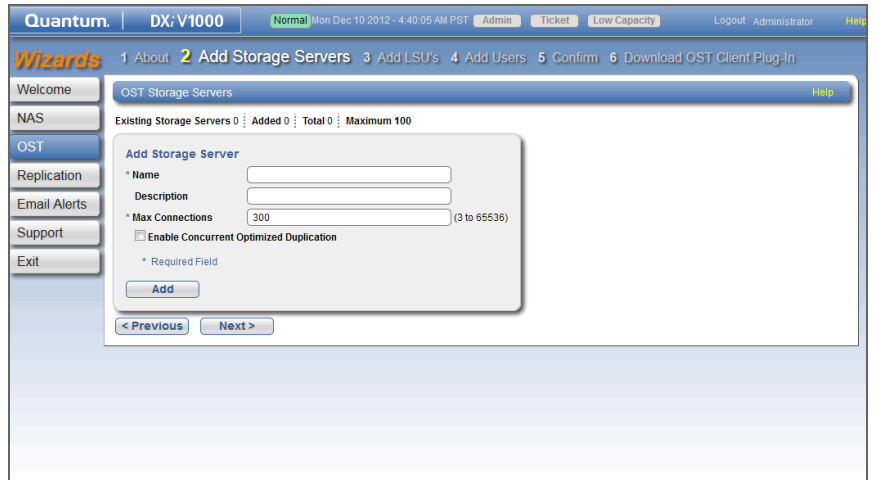
Step 3: Add LSUs

1 Enter information about the LSU (see Figure 17).

- **Storage Server** - Select the storage server that will contain the new LSU.

- **Use Available Capacity** - Select this option to add an LSU that uses the available capacity on the system.

  You cannot add an available capacity LSU to a storage server that already contains an LSU. Also, if you add an available capacity LSU to a storage server, you cannot add additional LSUs to that same storage server.

  Note: After you add an LSU that uses the **Available Capacity** option, you cannot change the LSU to use the **Specific Capacity** option. Instead, you must delete the LSU, then add a new LSU and choose the **Specific Capacity** option (see Deleting an LSU on page 169).

- **Specify Capacity** - Select this option to specify the physical capacity of the LSU, and then enter the following information.

  - **LSU Name** - Enter the name of the LSU.

  - **Physical Capacity** - Enter the physical capacity of the LSU (1 to 1048576 GB).

2 Click **Add**.

The LSU displays in the **LSUs Added** table.

3 (Optional) To add additional LSUs, repeat Steps 1–2.

To remove an LSU, select it in the **LSUs Added** table and click **Delete**.

4 Click **Next** to continue.

Figure 17 OST Wizard: Add LSUs
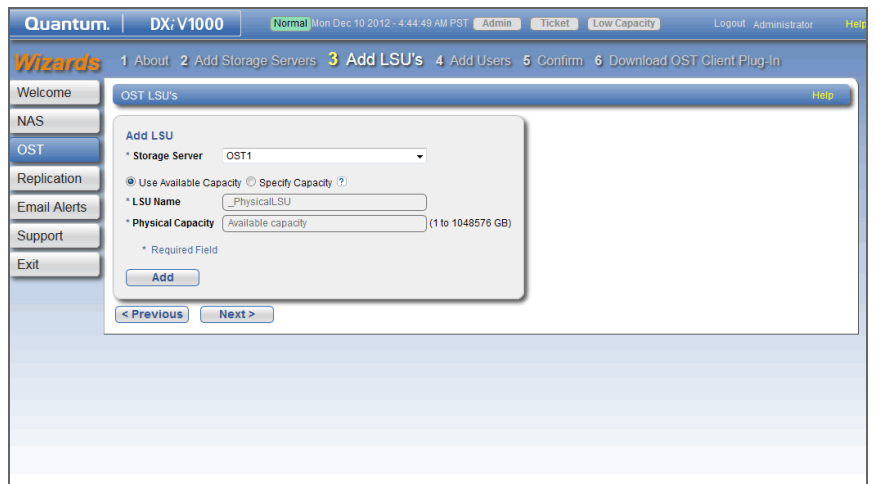
Step 4: Add Users

1 Enter information about the authenticated user (see Figure 18):

- **Username** - Enter the name of the authenticated user.

- **Password** - Enter the password for the authenticated user.

- **Confirm Password** - Enter the password again to confirm it.

- **Description** - (Optional) Enter a brief description of the authenticated user.

2 Click **Add**.

The user displays in the **Users Added** table.

3 (Optional) To add additional users, repeat Steps 1–2.

To remove a user, select it in the **Users Added** table and click **Delete**.

4 Click **Next** to continue.

Figure 18 OST Wizard: Add
Users
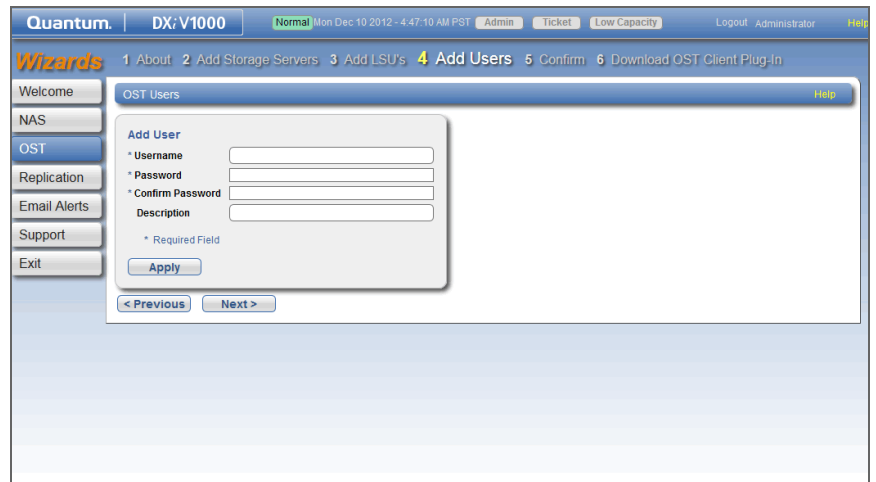
Step 5: Confirm

1 Review the settings you selected to make sure they are correct (see Figure 19). The items to be added display in the **Storage Servers Added**, **LSUs Added**, and **Users Added** tables. If necessary, click **Previous** to return to a previous step to make changes.

2 To make changes to storage servers, LSUs, or users you added, click **Previous** to return to the appropriate step. Select the incorrect item and click **Delete** to remove it, and then add a new item.

3 After you have confirmed all settings, click **Finish**. The wizard configures the DXi V-Series with the settings you selected.

4 Click **Yes** to continue with downloading the OST Plug-in.

Figure 19 OST Wizard:
Confirm
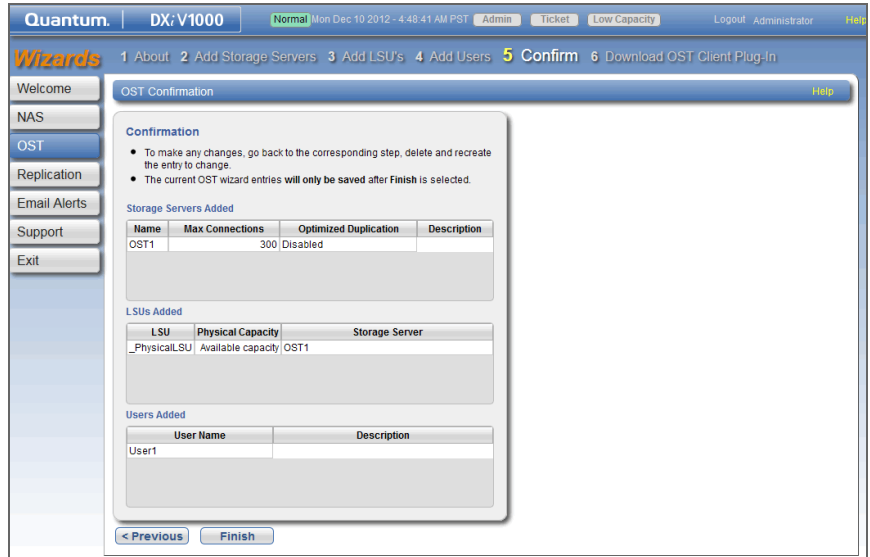
Step 6: Download OST Client Plug-In

To download the OST Plug-in, click **Client Plug-in Download** (see Figure 20). On the download page, download the correct OST Plug-in for your backup application and operating system.

Also on the download page, click **Installation Instructions**, to download the *OST Plug-in Installation Instructions*. Follow the instructions to install the OST Plug-in on your media server.

Figure 20 OST Wizard:
Download OST Client Plug-in
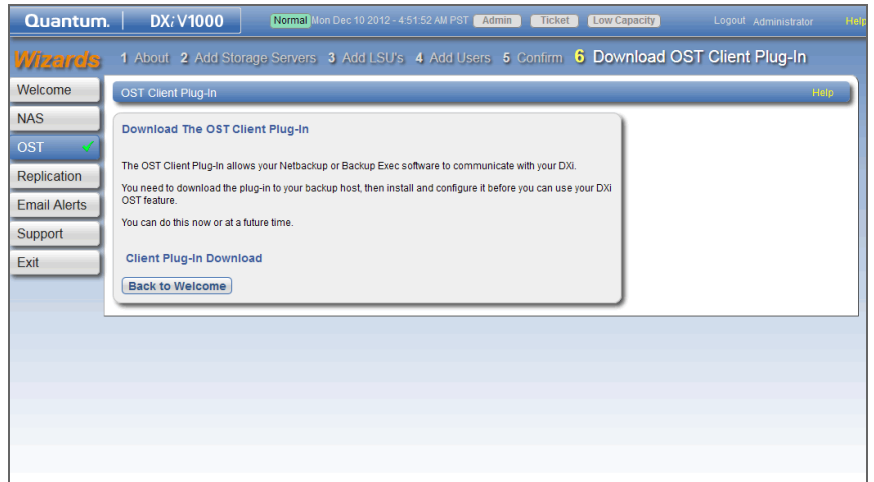
Replication Wizard

The **Replication** wizard provides guided assistance for configuring the DXi V-Series to send replicated data to another DXi system as part of disaster recovery plan. The wizard can also help you configure the DXi V-Series to receive replicated data from another DXi system.

Sources *send* replicated data, and targets *receive* replicated data. A target system can receive data from up to 10 sources. However, a source system can send data to only a single target. Finally, one system can act as both a source and a target.

Note: For more information about working with data replication, see DXi V-Series Replication on page 69.

Note: Use the **Replication** wizard (or the **Configuration > Replication** page) to configure other DXi systems that this DXi V-Series is configured to send replicated data to or receive replicated data from. You should configure a target system before configuring source systems.

To begin the **Replication** wizard, on the **Wizards** menu, click **Replication**.

Step 1: About

1 Read the information about the wizard (see Figure 21).

2 Click **Next** to continue.

Note: At any time while using the wizard, you can click **Previous** to return to the previous step.

Figure 21 Replication Wizard: About
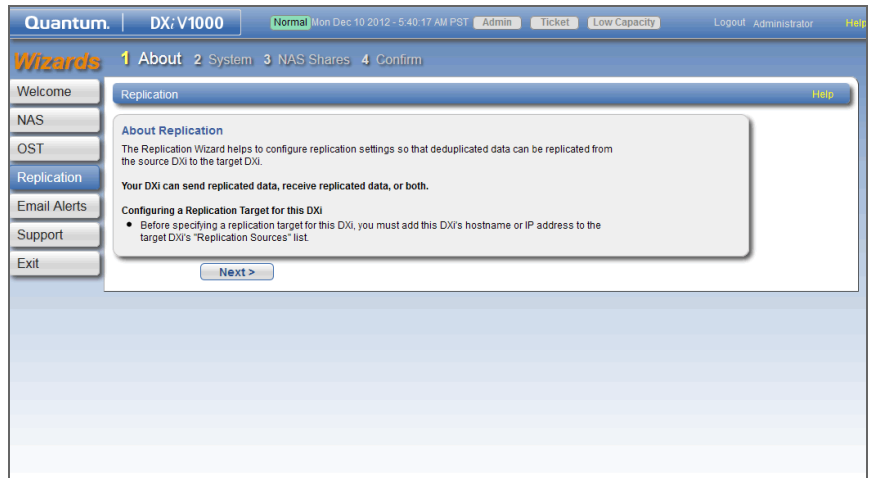
Step 2: System

1 If data on this DXi V-Series will be replicated to another DXi system, enter the following information under **Target DXi** (see Figure 22):

   a In the **Target Hostname or IP Address** box, enter the hostname or IP address of the system that will receive the replicated data.

     Note: When entering IP addresses, never use an address that is in a reserved IP address range. To see a list of reserved IP address ranges, click the quick tip icon **[?]** located near the IP address field.

> **Note:** To use hostname format, you must specify at least one
> DNS IP address on the **Network** page (see <u>Network</u> on
> page 193).

  b In the **Source IP Address** field, enter the IP address that is used
to uniquely identify the source DXi to the target. This may be
different than the actual network IP address of the source DXi.

    If the target system is at DXi 2.1 Software or higher, this field is
not required. If the target system is at DXi 2.0.1.x Software or
below, then you must enter the IP address by which the target
system recognizes the source system. The default value is
0.0.0.0.

  c (Optional) Leave the **Encrypt data before replication** check
box selected to enable encryption when sending replication
data to the target system. Or clear the **Encrypt data before
replication** check box to disable encryption when sending
replication data to the target system.

    If encryption is enabled, select an encryption strength (**128-bit**
or **256-bit**). Using 256-bit encryption (default) provides a
stronger level of security but may have an impact on system
performance in some situations.

> **Note:** Encryption is enabled by default. However, for best
> performance, if your data network is already secured,
> you should clear the **Encrypt data before replication**
> check box.

2 If data on other DXi systems will be replicated to this DXi V-Series,
enter the following information under **Source DXis**:

  a In the **Source Hostnames or IP Addresses** box, enter the
hostname or IP address of the system that will send the
replicated data to the DXi V-Series.

    To enter multiple sources, press **<Enter>** after each entry. You
can specify up to 10 replication sources.

  b In the **Maximum Snapshots Per Share** drop-down box, select
the number of snapshots to retain for each replicated share (up
to 24).

    During scheduled or manual data replication, the DXi V-Series
receives a snapshot from the source system. A snapshot

contains all of the data necessary to fully recover or failback a NAS share to the point in time when the snapshot was saved.

3 Click **Next** to continue.

Figure 22 Replication Wizard: System
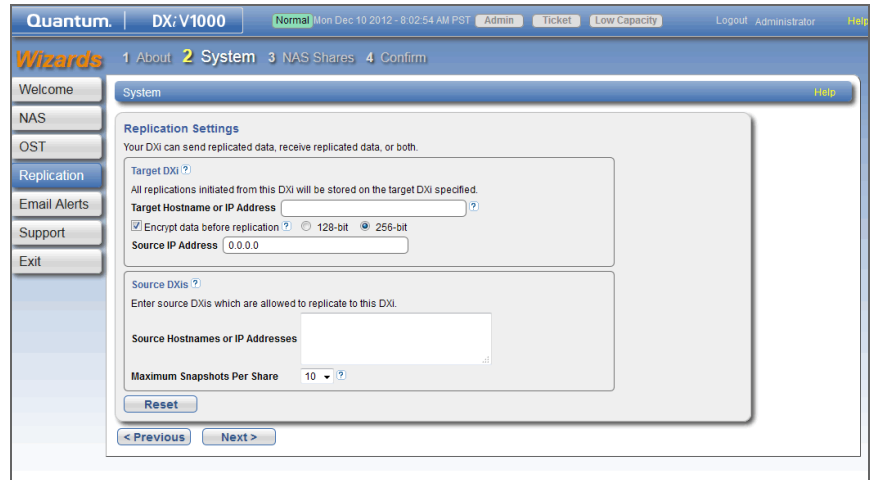
Step 3: NAS Shares

1 Select a NAS share in the **Replication Settings for NAS Shares** section to manage its replication settings (see Figure 23).

> **Note:** For help adding NAS shares to the system, use the **NAS Configuration Wizard** (see NAS Wizard on page 26).

2 To configure the share to replicate its data to another DXi system, enter the following information under **Send**:

a Select the **Enable replication for selected share** check box to enable replication for the share.

b (Optional) Select the **Enable Directory/File based replication to target** check box to enable Directory/File Based Replication for the share, and then enter a **Sync ID** in the box.

With Directory/File Based Replication, a file is automatically replicated when it is closed or a period of time after it is modified. After replication, the replicated files are immediately available on the target system.

The Sync ID is used to identify the target share that will receive replicated data from the source share. The Sync ID *must* be identical to the Sync ID of the target share on the target system.

3 To configure the share to receive replicated data from another DXi system, enter the following information under **Receive**:

a (Optional) Select the **Enable Directory/File based replication to this DXi** check box to enable Directory/File Based Replication for the share, and then enter a **Sync ID** in the box.

The Sync ID is used to identify the source share that will send replicated data to the target share. The Sync ID *must* be identical to the Sync ID of the source share on the source system.

b If you enabled Directory/File Based Replication, select an **Access** option:

- **Locked** - The share is not allowed to receive new Directory/File Based Replication data.

- **Unlocked** - The share is allowed to receive new Directory/File Based Replication data.

Note: You cannot configure a share to both send and receive Directory/File Based Replication data.

4 Click **Apply**.

5 (Optional) To configure additional shares for replication, repeat Steps 1–4.

6 Click **Next** to continue.

Figure 23 Replication Wizard:
NAS Shares
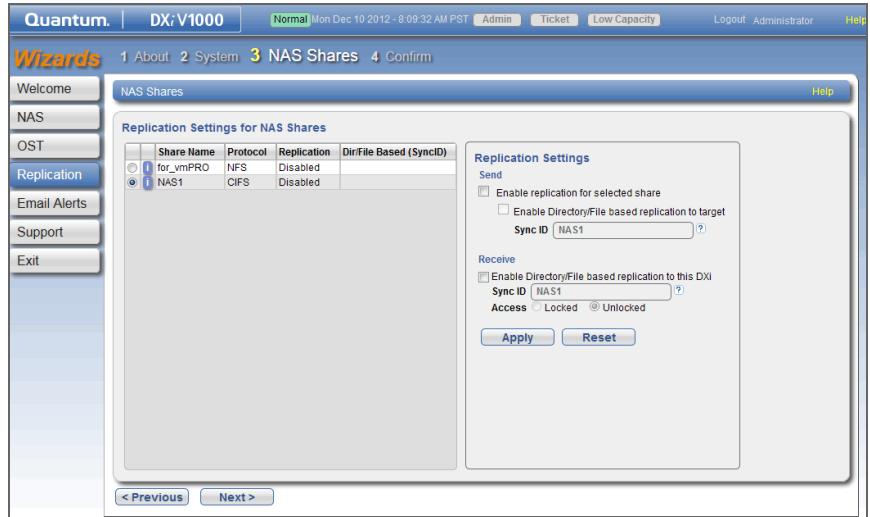
Step 4: Confirm

1 Review the settings you selected to make sure they are correct. If necessary, click **Previous** to return to a previous step to make changes (see Figure 24).

2 After you have confirmed all settings, click **Finish**. The wizard configures the DXi V-Series with the settings you selected.

Figure 24 Replication Wizard:
Confirm
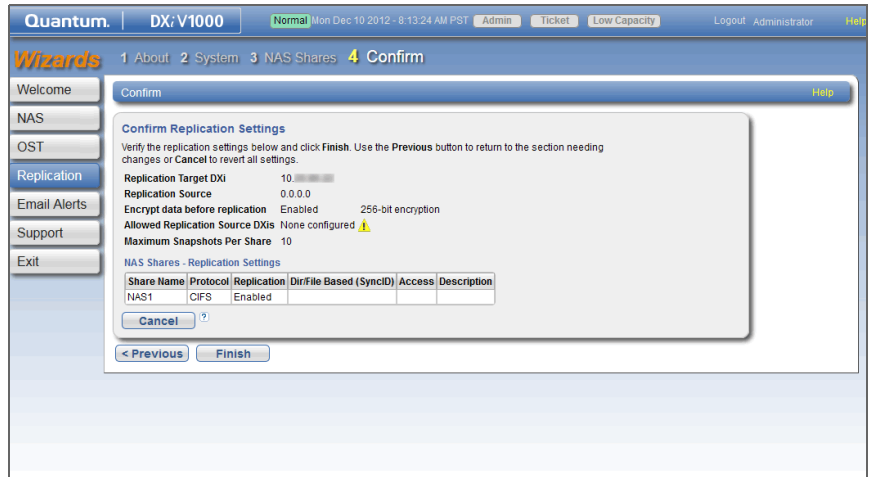
Email Alerts Wizard

The **Email Alerts** wizard provides guided assistance for configuring the DXi V-Series to automatically send notifications and reports to selected recipients. The wizard helps you configure an outgoing e-mail server. Then the wizard guides you through the process of specifying e-mail recipients and selecting the notifications and reports to send to the recipients.

Note: For more information about sending e-mail alerts, see Email on page 221.

To begin the **Email Alerts** wizard, on the **Wizards** menu, click **Email Alerts**.

Step 1: About

1 Read the information about the wizard (see Figure 25).

2 Click **Next** to continue.

Note: At any time while using the wizard, you can click **Previous** to return to the previous step.

Figure 25 Email Alerts Wizard: About
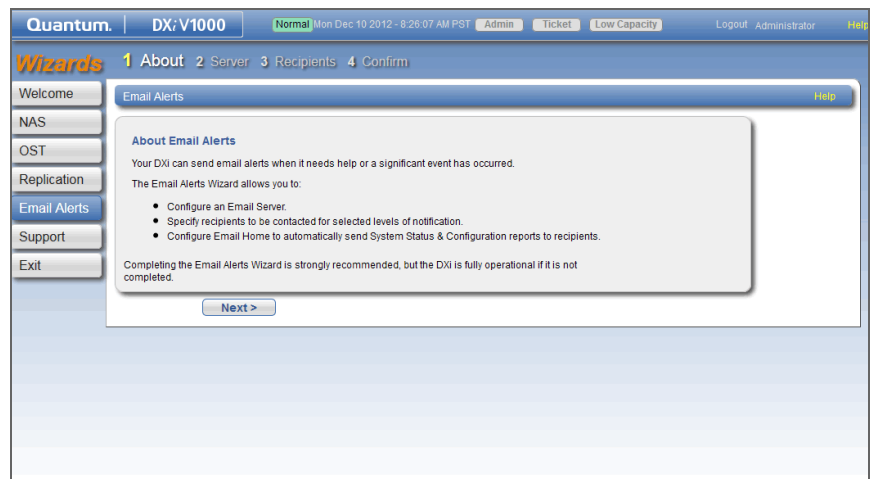
Step 2: Server

1 In the **Hostname or IP Address** box, enter the hostname or IP address of the outgoing e-mail server (see Figure 26).

> **Note:** When entering IP addresses, never use an address that is in a reserved IP address range. To see a list of reserved IP address ranges, click the quick tip icon **[?]** located near the IP address field.

> **Note:** To use hostname format, you must specify at least one DNS IP address on the **Network** page (see Network on page 193).

2 In the **From Email Address** box, enter the return e-mail address displayed in e-mails sent by the DXi V-Series.

Specify a return address that lets you easily identify the system that generated the e-mail (for example, `systemname@any-domain.com`). The return address must contain an @ symbol and a valid domain name, including a period.

3 Click **Next** to continue.

Figure 26 Email Alerts Wizard: Server

Step 3: Recipients

1 Under **Add Email Recipient**, enter information about the recipient (see Figure 27):

   • **Name** - The name of the recipient.

   • **Email Address** - The e-mail address of the recipient.

   • **Notification Type** - Select the types of notifications to send to the recipient:

      • **High** - Send e-mail notifications for High service tickets.

        High service tickets indicate that a critical problem has occurred and needs to be resolved immediately. The operation and performance of the DXi V-Series are degraded, and there is a risk of system failure or data loss.

      • **High and Medium** - Send e-mail notifications for High and Medium service tickets.

        Medium service tickets indicate that a serious problem occurred and needs to be resolved, but it does not necessarily need to be fixed immediately. The operation and performance of the DXi V-Series may be degraded.

      • **All** - Send e-mail notifications for High, Middle, and Low service tickets, as well as any administration alerts.

        Low service tickets indicate that a minor problem occurred and needs to be resolved, but the operation and performance of the DXi V-Series are not significantly affected.

2 Select the **Notification Enabled** check box to enable sending of notifications to the recipient.

3 Click **Add**.

4 (Optional) To add additional recipients, repeat Steps 1–3

5 Click **Next** to continue.

Figure 27 Email Alerts Wizard:
Recipients

Step 4: Confirm

1 Review the settings you selected to make sure they are correct. If necessary, click **Previous** to return to a previous step to make changes (see Figure 28).

2 To make changes to an e-mail recipient you added, first select the recipient and click **Delete** to delete the recipient. Then click **Previous** to return to the previous step and add a new recipient.

3 After you have confirmed all settings, click **Finish**. The wizard configures the DXi V-Series with the settings you selected.

Figure 28 Email Alerts Wizard:
Confirm
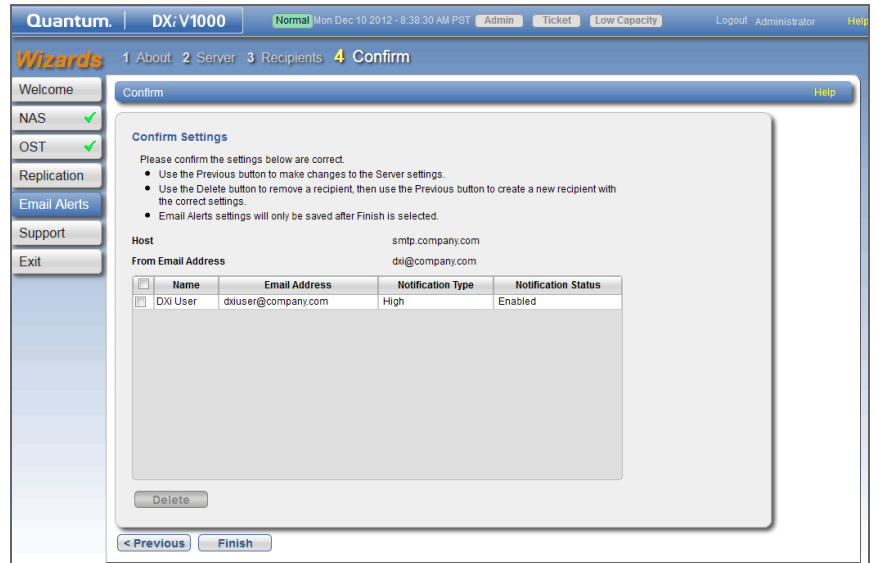
Support Wizard

The **Support** wizard provides guided assistance to help you enable licensed features on the DXi V-Series and register your system with Quantum. The wizard also guides you through other tasks that will aid Quantum customer support in assisting you, such as creating a system log.

To begin the **Support** wizard, on the **Wizards** menu, click **Support**.

Step 1: About

1 Read the information about the wizard (see Figure 29).

2 Click **Next** to continue.

Note: At any time while using the wizard, you can click **Previous** to return to the previous step.

Figure 29 Support Wizard:
About
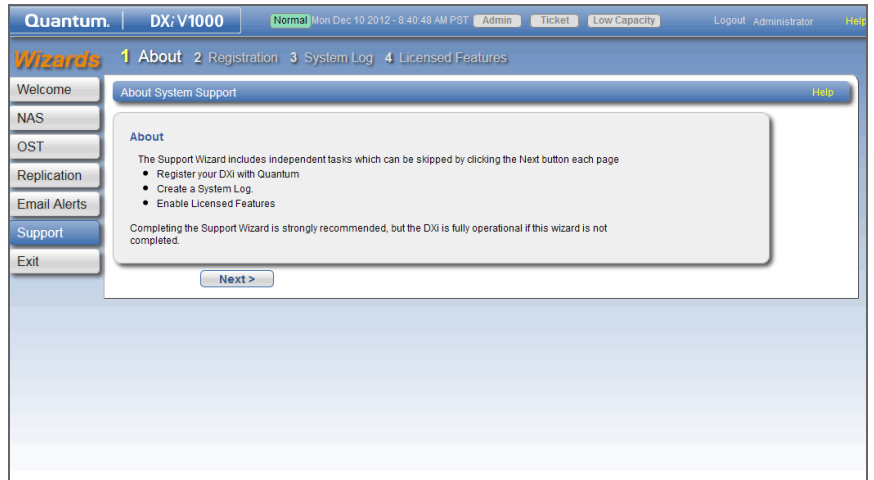
Step 2: Registration

You must register your DXi V-Series to receive service and support from Quantum.

Note: Registration is for Enterprise Edition users only.

1 Click the link for Quantum's Product Registration site (see Figure 30).

2 Follow the onscreen instructions to register your system.

3 When you are finished, switch back to the **Support** wizard.

4 Click **Next** to continue.

Figure 30 Support Wizard:
Registration

Step 3: System Log

This system diagnostics file contains the diagnostic logs for all of the system components. The diagnostic files are helpful when troubleshooting problems on the DXi V-Series. You should generate a system diagnostic file after setting up your DXi V-Series and save it for future reference.

1 Click **Generate New** to generate a new system diagnostics file (see Figure 31).

The system generates a new diagnostics file. This can take several minutes.

2 After the file finishes generating, click the link to enable the **Download Current** button.

3 To download the generated diagnostics file, click **Download Current**.

A dialog box displays asking if you want to open or save the file.

4 Click **Save** or **OK** to download the file.

5 Click **Next** to continue.

Figure 31 Support Wizard:
System Log

**Step 4: Licensed
Features**

Add a license key to enable new functionality on the DXi V-Series, for example, to add capacity or extend a Time-Based license.

Contact your Quantum sales representative to purchase a license. You will receive a License Certificate with instructions for obtaining and installing the license key.

> **Note:** For more information about licensed features, see License Keys on page 260.

There are three methods for adding a license key:

- (Recommended) Automatically Retrieving a License Key

- Uploading a License Key File

- Entering a License Key

Automatically Retrieving a License Key

The DXi V-Series automatically checks the license server each day to make sure the appropriate licenses are installed, based on your product serial number. If you have purchased a license but the DXi V-Series has not yet automatically retrieved the license, you can follow the procedure below to prompt the system to check for the new license and install it.

To automatically retrieve a license key from the license server:

1 On the **License Keys** page, select the **Retrieve License Key from the server** option.

2 Click **Apply**.

The DXi V-Series automatically retrieves and installs the appropriate licenses based on the product serial number.

> **Note:** To automatically retrieve license keys, the DXi V-Series must have access to the Internet. In addition, firewall port 443 (HTTPS) must be open on the network.

3 Click **Finish** to complete the **Support** wizard.

Uploading a License Key File

Use this method to install a license if Internet access via HTTPS (port 443) is not available and you have a **license.crt** file.

To manually upload a license key file:

1 Follow the instructions on the License Certificate you received to obtain the license key file.

2 On the **License Keys** page, select the **Upload License Key** option.

3 Click **Browse** to browse the system and locate the license key file. The license key file must be named **license.crt**.

4 Click **Apply**.

The license key is installed on the system.

5 Click **Finish** to complete the **Support** wizard.

Entering a License Key

Use this method to install a license if Internet access via HTTPS (port 443) is not available and you have a license key.

To manually enter a license key:

1 Follow the instructions on the License Certificate you received to obtain the license key.

2 On the **License Keys** page, select the **License Key** option.

3 Copy the license key and then paste it into the **License Key** box.

4 Click **Apply**.

The license key is installed on the system.

5 Click **Finish** to complete the **Support** wizard.

Figure 32 Support Wizard: Licensed Features
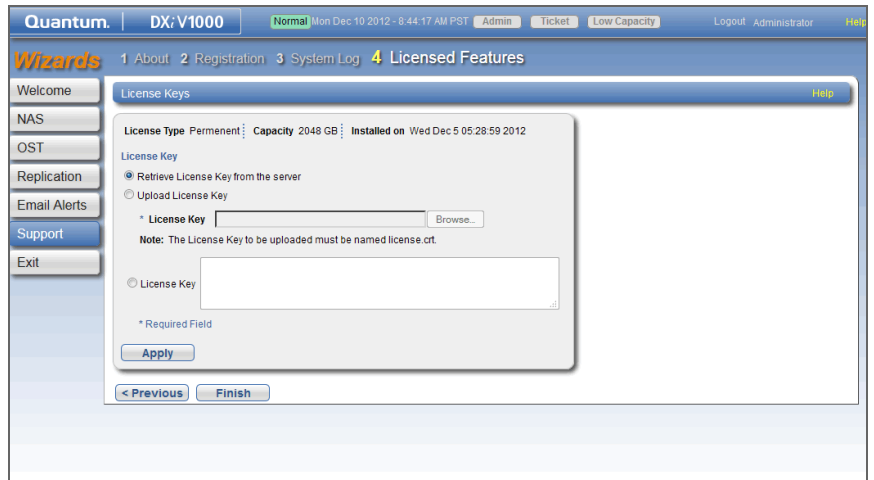
Chapter 4
DXi V-Series Home Page

The first page that displays after you log on to the DXi V-Series remote management console is the **Home** page (see Figure 33). Use the **Home** page to see important performance information at a glance, including disk usage, data reduction statistics, and replication activity.

To return to the **Home** page at any time, click **Home** on the main menu.

The **Home** page contains the following overviews:

- DXi V-Series System Overview
- Disk Usage Overview
- Data Reduction Statistics Overview
- Replication Overview
- Current Activity Overview

Note: Disk usage statistics, data reduction statistics, replication statistics, and current activity are updated every 30 seconds.

Figure 33 Home Page
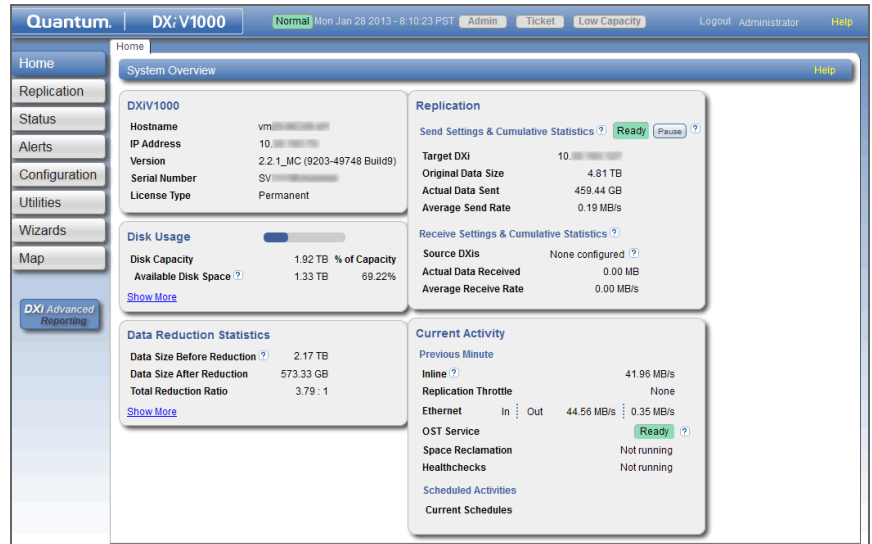
DXi V-Series System Overview

The **DXi V-Series System Overview** on the **Home** page (see Figure 34) displays the following information about the system:

- **Hostname** - The hostname of the DXi V-Series. Click to change the hostname (see Network on page 193).

- **IP Address** - The IP address of the DXi V-Series. Click to change the IP address (see Network on page 193).

- **Version** - The software version installed on the DXi V-Series. (To update the software, see Software Upgrade on page 267.)

- **Serial Number** - The serial number of the DXi V-Series. (You need to know the serial number to add a licensed feature. For more information, see License Keys on page 260.)

- **License Type** - The type of license currently installed on the DXi V-Series (**Permanent**, **Subscription**, or **Time-Based**). (To view or add licenses, see License Keys on page 260).

Figure 34 DXi V-Series System
Overview

Disk Usage Overview

The **Disk Usage** overview on the **Home** page (see Figure 35) displays the following information about disk usage on the system:

Note: Values are displayed as an amount and as a percentage of the total capacity in the system.

Note: Click an item to view detailed statistics for disk usage (see Disk Usage on page 107).

• **Disk Capacity** - The total usable disk capacity of the DXi V-Series.

• **Available Disk Space** - The disk space available for data storage (free space).

On the disk space meter, blue (left side of meter) indicates used disk space and gray (right side of meter) indicates available disk space. The left side of the meter changes color based on the amount of remaining free disk space and the state of the DXi V-Series:

• **I/O Write Low Threshold state (Yellow)** - Free disk space is equal to or less than 50 GB (DXi V1000) or 500 GB (DXi V4000)

• **Stop Write state (Red)** - Free disk space is equal to or less than 10 GB (DXi V1000) or 250 GB (DXi V4000)

• **Stop I/O state (Red)** - Free disk space is equal to or less than 5 GB (DXi V1000) or 10 GB (DXi V4000)

> **Note:** When disk space is low, click the **Quick Warning** icon **[!]** next to the space meter to see more information.

> **Note:** When disk capacity is low, target replication to the system is paused (see Replication Service on page 98). In addition, space reclamation is automatically started to free up disk space (see Space Reclamation on page 256).

> **Note:** For optimal system performance, Quantum recommends keeping the amount of **Available Disk Space** (free space) at 20% or more.

Click **Show More** to display additional information:

- **Free Space** - The disk space that can be used for new deduplicated or non-deduplicated data.

- **Reclaimable Space** - The disk space that can be used for new deduplicated data. If the DXi is configured with non-deduplicated shares, the DXi will automatically compact reclaimable space to create more free space as needed.

- **Used Disk Space** - The disk space that already holds data, including deduplicated data, system metadata, and data not intended for deduplication.

- **Deduplicated Data** - The amount of data that has been deduplicated.

- **Data Not Intended for Deduplication** - The amount of data on shares that do not have deduplication enabled.

- **System Metadata** - The amount of disk space used for internal operations of the DXi, including system configuration files as well as temporary files created during replication, space reclamation, and healthchecks.

> **Note:** Used disk space includes data that is eligible for space reclamation. Because of this, it may appear that your system is using more disk space than you expected. Space is only reclaimed as needed to allow for optimal performance in the event you need to restore your data.

Figure 35 Disk Usage Overview

Disk Usage

		% of Capacity
Disk Capacity	1.92 TB	% of Capacity
Available Disk Space ?	1.32 TB	68.82%
Free Space	1.04 TB	53.95%
Reclaimable Space	286.02 GB	14.87%
Used Disk Space	886.02 GB	46.05%
Deduplicated Data	581.12 GB	30.20%
Data Not Intended For Deduplication	0.00 MB	0.00%
System Metadata	18.88 GB	0.98%

Show Less
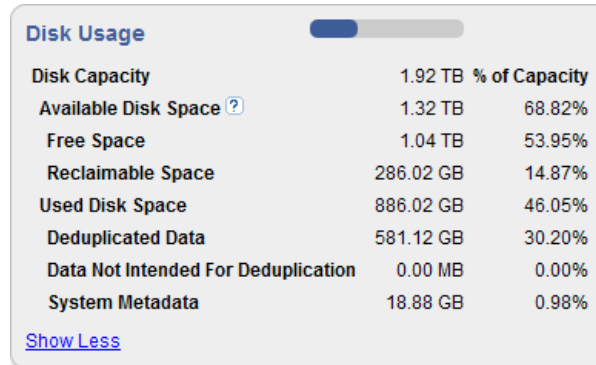
Data Reduction Statistics Overview

The **Data Reduction Statistics** overview on the **Home** page (see Figure 36) displays the following information about the results of data reduction:

> **Note:** Click an item to view detailed statistics for disk usage (see Disk Usage on page 107).

- **Data Size Before Reduction** - The original, native size of all data that has been processed by the data deduplication and compression engines.

- **Data Size After Reduction** - The final, reduced size of all data that has been processed by the data deduplication and compression engines.

- **Total Reduction Ratio** - The total reduction ratio of all data that has been processed by the data deduplication and compression engines (**Data Size Before Reduction** divided by **Data Size After Reduction**).
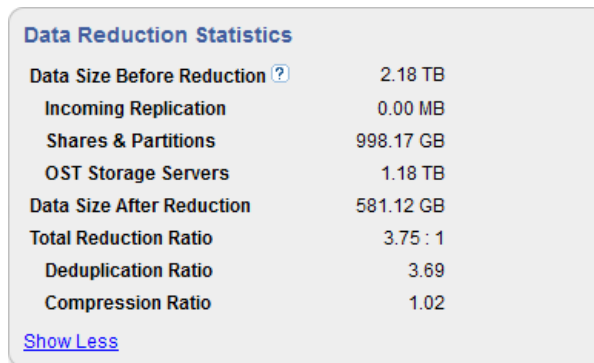
Click **Show More** to display additional information:

- **Incoming Replication** - The amount of data stored on the DXi via replication from another DXi. This does *not* include incoming data

from Directory/File Based Replication, or incoming data from Failback replication.

- **Shares** - The amount of data stored on the DXi via local I/O. This includes incoming data from Directory/File Based Replication, and incoming data from Failback replication.

- **OST Storage Servers** - The amount of data stored in deduplicated OpenStorage (OST) storage servers. This includes incoming data for OST and DXi Accent.

- **Deduplication Ratio** - The deduplication ratio of all data that has been processed by the data deduplication engine.

- **Compression Ratio** - The compression ratio of all data that has been processed by the compression engine.

Figure 36 Data Reduction Statistics Overview

Data Reduction Statistics

Data Size Before Reduction ?	2.18 TB
Incoming Replication	0.00 MB
Shares & Partitions	998.17 GB
OST Storage Servers	1.18 TB
Data Size After Reduction	581.12 GB
Total Reduction Ratio	3.75 : 1
Deduplication Ratio	3.69
Compression Ratio	1.02

Show Less

Replication Overview

The **Replication** overview on the **Home** page (see Figure 37) displays the following information about target and source replication activity:

- **Status** - The replication status of the DXi V-Series.

  - **Ready** - (Green) The system is ready to perform replication.

  - **In Progress** - (Blue) A replication job is currently in progress.

- **Queued** - (Blue) A replication job is queued and will continue when the system is ready.

- **Waiting** - (Blue) A replication job is waiting for another replication job to complete before beginning.

- **Partial** - (Yellow) A replication job was partially completed. Generate a replication report to see the files that were not replicated (see Reports on page 100).

- **Manually Paused** - (Yellow) Replication was manually paused. To resume replication, click **Resume**.

- **System Paused** - (Yellow) The system has automatically paused replication due to a problem, for example, low disk space or a problem on the target system.

  To see more information about the problem that occurred, click **Admin** at the top of the remote management console to view administration alerts (see Admin Alerts on page 115). You may also need to view alerts on the target DXi.

- **Failed** - (Red) A replication job was not completed.

- **Internal Error** - (Red) An error occurred during replication.

- **Pause/Resume** - The source DXi controls the replication pause behavior. To manually pause replication between the source and target, click **Pause** on the source DXi. To manually restart replication, click **Resume** on the source DXi.

  Note: When the target DXi enters low disk space condition, replication on the source DXi is automatically paused. Replication will resume when the target leaves low disk space condition.

- **Send Settings & Cumulative Statistics** - Statistics for all data sent from the system since system installation or since **Send** cumulative replication statistics were last cleared by clicking **Clear Send** on the **Replication Actions** page (see Replication Performance on page 100).

  - **Target DXi** - The hostname or IP address of the target system that the DXi V-Series is configured to replicate data to. Click to specify a replication target (see Replication Send on page 145).

  - **Original Data Size** - The original, native size of data sent during replication or failback. This value does not represent the amount

of data actually sent over the network during replication or failback because data is deduplicated and compressed before being sent.

- **Actual Data Sent** - The amount of data actually sent over the network during replication or failback. This value is usually much less than the **Original Data Size** due to the benefits of data deduplication and compression.

- **Average Send Rate** - The average send rate (in MB/s) of data sent over the network during replication or failback (**Actual Data Sent** divided by the amount of time required to complete replication or failback).

- **Receive Settings & Cumulative Statistics** - Statistics for all data received by the system from all sources since system installation or since **Receive** cumulative replication statistics were last cleared by clicking **Clear Receive** on the **Replication Actions** page (see Replication Performance on page 100).

  - **Source DXis** - The number of source systems configured to replicate data to the DXi V-Series. Click to specify replication sources (see Replication Receive on page 148).

  - **Actual Data Received** - The amount of data actually received over the network during replication or failback. Click to view detailed statistics for replication (see Replication Receive on page 148).

  - **Average Receive Rate** - The average receive rate (in MB/s) of data received over the network during replication or failback (**Actual Data Received** divided by the amount of time required to complete replication or failback). Click to view detailed statistics for replication (see Replication Receive on page 148).

Figure 37 Replication
Overview
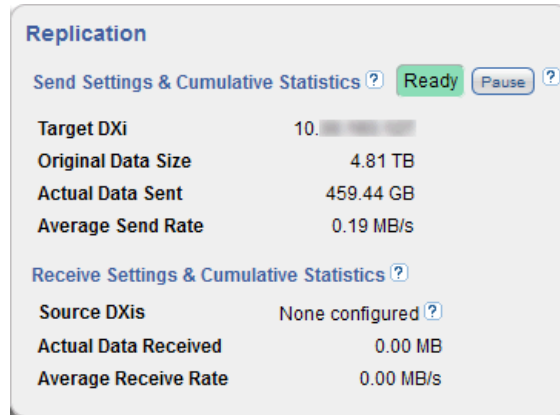
Current Activity Overview

The **Current Activity** overview on the **Home** page (see Figure 38)
displays the following information about system activity that occurred
in the previous minute:

- **Inline** - The inline data flow throughput (in MB/s). Inline data flow
  includes deduplicated and non-deduplicated backup data as well as
  received replication data. Click to view detailed statistics for inline
  performance (see Inline on page 104).

- **Replication Throttle** - The system replication throttle currently in
  effect (in KB/s or MB/s). When a constant throttle is enabled, the DXi
  limits the amount of data it sends during source replication so that
  it does not exceed the specified bandwidth. Click to enable or
  disable system throttling (see Replication Send on page 145).

- **Ethernet** - The amount of data received (**In**) and sent (**Out**) by all
  Ethernet ports (in MB/s). Click to view details statistics for Ethernet
  performance (see Ethernet on page 105).

- **OST Service** - The status of the OST service. OST settings can be
  configured in **Ready**, **Stopped**, or **Verifying** state. The OST server is
  available for backup only in **Ready** state.

- **Space Reclamation** - The status of space reclamation (**Not running** or **Percent complete**). Click to start or stop space reclamation (see Space Reclamation on page 256).

- **Healthchecks** - The status of healthchecks (**Not running** or **Percent complete**). Click to start or stop space healthchecks (see Healthchecks on page 249).

- **Accent** - DXi Accent activity for all DXi Accent enabled media servers.

  Note: DXi Accent activity displays only if DXi Accent is currently enabled or was previously enabled (see DXi Accent on page 179).

  - **Inline (Accent)** - The inline data flow throughput (in MB/s). Inline data flow represents the original, native size of the data protected by the DXi.

  - **Ethernet In (Accent)** - The amount of data received by all Ethernet ports (in MB/s). This amount represents the reduced size of the data protected by the DXi (after deduplication and compression on the media servers).

  - **Accent Bandwidth Reduction** - The percentage by which network bandwidth utilization was reduced by enabling Accent.

To view or modify scheduled system activity, click **Current Schedules** (see Scheduler on page 181).

Note: For more detailed information about all system activity, see DXi V-Series Status on page 103.

Figure 38 Current Activity Overview
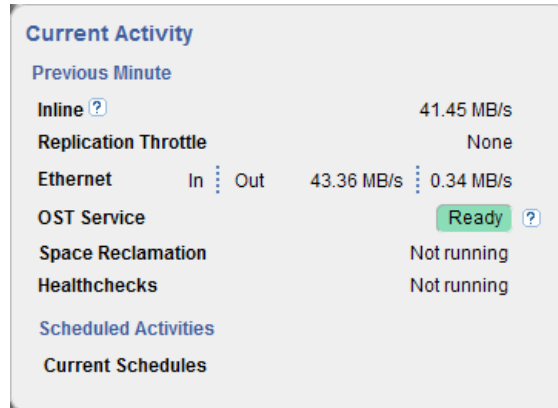
DXi V-Series Replication

The DXi V-Series provides data replication capabilities that you can use as an integral part of a disaster recovery plan. Replication allows you to configure the DXi V-Series to create a copy of your data on another DXi system at scheduled intervals (or manually as needed).

In the event of a disaster in which the original data is lost, you can quickly recover the replicated data on the remote system, allowing your business to resume normal operations. Once the original system is available again, you can restore all data back to its original location.

> **Note:** Quantum recommends that you configure and start replication before storing large amounts of data on the DXi V-Series.

> **Note:** A DXi V-Series can replicate data to, or receive replicated data from, a DXi system running DXi 2.x software. Replication to or from a DXi system running version 1.x software is not supported.

See the following sections for more information about the data replication capabilities of the DXi V-Series:

- Understanding Data Replication
- Performing Data Replication

> **Note:** To schedule replication for a share, use the **Configuration > Scheduler** page (see Scheduling a Share for Replication on page 186). To limit the amount of network bandwidth used for replication, enable a constant throttle (see Replication Send on page 145), or schedule replication throttling (see Scheduling Replication Throttling on page 187).

Understanding Data Replication

During data replication, data is sent from one system (the source) to another system, usually in another location (the target). For example, you might replicate data from a branch office (the source) to a central office (the target).

Sources *send* replicated data, and targets *receive* replicated data. A target system can receive data from 1 source (DXi V1000) or up to 10 sources (DXi V4000). A source system can send data to one target.

Replication works only with deduplicated data, and data is compressed before it is replicated. Because of this, the amount of data transmitted between systems during replication is greatly reduced compared to the original amount of data stored. In addition, a data block is transmitted only if the target does not already have a copy of the block. Finally, data can optionally be encrypted before it is transmitted.

The DXi V-Series can perform the following types of replication:

- Replication
- Directory/File Based Replication
- OST Optimized Duplication

Replication

Replication occurs when replication is enabled for a deduplicated NAS share and a replication schedule is configured (or manual replication is performed on a regular basis). For replication to occur, the source system must be configured to point to the target system. Similarly, the target system must be configured to accept data from the source system.

To optimize the replication process, deduplicated data is continuously sent in the background from the source system to the target system. However, a snapshot that preserves the file structure of your data is sent to the target system only when a scheduled or manual replication job occurs. A snapshot contains all of the information that is necessary to recreate a share just as it was at the point in time when the snapshot was created.

Caution: A saved snapshot is necessary to recover your data at a later time. For this reason, it is not enough to simply enable replication for a share. You must also configure a replication schedule (recommended) or perform manual replication on a regular basis to send snapshots of the share to the target system.

If the source system ever becomes unavailable, you can recover the share on the target system using a saved snapshot. After you recover a share, it is recreated on the target system and is available for use. Once the source system becomes available again, you can perform a failback operation to restore the share to its original location.

Directory/File Based Replication

Like replication, Directory/File Based Replication sends data from a NAS share to another system where it can be accessed. However, Directory/File Based Replication differs in a number of important ways:

- Both replication and Directory/File Based Replication must be enabled for the share.

- A unique Sync ID is used to associate the replicated share on the source system with the share that will receive the replicated data on the target system.

- You do not need to schedule or manually perform Directory/File Based Replication through the remote management console. Instead, replication is triggered when a file is closed or a period of time after it is modified (NAS shares).

  Note: For CIFS shares, a file is replicated immediately after it is closed. For NFS shares, a file is replicated after it has been idle (not accessed) for several minutes.

> **Note:** To optimize the replication process, deduplicated data is
> continuously sent in the background from the source
> system to the target system. Any remaining data is sent
> (along with metadata) at the time a file is closed.

- After directories and files are replicated using Directory/File Based
  Replication, they are automatically recovered on the target system
  and are immediately available for use. There is no need to first
  recover the share to access its data.

- Deletions are automatically propagated from the source system to
  the target system in order to free up space on the target. In
  addition, you can manually initiate a synchronization from the
  source system at any time. Synchronizing ensures that the contents
  of the source share are exactly the same as the target share.

> **Note:** If you delete a share configured for Directory/File Based
> Replication on the source DXi, the share is *not* automatically
> deleted on the target DXi. If you do not want to retain the
> share on the target DXi, you can manually delete it.

OST Optimized Duplication

The DXi V-Series can duplicate the data on an LSU (logical storage unit)
to another location using the OST optimized duplication (OST
replication) feature supported by Symantec NetBackup and Backup
Exec. If you are using Symantec NetBackup 7.1 or higher, you can
configure an LSU for Automatic Image Replication.

For information about configuring and using OST optimized duplication
and Automatic Image Replication, see Replicating OST Data on
page 152.

Performing Data Replication

The **Replication** page allows you to set up replication for NAS shares
and to replicate and recover data.

To access the **Replication** page, click the **Replication** menu.

The **Replication** page contains the following tabs:

- Send NAS

- Receive NAS

- Actions

- Reports

Use the DXi V-Series data replication features to perform the following tasks:

- Replicate all data on a share to another system where it can be recovered at a later time (see Task Overview: Setting Up and Performing Replication on page 73).

- Automatically replicate directories and files to another system where they are immediately available (see Task Overview: Setting Up and Performing Directory/File Based Replication on page 74).

- Recover data from a lost or damaged share (see Task Overview: Recovering a Replicated Share on page 75).

- Restore a lost or damaged share back to its original location (see Task Overview: Performing a Share Failback on page 76).

Note: The **Replication** wizard provides guided assistance for configuring data replication (see DXi V-Series Configuration Wizards on page 25).

Task Overview: Setting Up and Performing Replication

To replicate all data on a NAS share from a source system to a target system:

1 On the target system, add the source system to the list of allowed replication sources (see Replication Receive on page 148).

2 On the source system, specify the target system that will receive replicated data (see Replication Send on page 145).

3 On the source system, create a new share with deduplication enabled (see Adding a NAS Share on page 130).

4 Enable replication for the new share (see Enabling Replication For a Share on page 80).

5 Before writing any data to the new share, replicate the new share (see Replicating a Share on page 83).

Quantum recommends that you always replicate a new share immediately after creating it. This establishes the initial data structure on the target system and greatly increases the speed of the first replication.

6 Choose one of the following methods to regularly replicate the new share:

- (Recommended) Use the **Scheduler** page to set up a schedule for performing replication automatically after backups complete (see Scheduling a Share for Replication on page 186).

- Manually perform replication at frequent intervals (see Replicating a Share on page 83).

After replication, a snapshot is sent to the target system. You can use the snapshot to recover the replicated share on the target system (see Task Overview: Recovering a Replicated Share on page 75) or restore the share to its original location on the source system (see Task Overview: Performing a Share Failback on page 76).

Caution: If you do not configure a replication schedule or manually replicate the share on a regular basis, your data is *not* protected. While the DXi V-Series continually sends data to the target system in the background to optimize the replication process, a snapshot that preserves the complete structure of your data is sent to the target system *only* when a scheduled or manual replication job occurs. If you do not regularly and frequently replicate your data as described in Step 6 above, it cannot be restored at a later time.

Note: To limit the amount of network bandwidth used for replication, enable a constant throttle (see Replication Send on page 145), or schedule replication throttling (see Scheduling Replication Throttling on page 187).

Task Overview: Setting Up and Performing Directory/File Based Replication

To automatically replicate directories and files from a source system and immediately recover them for use on a target system:

1 Perform the following steps on the target system:

    a Add the source system to the list of allowed replication sources (see Replication Receive on page 148).

    b Create a new share with deduplication enabled (see Adding a NAS Share on page 130).

    c Enable Directory/File Based Replication for the new share and specify the Sync ID (see Configuring a Target Share for Directory/File Based Replication on page 95).

2 Perform the following steps on the source system:

    a Specify the target system that will receive replicated data (see Replication Send on page 145).

    b Create a new share with deduplication enabled (see Adding a NAS Share on page 130).

    c Enable Directory/File Based Replication for the new share and specify the Sync ID (see Configuring a Source Share for Directory/File Based Replication on page 81).

A file is automatically replicated when it is closed or a period of time after it is modified. After replication, the replicated directories and files are immediately available on the target system. There is no need to recover the share to make the directories and files available.

Note: To limit the amount of network bandwidth used for replication, enable a constant throttle (see Replication Send on page 145), or schedule replication throttling (see Scheduling Replication Throttling on page 187).

Task Overview: Recovering a Replicated Share

If a NAS share is lost or damaged on the source system, you can recover it on the target system using a received snapshot. When you recover a share, it is recreated on the target system just as it was at the point in time when the snapshot was saved.

To recover a replicated share:

1 On the target system, select a received snapshot and perform a recover operation (see Recovering a Share on page 87).

    The share is now available on the target system.

2 (Optional) Map your backup application to the recovered share on the target system to continue making backups.

3 When the source system is operating correctly again, choose one of the following actions:

- Failback the share to restore it on the original source system (see Task Overview: Performing a Share Failback on page 76). Then, if necessary, map your backup application to the restored share on the original source system.

- Continue to make backups to the recovered share on the original target system. In addition, set up replication to replicate the share back to the original source system (see Task Overview: Setting Up and Performing Replication on page 73). In this scenario, the original source system is now the target, and the original target system is now the source.

Task Overview: Performing a Share Failback

If a NAS share is lost or damaged on the source system, you can failback the share to the source system using a received snapshot on the target system. When you failback a share, it is restored on the source system just as it was at the point in time when the snapshot was saved.

To perform a share failback:

1 On the original source system, add the original target system to the list of allowed replication sources (see Replication Receive on page 148).

> **Note:** For the purposes of failback, the original source system is now acting as a target because it will receive the snapshot from the original target system.

2 On the original target system, select a received snapshot and perform a failback operation pointing to the original source system, and then recover the share on the original source system (see Performing a Failback For a Share on page 89).

The share is now available on the original source system.

3 (Optional) If necessary, map your backup application to the restored share on the original source system.

Send NAS

The **Send NAS** page allows you to manage outgoing replication activity for NAS shares. You can replicate shares on the DXi V-Series (the source) to another DXi system that supports NAS (the target).

Note: Before you can replicate shares, you must specify the replication target (see Replication Send on page 145).

To access the **Send NAS** page, click the **Replication** menu, and then click the **Send > NAS** tab (see Figure 39).

Figure 39 Send NAS Page
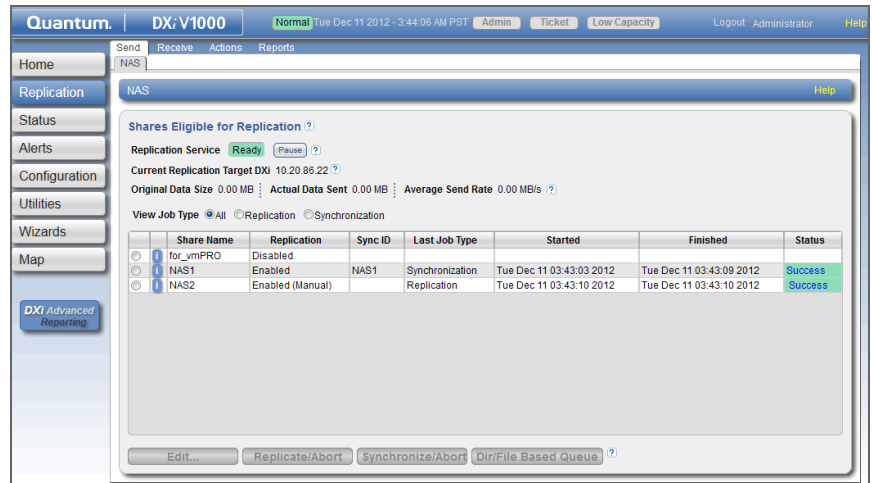
Use the **Send NAS** page to perform the following tasks:

- View replication information for shares (see Shares Eligible for Replication on page 78).

- Enable or disable replication for a share (see Enabling Replication For a Share on page 80).

- Configure Directory/File Based Replication for a share (see Configuring a Source Share for Directory/File Based Replication on page 81).

- Initiate replication for a share (see Replicating a Share on page 83).

- Synchronize a share configured for Directory/File Based Replication (see Synchronizing a Share on page 83).

- View replication statistics for a share configured for Directory/File Based Replication (see Directory/File Based Queue on page 84).

Shares Eligible for Replication

The **Shares Eligible for Replication** section displays replication statistics for all NAS shares on the DXi V-Series that are eligible for replication. To be eligible for replication, a share must have data deduplication enabled at the time it is created.

Note: For information about creating NAS shares, see Adding a NAS Share on page 130.

The **Shares Eligible for Replication** section displays the following information:

- **Replication Service** - The replication status of the DXi V-Series. Click **Pause** to pause replication activity. Click **Resume** to resume replication activity.

   Note: For a detailed description of all possible replication statuses, see Replication Overview on page 62.

- **Current Replication Target DXi** - The hostname or IP address of the target system that the DXi V-Series is configured to replicate data to. (To change the target system, see Replication Send on page 145.)

- **Cumulative Statistics** - Statistics for all data sent from the system since system installation or since cumulative replication statistics were last cleared. (To clear cumulative replication statistics, see Replication Performance on page 100.)

   - **Original Data Size** - The original, native size of data sent during replication or failback. This value does not represent the amount of data actually sent over the network during replication or failback because data is deduplicated and compressed before being sent.

   - **Actual Data Sent** - The amount of data actually sent over the network during replication or failback. This value is usually much less than the **Original Data Size** due to the benefits of data deduplication and compression.

- **Average Send Rate** - The average send rate (in MB/s) of data sent over the network during replication or failback (**Actual Data Sent** divided by the amount of time required to complete replication or failback).

- **View Job Type** - Select an option to filter the list of NAS shares:

  - **All** - Displays all shares.

  - **Replication** - Displays shares with replication jobs.

  - **Synchronization** - Displays shares with synchronization jobs.

- **Share Name** - The name of the share.

- **Replication** - The replication state (**Enabled** or **Disabled**).

  The **Scheduled** link displays if replication is scheduled for the share. Click the link to view or modify the schedule (see Scheduling a Share for Replication on page 186).

- **Sync ID** - The Sync ID of the share if Directory/File Based Replication is enabled.

- **Last Job Type** - The type of the most recent replication job (**Replication** or **Synchronization**).

- **Started** - The time the most recent replication job was started.

- **Finished** - The time the most recent replication job finished.

- **Status** - The status of the most recent replication job (see Replication and Synchronization Status on page 79). Click the status to display detailed information about the most recent replication job.

Note: Click a column heading to sort the rows in the table by that column. Click the column heading again to reverse the sort order.

Note: Click the **Information** button **[i]** next to a share to display detailed information about the share and recent replication activity.

Replication and Synchronization Status

A replication job can have one of the following statuses:

- **In Progress** - The replication job is in progress.

- **Partial** - The replication job was partially completed. Generate a replication report to see the files that were not replicated (see Reports on page 100).

- **Queued** - The replication job is queued and will continue when the system is ready.

- **Waiting** - The replication job is waiting for another job to complete before beginning.

- **Success** - The replication job was completed successfully.

- **Failed** - The replication job was not completed.

A synchronization job can have one of the following statuses:

- **Queued** - The synchronization job is queued and will continue when the system is ready.

- **Success** - The synchronization job was completed successfully.

- **Recovering** - The recover operation is in process.

- **Replicating** - The replication operation is in process.

- **Failed** - The synchronization job was not completed.

Enabling Replication For a Share

Enable replication for a NAS share to allow the share's data to be replicated to another DXi system (the target). Disable replication if you do not want to replicate the share's data to another DXi system.

> **Note:** To be eligible for replication, a share must have data deduplication enabled at the time it is created.

To enable or disable replication for a share:

1 Select the share and click **Edit**.

The **Edit NAS Share** page displays (see Figure 40).

Figure 40 Edit NAS Share Page
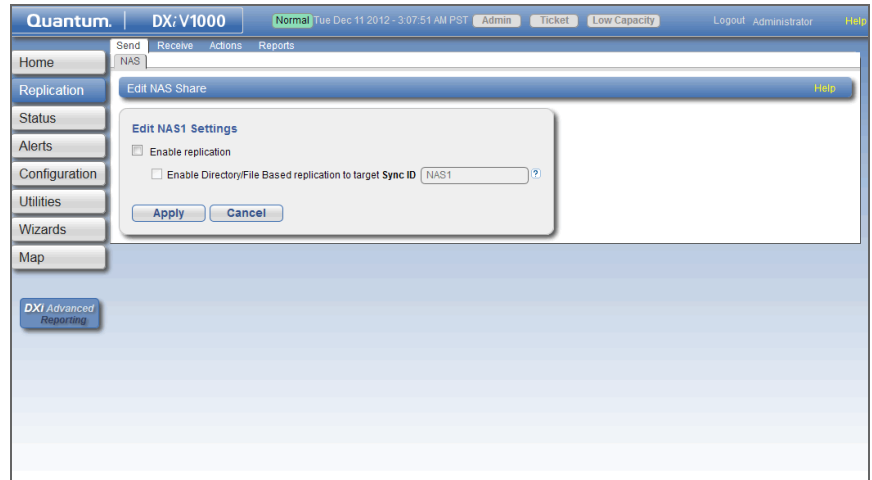
2 Select the **Enable replication** check box to enable replication for the share.

Or clear the **Enable replication** check box to disable replication for the share.

3 Click **Apply**.

Note: Quantum recommends scheduling replication to run after backups are complete (see Scheduling a Share for Replication on page 186). If you do not enable scheduled replication, replication will only occur if you manually replicate a share (see Replicating a Share on page 83) or if you configure Directory/File Based Replication (see Configuring a Source Share for Directory/File Based Replication on page 81).

Note: Disabling replication for a share does not delete any scheduled replication events for that share. If you no longer want to schedule the share for replication, manually delete the schedule (see Deleting a Scheduled Event on page 191).

Configuring a Source Share for Directory/File Based Replication

Configure a NAS share for Directory/File Based Replication to automatically replicate files to a target system. A file is automatically replicated when it is closed or a period of time after it is modified. After

replication, the replicated files are immediately available on the target system. There is no need to recover the share to make the files available. Disable Directory/File Based Replication if you do not want to automatically replicate files.

When you configure a share for Directory/File Based Replication, you specify a Sync ID for the share. The Sync ID associates the share on the source system with the share on the target system that will received the replicated data. As long as you specify a matching Sync ID for both the source and target shares, the shares do not have to have the identical names. However, if you do not specify a Sync ID, the source and target shares must have identical names. Quantum recommends that you assign a matching Sync ID to the source and target shares.

> **Note:** For information about specifying the Sync ID on the target share, see Configuring a Target Share for Directory/File Based Replication on page 95.

To configure a share for Directory/File Based Replication:

1   Select the share and click **Edit**.

    The **Edit NAS Share** page displays (see Figure 40).

2   If it is not already selected, select the **Enable replication** check box to enable replication for the share.

3   Select the **Enable Directory/File Based replication to target Sync ID** check box to enable Directory/File Based Replication for the share.

    Or clear the **Enable Directory/File Based replication to target Sync ID** check box to disable Directory/File Based Replication for the share.

4   Enter a **Sync ID** in the box.

    The Sync ID is used to identify the target share that will receive replicated data from the source share. The Sync ID *must* be identical to the Sync ID of the target share on the target system.

5   Click **Apply**.

> **Note:** After you configure a share for Directory/File Based Replication, you should periodically synchronize it to keep it in sync with the target share (see Synchronizing a Share on page 83).

Replicating a Share

Replicate a NAS share to send a snapshot of the share to the target system. A snapshot is required to recover the data on the share at a later time. If you have not configured a replication schedule for a share, replication only occurs when you manually initiate it (see Scheduling a Share for Replication on page 186).

Note: During replication, files that are in use on a share are skipped.

To replicate a share, select the share and click **Replicate Now**. The status of the replication job displays in the **Status** column.

To cancel the replication job, select the share and click **Abort Replication**.

Synchronizing a Share

Synchronize a NAS share to synchronize the contents of the share with the corresponding share on the target system. To synchronize a share, it must be configured for Directory/File Based Replication (see Configuring a Source Share for Directory/File Based Replication on page 81).

Synchronizing a share ensures that the contents of the source share are the same as the target share. The synchronization verifies that the same files exist in both locations, and that no additional files exist in either location.

You should perform a synchronization in any of the following situations:

- When Directory/Filed Based Replication is first enabled for a share.

- If a Directory/File Based Replication job fails.

- If Directory/File Based Replication is disabled for a time and then is re-enabled.

Note: Even when replication is paused, the system continues to queue Directory/Filed Based Replication operations. Each time an operation is queued, the system logs an administration alert that reports the total number of queued Directory/Filed Based Replication requests.

Note: If a synchronization fails, make sure the target share is unlocked (see Configuring a Target Share for Directory/File Based Replication on page 95).

To synchronize a share, select the share and click **Synchronize Now**. The status of the synchronization job displays in the **Status** column.

To cancel the synchronization job, select the share and click **Abort Sync**.

Directory/File Based Queue

The Directory/File Based Queue displays replication statistics for shares that are configured for Directory/File Based Replication (see Configuring a Source Share for Directory/File Based Replication on page 81).

To view the Directory/File Based Queue:

1 Select a share that is configured for Directory/File Based Replication.

2 Click **Dir/File Based Queue**.

The Directory/File Based Queue displays (see Figure 41).

Figure 41 Directory/File Based Queue
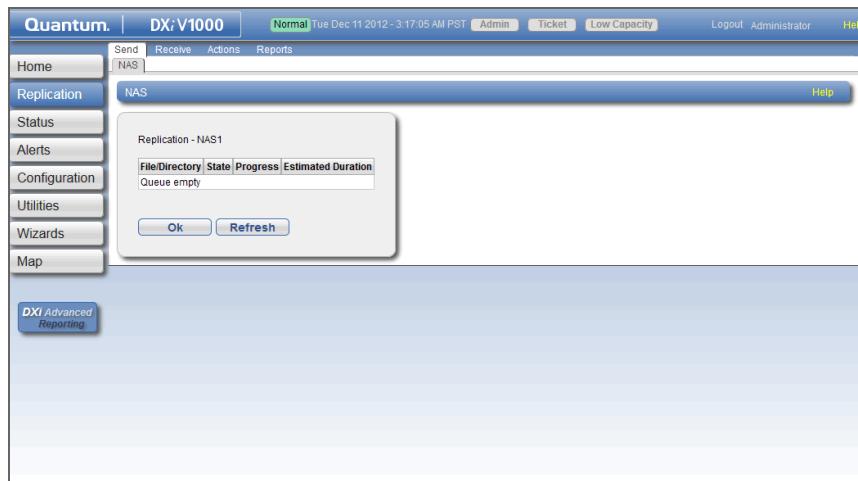
The Directory/File Based Queue displays the following information for the share:

- **File/Directory** - The file or directory to be replicated.

- **State** - The replication state for the file or directory.

- **Progress** - The percentage complete for replication of the file or directory.

- **Estimated Duration** - The estimated time it will take to complete replication for the file or directory.

> **Note:** The estimated duration may display as **unknown** if replication has been very recently initiated. After the system has enough information to calculate a value, the estimated duration will display.

To update the statistics with the latest information, click **Refresh**.

> **Note:** The contents of the Directory/File Based Queue are dynamic. Because of this, statistics are subject to change if items are added to the queue.

3 To return to the **Send NAS** page, click **OK**.

Receive NAS

The **Receive NAS** page allows you to manage incoming replication activity for NAS shares. You can recover a replicated share on the target system if the source system is unavailable. Once the source system becomes available, you can failback the share to make it available on the source system again.

> **Note:** Before you can receive replicated shares, you must specify one or more replication sources (see Replication Receive on page 148).

To access the **Receive NAS** page, click the **Replication** menu, and then click the **Receive > NAS** tab.

Use the **Receive NAS** page to perform the following tasks:

- View received snapshots and recover, failback, or delete snapshots (see Received Snapshots on page 86).

- Manage recovery jobs (see Recovery Jobs on page 92).

- Manage failback jobs (see Failback Jobs on page 93).

- Manage shares configured for Directory/File Based Replication (see Directory/File Based on page 94).

Received Snapshots

The **Received Snapshots** page allows you to view and work with received snapshots. When a replicated NAS share is received from a source system, it is saved as a snapshot. The snapshot contains all of the data necessary to fully recover or failback the share to the point in time when the snapshot was saved.

To access the **Received Snapshots** page, on the **Receive NAS** page, click the **Received Snapshots** tab (see Figure 42).

Figure 42 Received Snapshots Page
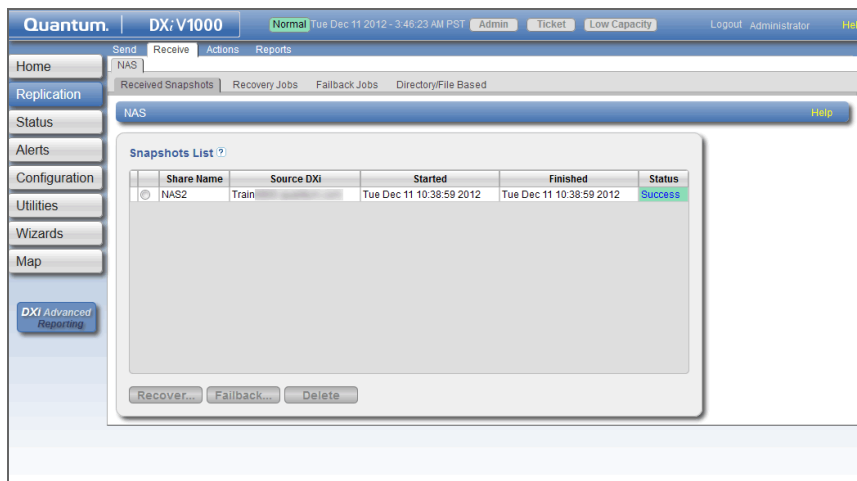
Use the **Received Snapshots** page to perform the following tasks:

- View information about received snapshots (see Snapshots List on page 87).

- Recover a share on the target system (see Recovering a Share on page 87).

- Failback a share to the source system (see Performing a Failback For a Share on page 89).

- Delete a received snapshot (see Deleting a Snapshot on page 91).

> **Note:** The target system will retain up to 10 replication snapshots (default setting) for each replicated share. Once 10 snapshots have been saved, the oldest snapshot is deleted to make room for each new snapshot that is received. (To change the maximum number of snapshots retained for each share, see Replication Receive on page 148).

Snapshots List

The **Snapshots List** displays all available snapshots that have been received from configured replication sources. Snapshots are grouped by NAS share. To see all available snapshots for a share, click the plus icon **[+]** next to the share name.

The **Snapshots List** displays the following information about each snapshot:

- **Share Name** - The name of the share.
- **Source DXi** - The hostname of the system that the snapshot was sent from.
- **Started** - The time the most recent replication job was started.
- **Finished** - The time the most recent replication job finished.
- **Status** - The status of the most recent replication job (see Replication and Synchronization Status on page 79). Click the status to display detailed information about the most recent replication job.

> **Note:** Click a column heading to sort the rows in the table by that column. Click the column heading again to reverse the sort order.

Recovering a Share

Recover a NAS share if the source system is unavailable and you need to access the share (for example, to continue performing backups). When you recover a share, you select a received snapshot. The DXi V-Series uses the snapshot to recreate the share on the target system just as it was at the point in time when the snapshot was saved.

Note: Before recovering a share, you must enable CIFS on the DXi (see
Windows Domain on page 135). Also, if the DXi is not using
Active Directory, you must configure at least one workgroup
user to own recovered CIFS shares (see Share Access on
page 138).

To recover a share:

1 On the target system, select a snapshot in the **Snapshots List** and
click **Recover**.

The **Recovered Share Name** page displays (see Figure 43).

Figure 43 Recovered Share
Name Page
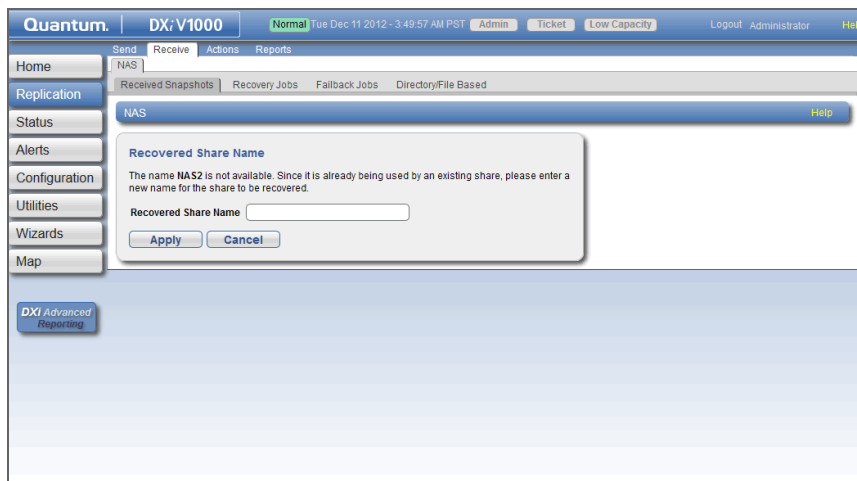
2 (Optional) In the **Recovered Share Name** box, type a new name for
the recovered share. (The default name is the original share name.)

3 Click **Apply**.

4 If the DXi is joined to a Windows workgroup, select the workgroup
user that will own the recovered share, and then click **Apply**.

The share is recovered on the target system. All data stored on the share
at the time the snapshot was saved is available. The original export
protocol of the share (NFS or CIFS) is retained in the recovery process.

> **Note:** After you recover a share, if you want to continue backing up data to the share, you must remap your backup application to point to the target system instead of the source system.

Performing a Failback For a Share

Perform a failback of a NAS share if a source system that was previously unavailable becomes available again. When you failback a share, you select a received snapshot. The DXi V-Series copies the snapshot from the target system back to the source system. You can then perform a recover operation to recreate the share on the source system just as it was at the point in time when the snapshot was saved.

> **Note:** Before you can failback a share, on the original source system, you must add the original target system to the list of allowed replication sources (see Replication Receive on page 148). This is because, during failback, the original target is acting as a source when it sends a snapshot to the original source.

To perform a share failback:

1 On the target system, select a snapshot in the **Snapshots List** and click **Failback**.

The **Failback Target** page displays (see Figure 44).

Figure 44 Failback Target Page
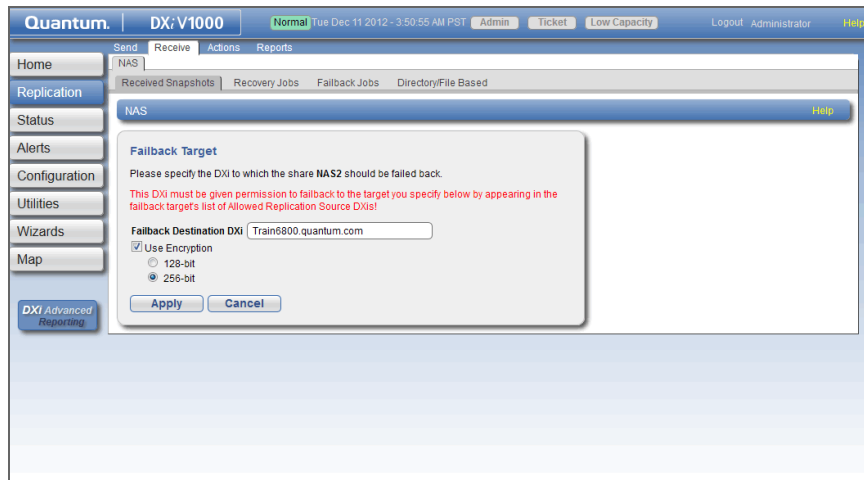
2 (Optional) In the **Failback Destination DXi** box, type the hostname or IP address of a new destination system to failback the share to. (The default destination is the original source system.)

Note: To use hostname format, you must specify at least one DNS IP address on the **Network** page (see Network on page 193).

---

3 (Optional) Leave the **Use Encryption** check box selected to enable encryption when sending the snapshot to the destination. Or clear the **Use Encryption** check box to disable encryption when sending the snapshot to the destination.

If encryption is enabled, select an encryption strength (**128-bit** or **256-bit**). Using 256-bit encryption (default) provides a stronger level of security but may have an impact on system performance in some situations.

Note: Encryption is enabled by default. However, for best performance, if your data network is already secured, you should clear the **Use Encryption** check box.

---

4 Click **Apply**.

The snapshot is sent to the source system.

5 On the source system, in the **Snapshots List**, select the snapshot that was sent during the failback operation and click **Recover**.

The **Recovered Share Name** page displays (see <u>Figure 43</u>).

6 (Optional) In the **Recovered Share Name** box, type a new name for the recovered share. (The default name is the original share name.)

7 Click **Apply**.

The share is recovered on the source system. All data stored on the share at the time the snapshot was saved is available. The original export protocol of the share (NFS or CIFS) is retained in the recovery process.

Note: If you previously remapped your backup application to a recovered share on the target system, after you failback the share, you must remap your backup application again to point to the source system.

Deleting a Snapshot

Delete a snapshot if it is no longer needed. After you delete a snapshot, it can no longer be used to recover or failback a NAS share.

Note: You cannot delete a snapshot if a failback operation is in progress for the snapshot. Wait for the failback operation to complete, or abort the operation (see <u>Failback Jobs</u> on page 93).

To delete a snapshot:

1 Do one of the following actions:

- On the source system, disable replication for the share associated with the snapshot (see <u>Enabling Replication For a Share</u> on page 80).

- On the target system, delete the source system associated with the snapshot from the list of allowed replication sources (see <u>Replication Receive</u> on page 148).

2 On the target system, select a snapshot in the **Snapshots List** and click **Delete**.

Note: You cannot delete a snapshot if it is the last received snapshot for a share.

---

3 Click **Yes** to confirm the action.

Recovery Jobs

The **Recovery Jobs** page allows you to view information about snapshot recover operations that were previously completed.

To access the **Recovery Jobs** page, on the **Receive NAS** page, click the **Recovery Jobs** tab (see Figure 45).

Figure 45 Recovery Jobs Page
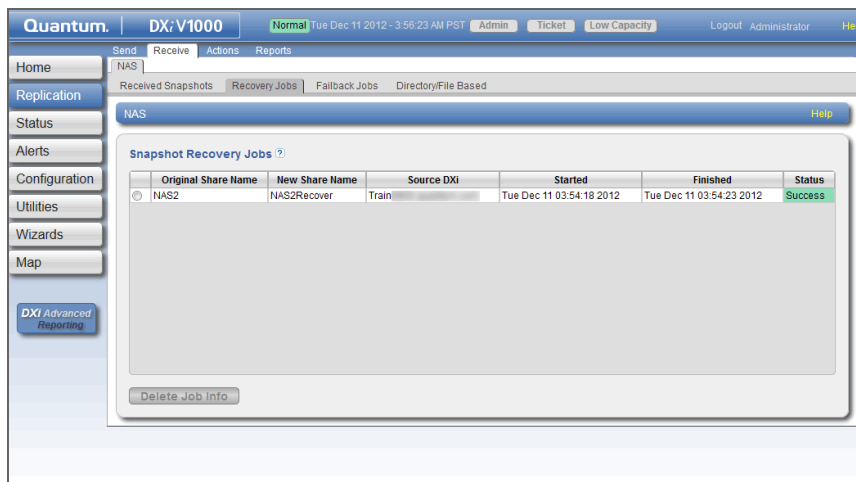
The **Snapshot Recovery Jobs** section displays the following information about recovery jobs:

- **Original Share Name** - The name of the share the snapshot was created from.

- **New Share Name** - The name of the share the snapshot was recovered to.

- **Source DXi** - The hostname of the system that the snapshot was received from.

- **Started** - The time the recovery job was started.

- **Finished** - The time the recovery job finished.

- **Status** - The status of the recovery job (**Success**, **In Progress**, or **Failed**).

To delete information for a recovery job, select it in the **Snapshot Recovery Jobs** list and click **Delete Job Info**.

Failback Jobs

The **Failback Jobs** page allows you to view information about snapshot failback operations that were previously completed. You can also abort a failback that is currently in progress.

To access the **Failback Jobs** page, on the **Receive NAS** page, click the **Failback Jobs** tab (see Figure 46).

Figure 46 Failback Jobs Page
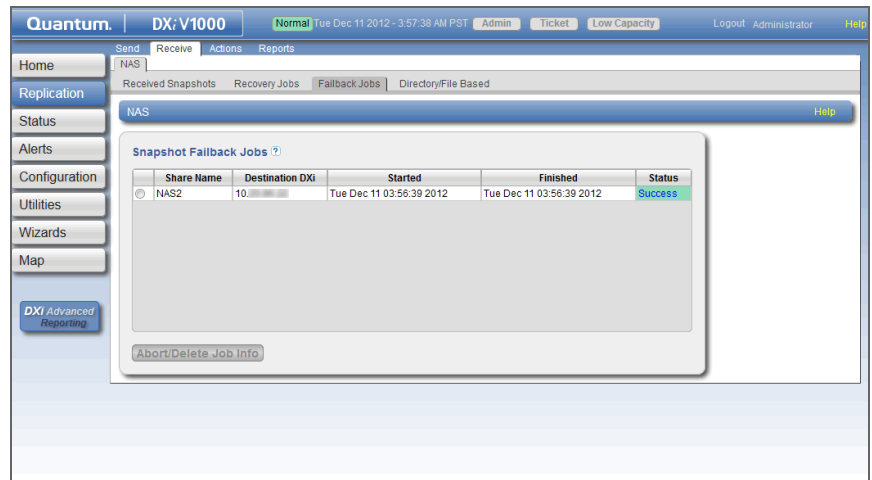
The **Snapshot Failback Jobs** section displays the following information about failback jobs:

- **Share Name** - The name of the share the snapshot was created from.

- **Destination DXi** - The hostname of the system that the snapshot was sent to.

- **Started** - The time the failback job was started.

- **Finished** - The time the failback job finished.

- **Status** - The status of the failback job (**Success**, **In Progress**, or **Failed**).

Use the **Failback Jobs** page to perform the following tasks:

- To delete information for a failback job, select it in the **Snapshot Failback Jobs** section and click **Delete Job Info**.

- To abort a failback job that is in progress, select it in the **Snapshot Failback Jobs** section and click **Abort**.

Directory/File Based

The **Directory/File Based** page allows you to manage Directory/File Based Replication on the target system. You can configure a NAS share to receive Directory/File Based Replication data sent from a source system and view replication statistics for the share.

> **Note:** For information about creating NAS shares, see Adding a NAS Share on page 130.

To access the **Directory/File Based** page, on the **Receive NAS** page, click the **Directory/File Based** tab (see Figure 47).

Figure 47 Directory/File Based Page
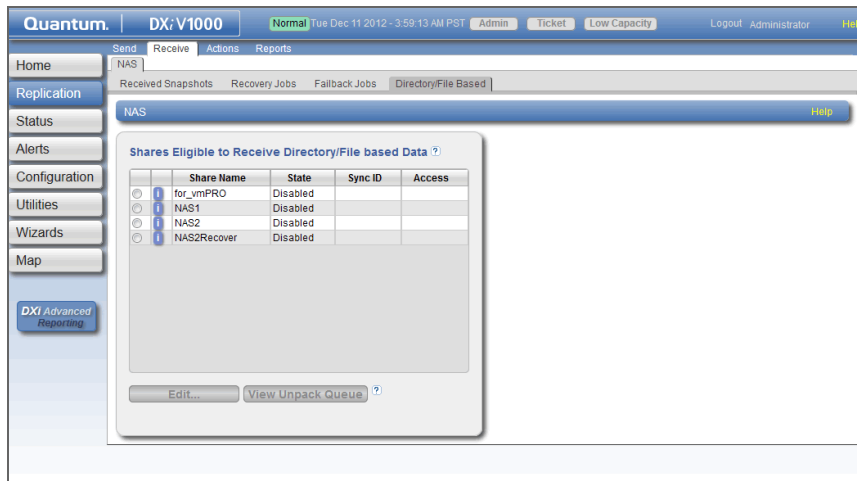
Use the **Directory/File Based** page to perform the following tasks:

- View shares eligible to receive Directory/File Based data (see Shares Eligible to Receive Directory/File Based Data on page 95)

- Configure a share to receive Directory/File Based Replication data (see Configuring a Target Share for Directory/File Based Replication on page 95)

- View statistics for shares configured for Directory/File Based Replication (see Unpack Queue on page 97)

Shares Eligible to Receive Directory/File Based Data

The **Shares Eligible to Receive Directory/File Based Data** section displays information for all NAS shares on the DXi V-Series that are eligible to receive Directory/File Based Replication data from a source share. To be eligible to receive Directory/File Based Replication data, a share must have data deduplication enabled at the time it is created.

The **Shares Eligible for Replication** section displays the following information:

- **Share Name** - The name of the share.
- **State** - The state of Directory/File Based Replication for the share (**Enabled** or **Disabled**).
- **Sync ID** - The Sync ID used to identify the source share that will send replicated data to the share.
- **Access** - The selected access option for the share (**Locked** or **Unlocked**).

Note: Click the Information button **[i]** next to a share to display detailed information about the share and recent replication activity.

Configuring a Target Share for Directory/File Based Replication

Configuring a NAS share for Directory/File Based Replication enables the automatic replication of files and directories on the source share to the target share. Before you configure a share on the source system for Directory/File Based Replication, you must configure a share on the target system to receive the replicated data from the source share.

Note: For information about configuring Directory/File Based Replication on the source system, see Configuring a Source Share for Directory/File Based Replication on page 81.

To configure a target share for Directory/File Based Replication:

1 Select the share and click **Edit**.

The **Edit Share Settings** page displays (see Figure 48).

Figure 48 Edit Share Settings
Page
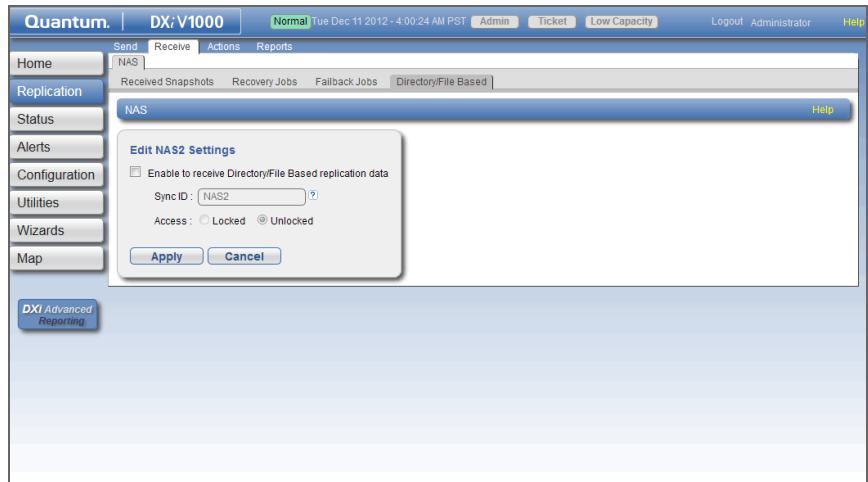
2 Select the **Enable to receive Directory/File Based replication data** check box to enable Directory/File Based Replication for the share.

Or clear the **Enable to receive Directory/File Based replication data** check box to disable Directory/File Based Replication for the share.

3 Enter a **Sync ID** in the box.

The Sync ID is used to identify the source share that will send replicated data to the target share. The Sync ID *must* be identical to the Sync ID of the source share on the source system.

4 Select an **Access** option:

- **Locked** - The share is not allowed to receive new Directory/File Based Replication data.

- **Unlocked** - The share is allowed to receive new Directory/File Based Replication data.

Note: If a share configured for Directory/Filed Based Replication is locked on the target system, synchronization jobs may fail on the source system.

5 Click **Apply**.

Unpack Queue

Use the **Unpack Queue** to view Directory/File Based Replication statistics for data received from the source system.

To view the **Unpack Queue**, select a share and click **View Unpack Queue** (see Figure 49).

Figure 49 Unpack Queue
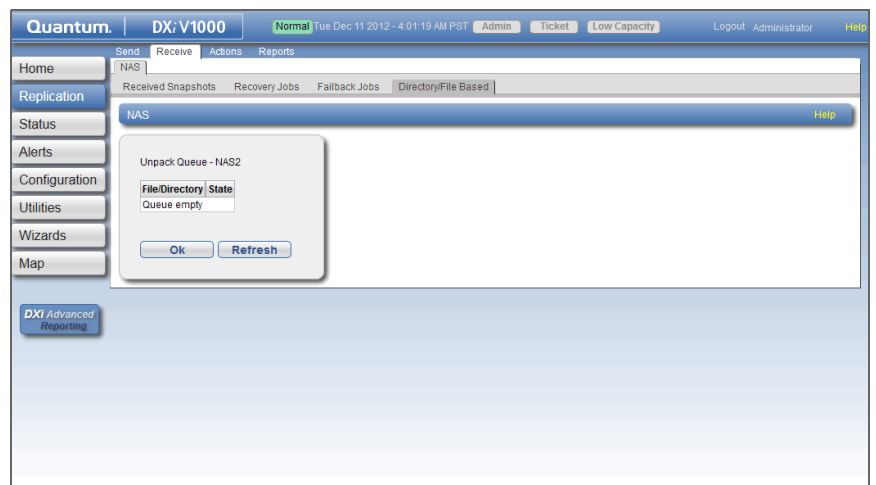
The **Unpack Queue** displays the following information:

- **File/Directory** - The file or directory to be replicated.
- **State** - The replication state of the file or directory.

Click **Refresh** to update the statistics in the Unpack Queue. Click **OK** to return to the **Directory/File Based** page.

Actions

The **Actions** page allows you to manage replication activity on the DXi V-Series. You can pause the replication service, enable the replication state, and clear performance statistics.

To access the **Actions** page, click the **Replication** menu, and then click the **Actions** tab (see Figure 50).

Figure 50 Actions Page
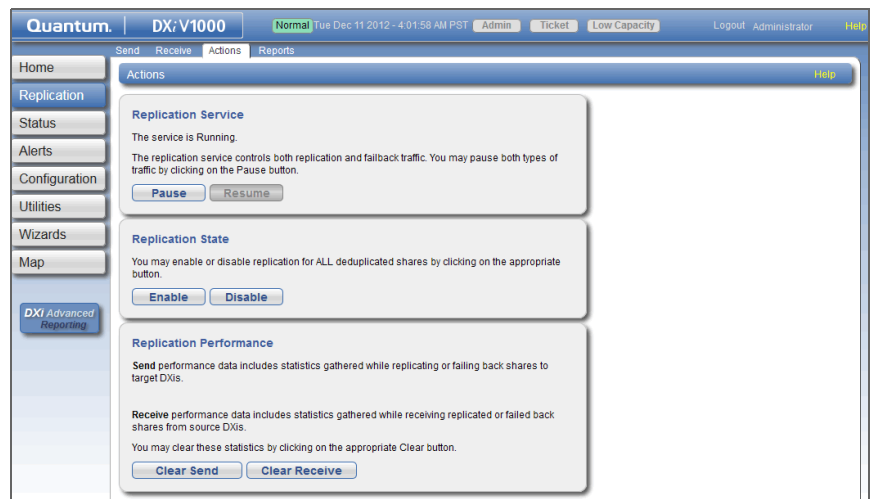
Use the **Actions** page to perform the following tasks:

- Pause or resume the replication service (see Replication Service on page 98).

- Enable or disable the replication state (see Replication State on page 99).

- Clear cumulative replication statistics (see Replication Performance on page 100).

Replication Service

The replication service controls replication and failback traffic on the DXi V-Series.

- Click **Pause** to pause all replication and failback traffic.

If a replication job is currently in progress, the system continues to replicate the current block of data. The process of replicating the current block can take up to 15 minutes to complete. After the block has completed replication, the system pauses replication.

Note: If you pause a replication job that is in process, a Failure event is logged in the replication report (see Reports on page 100).

• Click **Resume** to resume all incoming and outgoing replication and failback traffic.

If a replication job was in progress when replication was paused, the replication job continues.

Replication State

The replication state applies to all NAS shares on the DXi V-Series that are eligible for replication (that is, all deduplicated shares).

Note: The **Replication Actions** page may appear busy for a few moments when enabling or disabling the replication state. Wait for the process to complete before performing other actions.

• Click **Enable** to enable replication for all shares.

• Click **Disable** to disable replication for all shares.

If a replication job is currently in progress, the system continues until the entire replication job is complete. After the replication job has completed, the system disables replication. The system will not be able to replicate data for any shares until you click **Enable**.

Note: To disable replication for a single share, select it on the **Replication > Send** page and click **Edit**. Clear the **Enable replication** and the **Enable scheduled replication** check boxes, and then click **Apply**. For more information, see Send NAS on page 77.

**Replication
Performance**

The DXi V-Series maintains cumulative performance statistics for send and receive replication activity. The statistics appear on the **Home** page and elsewhere. To reset these statistics so the system will calculate them with new data going forward, click **Clear**.

- Click **Clear Send** to reset cumulative performance statistics gathered while replicating shares to target systems, or when sending a snapshot during a failback operation.

- Click **Clear Receive** to reset cumulative performance statistics gathered while receiving replicated shares from source systems, or when receiving a snapshot during a failback operation.

Reports

The **Reports** page allows you to generate and download a replication report. The report includes detailed information about all replication activity, including Directory/File Based Replication.

To access the **Reports** page, click the **Replication** menu, and then click the **Reports** tab (see Figure 51).

Figure 51 Reports Page
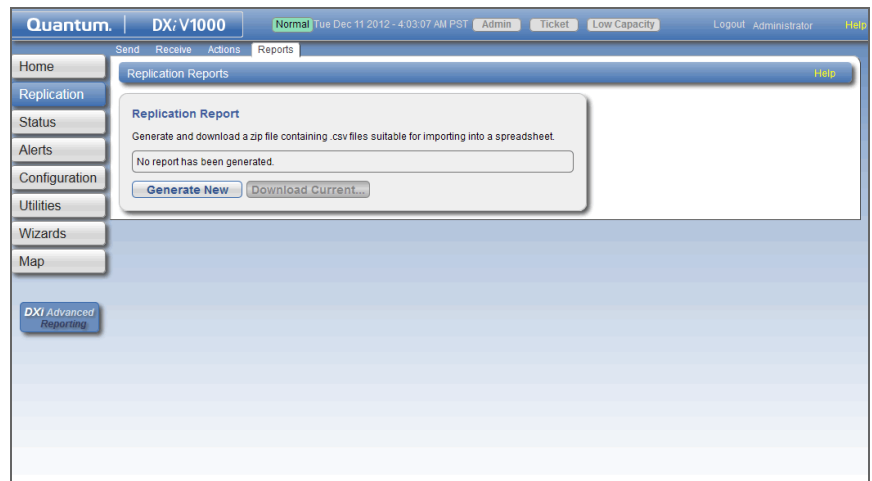
Use the **Reports** page to perform the following tasks:

- To generate a new replication report, click **Generate New.**

- To download the most recently generated replication report, click **Download Current**.

  Save the replication report to your local workstation, and then unzip the downloaded file. The report consists of a ZIP file that contains multiple CSV (comma separated value) files. To view the CSV files, open them in a compatible spreadsheet application.

Chapter 6
DXi V-Series Status

The **Status** page allows you to view performance and disk usage information.

To access the **Status** pages, click the **Status** menu.

The **Status** pages contains the following tabs:

- Performance
- Disk Usage
- DXi Accent Status
- Activity Log

Performance

The **Performance** page allows you to view information about system performance, including inline throughput, network throughput, and CPU usage.

To access the **Performance** page, click the **Status** menu, and then click the **Performance** tab.

The **Performance** page contains the following tabs:

- Inline

- [Ethernet](#)
- [CPU](#)

Inline

The **Inline** page allows you to view throughput performance for inline data flow. Inline data flow includes deduplicated and non-deduplicated backup data as well as received replication data.

To access the **Inline** page, on the **Performance** page, click the **Inline** tab (see Figure 52).

Figure 52 Inline Page
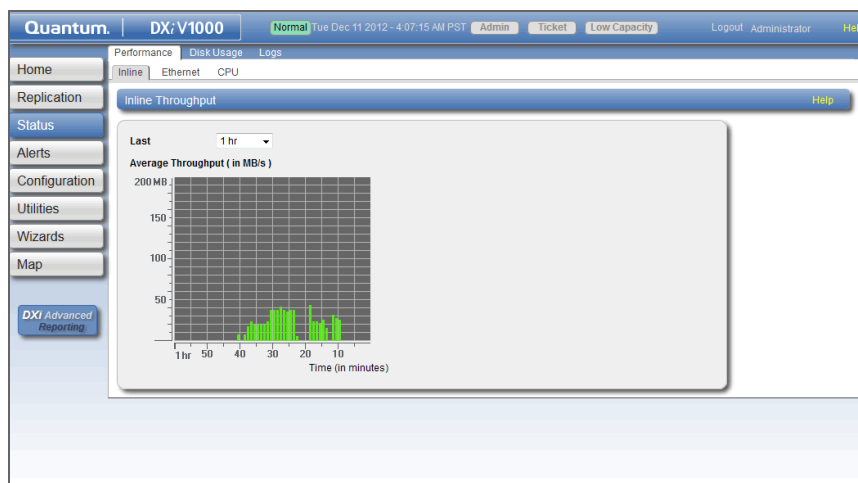
Use the **Inline** page to display recent inline data flow activity in a dynamic graph:

- Select the amount of time to display in the **Last** list (1–24 hours).
- The horizontal axis displays time (in minutes).
- The vertical access displays inline throughput (0–2,000 MB/s).

  Note: The range represented by the Y-axis changes based on the maximum value, increasing in 200 MB increments as needed.

- Each bar on the graph represents approximately 1 minute of time.
- Hold the cursor over a bar to display the value of the bar.

Ethernet

The **Ethernet** page allows you to view throughput performance for network send and receive activity.

To access the **Ethernet** page, on the **Performance** page, click the **Ethernet** tab (see Figure 53).

Figure 53 Ethernet Page

Use the **Ethernet** page to display recent network activity in dynamic graphs:

- The top graph reports data received and the bottom graph reports data sent.

- Select the port to monitor in the **Ethernet** drop-down box, or select **Avg** to display an average of all ports.

- The horizontal axis displays time (0–100 seconds).

- The vertical axis displays data throughput (0–125 MB/s for 1 GbE ports or 0–1.25 GB/s for 10 GbE ports).

- Values that exceed the maximum value of the vertical axis are shown in lighter green.

- Each bar on the graph represents approximately 1 second of time.

- Hold the cursor over a bar to display the value of the bar.

CPU

The **CPU** page allows you to view CPU usage.

To access the CPU page, on the **Performance** page, click the **CPU** tab (see Figure 54).

Figure 54 CPU Page
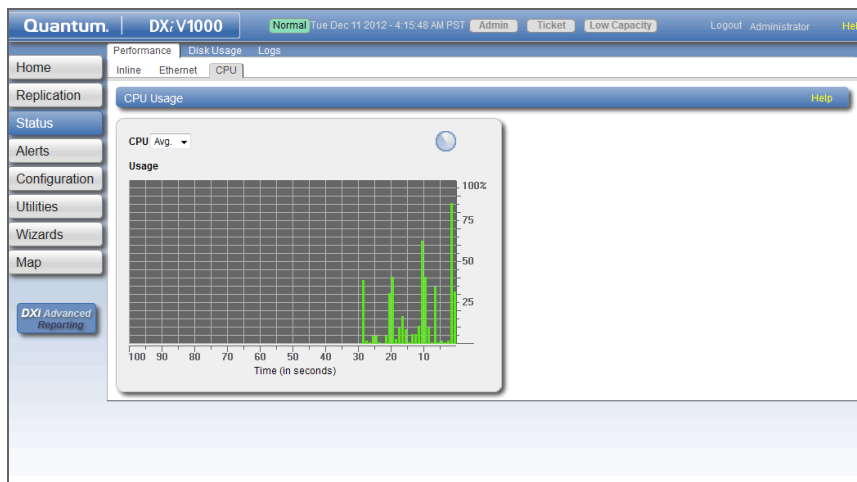
Use the **CPU** page to display recent CPU usage in a dynamic graph:

- Select the CPU core to monitor in the **CPU** drop-down box, or select **Avg** to display an average of all CPUs.

    Note: The **CPU** drop-down box lists all CPU threads. Each hyper-threaded CPU core counts as two threads.

- The horizontal axis displays time (0–100 seconds).

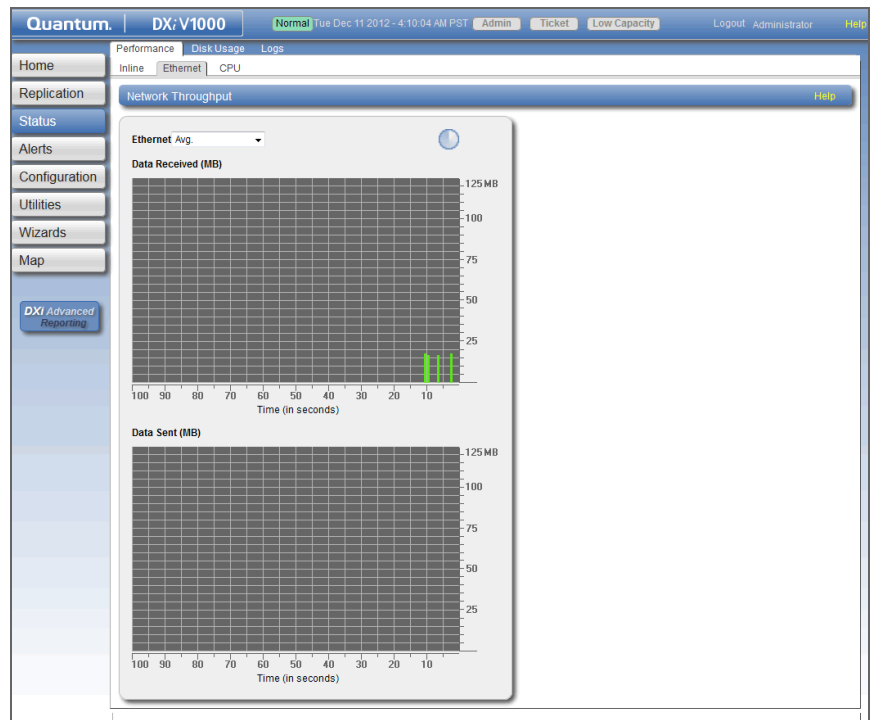- The vertical axis displays CPU usage (0–100%).

- Each bar on the graph represents approximately 1 second of time.

- Hold the cursor over a bar to display the value of the bar.

Disk Usage

The **Disk Usage** page allows you to view information about free and used disk space on the system. You can also view data reduction statistics.

To access the **Disk Usage** page, click the **Status** menu, and then click the **Disk Usage** tab (see Figure 55).

Figure 55 Disk Usage Page
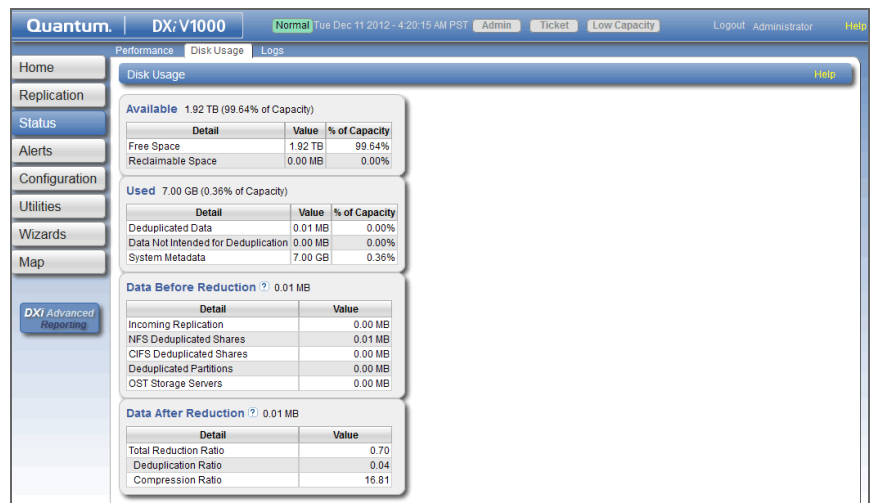
Use the **Disk Usage** page to view the following information:

* Available

* Used

* Data Before Reduction

* Data After Reduction

Available

Available space is the area that is available for data storage. The **Available** value is displayed as an amount and as a percentage of the total capacity in the system.

Available space is divided into the following categories:

- **Free Space** - The disk space that can be used for new deduplicated or non-deduplicated data.

- **Reclaimable Space** - The disk space that can be used for new deduplicated data. If the DXi is configured with non-deduplicated shares, the DXi will automatically compact reclaimable space to create more free space as needed.

Note: For optimal system performance, Quantum recommends keeping the amount of **Available** disk space at 20% or more.

Used

Used space is the area that already holds data. The **Used** value is displayed as an amount and as a percentage of the total capacity in the system.

Used space is divided into the following categories:

Note: The value for each category is displayed as an amount and as a percentage of the total capacity in the system.

- **Deduplicated Data** - The amount of data that has been deduplicated.

- **Data Not Intended For Deduplication** - The amount of data that will not be deduplicated (data on shares that do not have deduplication enabled).

- **System Metadata** - The amount of disk space used for internal operations of the DXi, including system configuration files as well as temporary files created during replication, space reclamation, and healthchecks.

Data Before Reduction

The **Data Before Reduction** value represents the original, native size of all data that has been processed by the data deduplication and compression engines.

Data before reduction is divided into the following categories:

- **Incoming Replication** - The amount of data stored on the DXi via replication from another DXi. This does *not* include incoming data from Directory/File Based Replication, or incoming data from Failback replication.

- **NFS Deduplicated Shares** - The amount of data stored in deduplicated shares configured in Network File System (NFS) format for Linux systems. This includes incoming data from Directory/File Based Replication, and incoming data from Failback replication.

- **CIFS Deduplicated Shares** - The amount of data stored in deduplicated shares configured in Common Internet File System (CIFS), also known as Server Message Block (SMB), format for Windows systems. This includes incoming data from Directory/File Based Replication, and incoming data from Failback replication.

- **OST Storage Servers** - The amount of data stored in deduplicated OpenStorage (OST) storage servers. This includes incoming data for OST and DXi Accent.

Data After Reduction

The **Data After Reduction** value represents the final, reduced size of all data that has been processed by the data deduplication and compression engines.

Data after reduction is divided into the following categories:

- **Total Reduction Ratio** - The total reduction ratio of all data that has been processed by the data deduplication and compression engines (**Data Before Reduction** divided by **Data After Reduction**).

- **Deduplication Ratio** - The deduplication ratio of all data that has been processed by the data deduplication engine.

- **Compression Ratio** - The compression ratio of all data that has been processed by the compression engine.

DXi Accent Status

Use the **Accent Status** page to view information about recent DXi Accent activity.

Note: The **Accent Status** page displays only if DXi Accent is currently enabled or was previously enabled (see DXi Accent on page 179).

To access the **Accent Status** page, click the **Status** menu, and then click the **Accent** tab (see Figure 56).

Figure 56 Accent Status Page
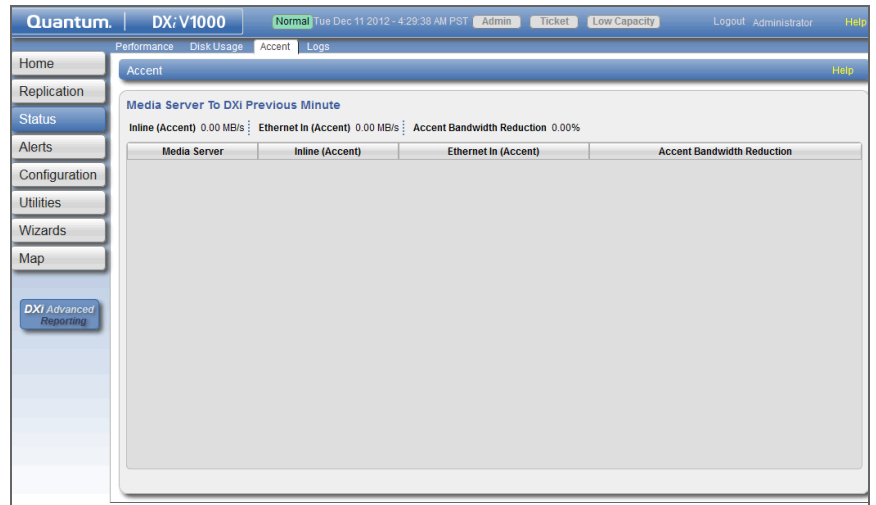
The **Accent** section displays the following information about DXi Accent activity in the previous minute:

- **Media Server To DXi Previous Minute** - DXi Accent activity for all Accent enabled media servers.

  - **Inline (Accent)** - The inline data flow throughput (in MB/s). Inline data flow represents the original, native size of the data protected by the DXi.

  - **Ethernet In (Accent)** - The amount of data received by all Ethernet ports (in MB/s). This amount represents the reduced size of the data protected by the DXi (after deduplication and compression on the media servers).

  - **Accent Bandwidth Reduction** - The percentage by which network bandwidth utilization was reduced by enabling Accent.

- **Media Server** - The IP address of the media server.

- **Inline (Accent)** - The inline data flow throughput (in MB/s). Inline data flow represents the original, native size of the data protected by the DXi.

- **Ethernet In (Accent)** - The amount of data received by all Ethernet ports (in MB/s). This amount represents the reduced size of the data

protected by the DXi (after deduplication and compression on the media server).

• **Accent Bandwidth Reduction** - The percentage by which network bandwidth utilization was reduced by enabling Accent.

Activity Log

The **Activity Log** page allows you to view a record of all activities performed by administrative and service users in the past 90 days. You can view the user who performed the activity, the time the activity was performed, and other information. You can also download the activity log to an XML file.

To access the **Activity Log** page, click the **Status** menu, and then click the **Logs** tab (see Figure 57).

Figure 57 Activity Log Page

Use the **Activity Log** page to perform the following tasks:

- View information about activities that have been recorded in the log (see Viewing Logged Activities on page 112).

- Enable or disable the recording of activities in the log (see Enabling or Disabling Activity Logging on page 113).

- Delete one or more activities from the log (see Deleting Logged Activities on page 114).

- Download the activity log in XML format (see Downloading the Activity Log on page 114).

Viewing Logged Activities

The **Administrative Activity Log** list displays the following information for each entry:

- **User** - The user that performed the activity (**Administrator**, **Monitor**, **Service**, **Engineering**, **cliadmin**, or **root**).

- **Date/Time** - The date and time the activity was performed.

- **Origin** - The interface where the activity originated. Possible origins are the **GUI** (remote management console) or the **CLI** (command line interface).

- **Action** - The type of activity performed (**Create**, **Update**, or **Delete**).

- **Category** - The category of the activity (**Alert**, **Analyzer**, **Cluster**, **Date Time**, **Email**, **Event**, **Hard Drive Security**, **Healthcheck**, **NAS**, **Network**, **OST**, **Replication**, **Security**, **SNMP**, **Utility**).

- **Role** - The role of the user that performed the activity (**Admin**).

- **Summary** - Details about the activity that was performed, including CLI commands and field values.

Note: Click a column heading to sort the rows in the table by that column. Click the column heading again to reverse the sort order.

Note: To rearrange the order of the columns, click and drag a column heading left or right. To show or hide columns, click the arrow to the right of a column heading. In the pop-up menu, point to **Columns**, then select the name of a column to show or hide it.

Navigating in the Activity Log

Use the controls at the bottom of the **Administrative Activity Log** list to adjust the activity log view (see Figure 58):

- To navigate between pages in the list, use the left and right arrows.

- To view a specific page, type the page number in the box.

- To update the activity log with latest data, click the **Refresh** icon.

Figure 58 Activity Log View Controls

Page backward or forward

Refresh

Enter page number
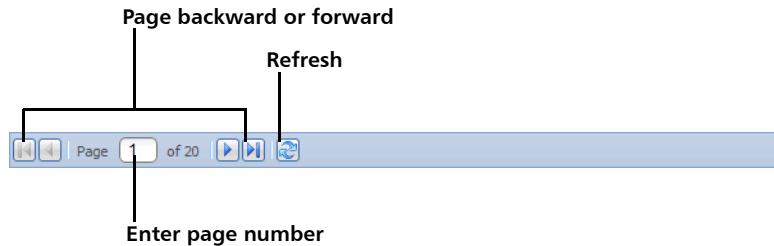
Enabling or Disabling Activity Logging

By default, activity logging is enabled on the DXi V-Series. Use the toolbar above the **Administrative Activity Log** list to enable or disable activity logging (see Figure 59).

- To enable the logging of administrative and service actions, click **Enable Logging** on the toolbar.

- To disable the logging of administrative and service actions, click **Disable Logging** on the toolbar.

Figure 59 Activity Log View Controls

Delete selected log entry

Delete all log entries

Download log as XML

Enable or disable activity logging
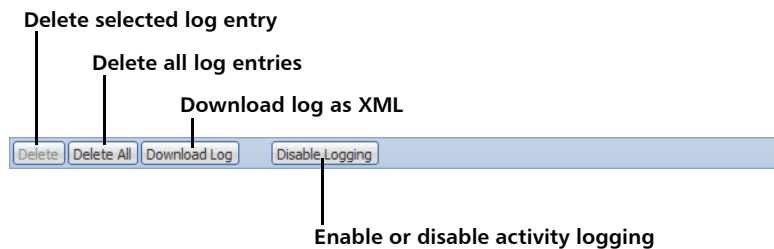
Deleting Logged Activities

Use the toolbar above the **Administrative Activity Log** list to delete one or more entries in the activity log (see Figure 59).

- To delete a log entry, select the entry and click **Delete**.

- To delete all entries in the activity log, click **Delete All**.

Downloading the Activity Log

Use the toolbar above the **Administrative Activity Log** list to save the activity log in XML format (see Figure 59). You can then open the log file in another program that is compatible with XML.

To download the activity log, click **Download Log**. Specify a location to save the file, and then click **OK** or **Save**.

Chapter 7
DXi V-Series Alerts

The **Alerts** page allows you to view and work with administration alerts and service tickets. The DXi V-Series generates administration alerts and service tickets when a hardware or software event occurs.

To access the **Alerts** page, click the **Alerts** menu.

The **Alerts** page contains the following tabs:

- Admin Alerts
- Service Tickets

Admin Alerts

The **Admin Alerts** page allows you to view and work with administration alerts. The DXi V-Series generates an administration alert when the condition of the system has changed, such as going from the offline state to the online state.

> **Note:** In addition to viewing administration alerts on the **Admin Alerts** page, you can configure the system to send alerts to an e-mail address (see Recipients on page 222).

To access the **Admin Alerts** page, click the **Alerts** menu, and then click the **Admin Alerts** tab (see Figure 60).

Figure 60 Admin Alerts Page
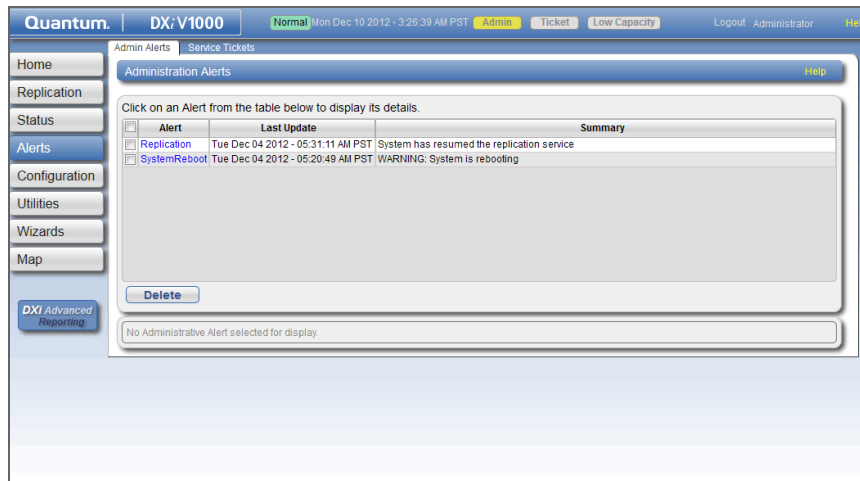
The **Admin Alerts** page displays the following information about administration alerts:

- **Alert** - The name of the administration alert.

- **Last Update** - The date when the administration alert was last updated by the system.

- **Summary** - A brief description of the administration alert.

Note: Click a column heading to sort the rows in the table by that column. Click the column heading again to reverse the sort order.

Use the **Admin Alerts** page to perform the following tasks:

- To view details about an administration alert, click the alert name. Detailed information about the alert appears in the **Activity Status History** section.

- To delete an administration alert, select it and click **Delete**.

Service Tickets

The DXi V-Series has the capability to automatically detect and resolve problems encountered by the system during operation. If a problem cannot be resolved automatically and requires user intervention or servicing, the system generates a service ticket.

A service ticket contains detailed information about the problem and, if appropriate, steps you can take to resolve it. If the DXi V-Series detects that the problem is resolved, the system automatically closes the service ticket. You can also manually close a service ticket after the problem is corrected.

Note: Tickets that are not resolved are generated again after 24 hours.

See the following sections for more information about service tickets:

- Service Ticket Priority
- Recommended Actions
- Working With Service Tickets

Service Ticket Priority

The system assigns each service ticket a priority based on the criticality of the problem that caused the system to generate the ticket. There are three priority levels:

- **Low** - A minor problem occurred and needs to be resolved, but the operation and performance of the DXi V-Series are not significantly affected.

- **Middle** - A serious problem occurred and needs to be resolved, but it does not necessarily need to be fixed immediately. The operation and performance of the DXi V-Series may be degraded.

- **High** - A critical problem has occurred and needs to be resolved immediately. The operation and performance of the DXi V-Series are degraded, and there is a risk of system failure or data loss.

Recommended Actions

If appropriate, a service ticket includes recommended actions. The recommended actions provide instructions for resolving the problem that caused the system to generate the ticket.

Perform the recommended actions to try to resolve the problem before contacting Quantum customer support. If you are able to resolve the problem, you can close the service ticket.

Note: The recommended actions should be performed by a user who is familiar with operating the DXi V-Series.

Note: For DXi V1000 Standard Edition users, documentation, community support, and other resources are available through Forum V (http://www.quantum.com/forumv), Quantum's online support forum for virtualization products. Quantum customer support options are available for DXi V-Series Enterprise Edition users. To learn more about upgrading to Enterprise Edition, contact your Quantum Sales Representative.

Working With Service Tickets

The **Service Tickets** page allows you to view and work with service tickets.

To access the **Service Tickets** page, click the **Alerts** menu, and then click the **Service Tickets** tab (see Figure 61).

Figure 61 Service Tickets Page
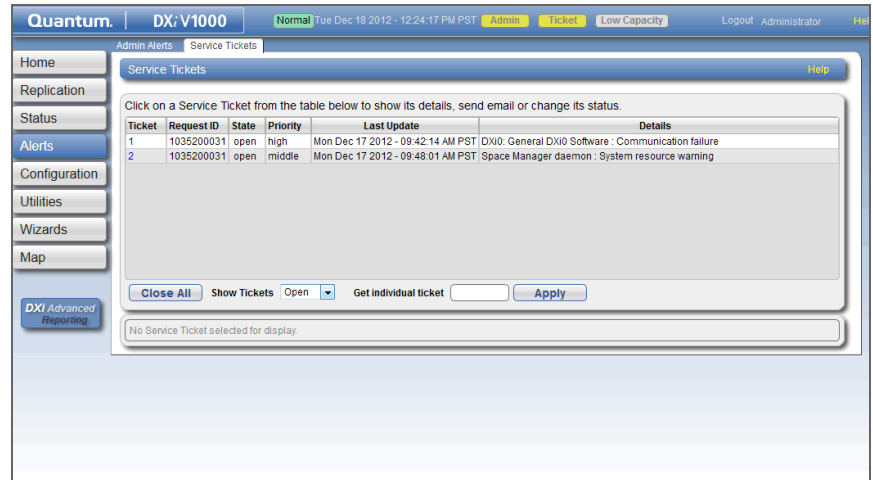
The **Service Tickets** page displays the following information about open service tickets:

- **Ticket** - The service ticket number.

- **Request ID** - The Request ID of the ticket.

- **State** - The current status of the service ticket (**Open** or **Closed**).

- **Priority** - The priority level of the service ticket (**Low, Middle**, or **High**).

- **Last Update** - The date when the service ticket was last updated by the system.

- **Details** - A brief description of the service ticket.

- **Close All** - Click to close all open service tickets.

- **Show Tickets** - Select an option to display **Open** tickets, **Closed** tickets, or **All** tickets.

- **Get individual ticket** - To display a specific ticket in the list, enter a ticket number and click **Apply**.

Note: Click a column heading to sort the rows in the table by that column. Click the column heading again to reverse the sort order.

Use the **Service Tickets** page to perform the following tasks:

- View details for a service ticket, including recommended actions (see Viewing a Service Ticket on page 120).

- Add information to a service ticket (see Modifying a Service Ticket on page 122).

- Send a service ticket to an e-mail address (see Sending a Service Ticket on page 123).

- Close a service ticket that has been resolved (see Closing a Service Ticket on page 124).

Viewing a Service Ticket

View a service ticket to see detailed information about the problem that caused the system to generate the ticket and to view recommended actions.

To view a service ticket:

1 In the list of service tickets, click the ticket number.

The **Ticket Details** section at the bottom of the page displays information about the service ticket, including the time the ticket was opened and closed, the ticket status, and detailed information about the problem (see Figure 62).

> **Note:** The time indicated in the service ticket may not match the DXi V-Series system time.

Figure 62 Ticket Details
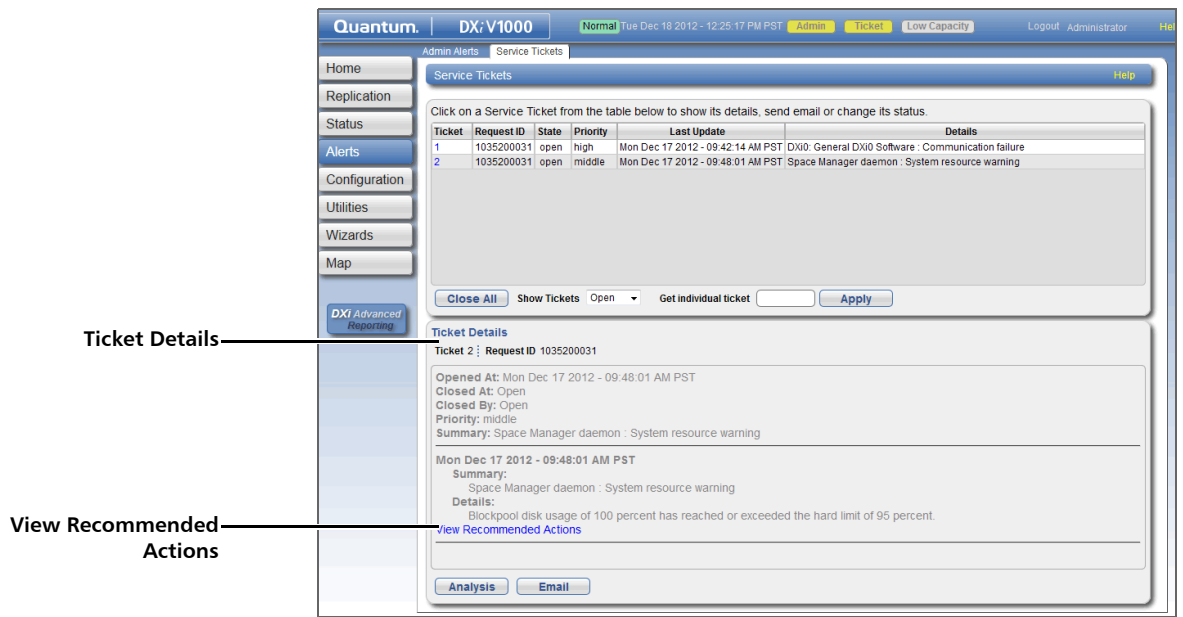
2 (Optional) Click **View Recommended Actions** to view instructions for resolving the problem.

The recommended actions display in a new Web browser window (see Figure 63). Follow the instructions to resolve the problem. When you are finished, click the close button **[x]** on the upper right corner of the window.

Figure 63 Recommended
Actions

Modifying a Service Ticket

Modify a service ticket to add additional information to the ticket, for example, troubleshooting steps you have taken or a record of calls made to Quantum customer support. The additional information is saved with the service ticket and remains associated with the ticket even after it is closed.

To modify a service ticket:

1 In the list of service tickets, click the ticket number.

2 Click **Analysis** at the bottom of the page.

The **Ticket Analysis** section displays at the bottom of the page (see Figure 64).

Figure 64 Ticket Analysis
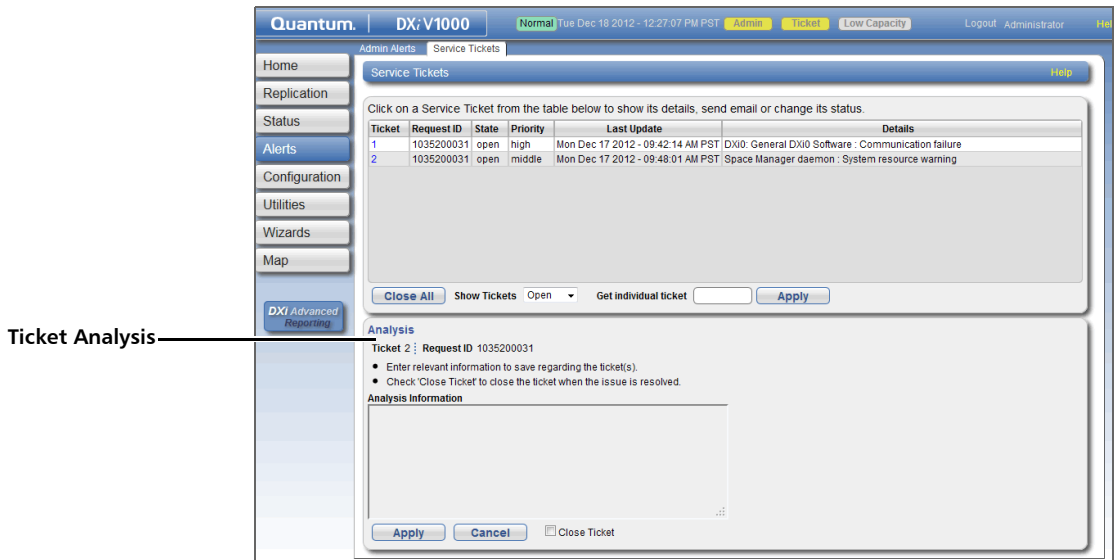
3 In the **Analysis Information** box, enter all relevant information about actions taken to resolve the issue.

4 Click **Apply**.

Sending a Service Ticket

Send a service ticket to send the ticket details to an e-mail address. You can also add optional comments to the e-mail.

> **Note:** To enable the DXi V-Series to send e-mail, you must specify an outgoing e-mail server (see Server on page 227).

To send a service ticket:

1 In the list of service tickets, click the ticket number.

2 Click **Email** at the bottom of the page.

The **Email Ticket Information** section displays at the bottom of the page (see Figure 65).

Figure 65 Email Ticket
Information
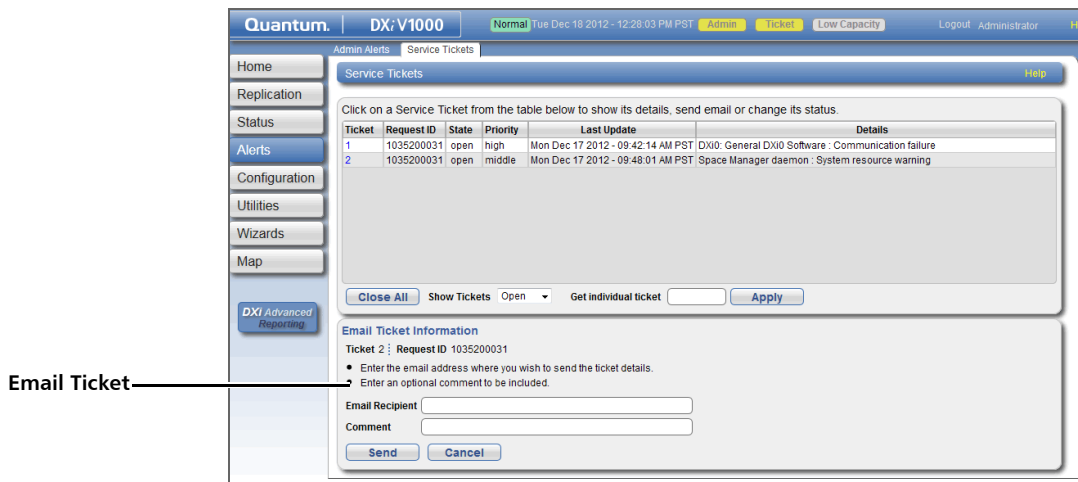
3 In the **Email Recipient** box, enter the e-mail address where you want to send the ticket details.

4 (Optional) In the **Comment** box, enter additional information to send with the ticket.

5 Click **Send**.

Closing a Service Ticket

Close a service ticket if the problem the caused the system to generate the ticket is resolved. You can also close all service tickets that are currently open.

> **Note:** You can still view and modify a ticket after it has been closed.

To close all service tickets that are currently open, below the list of service tickets, click **Close All**.

To close a single service ticket:

1 In the list of service tickets, click the ticket number.

2 Click **Analysis** at the bottom of the page.

The **Ticket Analysis** section displays at the bottom of the page (see Figure 64).

3 Select the **Close Ticket** check box.

4 Click **Apply**.

Chapter 8
DXi V-Series Configuration

The **Configuration** page allows you to configure the features of the DXi V-Series, including storage presentation, data replication, system settings, and notifications.

To access the **Configuration** page, click the **Configuration** menu.

The **Configuration** page contains the following tabs:

- NAS
- Replication
- OST (including DXi Accent with OST)
- Scheduler
- System
- Notifications
- Contacts

NAS

The **NAS** page allows you to configure the DXi V-Series to present its storage capacity as NAS (network attached storage) shares that are compatible with standard backup applications. You can create NAS

shares for use with Windows or Linux networks. You can also join the DXi V-Series to a Windows domain or workgroup and manage users.

Note: The **NAS** wizard provides guided assistance for configuring NAS shares (see DXi V-Series Configuration Wizards on page 25).

Caution: Caution: Filenames on NAS shares are limited to a length of 256 bytes. If a filename uses Japanese characters, the filename can be no longer than 85 characters. This is because each Japanese character is represented by 3 bytes.

To access the **NAS** page, click the **Configuration** menu, and then click the **NAS** tab.

The **NAS** page contains the following tabs:

- NAS Summary
- Windows Domain
- Share Access
- Advanced Setting

NAS Summary

The **NAS Summary** page allows you to manage NAS shares on the DXi V-Series. You can view information about existing shares, add or edit shares, and delete shares.

To access the **NAS Summary** page, on the **NAS** page, click the **Summary** tab (see Figure 66).

Figure 66 NAS Summary Page
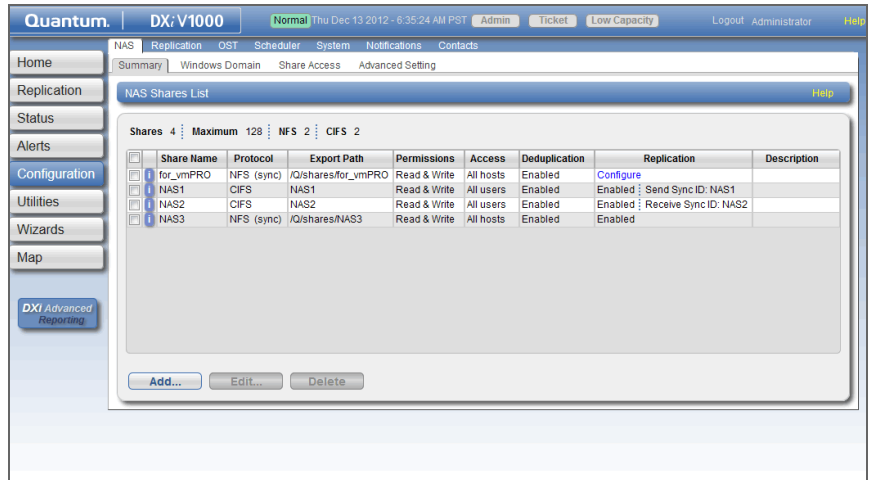
Use the **NAS** page to perform the following tasks:

- View information about existing NAS shares (see <u>NAS Shares List</u> on page 129).

- Add a new NAS share to the system (see <u>Adding a NAS Share</u> on page 130).

- Edit properties for an existing NAS share (see <u>Editing a NAS Share</u> on page 132).

- Delete a NAS share from the system (see <u>Deleting a NAS Share</u> on page 134).

NAS Shares List

The **NAS Shares List** section displays the following information for all NAS shares on the DXi V-Series:

- **Shares** - The number of shares that have been added to the system.

- **Maximum** - The maximum number of shares that can be added to the system.

- **NFS** - The number of existing shares configured to use the NFS protocol (for Linux networks).

- **CIFS** - The number of existing shares configured to use the CIFS protocol (for Windows networks).

- **Share Name** - The name of the share.

- **Protocol** - The protocol (**CIFS** or **NFS**) the share is configured to use.

  For NFS shares, the **Protocol** column displays the commit type of the share (**sync** for synchronous or **async** for asynchronous). For information about changing the commit type of NFS shares, see the *DXi-Series Command Line Interface (CLI) Guide* (6-67081).

- **Export Path** - The export path of the share (different for CIFS and NFS shares).

- **Permissions** - The permissions in use on the share (**Read & Write** or **Read Only**).

- **Access** - The access type of the share (**all hosts** or specific users).

- **Deduplication** - The data deduplication state of the share (**Enabled** or **Disabled**).

- **Replication** - The current state of replication for the share:

  - **Enabled** - Replication is enabled.

  - **Send/Receive Sync ID** - Directory/File Based Replication is enabled.

  - **Configure** - Click to configure replication for the share (see Editing a NAS Share on page 132)

  - **Scheduled** - Replication is scheduled for the share. Click to view or modify the schedule (see Scheduling a Share for Replication on page 186).

- **Description** - A brief description of the NAS share (if available).

Note: Click a column heading to sort the rows in the table by that column. Click the column heading again to reverse the sort order.

Note: Click the Information button **[i]** next to a share to display detailed information about the share and recent replication activity.

Adding a NAS Share

Add a NAS share to present the storage capacity of the DXi V-Series as a NAS share that is compatible with standard backup applications. You can add up to 128 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).

> **Note:** If you are adding a CIFS share for use with a Windows network, you must configure the Windows domain before adding the new share (see Windows Domain on page 135).

To add a NAS share:

1 Click **Add**.

The **Add NAS Share** page displays (see Figure 67).

Figure 67 Add NAS Share Page

2 Under **NAS Share Settings**, enter information about the share:

- **Name** - Enter the name of the NAS share.

- **Description** - (Optional) Enter a brief description of the share.

- **Hide from network browsing** - (CIFS shares only) Select the check box to hide the share from network browsing. If selected, you cannot see the share when browsing the network.

- **Enable data deduplication** - Select the check box to enable data deduplication. Quantum recommends that you enable data deduplication to optimize disk usage.

> **Note:** Data deduplication is enabled by default. You cannot enable or disable data deduplication after the share is added. If data duplication is disabled, then data compression is also disabled.

- **Export Protocol** - Select the export protocol for the share:
  - **CIFS** - Select the CIFS option to use the share on a Windows network.
  - **NFS** - Select the NFS option to use the share on a UNIX or Linux network.

3 (Optional) Under **Replication Settings**, specify replication settings.

For more information about configuring replication for a share, or to set up replication for the share at a later time, see <u>DXi V-Series Replication</u> on page 69.

4 Click **Apply**.

> **Note:** When you create a CIFS share, the initial permissions are the same as the default permissions for a Windows 2003 share with the addition of an ACE (Access Control Entry) that permits full access to the share for all authenticated users. Administrators can choose to remove this full access ACE, set up custom permissions, or leave the ACL (Access Control List) as it is if the server is set up in a fully trusted environment.

Editing a NAS Share

Edit a NAS share to modify the settings for the share, for example, to change the description of the share or to select different options.

To edit a NAS share:

1 Select the share and click **Edit**.

The **Edit NAS Share & Replication Settings** page displays (see <u>Figure 68</u>).

Figure 68 Edit NAS Share &
Replication Settings Page
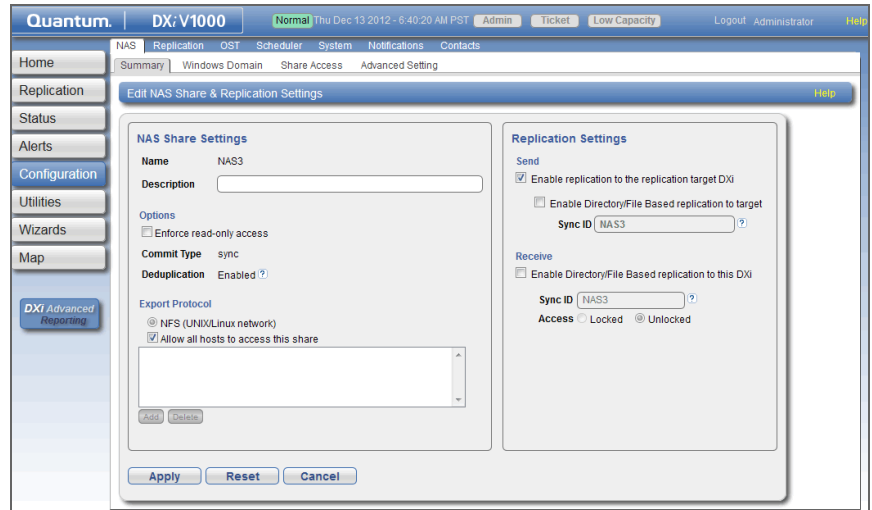
2 Under **NAS Share Settings**, enter information about the share:

> **Note:** If you are editing a share, only the **Description**, **Enforce read-only access**, **Hide from network browsing**, and **Allow all users to access this share** options can be changed.

- **Description** - (Optional) Enter a brief description of the share.

- **Enforce read-only access** - Select the check box to make the share read only. If selected, you cannot write to the share.

- **Hide from network browsing** - (CIFS shares only) Select the check box to hide the share from network browsing. If selected, you cannot see the share when browsing the network.

- **Allow all users/hosts to access this share** - Select this check box to allow all users (CIFS shares) or hosts (NFS shares) to access the share.

  Or clear the check box to allow only specified users or hosts to access the share. To add a user or host to the access list, click **Add**. Specify the **Workgroup User** (CIFS shares) or the **Hostname or IP Address** (NFS shares) and the associated permissions (**Read Only** or **Read & Write**), and then click **Apply**.

> **Note:** To modify the users that are available in the
> **Workgroup User** list, see <u>Share Access</u> on page 138.

> **Note:** After you add a user or host to the access list, you
> cannot change their permissions. Instead, select the
> user or host in the access list and click **Delete** to
> remove them from the list. Then add the user or host
> again with the correct permissions.

3 (Optional) Under **Replication Settings**, specify replication settings.

For more information about configuring replication for a share, or
to set up replication for the share at a later time, see <u>DXi V-Series
Replication</u> on page 69.

4 Click **Apply**.

> **Note:** If you modify a NAS share that uses the CIFS protocol, you
> must restart the CIFS service for the changes to take effect. To
> restart the CIFS service, first disjoin the Windows workgroup,
> then join it again (see <u>Windows Domain</u> on page 135).
> Restarting the CIFS service will close all active connections to
> the share. Most Windows workstations will automatically
> reconnect, but some applications may be affected.

Deleting a NAS Share

Delete a NAS share if it is no longer needed. When you delete a share, all
data stored on the share is lost, and any schedules associated with the
share are deleted.

> **Note:** If you delete a share configured for Directory/File Based
> Replication on the source DXi, the share is *not* automatically
> deleted on the target DXi. If you do not want to retain the
> share on the target DXi, you can manually delete it.

To delete a NAS share:

1 Select the share and click **Delete**.

> **Note:** You can select multiple shares to delete at once.

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

Windows Domain

The **Windows Domain** page allows you to join the DXi V-Series to a Windows workgroup or a Windows domain using **SMB**. To use a NAS share configured for the CIFS protocol on a Windows network, you must first join the DXi V-Series to a workgroup or a domain. After you join the DXi V-Series to a workgroup or a domain, CIFS shares are available for use on the Windows network.

To access the **Windows Domain** page, on the **NAS** page, click the **Windows Domain** tab (see Figure 69).

Figure 69 Windows Domain Page

Use the **Windows Domain** page to perform the following tasks:

- Join the DXi V-Series to a Windows workgroup (see Joining a Windows Workgroup on page 136).

- Join the DXi V-Series to a Windows domain (see Joining a Windows Domain on page 136).

- Remove the DXi V-Series from a Windows workgroup or domain (see Disjoining a Workgroup or Domain on page 137).

Joining a Windows Workgroup

Join a Windows workgroup to add the DXi V-Series to a workgroup on a Windows network. After you join a workgroup, CIFS shares are available for use on the Windows network.

To join a Windows workgroup:

1 Enter the following information about the Windows domain:

- **Domain Type** - Select Workgroup.

- **Domain/Workgroup Name** - Enter the workgroup name.

  The workgroup name can be the name of an existing workgroup or a new workgroup (for example, **Workgroup** or **Sales**).

2 Click **Apply**.

Note: When an SMB server is joined to a workgroup, share security is managed directly from the remote management console. For a CIFS share, security is provided through the read only or read/write access to the share. By default, when a CIFS share is created, the default security setting allows access for all users. Any access restrictions on individual users can be managed by editing a share on the NAS Summary page (see Editing a NAS Share on page 132).

Joining a Windows Domain

Join a Windows domain to add the DXi V-Series to a Windows network using Active Directory. After you join a domain, CIFS shares are available for use on the Windows network.

Before joining a Windows domain, make sure the date and time on the DXi V-Series is correct and is synchronized with the Active Directory Services (ADS) server (see Date & Time on page 211). The time difference between the DXi V-Series and the ADS server (domain controller) must be less than 300 seconds. Quantum recommends using the same NTP server for the DXi V-Series and the ADS server to keep them synchronized.

To join a Windows domain:

1 Enter the following information about the Windows domain:

- **Domain Type** - Select **Active Directory**.

- **Domain/Workgroup Name** - Enter the domain name.

- **Primary Domain Controller** - Select an option for the Primary Domain Controller (PDC):

  - **Use DNS Discovery** - Discover the PDC automatically.

  - **Specify Address** - Enter the fully qualified name or the IP address of the PDC.

- **Organization Unit** - (Optional) Enter the name of the organizational unit in the domain.

  The DXi V-Series will become a member of this organization.

- **Administrator Name** - Enter **Administrator** or any user that has the right to join the domain.

  By default, any user belonging to the **Administrators** group or the **Domain Admins** group has the right to join the domain. In addition, any user can join the domain if they are specifically delegated this right by a member of the **Administrators** group.

- **Administrator Password** - Enter the password for the user entered above.

2 Click **Apply**.

Note: When the system is joined to the Active Directory domain, share security is managed by the MMC (Microsoft Management Console) that is running on the domain controller. By default, when a CIFS share is created, the default security setting allows access for all users. Any access restrictions on individual users must be managed from the MMC.

Disjoining a Workgroup or Domain

Disjoin a workgroup or a domain to remove the DXi V-Series from a Windows workgroup or domain. After you disjoin the workgroup or domain, CIFS shares are no longer available for use on the Windows network

To disjoin a workgroup or domain, click **Disjoin**.

Share Access

The **Share Access** page allows you to manage workgroup users when the DXi V-Series is joined to a Windows workgroup, or manage share administrators when the DXi V-Series is joined to a Windows domain using Active Directory. You can add users or administrators, change user privileges, and delete users or administrators. Available users or administrators can be granted access to NAS shares configured for the CIFS protocol.

Note: You must join a Windows workgroup or domain before you can add workgroup users or share administrators (see Windows Domain on page 135). The **Share Access** page is different depending on whether the DXi is joined to a workgroup or domain.

To access the **Share Access** page, on the **NAS** page, click the **Share Access** tab (see Figure 70 and Figure 71).

Figure 70 Share Access Page (Windows Workgroup)
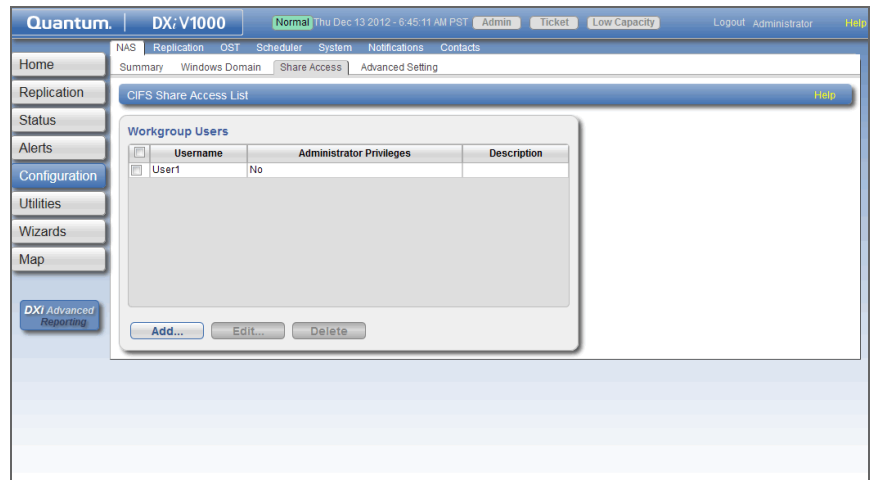
Figure 71 Share Access Page
(Active Directory)
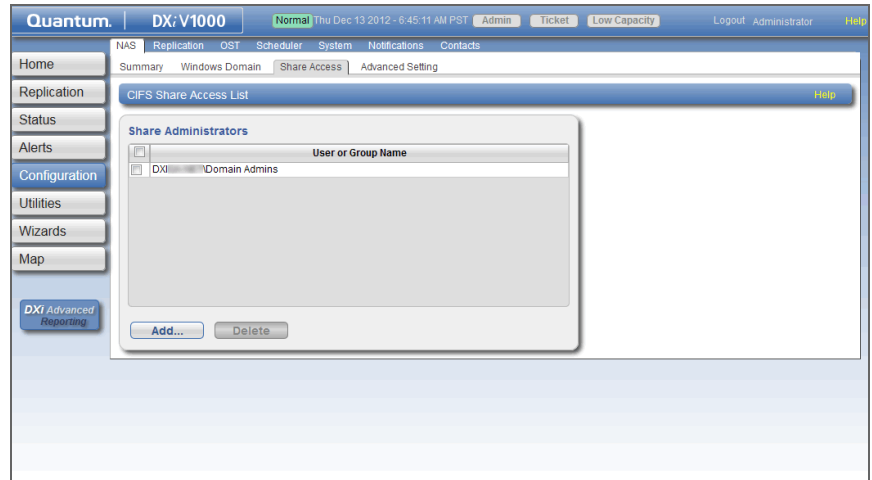
Use the **Share Access** page to perform the following tasks:

- View information about workgroup users or share administrators (see Workgroup Users or Share Administrators on page 139).

- Add a workgroup user or a share administrator (see Adding a Workgroup User or Share Administrator on page 140).

- Edit a workgroup user (see Editing a Workgroup User on page 141).

- Delete a workgroup user or a share administrator (see Deleting a Workgroup User or Share Administrator on page 143).

Workgroup Users or Share Administrators

If the DXi V-Series is joined to a Windows workgroup, the **Workgroup Users** section displays the following information about workgroup users:

- **Username** - The name of the workgroup user.

- **Administrator Privileges** - The privileges of the workgroup user (**Yes** if the user has administrator privileges, **No** if they do not.)

- **Description** - A brief description of the workgroup user (if available).

If the DXi V-Series is joined to a Windows domain using Active Directory, the **Share Administrators** section displays the following information about share administrators:

> • **User or Group Name** - The fully qualified name of the user or group.

Adding a Workgroup User or Share Administrator

Add a workgroup user or share administrator to be able to grant that user or administrator access to CIFS shares.
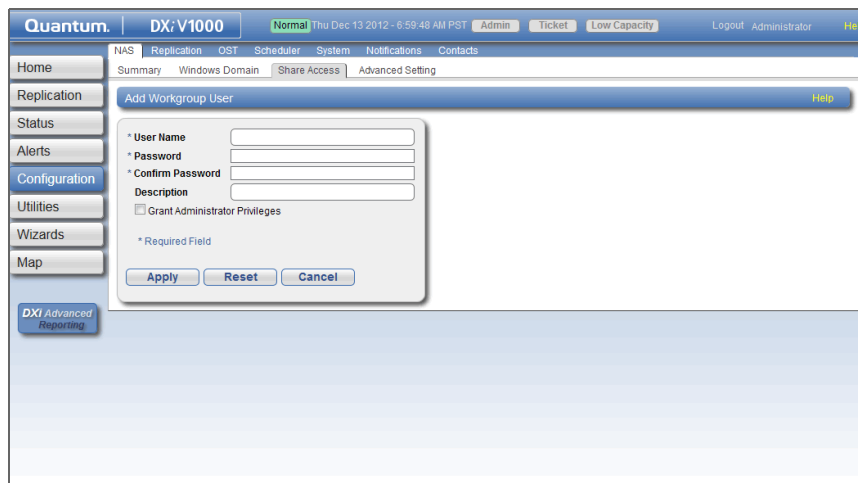
Windows Workgroup

To add a workgroup user for a Windows workgroup:

1 Click **Add**.

The **Add Workgroup User** page displays (see Figure 72).

Figure 72 Add Workgroup User Page

2 Enter information about the workgroup user:

- **User Name** - Enter the name of the workgroup user.

- **Password** - Enter the password for the workgroup user.

- **Confirm Password** - Enter the password again to confirm it.

- **Description** - (Optional) Enter a brief description of the workgroup user.

- **Grant Administrator Privileges** - Select the check box to add the workgroup user to the Windows Administrators group.

This allows the workgroup user to override certain permissions settings and prevents the workgroup user from being locked out of shares or directories.

3 Click **Apply**.

After you create a workgroup user, you can grant the user access to a NAS share (see Editing a NAS Share on page 132).

Windows Domain

To add a share administrator for a Windows domain:

1 Click **Add**.

The **Add Share Administrator** page displays (see Figure 73).

Figure 73 Add Share
Administrator Page
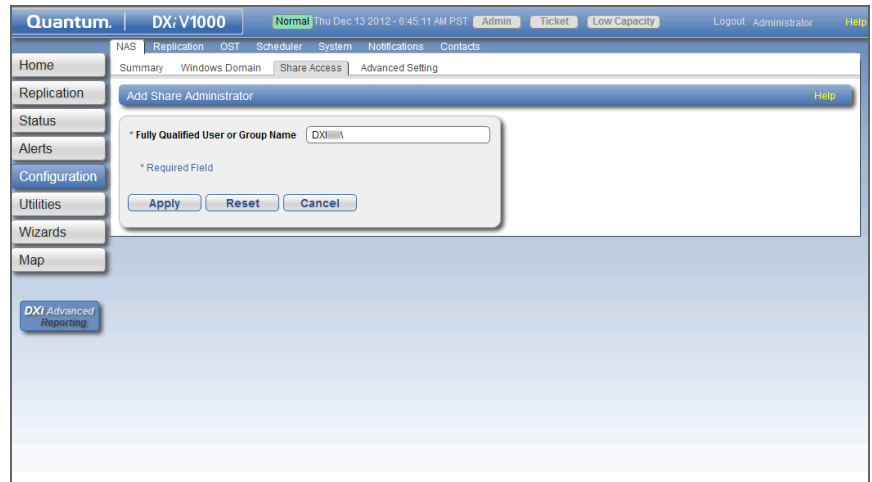
2 Enter the **Fully Qualified User or Group Name** of the share administrator.

3 Click **Apply**.

Use the MMC (Microsoft Management Console) to manage users (see ADS Share Permissions on page 143).

Editing a Workgroup User

Edit a workgroup user to change the user's password or description, or to change the user's administrator privileges.
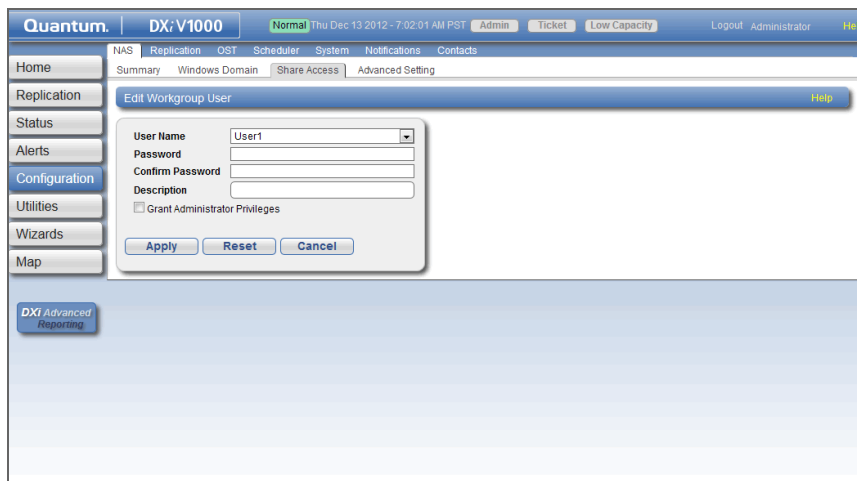
> **Note:** You cannot edit a share administrator. Instead, delete the share administrator, then add a new share administrator.

To edit a workgroup user:

1 Select the user and click **Edit**.

The **Edit Workgroup User** page displays (see Figure 74).

Figure 74 Edit Workgroup
User Page

2 Enter information about the workgroup user:

> **Note:** If you are editing a workgroup user, you cannot change the **User Name**.

- **User Name** - (Optional) Select a different workgroup user to edit.

- **Password** - Enter the password for the workgroup user.

- **Confirm Password** - Enter the password again to confirm it.

- **Description** - (Optional) Enter a brief description of the workgroup user.

- **Grant Administrator Privileges** - Select the check box to add the workgroup user to the Windows Administrators group.

This allows the workgroup user to override certain permissions settings and prevents the workgroup user from being locked out of shares or directories.

3 Click **Apply**.

Deleting a Workgroup User or Share Administrator

Delete a workgroup user or share administrator if the user or administrator no longer needs to access CIFS shares.

To delete a workgroup user or share administrator, select the user or administrator and click **Delete**.

Note: You can select multiple users or administrators to delete at once.

ADS Share Permissions

To manage user access to CIFS shares when the DXi V-Series is joined to a Windows domain, use the MMC (Microsoft Management Console). Log onto the MMC on the domain controller and access a share's properties to set share permissions for users.

Note: In some cases, when you view file permissions on a Windows system, you will not see the user and group information. Instead you will see the SID (security ID) which appears as a series of numbers. This occurs when you move files (for example, using a backup utility or DOS **xcopy**) from one system to another system, and the user and group from the source system do not exist on the target system.

Often users and groups are unique to a particular scope, such as a Windows system or an ADS domain. As a result, some assigned permissions might not be available on the target system because the associated user and group do not exist there. However, common groups (for example, **Administrators**, **Users**, and **Everyone**) are recognized on most Windows systems and domains.

Advanced Setting

The **Advanced Setting** page allows you to enable or disable advanced SMB settings.

To access the **Advanced Setting** page, on the **NAS** page, click the **Advanced Setting** tab (see Figure 75).

Figure 75 Advanced Setting Page
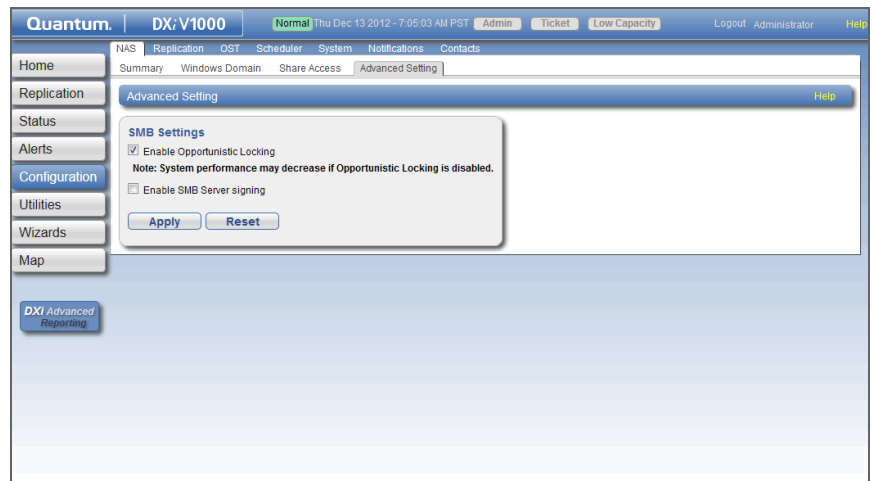
To enable or disable advanced SMB settings:

1 Select the check box to enable, or clear the check box to disable, the following settings:

• **Enable Opportunistic Locking** - (Enabled by default) Opportunistic locking lets clients lock files and locally cache information without the risk of another user changing the file. This increases performance for many file operations, but it may decrease performance in other operations because the server that grants the opportunistic lock must manage the breaking of that lock when another user requests access to the file.

Note: System performance may decrease if **Opportunistic Locking** is disabled.

• **Enable SMB Server signing** - (Disabled by default) SMB server signing improves security on Windows networks by requiring clients to provide a security signature to connect to a server. If the DXi V-Series is joined to a Windows domain that is

configured to require signing, you should enable SMB server signing.

2 Click **Apply**.

Replication

The **Replication Configuration** page allows you to configure the DXi V-Series to act as a replication source or target. A target system can *receive* data from 1 source (DXi V1000) or up to 10 sources (DXi V4000). A source system can *send* data to one target.

> **Note:** For more information about data replication, or to perform data replication, see <u>DXi V-Series Replication</u> on page 69.

To access the **Replication Configuration** page, click the **Configuration** menu, and then click the **Replication** tab.

The **Replication Configuration** page contains the following tabs:

- <u>Replication Send</u>
- <u>Replication Receive</u>

Replication Send

The **Replication Send** page allows you to specify the target system the DXi V-Series will send replicated data to. You must specify the replication target before you enable replication for a NAS share. When replication is enabled for a share, replicated data is sent to the target system during scheduled or manual replication. Optionally, you can choose to encrypt replication data or specify a constant throttle to limit the network bandwidth used for replication.

> **Note:** For more information about enabling and scheduling replication for a share, see <u>Send NAS</u> on page 77.

To access the **Replication Send** page, on the **Replication Configuration** page, click the **Send** tab (see <u>Figure 76</u>).

Figure 76 Replication Send
Page
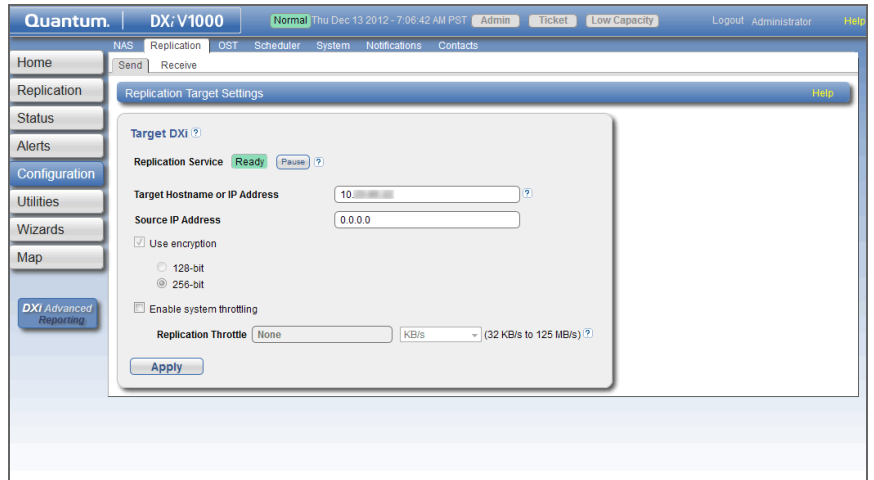
To specify the replication target:

1 If you have previously specified a replication target, you must pause
the replication service before changing the target.

Replication Service displays the replication status of the
DXi V-Series. Click **Pause** to pause replication activity. Click **Resume**
to resume replication activity.

> **Note:** For a detailed description of all possible replication
> statuses, see Replication Overview on page 62.

2 In the **Target Hostname or IP Address** box, enter the hostname or
IP address of the system that will receive the replicated data.

> **Note:** When entering IP addresses, never use an address that is in
> a reserved IP address range. To see a list of reserved IP
> address ranges, click the quick tip icon **[?]** located near the
> IP address field.

> **Note:** To use hostname format, you must specify at least one DNS
> IP address on the **Network** page (see Network on
> page 193).

3 In the **Source IP Address** field, enter the IP address that is used to uniquely identify the source DXi to the target. This may be different than the actual network IP address of the source DXi.

If the target system is at DXi 2.1 Software or higher, the **Source IP Address** field is not required. If the target system is at DXi 2.0.1.x Software or below, then you must enter the IP address by which the target system recognizes the source system. The default value is **0.0.0.0**.

> **Note:** The **Source IP Address** field does not accept fully qualified domain names. You must enter a valid IP address. Make sure this IP address is configured in the allowable sources list on the target DXi.

> **Note:** When configuring segmented network interfaces, if the source DXi replication, data, and management interfaces are on the same subnet, you must add a host route on the source DXi to make sure the replication interface is correctly selected when replicating data to the target DXi (see Understanding Interface Routing on page 206).

4 (Optional) Leave the **Use Encryption** check box selected to enable encryption when sending replication data to the target system. Or clear the **Use Encryption** check box to disable encryption when sending replication data to the target system.

If encryption is enabled, select an encryption strength (**128-bit** or **256-bit**). Using 256-bit encryption (default) provides a stronger level of security but may have an impact on system performance in some situations.

> **Caution:** Select 128-bit encryption if you are sending data to a DXi running a system software version prior to DXi 2.1 Software.

> **Note:** Encryption is enabled by default. However, for best performance, if your data network is already secured, you should clear the **Use Encryption** check box.

5 (Optional) Select the **Enable system throttling** check box to enable a constant replication throttle for the system. Or clear the **Enable**

system throttling check box to disable the constant replication throttle.

When a constant throttle is enabled, the DXi limits the amount of data it sends during source replication so that it does not exceed the specified bandwidth.

Specify the maximum allowed bandwidth by entering a value in the **Replication Throttle** box and select the units in the drop-down box (**KB/s** or **MB/s**). The lowest value you can set is 32 KB/s. The highest value you can set is 125 MB/s.

> **Caution:** Do not set the maximum allowed bandwidth to a value that is lower than necessary. If the maximum allowed bandwidth is set to the lowest value, large replication jobs may fail.

> **Note:** To vary the replication throttle rate over time, use the **Configuration > Scheduler** page (see Scheduler on page 181). Do *not* enable a constant throttle if a throttle schedule is configured. The scheduled replication throttling bandwidth settings take precedence over the constant throttle value. (The currently active replication throttle rate appears on the **Home** page under **Current Activity**.)

6 Click **Apply**.

7 If necessary, click **Resume** to resume the replication service.

Replication Receive

The **Replication Receive** page allows you to specify the source system the DXi V-Series will receive replicated data from. You must add a source system to the list of allowed replication sources before you configure the source to send replicated data to the DXi V-Series. The DXi V-Series can receive replicated data from 1 source (DXi V1000) or up to 10 sources (DXi V4000). You can also specify the number of received snapshots that are retained for each source.

> **Note:** For more information about working with received snapshots, see Receive NAS on page 85.

> **Note:** It is typical for the target DXi to require additional disk space for replication data compared to the source DXi. This is because complete replication data is sent to the target before old data is deleted. For optimal performance, if the DXi is a replication target, Quantum recommends keeping the amount of free space at 20% or more (see <u>Disk Usage</u> on page 107).

To access the **Replication Receive** page, on the **Replication Configuration** page, click the **Receive** tab (see <u>Figure 77</u>).

Figure 77 Replication Receive Page
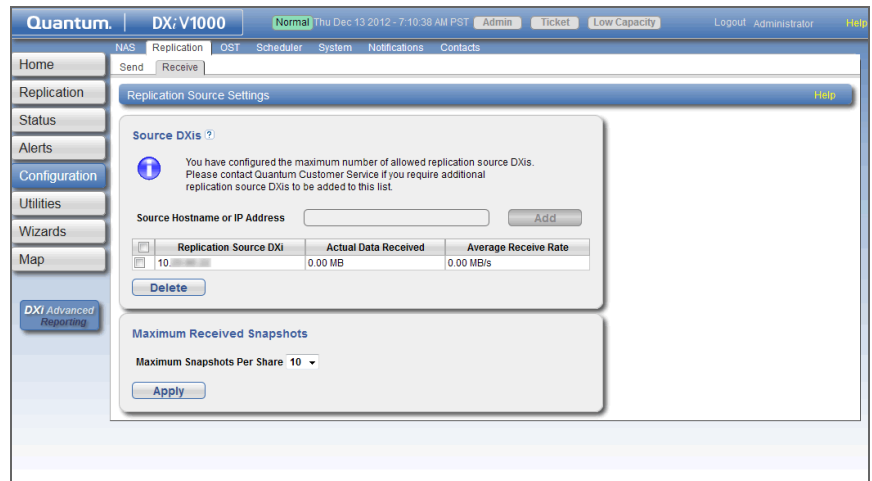
Use the **Replication Receive** page to perform the following tasks:

- View information about allowed replication source systems (see <u>Source DXis</u> on page 150).

- Add a system to the list of allowed replication sources (see <u>Adding a Replication Source</u> on page 150).

- Delete a system from the list of allowed replication sources (see <u>Deleting a Replication Source</u> on page 150).

- Specify the maximum number of received snapshots to retain for each source (see <u>Maximum Received Snapshots</u> on page 151).

Source DXis

The **Replication Receive** page displays the following information for each source DXi:

- **Replication Source DXi** - The IP address of the source system that is allowed to send data to the DXi V-Series.

- **Actual Data Received** - The amount of data actually received over the network during replication or failback.

- **Average Receive Rate** - The average receive rate (in MB/s) of data received over the network during replication or failback (**Actual Data Received** divided by the amount of time required to complete replication or failback).

Note: The statistics on the **Replication Receive** page are for each source DXi rather than a cumulative total for all sources as is displayed on the **Home** page.

Adding a Replication Source

Add a system to the list of replication sources to allow it to send replicated data to the DXi V-Series. You can specify 1 replication source (DXi V1000) or up to 10 replication sources (DXi V4000).

To add a replication source:

1 In the **Source Hostname or IP Address** box, enter the hostname or IP address of the system that will send the replicated data to the DXi V-Series.

Note: To use hostname format, you must specify at least one DNS IP address on the **Network** page (see).

2 Click **Add**.

Deleting a Replication Source

Delete a system from the list of replication sources if it will no longer send replicated data to the DXi V-Series. After the source system is deleted, the DXi V-Series will no longer accept replicated data from that system.

To delete a replication source:

1 Select the system in the **Source DXis** list.

2 Click **Delete**.

Note: If a source DXi is deleted from the list, its contribution to the
cumulative totals on the **Home** page are not removed until you
clear **Receive** statistics (see Replication Performance on
page 100).

Maximum Received Snapshots

During scheduled or manual data replication, the DXi V-Series receives a
snapshot from the source system. A snapshot contains all of the data
necessary to fully recover or failback a NAS share to the point in time
when the snapshot was saved.

The DXi V-Series can retain up to 24 snapshots for each replicated share.
Once the maximum number of snapshots have been saved, the oldest
snapshot is deleted to make room for each new snapshot that is
received.

To configure the maximum number of received snapshots:

1 In the **Maximum Snapshots Per Share** drop-down box, select the
number of snapshots to retain for each replicated share.

The default value is 10. The maximum value is 24.

2 Click **Apply**.

OST

The **OST** page allows you to configure the DXi V-Series to present its
storage capacity as storage servers using OpenStorage (OST)
technology. You can add one or more Logical Storage Units (LSUs) to a
storage server. Storage servers and LSUs are compatible with backup
applications that support OST, such as Symantec NetBackup and
Symantec Backup Exec. In addition, OST data can be duplicated
(replicated) between DXi systems using NetBackup (see Replicating OST

Data on page 152).

To authenticate OST devices on a media server, you must create OST user credentials. After you create the OST user credentials, enter them in the backup application to authenticate OST devices on the media server.

To access the **OST** page, click the **Configuration** menu, and then click the **OST** tab.

The **OST** page contains the following tabs:

- Storage Servers
- LSU
- Manage Users
- Manage Remote Users
- Target IP Mapping
- DXi Accent
- OST Client Plug-In

Replicating OST Data

The DXi V-Series can replicate (duplicate) OST data to another DXi using the following methods:

- **Optimized Duplication** - With optimized duplication, backup images on a storage server can be replicated to another storage server on a DXi that resides in the same NetBackup domain. The duplication occurs when it is initiated in NetBackup.

- **Automatic Image Replication (AIR)** - If you are using Symantec NetBackup 7.1 or higher, you can configure an LSU for Automatic Image Replication (see Task Overview: Setting Up Automatic Image Replication on page 153). If enabled, data on an LSU is automatically replicated to a remote LSU that resides on a DXi in a different NetBackup domain. The timing of the duplication, as well as the backup images that are duplicated, are determined by the storage lifecycle policies (SLPs) configured in NetBackup.

- **Concurrent Optimized Duplication** - For both optimized duplication and Automatic Image Replication, you can optionally enable Concurrent Optimized Duplication. If enabled, as data is written to the storage server, it is simultaneously replicated to the target DXi. When optimized duplication or Automatic Image Replication subsequently occurs, the operation is more efficient

because a portion of the required data has already been replicated to the target storage server.

It is important to remember that, with Automatic Image Replication, the local and remote LSUs reside in *different* NetBackup domains. This differs from optimized duplication, which occurs between two LSUs residing within *the same* NetBackup domain.

Note: For more information about configuring the DXi V-Series for optimized duplication or Automatic Image Replication, see the *DXi-Series NetBackup and Backup Exec OST Configuration Guide* (6-67079).

Note: For information about configuring NetBackup for optimized duplication or Automatic Image Replication (also referred to as duplicating images to a remote master server domain), see the *Symantec NetBackup Administrator's Guide*.

Task Overview: Setting Up Automatic Image Replication

Setting up Automatic Image Replication (AIR) requires that you first configure the target (remote) DXi and then the source DXi (see [Figure 78](#)). In addition, you must create storage lifecycle policies (SLPs) in NetBackup that define when the automatic replication occurs and which backup images are duplicated.

To automatically replicate (duplicate) all data on an LSU to a remote LSU that resides on a DXi in a different NetBackup domain:

1 On the target system, add the source system to the list of allowed replication sources (see [Replication Receive](#) on page 148).

2 On the target system, create a local OST user (see [Manage Users](#) on page 169).

Caution: On the target system, make sure to create a *local* user on the **Configuration > OST > Manage Users** page.

---

3 On the target system, create a storage server and LSU to receive the replicated OST data (see [Adding a Storage Server](#) on page 157).

> **Note:** Quantum recommends selecting the **Available Capacity** option when creating an LSU for use with Automatic Image Replication.

4 On the source system, specify the target system that will receive the replicated data (see Replication Send on page 145).

5 On the source system, create a remote OST user with the same user name and password that you used in step 2 above (see Manage Remote Users on page 172).

> **Caution:** On the source system, make sure to create a *remote* user on the **Configuration > OST > Manage Remote Users** page.

6 On the source system, create a storage server and LSU, and enable the LSU for Automatic Image Replication (see Adding a Storage Server on page 157).

For **Remote Storage Server** and **Remote LSU**, make sure to specify the storage server and LSU created in step 3 above. Also, for **Remote User**, make sure to select the remote user created in step 5 above.

7 Configure storage lifecycle policies in NetBackup to control when automatic replication of the LSU occurs (see the *Symantec NetBackup Administrator's Guide*).

Figure 78 Setting Up OST
Automatic Image Replication

1 Configure target DXi:

- Add allowed replication source.

- Create *local* OST user.

- Create storage server and LSU.

Domain 1

Local LSU
(Source DXi)

NetBackup
Server

Domain 2

Remote LSU
(Target DXi)

NetBackup
Server

2 Configure source DXi:

- Specify replication target.

- Create *remote* OST user.

- Create storage server and LSU with AIR enabled.

3 Create storage lifecycle policies (SLPs) on the NetBackup server in each domain to control when duplication occurs and images are imported.

Storage Servers

The **Storage Servers** page allows you to manage OST storage servers on the DXi V-Series. You can view information about existing storage servers, add or edit storage servers, and delete storage servers.

To access the **Storage Servers** page, on the **OST** page, click the **Storage Servers** tab (see Figure 79).

Figure 79 Storage Servers Page
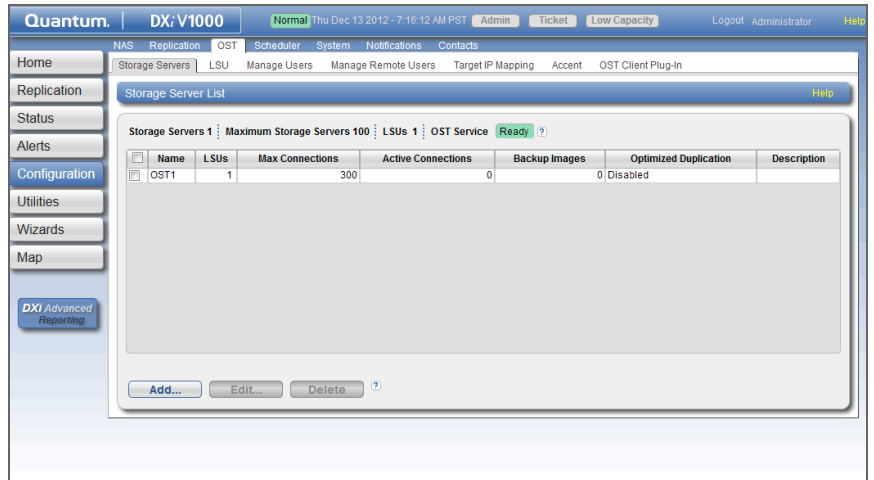
Use the **Storage Servers** page to perform the following tasks:

- View information about existing storage servers (see Storage Server List on page 156).

- Add a new storage server to the system (see Adding a Storage Server on page 157).

- Edit properties for an existing storage server (see Editing a Storage Server on page 161).

- Delete a storage server from the system (see Deleting a Storage Server on page 162).

Storage Server List

The **Storage Server List** displays the following information for all storage servers on the DXi V-Series:

- **Storage Servers** - The number of storage servers that have been added to the system.

- **Maximum Storage Servers** - The maximum number of storage servers that can be added to the system.

- **LSUs** - The number of logical storage units (LSUs) that have been added to the system (see LSU on page 163).

- **OST Service** - The status of the OST service. OST settings can be configured in **Ready**, **Stopped**, or **Verifying** state. The OST server is available for backup only in **Ready** state.

- **Name** - The name of the storage server.

- **LSUs** - The number of LSUs that have been added to the storage server.

- **Max Connections** - The maximum number of connections allowed to the storage server.

- **Active Connections** - The number of currently active connections to the storage server.

- **Backup Images** - The number of backup images on the storage server.

- **Optimized Duplication** - That status of Concurrent Optimized Duplication for the storage server (**Enabled** or **Disabled**).

- **Description** - A brief description of the storage server (if available).

Note: Click a column heading to sort the rows in the table by that column. Click the column heading again to reverse the sort order.

Note: The connections of a storage server that are used equals the data streams plus one for each LSU polling. A backup job may generate more than one data stream if the data can be read in parallel. For example, a policy that is backing up A, B, C, and D drives of a Windows system can generate four data streams in parallel.

Adding a Storage Server

Add a storage server to present the storage capacity of the DXi V-Series as LSUs that are compatible with backup applications that support OST. You can add up to 100 storage servers. When adding a storage server, you must also add an LSU to the storage server. (For more information about LSUs, see LSU on page 163.)

Note: Data on storage servers is always deduplicated.

To add a storage server:

1 Click **Add**.

The **Add Storage Server** page displays (see Figure 80).

Figure 80 Add Storage Server
Page
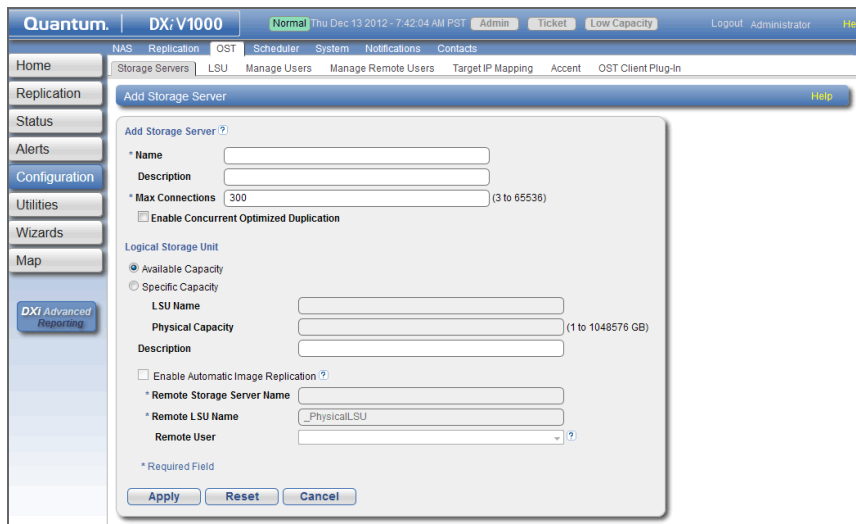
2 Under **Add Storage Server**, enter information about the storage server:

- **Name** - Enter the name of the storage server.

Caution:	Do not use an underscore (_) in the name of the storage server.

- **Description** - (Optional) Enter a brief description of the storage server.

- **Max Connections** - Enter the maximum number of connections allowed to the storage server (3 to 65536).

Note:	Quantum recommends setting **Max Connections** to 300.

- **Enable Concurrent Optimized Duplication** - Select the check box to enable optimized duplication during OST ingest.

  Concurrent Optimized Duplication is disabled by default. If enabled, as data is written to the storage server, it is

simultaneously replicated to the target DXi. When optimized duplication or Automatic Image Replication subsequently occurs, the operation is more efficient because a portion of the required data has already been replicated to the target storage server.

> **Note:** To configure the target DXi, see [Replication Send](#) on page 145.

> **Note:** When Concurrent Optimized Duplication is enabled, all data on the storage server is duplicated, not just the specified images.

3 Under **Logical Storage Unit**, select the type of LSU to add to the new storage server:

- **Available Capacity** - (Recommended for best performance) Select this option to add an LSU that uses the available capacity on the system.

  You cannot add an available capacity LSU to a storage server that already contains an LSU. Also, if you add an available capacity LSU to a storage server, you cannot add additional LSUs to that same storage server.

  > **Note:** After you add an LSU that uses the **Available Capacity** option, you cannot change the LSU to use the **Specific Capacity** option. Instead, you must delete the LSU, then add a new LSU and choose the **Specific Capacity** option (see [Deleting an LSU](#) on page 169).

- **Specific Capacity** - Select this option to specify the physical capacity of the LSU, and then enter the following information.

  - **LSU Name** - Enter the name of the LSU.

  - **Physical Capacity** - Enter the physical capacity of the LSU (1 to 1048576 GB).

    > **Note:** Quantum recommends setting LSUs to maximum size (1048576 GB) because spanning them on a backup is not possible.

4 (Optional) In the **Description** box, enter a brief description of the LSU.

5 (Optional) Select the **Enable Automatic Image Replication** check box to automatically replicate (duplicate) data on the LSU to a remote LSU on another DXi.

Automatic Image Replication (AIR) is disabled by default. If enabled, data on an LSU is automatically replicated to a remote LSU that resides on a DXi in a different NetBackup domain. The timing of the duplication, as well as the backup images that are duplicated, are determined by the storage lifecycle policies (SLPs) configured in NetBackup.

OST AIR requires NetBackup 7.1 or higher. For information about configuring NetBackup for Automatic Image Replication, see the *DXi-Series Symantec NetBackup OST Configuration Guide* (6-67079).

Note: You must configure at least one remote user before you can enable Automatic Image Replication (see Manage Remote Users on page 172).

If Automatic Image Replication is enabled, specify the following information:

- **Remote Storage Server Name** - The name of the remote storage server (on the target DXi) to replicate data to. The source DXi and target DXi must reside in different NetBackup domains.

    Note: To configure the target DXi, see Replication Send on page 145.

- **Remote LSU Name** - The name of the LSU in the remote storage server that will receive the replicated data.

- **Remote User** - The OST user credentials to use for authentication on the remote (target) DXi. The selected remote user *must* match a local user on the **Configuration > OST > Manage Users** page on the target DXi (see Manage Users on page 169).

6 Click **Apply**.

Editing a Storage Server

Edit a storage server to change the description of the storage server or the maximum number of allowed connections.

To edit a storage server:

1 Select the storage server and click **Edit**.

The **Edit Storage Server** page displays (see Figure 81).

Figure 81 Edit Storage Server Page
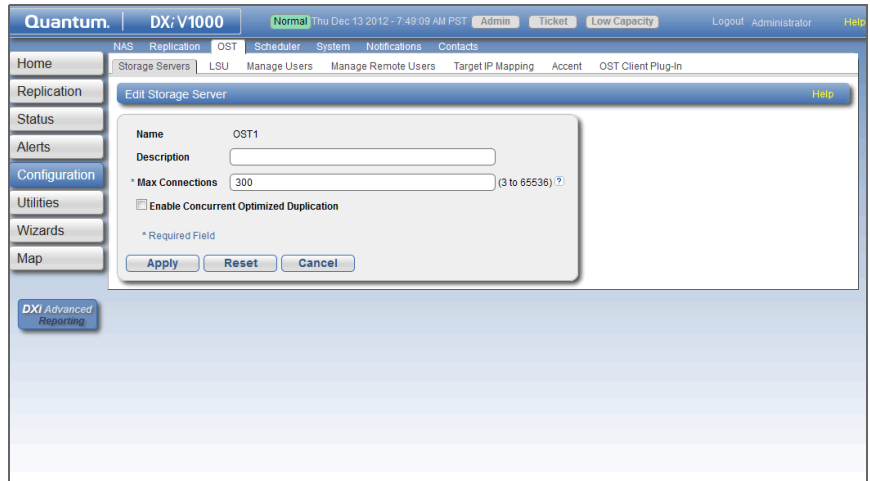
2 Enter information about the storage server:

Note: If you are editing a storage server, the **Name** option cannot be changed.

• **Description** - (Optional) Enter a brief description of the storage server.

• **Max Connections** - Enter the maximum number of connections allowed to the storage server (3 to 65536).

The maximum number of connections cannot be changed if the storage server has more than zero currently active connections. The number of active connections is displayed on the **OST** page (see Storage Server List on page 156).

> **Note:** Quantum recommends setting **Max Connections** to 300.

- **Enable Concurrent Optimized Duplication** - Select the check box to enable optimized duplication during OST ingest.

  Concurrent Optimized Duplication is disabled by default. If enabled, as data is written to the storage server, it is simultaneously replicated to the target DXi. When optimized duplication or Automatic Image Replication subsequently occurs, the operation is more efficient because a portion of the required data has already been replicated to the target storage server.

  > **Note:** To configure the target DXi, see Replication Send on page 145.

  > **Note:** When Concurrent Optimized Duplication is enabled, all data on the storage server is duplicated, not just the specified images.

3 Click **Apply**.

Deleting a Storage Server

Delete a storage server if it is no longer needed. When you delete a storage server, all data stored on the storage server is lost.

> **Note:** If you deleted the storage server from Symantec NetBackup or Symantec Backup Exec, you must wait several minutes before deleting the storage server from the DXi V-Series.

To delete a storage server:

1 Select the storage server in the **Storage Server List**.

You cannot delete a storage server if it has more than zero currently active connections. The number of active connections is displayed on the **OST** page (see Storage Server List on page 156). Also, you cannot delete a storage server if it contains LSUs. Before deleting the storage server, you must first delete any LSUs it contains (see Deleting an LSU on page 169).

> **Note:** You can select multiple storage servers to delete at once.

---

2 Click **Delete**.

LSU

The **LSU** page allows you to manage the logical storage units (LSUs) contained on OST storage servers on the DXi V-Series. You can view information about existing LSUs, add or edit LSUs, and delete LSUs.

To access the **LSU** page, on the **OST** page, click the **LSU** tab (see Figure 82).

Figure 82 LSU Page
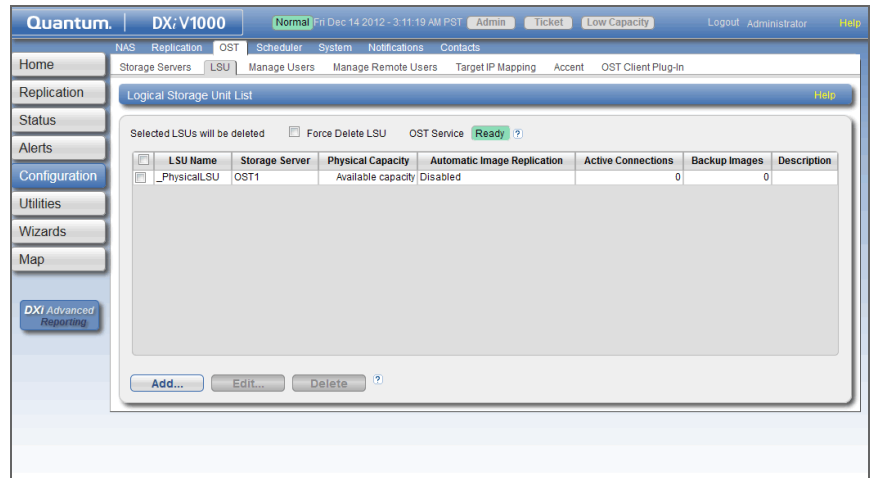
Use the **LSU** page to perform the following tasks:

- View information about existing LSUs (see Logical Storage Unit List on page 164).

- Add a new LSU to the system (see Adding an LSU on page 164).

- Edit properties for an existing LSU (see Editing an LSU on page 167).

- Delete an LSU from the system (see Deleting an LSU on page 169).

Logical Storage Unit List

The **Logical Storage Unit List** displays the following information for all LSUs on the DXi V-Series:

- **OST Service** - The status of the OST service. OST settings can be configured in **Ready**, **Stopped**, or **Verifying** state. The OST server is available for backup only in **Ready** state.

- **LSU Name** - The name of the LSU.

- **Storage Server** - The storage server that contains the LSU.

- **Physical Capacity** - The physical storage capacity of the LSU.

- **Automatic Image Replication** - That status of Automatic Image Replication (AIR) for the LSU (**Enabled** or **Disabled**).

  Note: To view details about the remote LSU if AIR is enabled, use the **Edit Logical Storage Unit** page (see Editing an LSU on page 167).

- **Active Connections** - The number of currently active connections to the LSU.

- **Backup Images** - The number of backup images on the LSU.

- **Description** - A brief description of the LSU (if available).

Note: Click a column heading to sort the rows in the table by that column. Click the column heading again to reverse the sort order.

Adding an LSU

Add an LSU to a storage server to present the storage capacity of the DXi V-Series as an LSU that is compatible with backup applications that support OST. You can add an LSU with a specific capacity, or you can add an LSU that uses the available capacity of the DXi V-Series.

Note: You must create a storage server before you can add an LSU (see Adding a Storage Server on page 157).

To add an LSU to a storage server:

1 Click **Add**.

The **Add Logical Storage Unit** page displays (see Figure 83).

Figure 83 Add Logical Storage Unit Page
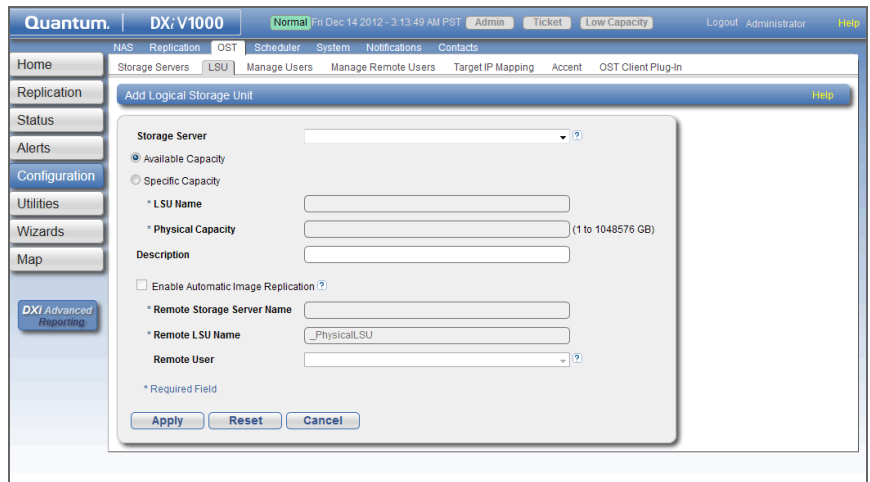
2 Enter information about the LSU.

- **Storage Server** - Select the storage server that will contain the new LSU.

- **Available Capacity** - (Recommended for best performance) Select this option to add an LSU that uses the available capacity on the system.

  You cannot add an available capacity LSU to a storage server that already contains an LSU. Also, if you add an available capacity LSU to a storage server, you cannot add additional LSUs to that same storage server.

  > **Note:** After you add an LSU that uses the **Available Capacity** option, you cannot change the LSU to use the **Specific Capacity** option. Instead, you must delete the LSU, then add a new LSU and choose the **Specific Capacity** option (see Deleting an LSU on page 169).

- **Specific Capacity** - Select this option to specify the physical capacity of the LSU, and then enter the following information.

  - **LSU Name** - Enter the name of the LSU.

> • **Physical Capacity** - Enter the physical capacity of the LSU (1 to 1048576 GB).

> **Note:** Quantum recommends setting LSUs to maximum size (1048576 GB) because spanning them on a backup is not possible.

3 (Optional) In the **Description** box, enter a brief description of the LSU.

4 (Optional) Select the **Enable Automatic Image Replication** check box to automatically replicate (duplicate) data on the LSU to a remote LSU on another DXi.

Automatic Image Replication (AIR) is disabled by default. If enabled, data on an LSU is automatically replicated to a remote LSU that resides on a DXi in a different NetBackup domain. The timing of the duplication, as well as the backup images that are duplicated, are determined by the storage lifecycle policies (SLPs) configured in NetBackup.

OST AIR requires NetBackup 7.1 or higher. For information about configuring NetBackup for Automatic Image Replication, see the *DXi-Series Symantec NetBackup OST Configuration Guide* (6-67079).

> **Note:** You must configure at least one remote user before you can enable Automatic Image Replication (see Manage Remote Users on page 172).

If Automatic Image Replication is enabled, specify the following information:

• **Remote Storage Server Name** - The name of the remote storage server (on the target DXi) to replicate data to. The source DXi and target DXi must reside in different NetBackup domains.

> **Note:** To configure the target DXi, see Replication Send on page 145.

• **Remote LSU Name** - The name of the LSU in the remote storage server that will receive the replicated data.

• **Remote User** - The OST user credentials to use for authentication on the remote (target) DXi. The selected remote

user *must* match a local user on the **Configuration > OST > Manage Users** page on the target DXi (see Manage Users on page 169).

5 Click **Apply**.

Editing an LSU

Edit an LSU to change the description of the storage server or the maximum number of allowed connections.

To edit an LSU:

1 Select the LSU and click **Edit**.

The **Edit Logical Storage Unit** page displays (see Figure 84).

2 Enter information about the LSU:

> **Note:** If you are editing an LSU, the **Name** option cannot be changed.

• **Physical Capacity** - (Specific capacity LSUs only) Enter the physical capacity of the LSU (1 to 1048576 GB).

The physical capacity cannot be changed if the LSU has more than zero currently active connections. The number of active connections is displayed on the **LSU** page (see Logical Storage

Unit List on page 164).

- **Description** - (Optional) Enter a brief description of the LSU.

3 (Optional) Select the **Enable Automatic Image Replication** check box to automatically replicate (duplicate) data on the LSU to a remote LSU on another DXi.

Automatic Image Replication (AIR) is disabled by default. If enabled, data on an LSU is automatically replicated to a remote LSU that resides on a DXi in a different NetBackup domain. The timing of the duplication, as well as the backup images that are duplicated, are determined by the storage lifecycle policies (SLPs) configured in NetBackup.

OST AIR requires NetBackup 7.1 or higher. For information about configuring NetBackup for Automatic Image Replication, see the *DXi-Series Symantec NetBackup OST Configuration Guide* (6-67079).

Note: You must configure at least one remote user before you can enable Automatic Image Replication (see Manage Remote Users on page 172).

If Automatic Image Replication is enabled, specify the following information:

- **Remote Storage Server Name** - The name of the remote storage server (on the target DXi) to replicate data to. The source DXi and target DXi must reside in different NetBackup domains.

  Note: To configure the target DXi, see Replication Send on page 145.

- **Remote LSU Name** - The name of the LSU in the remote storage server that will receive the replicated data.

- **Remote User** - The OST user credentials to use for authentication on the remote (target) DXi. The selected remote user *must* match a local user on the **Configuration > OST > Manage Users** page on the target DXi (see Manage Users on page 169).

4 Click **Apply**.

Deleting an LSU

Delete an LSU if it is no longer needed. When you delete an LSU, all data stored on the LSU is lost.

> **Note:** If you deleted the LSU from Symantec NetBackup or Symantec Backup Exec, you must wait several minutes before deleting the LSU from the DXi V-Series.

To delete an LSU:

1 Select the LSU in the **Logical Storage Unit List**.

You cannot delete an LSU if it has more than zero currently active connections. The number of active connections is displayed on the **LSU** page (see Logical Storage Unit List on page 164).

> **Note:** You can select multiple LSUs to delete at once.

2 (Optional) Select the **Force Delete LSU** check box to delete LSUs that are not empty.

Normally, you cannot delete an LSU if it contains existing backup images. If for some reason you cannot remove files from the LSU, selecting the **Force Delete LSU** check box allows you to delete the LSU even though it is not empty.

3 Click **Delete**.

Manage Users

The **Manage Users** page allows you to create and manage local authenticated users for use with OST. After you create the OST user credentials, enter them in the backup application to authenticate OST devices on the media server. When using OST Automatic Image Replication (AIR), the remote user credentials specified on the source DXi must match the local user credentials on the target (remote) DXi.

To access the **Manage Users** page, on the **OST** page, click the **Manage Users** tab (see Figure 85).

Figure 85 Manage Users Page
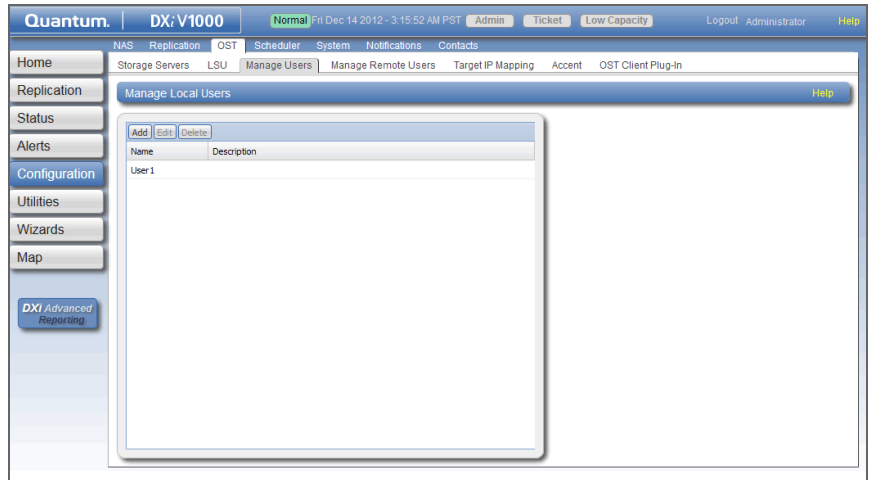
Use the **Manage Users** page to perform the following tasks:

- View information about local authenticated users (see Manage Local Users List on page 170).

- Add a local authenticated user (see Adding an Authenticated User on page 170).

- Edit a local authenticated user (see Editing an Authenticated User on page 171).

- Delete a local authenticated user (see Deleting an Authenticated User on page 172).

Manage Local Users List

The **Manage Local Users** list displays the following information for all local authenticated users:

- **Name** - The name of the local authenticated user.

- **Description** - A brief description of the local authenticated user (if available).

Adding an Authenticated User
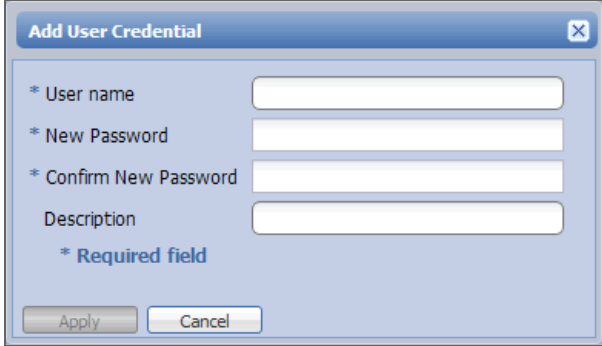
Add an authenticated user to create local OST user credentials. The OST user credentials are required to authenticate OST devices on a media server, or to enable the DXi to receive duplicated data using OST AIR.

To add an authenticated user:

1 Click **Add**.

The **Add User Credential** window displays (see Figure 86).

2 Enter information about the authenticated user:

- **User name** - Enter the name of the authenticated user.

- **New Password** - Enter the password for the authenticated user.

- **Confirm New Password** - Enter the password again to confirm it.

- **Description** - (Optional) Enter a brief description of the authenticated user.

3 Click **Apply**.

Editing an Authenticated User

Edit an authenticated user to change the user's password or description.

To edit an authenticated user:

1 Select the user and click **Edit**.

The **Edit User Credentials** window displays (see Figure 87).

Figure 87 Edit User Credentials

2 Enter information about the authenticated user:

> **Note:** If you are editing an authenticated user, you cannot change the **User name**.

- **New Password** - Enter the password for the authenticated user.
- **Confirm New Password** - Enter the password again to confirm it.
- **Description** - (Optional) Enter a brief description of the authenticated user.

3 Click **Apply**.

Deleting an Authenticated User

Delete an authenticated user if the OST user credentials are no longer needed to authenticate OST devices on a media server.

To delete an authenticated user, select the user and click **Delete**.

> **Note:** You can select multiple users to delete at once.

Manage Remote Users

The **Manage Remote Users** page allows you to create and manage remote users for use with OST Automatic Image Replication (AIR). You must configure at least one remote user before you can enable Automatic Image Replication for an LSU (see Adding an LSU on page 164). When using OST Automatic Image Replication (AIR), the

remote user credentials specified on the source DXi must match the local user credentials on the target (remote) DXi.

To access the **Manage Remote Users** page, on the **OST** page, click the **Manage Remote Users** tab (see Figure 88).

Figure 88 Manage Remote Users Page
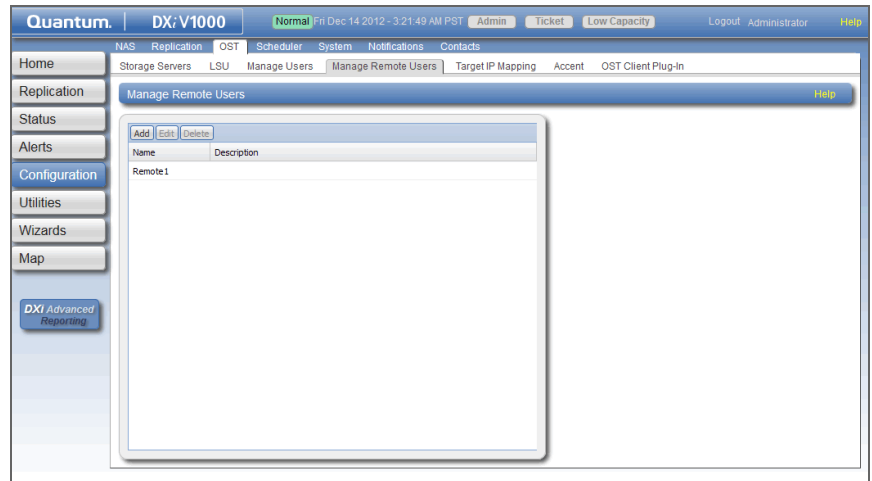
Use the **Manage Users** page to perform the following tasks:

- View information about remote users (see Manage Remote Users List on page 173).
- Add a remote user (see Adding a Remote User on page 174).
- Edit a remote user (see Editing a Remote User on page 174).
- Delete a remote user (see Deleting a Remote User on page 175).

Manage Remote Users List

The **Manage Remote Users** list displays the following information for all remote users:

- **Name** - The name of the remote user.
- **Description** - A brief description of the remote user (if available).

Adding a Remote User
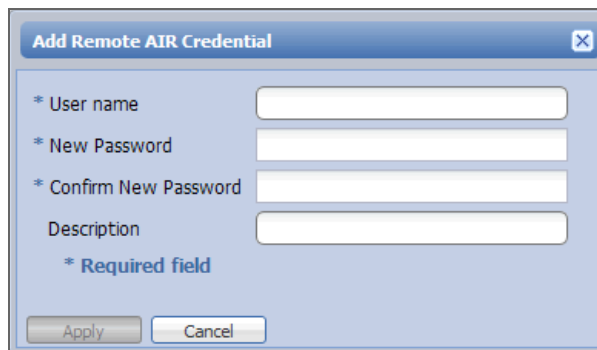
Add a remote user to create OST user credentials for use with OST AIR. When you enable Automatic Image Replication for an LSU, you specify a remote user. The remote user credentials on the source DXi must match the local user credentials on the target (remote) DXi.

To add a remote user:

1 Click **Add**.

The **Add Remote AIR Credential** window displays (see Figure 89).

Figure 89 Add Remote AIR Credential

2 Enter information about the remote user:

- **User name** - Enter the name of the remote user.
- **New Password** - Enter the password for the remote user.
- **Confirm New Password** - Enter the password again to confirm it.
- **Description** - (Optional) Enter a brief description of the remote user.

3 Click **Apply**.

Editing a Remote User
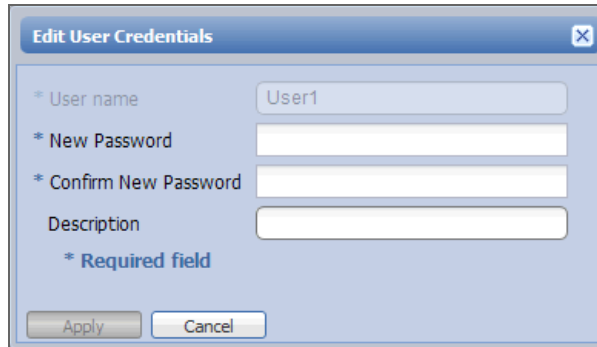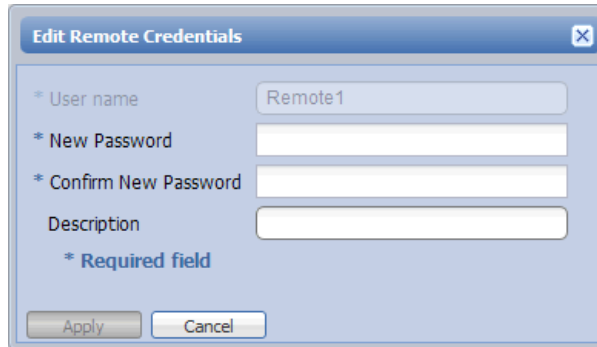
Edit a remote user to change the user's password or description.

To edit a remote user:

1 Select the user and click **Edit**.

The **Edit Remote Credentials** window displays (see Figure 90).

2 Enter information about the remote user:

> **Note:** If you are editing a remote user, you cannot change the
> **User name**.

- **New Password** - Enter the password for the remote user.
- **Confirm New Password** - Enter the password again to confirm it.
- **Description** - (Optional) Enter a brief description of the remote user.

3 Click **Apply**.

Deleting a Remote User

Delete a remote user if the OST user credentials are no longer needed to authenticate an LSU for Automatic Image Replication.

To delete a remote user, select the user and click **Delete**.

> **Note:** You can select multiple users to delete at once.

Target IP Mapping

The **Target IP Mapping** page allows you to map a target data IP address to route all network traffic sent to the data IP address to the specified replication IP address instead. This can be necessary if the target DXi is

configured with different network interfaces (and therefore different IP addresses) for data and replication traffic (see <u>Network</u> on page 193).

Generally, OST traffic is routed to the data network segment. However, the OST Automatic Image Replication (AIR) and Concurrent Optimized Duplication features use the replication network segment to transmit data to the target system. (Optimized duplication can optionally use the replication channel.) When a data IP address is mapped to a replication IP address, OST traffic that is sent to one of the IP addresses is routed to the other IP address as necessary.

Note: You must add target IP mapping information if you are performing optimized duplication on a segmented network and replication is not configured between the source DXi and target DXi.

Note: Quantum does not recommend mapping multiple data IP addresses to a single replication IP address. If you have mapped multiple data IP addresses and the routing is not working, try removing the additional data IP addresses, and map only a single data IP address.

To access the **Target IP Mapping** page, on the **OST** page, click the **Target IP Mapping** tab (see <u>Figure 91</u>).

Figure 91 Target IP Mapping Page
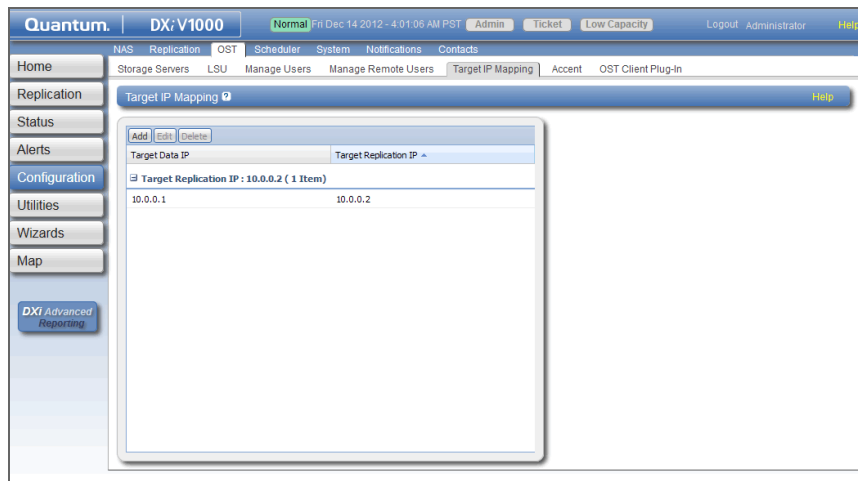
Use the **Target IP Mapping** page to perform the following tasks:

- View information about mapped data and replication IP addresses (see Target IP Mapping List on page 177).

- Map a target data IP address to a replication IP address (see Mapping a Target IP Address on page 177).

- Edit the mapping for a target data IP address (see Editing a Mapped IP Address on page 178).

- Delete the mapping for a target data IP address (see Deleting a Mapped IP Address on page 178).

Target IP Mapping List

The **Target IP Mapping** list displays the following information for all mapped IP addresses:

- **Target Data IP** - The mapped target data IP address.

- **Target Replication IP** - The replication IP address to which the data IP address is mapped.

Items in the list are grouped by target replication IP address.

Mapping a Target IP Address
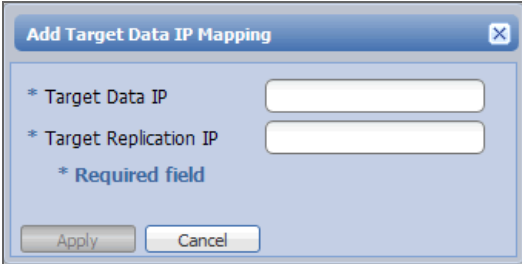
Add mapping for a target data IP address to route all network traffic sent to the address to the specified replication IP address instead.

To map a target IP address:

1 Click **Add**.

The **Add Target Data IP Mapping** window displays (see Figure 92).

Figure 92 Add Target Data IP Mapping

2 Enter information about the mapping:

- **Target Data IP** - The target data IP address to map.

- **Target Replication IP** - The replication IP address to map the data IP address to.

3 Click **Apply**.

Editing a Mapped IP Address
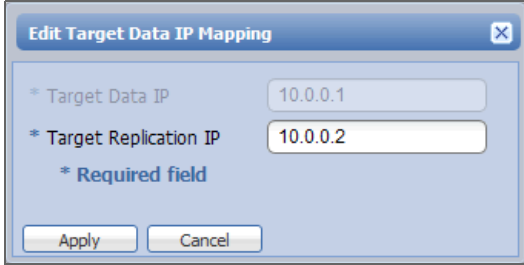
Edit a mapped IP address to route traffic sent to the target data IP address to a different replication IP address.

To edit a mapped IP address:

1 Select the mapped IP address and click **Edit**.

The **Edit Target Data IP Mapping** window displays (see Figure 93).

Figure 93 Edit Target Data IP Mapping

2 In the **Target Replication IP** box, enter the replication IP address to map the data IP address to.

> **Note:** If you are editing a mapped IP address, you cannot change the target data IP address.

3 Click **Apply**.

Deleting a Mapped IP Address

Delete a mapped IP address if traffic sent to the target data IP address no longer needs to be routed to a replication IP address

To delete a mapped IP address, select the IP address and click **Delete**.

> **Note:** You can select multiple mapped IP addresses to delete at once.

DXi Accent

Use the **Accent** page to enable or disable DXi Accent. Quantum's DXi Accent software accelerates backups and reduces network bandwidth requirements by distributing deduplication between the backup server and the DXi. OST data sent from the media server to the DXi can be encrypted using AES (Advanced Encryption Standard) encryption methods.

To access the **Accent** page, on the **OST** page, click the **Accent** tab (see Figure 85).

Figure 94 Accent Page
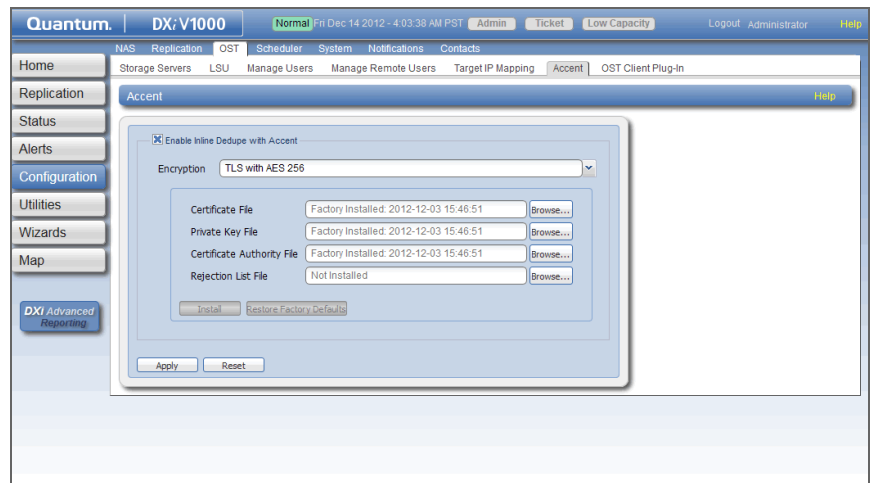
To configure DXi Accent:

1 To enable DXi Accent, select the **Enable Inline Dedupe with Accent** check box.

Or to disable DXi Accent, clear the **Enable Inline Dedupe with Accent** check box.

2 To enable or disable encryption when sending OST data from the media server to the DXi, select an option in the **Encryption** drop-down box:

- **None** - OST data is not encrypted.

- **Default AES 128** - OST data is encrypted using AES 128-bit encryption.

- **Default AES 256** - OST data is encrypted using AES 256-bit encryption.

• **TLS with AES 256** - OST data is encrypted using AES 256-bit encryption with Transport Layer Security (TLS).

Note: Using 256-bit encryption provides a stronger level of security but may have an impact on system performance in some situations.

---

3 If you selected the **TLS with AES 256** encryption option, you must install the required certificate and key files on the DXi:

• Certificate File

• Private Key File

• Certificate Authority File

• Rejection List FIle

To install a file, click the **Browse** button to browse the system and locate the file, and then click **Open**. Click **Install** to install the selected file on the DXi.

Caution: Installing certificate files requires a system reboot immediately after the changes are applied. Wait for at least 15 minutes before logging back in.

Note: You can install new certificate and key files at any time, as long as there are no active network connections between the OST media server and the DXi.

Note: To remove all certificate and key files, click **Restore Factory Defaults**.

---

4 Click **Apply**.

Note: To use DXi Accent, you must install the Quantum OST Client Plug-in on the media server. For information about installing the OST Plug-in and using DXi Accent, see the *Symantec NetBackup OST Configuration Guide* (6-67079).

OST Client Plug-In

Use the **OST Client Plug-In** page to download the Quantum OST Plug-in.

OST (OpenStorage) technology allows Symantec NetBackup and Backup Exec to seamlessly integrate with the DXi V-Series. Using OST, NetBackup and Backup Exec can manage backups through the DXi V-Series and can take advantage of the system's capabilities, such as data deduplication and replication. To use OST, you must first download the OST Plug-in and install it on the NetBackup or Backup Exec media server.

To download the OST Plug-in, click **Client Plug-in Download**. On the download page, download the correct OST Plug-in for your backup application and operating system. Also on the download page, click **Installation Instructions**, to download the *OST Plug-in Installation Instructions*. Follow the included instructions to install the OST Plug-in on your media server.

> **Note:** For information about configuring and using OST with the DXi V-Series, see the *Symantec NetBackup OST Configuration Guide* (6-67079) and the *Symantec Backup Exec OST Configuration Guide* (6-67080).

Scheduler

The **Scheduler** page allows you to manage scheduled events on the DXi V-Series, including replication and replication throttling, e-mail reports, healthchecks, and space reclamation. With schedules, you specify when certain events should occur, and the system automatically performs those events at the specified time. Events can be one-time only, or they can reoccur at defined intervals.

To access the **Scheduler** page, click the **Configuration** menu, and then click the **Scheduler** tab.

The **Scheduler** page contains the following tabs:

- Scheduler Calendar
- Scheduler NAS

Scheduler Calendar

The **Scheduler Calendar** page presents all currently scheduled events on the DXi V-Series in a calendar view. You can view events for a particular day, week, or month. You can also add, modify, and delete scheduled events.

To access the **Scheduler Calendar** page, on the **Scheduler** page, click the **Calendar** tab (see Figure 95).

Figure 95 Scheduler Calendar Page
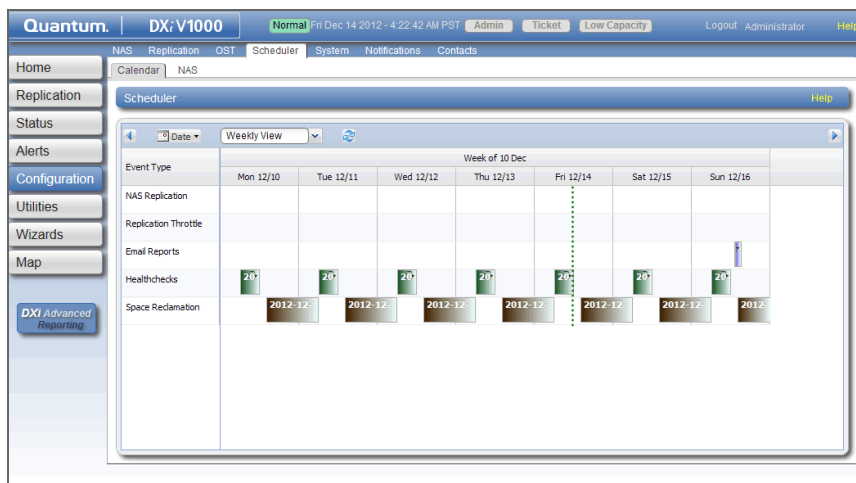
Use the **Scheduler Calendar** page to perform the following tasks:

- View currently scheduled events (see Viewing Scheduled Events on page 183).

- Add a new scheduled event or edit an existing event (see Adding or Editing a Scheduled Event on page 184).

- Configure NAS shares for scheduled replication (see Scheduling a Share for Replication on page 186).

- Configure replication throttle events (see Scheduling Replication Throttling on page 187).

- Configure the DXi V-Series to send status and configuration reports (see Scheduling E-mail Reports on page 189).

- Configure the DXi V-Series to run healthchecks (see Scheduling Healthchecks on page 189).

- Configure the DXi V-Series to run space reclamation (see Scheduling Space Reclamation on page 190).

- Specify when and how often an event reoccurs (see Setting Recurrence for a Scheduled Event on page 190).

- Remove an event occurrence or event series from the schedule (see Deleting a Scheduled Event on page 191).

Viewing Scheduled Events

The **Scheduler Calendar** page displays all replication, replication throttle, e-mail report, healthchecks, and space reclamation events scheduled to occur in a selected time period.

Use the following controls to adjust the schedule view (see Figure 95):

- To change the number of days displayed at a time, select **Daily View**, **Weekly View**, or **Monthly View** in the drop-down box at the top of the schedule view.

- To move the view backward or forward in time, click the arrows at the upper left and upper right of the schedule view.

- To view the schedule for a specific day, select it in the **Date** pop-up calendar.

- To update the schedule view with the latest data, click the **Refresh** icon.

Note: The thickness of the bars on the schedule view varies based on the type of event and the selected time frame. Healthcheck events have a span of 6 hours. Space Reclamation events have a span of 16 hours. All other open-ended events have a default span of 2 hours.

Note: If you see an error indicating there is not enough memory to complete the request, try using daily or weekly view, and use the arrows to move forward or backward in time.

Figure 96 Scheduler View
Controls

Select day

Select view

Refresh

Date ▾   Weekly View ▾   ↻

Move backward

Move forward
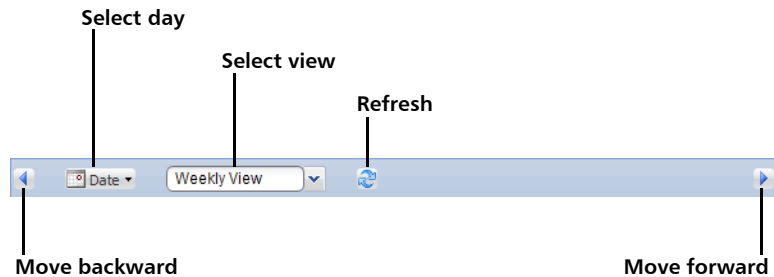
Adding or Editing a Scheduled Event

To add or edit a scheduled event:

1 On the **Scheduler Calendar** page, adjust the schedule view to
   display the time period when the event will occur (see Viewing
   Scheduled Events on page 183). Then do one of the following
   actions (see Figure 97):

   • To add a new event, click and drag on the schedule in the row
     for the type of event to add. A new event is added where you
     dragged the cursor.

     Note: The new event must begin after the current time,
     which is indicated by the dotted vertical line.

   • To edit an existing event, double-click the event. If the event is
     recurring, select **Open this occurrence** to edit only the one
     instance of the event, or select **Open the series** to edit the
     entire recurring series, and then click **OK**.

     Note: You cannot edit an event that occurred in the past.

   Note: You can also right-click an existing event to see options for
   adding a new event or editing an event.

Figure 97 Adding a New Event

Click and drag to add a new event

Double-click to edit an existing event
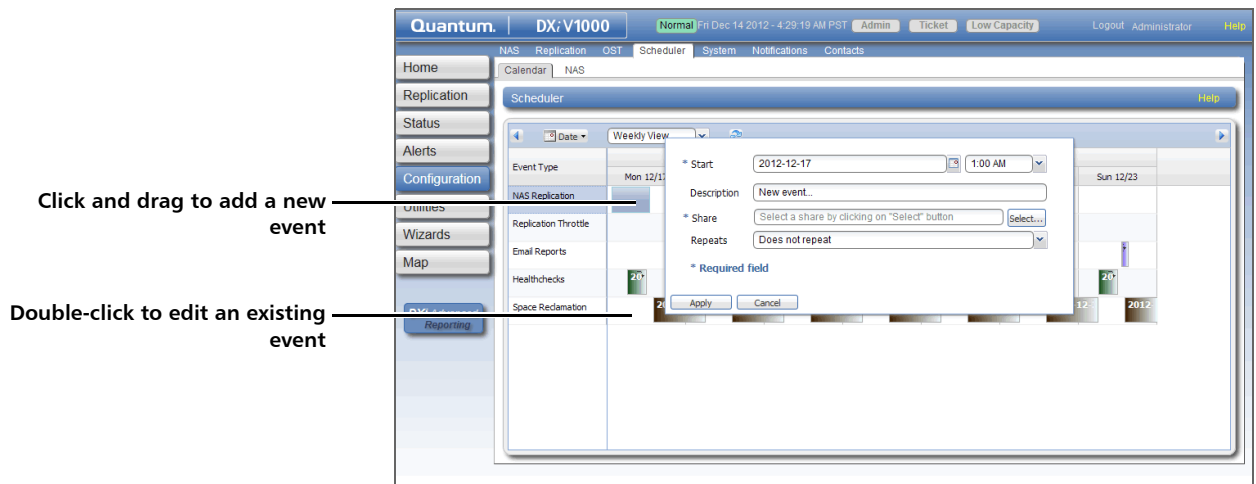
2 Define the start and, if applicable, the end of the event.

- Specify the **Start Date** and **Start Time** using the pop-up calendar and drop-down box.

- (Replication throttle events only) Specify the **End Date** and **End Time**. The end date and time must occur after the start date and time.

Note: For a new event, you can click and drag to adjust the start and end time. For an existing event, you can drag the event to change when it occurs. You can also drag the left or right edge of the event to adjust the start or end time.

---

3 Enter a brief description of the event in the **Description** box. (This description will display on the schedule view.)

4 Specify options specific to the type of event. See the following sections:

- Scheduling a Share for Replication on page 186
- Scheduling Replication Throttling on page 187
- Scheduling E-mail Reports on page 189
- Scheduling Healthchecks on page 189
- Scheduling Space Reclamation on page 190

5 (Required for healthchecks and space reclamation) Specify when and how often the event reoccurs (see Setting Recurrence for a Scheduled Event on page 190).

6 Click **Apply**.

7 Refresh the browser window to make sure the event settings are applied.

Caution: When adding multiple events of the same type, make sure the events do not overlap. If two events of the same type overlap, the later event takes precedence over the earlier event.

Scheduling a Share for Replication

Configure a replication schedule for a NAS share to automatically replicate the share data to the target system at regular intervals. Disable scheduled replication if you do not want to automatically replicate the share data to the target.

Note: For more information about configuring the DXi V-Series for replication, see DXi V-Series Replication on page 69.

Note: Disabling replication for a share does not delete any scheduled replication events for that share. If you no longer want to schedule the share for replication, manually delete the schedule (see Deleting a Scheduled Event on page 191).

To configure a replication schedule for a share:

1 On the **Scheduler Calendar** page, add or edit an event in the **NAS Replication** row (see Adding or Editing a Scheduled Event on page 184).

2 Click **Select**.

3 In the pop-up window, select the share to schedule for replication.

Only shares that are enabled for deduplication appear in the pop-up window. To filter the list, type the first few letters of the share name in the **Search** box.

> **Note:** Scheduling a share that has replication disabled will automatically enable replication.

4 Click **OK**.

5 (Optional) Specify when and how often the event reoccurs (see Setting Recurrence for a Scheduled Event on page 190).

6 Click **Apply**.

Scheduling Replication Throttling

During replication throttling, the DXi V-Series limits the amount of source replication data it sends to not exceed a specified maximum bandwidth. Schedule replication throttling to control the amount of network bandwidth used by source replication at certain times. For example, you might configure replication throttling to occur during planned backup times to avoid network contention.

> **Note:** For more information about configuring the DXi V-Series for replication, see DXi V-Series Replication on page 69.

To schedule replication throttling:

1 On the **Scheduler Calendar** page, add or edit an event in the **Replication Throttle** row (see Adding or Editing a Scheduled Event on page 184).

2 Specify the maximum allowed bandwidth by entering a value in the **Bandwidth** box and selecting the units in the drop-down box (**KB/s** or **MB/s**). The lowest value you can set is 32 KB/s. The highest value you can set is 125 MB/s.

> **Note:** Values of 1000 KB/s and higher are rounded down to the nearest whole MB/s value when the event is saved.

> **Note:** Do not enter a decimal value in the **Bandwidth** box. Instead, use whole values. For example, enter 2500 KB/s rather than 2.5 MB/s.

During the replication throttle event, the DXi will limit the amount of data it sends during source replication so that it does not exceed the specified bandwidth. After the replication throttle event ends,

the DXi will no longer throttle the sending of source replication data (until the next replication throttle event occurs).

> **Caution:** Do not set the maximum allowed bandwidth to a value that is lower than necessary. If the maximum allowed bandwidth is set to the lowest value, large replication jobs may fail.

> **Note:** To set a constant replication throttle, use the **Configuration > Replication > Send** page (see Replication Send on page 145). Do *not* configure a throttle schedule if a constant throttle is enabled. The scheduled replication throttling bandwidth settings take precedence over the constant throttle value. (The currently active replication throttle rate appears on the **Home** page under **Current Activity**.)

3 (Optional) Specify when and how often the event reoccurs (see Setting Recurrence for a Scheduled Event on page 190).

4 Click **Apply**.

About Replication Throttling Statistics

Keep in mind the following information when observing actual network bandwidth usage during a replication throttle event:

- During a replication throttle event, only outgoing replication data traffic is throttled, not other outgoing traffic. Because of this, you may observe network usage to be higher than the specified maximum bandwidth. Differences in the sampling time period may also cause discrepancies between the specified maximum bandwidth and observed traffic.

- If the DXi is configured to use a bonded network interface for replication traffic, load balancing is determined independently by the bonding mode selected for the interface (see Network on page 193). Because of this, you may need to sum the values for all slave devices in the bonded interface to calculate the overall outgoing traffic rate.

- The replication throttle bandwidth maximum is specified in KB/s or MB/s, so depending on the statistic or report you are observing, you

may need to convert the bandwidth maximum to Kb/s or Mb/s in order to correctly compare it to the observed values.

Scheduling E-mail Reports

The DXi V-Series can automatically generate a report with system status data or with configuration data and send it to all configured e-mail recipients.

> **Note:** For more information about e-mail reports and configuring e-mail recipients, see Email Reports on page 229.

To configure a schedule for e-mail reports:

1 On the **Scheduler Calendar** page, add or edit an event in the **Email Reports** row (see Adding or Editing a Scheduled Event on page 184).

2 In the **Report Type** drop-down box, select the type of e-mail report to schedule (**Status** or **Configuration**).

3 (Optional) Specify when and how often the event reoccurs (see Setting Recurrence for a Scheduled Event on page 190).

4 Click **Apply**.

Scheduling Healthchecks

During healthchecks, the DXi V-Series performs tests to verify the health and integrity of the data deduplication blockpool. Schedule healthchecks regularly to make sure the system is healthy and operating correctly. When you schedule healthchecks, only the healthchecks that are currently enabled are run.

> **Note:** For more information about enabling healthchecks, see Healthchecks on page 249.

To configure a schedule for healthchecks:

1 On the **Scheduler Calendar** page, add or edit an event in the **Healthchecks** row (see Adding or Editing a Scheduled Event on page 184).

2 Specify when and how often the event reoccurs (see Setting Recurrence for a Scheduled Event on page 190).

> **Caution:** For correct system operation, healthchecks *must* be run at regular intervals (at least once a week).You can schedule healthchecks to occur daily or weekly but not monthly or yearly. Also, recurrence is required.

3 Click **Apply**.

Scheduling Space Reclamation

During space reclamation, the DXi V-Series deletes unneeded tags from the blockpool to free up disk space. Schedule space reclamation regularly to make sure there is enough disk space to store data.

> **Caution:** Because space reclamation can affect system performance, avoid running space reclamation during known backup periods.

> **Note:** For more information about space reclamation, see Space Reclamation on page 256.

To configure a schedule for space reclamation:

1 On the **Scheduler Calendar** page, add or edit an event in the **Space Reclamation** row (see Adding or Editing a Scheduled Event on page 184).

2 Specify when and how often the event reoccurs (see Setting Recurrence for a Scheduled Event on page 190).

> **Caution:** For correct system operation, space reclamation *must* be run at regular intervals (at least once a week).You can schedule space reclamation to occur daily or weekly but not monthly or yearly. Also, recurrence is required.

3 Click **Apply**.

Setting Recurrence for a Scheduled Event

To specify when and how often the event reoccurs:

1 On the **Scheduler Calendar** page, add or edit an event (see <u>Adding or Editing a Scheduled Event</u> on page 184).

2 In the **Repeats** drop-down box, select **Does not repeat** to disable recurrence. Or to enable recurrence, select how often the event reoccurs:

Note: For healthchecks and space reclamation, recurrence is required, and **Monthly** and **Yearly** recurrence options are not available. Healthchecks and space reclamation must occur at least every seven days or once a week.

- **Daily** - Specify the recurrence interval in days.

- **Weekly** - Specify the recurrence interval in weeks, and select the days the event occurs on.

- **Monthly** - Specify the recurrence interval in months, and specify the day the event occurs on (for example, the 1st day of each month or the third Friday of each month).

- **Yearly** - Specify the recurrence interval in years, and specify the date and month the event occurs on (for example, the 15th day of March or the first Monday in May).

3 For recurring events, specify how long the recurrence continues (**forever**, **for** a certain number of occurrences, or **until** a specific date).

Note: For healthchecks and space reclamation, recurrence is always **forever**.

---

4 Click **Apply**.

Deleting a Scheduled Event

To delete an event occurrence or event series.

1 On the **Scheduler Calendar** page, right-click an event.

2 On the pop-up menu, select an option:

- **Delete** - Remove the selected event from the schedule.

- **Delete this occurrence** - Remove the selected occurrence in an event series from the schedule.

- **Delete all occurrences** - Remove the entire event series from the schedule.

The event or series is deleted from the schedule and will no longer occur.

Scheduler NAS

The **Scheduler NAS** page allows you to view a list of upcoming events for scheduled NAS replication activity on the DXi V-Series.

To access the **Scheduler NAS** page, on the **Scheduler** page, click the **NAS** tab (see Figure 98).

Figure 98 Scheduler NAS Page
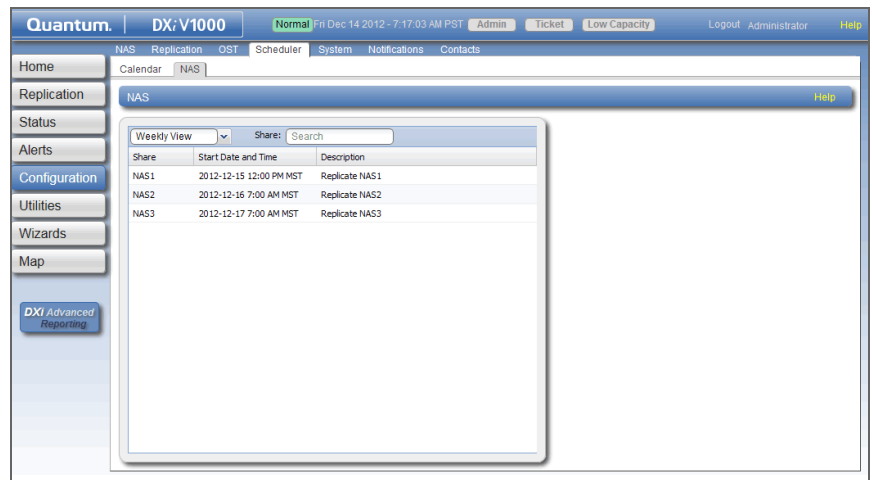
The **Scheduler NAS** page displays the following information about NAS replication events that are scheduled to occur:

- **Share** - The name of the NAS share.

- **Start Date and Time** - The date and time the scheduled replication will start.

- **Description** - The description of the event (if available).

To adjust the number of events displayed, do the following:

- In the drop-down box, select **Daily View**, **Weekly View**, or **Monthly View** to display events that will occur in the next day, week, or month.

- In the **Share** box, type the name of a NAS share to display only
events for that share. (The list is filtered as you type.)

Note: If you see an error indicating there is not enough memory to
complete the request, try using daily or weekly view, or type a
share name in the box to filter the results.

System

The **System** page allows you to configure system settings for the
DXi V-Series, including network settings, system date and time, and
security settings.

To access the **System** page, click the **Configuration** menu, and then
click the **System** tab.

The **System** page contains the following tabs:

- Network

- Date & Time

- Security

Network

The **Network** page allows you to view and change network
configuration information for the DXi V-Series. The DXi V-Series uses
this information to connect to the network.

Network configuration information is entered during initial setup
DXi V-Series. You should consult your network administrator before
making any changes to the network settings.

Caution: Changing the network configuration requires a system
reboot to allow all system services to function correctly.
Changing the network configuration requires a system
reboot immediately after the changes are applied.

Note: Rebooting the system can take several minutes. After the new network configuration is saved, close your Web browser and wait 15 minutes before logging in again. If you change the IP address that you use to log in to the system, you will temporarily lose your connection to the remote management console. Because of this, you might not see a confirmation page informing you that the new settings have been saved.

To access the **Network** page, on the **System** page, click the **Network** tab (see Figure 99).

Figure 99 Network Configuration

Configuring the Network

Using the **Network** page, each virtual Ethernet port in the DXi can be configured as a separate device. In addition, you can create bonded devices (logical ports) consisting of two or more virtual ports. For each port or device, you can specify the MTU (Maximum Transmission Unit) frame size, and you can optionally assign the port or device to a VLAN (Virtual Local Area Network).

After you define devices (single port or bonded), you can create up to ten network interfaces for each device. Each interface has its own IP address information, and you can specify the types of traffic allowed on the interface (management, replication, or data). Finally, you can add routing information for an interface to enable connectivity with devices on different subnets.

Note: You can choose to allow any traffic type (management, replication, or data) on an interface. In this case, the routing of different traffic types, as well as firewall capability, must be controlled using the network infrastructure (routers and switches) that the DXi is connected to.

Keep in mind the following information when configuring the network on the DXi V-Series:

• The DXi V-Series utilizes four VMware VMXNET3 virtual Ethernet ports, which appear on the **Network** page as eth0, eth1, eth2, and eth3.

• The link speed of eth0 and eth1 are always reported as 1GbE on the **Network** page. The link speed of eth2 and eth3 are always reported as 10GbE on the **Network** page. However, the actual link speed is determined by the physical Ethernet ports on the host ESXi server.

• By default, eth0 and eth1 are *not* bonded into a single device. Similarly, eth2 and eth3 are *not* bonded. While the **Network** page will not prevent configuring a bonded device, Quantum does not support bonding the virtual Ethernet ports on the DXi V-Series. In addition, network segmentation (routing management, replication, or data traffic on different interfaces) is not enforced when using DHCP.

• The DXi V-Series supports DHCP for automatic configuration of IP addresses. You can also manually specify IP addresses as required by your network.

- For correct operation, make sure the network switch connected to the ESXi server is properly configured. If the DXi V-Series is set to use LACP, then the network switch must be configured for (static) port trunking with a submode of LACP.

    The ESXi vSwitch should be configured for **Route based on IP hash** (ESXi node > Configuration tab > Ports tab > vSwitch > Edit button > NIC Teaming parameter > Load Balancing).

Configuring the network includes the following major steps:

Note: Before configuring the network, work with your network administrator to determine the network settings that will be required to properly integrate the DXi V-Series with your company's network.

---

1 <u>Configuring General Network Settings</u> on page 197

2 <u>Configuring Bonding Details</u> on page 199

3 <u>Configuring Interface Details</u> on page 201

4 <u>Configuring Interface IP Addresses</u> on page 202

5 <u>Configuring Interface Routing</u> on page 204

6 <u>Applying Network Settings</u> on page 206

Configuring General Network Settings

Under **General**, enter the following network information as provided by your network administrator (see <u>Figure 100</u>):

Figure 100 Network Page: General

Note: If DHCP is enabled for the device, you cannot specify DNS information. Instead, DNS information is automatically assigned by the DHCP server.

Note: When entering IP addresses, never use an address that is in a reserved IP address range. To see a list of reserved IP address ranges, click the quick tip icon [**?**] located near the IP address field.

- **Hostname** - The hostname of the DXi V-Series.

  The **Hostname** cannot be blank and must contain only letters [A–Z, a–z], numbers [0–9], hyphens [-], underscores [_], and dots [.].

- **Default Gateway** - The default gateway IP address.

  Specifying a default gateway is optional if all access is local to a particular subnet. For example, if the DXi V-Series and all of its clients are on the same subnet, you do not need to specify a default gateway.

  Caution: Specifying a default gateway is required to enable connectivity with all subnets other than those that the DXi V-Series is directly connected to. For example, if the DXi V-Series and its clients are on different subnets, or you are using an external NTP server, you must specify a default gateway.

- **DNS Suffix Search List** - (Optional) The local domain to search first when resolving domain names.

  The domain suffix is a single domain name. The domain name may contain only letters (A–Z), numbers (0–9), dots (.), and hyphens (-).

- **Primary, Secondary, and Tertiary DNS IP Address** - (Optional) The IP addresses of up to three DNS servers used to resolve domain names and translate them into IP addresses.

  Note: You must specify a DNS IP address if you plan to use hostname format when configuring an NTP time server, outgoing e-mail server, replication sources and targets, and other information.

> **Note:** The **DNS Suffix Search List** and **DNS IP Addresses** cannot be modified if the DXi V-Series is currently joined to a Windows domain. To disjoin a Windows domain, see Windows Domain on page 135.

Configuring Bonding Details

> **Note:** While the **Network** page will not prevent configuring a bonded device, Quantum does not support bonding the virtual Ethernet ports on the DXi V-Series. In addition, network segmentation (routing management, replication, or data traffic on different interfaces) is not enforced when using DHCP.

Under **IP Address Configuration > Bonding Details**, configure bonded devices (see Figure 101):

Figure 101 Network Page: Bonding Details
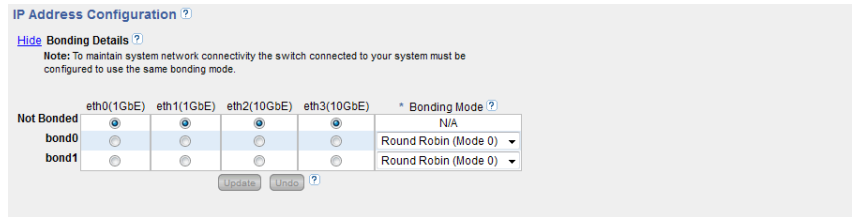
1 If necessary, click the **Show** link to show the bonding details table.

2 For each available bonded device (**bond0**, **bond1**, and so on), select two or more Ethernet ports with the same link speed to assign to the bond. Or select **Not Bonded** to leave a port unassigned to any bond.

   If no ports are assigned to a bond, the bond cannot be configured. That is, settings cannot be entered for the bond in the **Interface Details** or **IP Address** tables because no Ethernet ports are assigned to the device.

   All ports assigned to the same device are bonded together into a single logical port. For example, if you select **bond0** for port **eth0** and port **eth1**, both ports are bonded together in the **bond0** device. A bonded device can contain two or more ports.

> **Note:** All ports associated with a bond must have the same link
> speed (1GbE or 10GbE).

3 For each bonded device, specify the bonding mode:

> **Note:** To maintain network connectivity, the switch connected to
> the DXi V-Series must be configured to use the same
> bonding mode. The best time to change the bonding mode
> on the switch is during the next reboot of your system,
> after saving the new network settings. Changing the
> bonding mode on the switch before saving these settings
> and rebooting may result in the loss of network
> connectivity to the system.

- **Round Robin (Mode 0)** - This option sends Ethernet frames
  using the bonded Ethernet ports with a valid MII link. Frames
  are sent in a round-robin fashion, starting with the first slave
  device and then the rest of the devices. This only applies to the
  traffic sent from the DXi V-Series. The Ethernet switch needs to
  aggregate the ports, so the connected ports are treated as a
  logical port. The DXi frame reception is completely dependent
  on the transmission algorithm of the Ethernet switch. The
  bonding mechanism does not balance the frame reception.

- **LACP (Mode 4)** - This option (Link Aggregation Control
  Protocol) is based on the 802.3ad IEEE standard for aggregating
  Ethernet ports. If the bonding algorithm is set to LACP, the
  Ethernet switch ports must be configured in a 802.3ad based
  Link Aggregation group (LAG) in LACP mode. The DXi frame
  reception and transmission is controlled by the LACP between
  the bonded ports and the Ethernet switch ports.

- **Active Backup (Mode 1)** - This option does not require switch
  configuration but may not provide the same level of load
  balancing and performance as other bonding modes. Only one
  port in the bond is active at a time. If the active port fails,
  another port becomes active to take its place. Because only the
  MAC address of the active port is visible to the Ethernet switch,
  the switch does not require additional configuration.

4 Click **Update** to save the changes you made to the **Bonding Details**
table. (Clicking **Update** does not yet apply the new network settings
to the DXi V-Series.)

Click **Undo** to revert to all current Bonding Details changes to the last update.

Configuring Interface Details

Under **IP Address Configuration > Interface Details**, configure DHCP and jumbo Ethernet frame settings for each port or device (see Figure 102):

Figure 102 Network Page:
Interface Details

1   If necessary, click the **Show** link to show the interface details table.

2   For each device, select the **DHCP** check box to enable Dynamic Host Configuration Protocol for the device. When DHCP is enabled, IP address information is automatically assigned to the device by the DHCP server.

> **Note:** If you intend to use DHCP for long-term operation, Quantum recommends registering the DXi V-Series with the DNS server. Alternately, you can use a DHCP reservation. Doing so ensures that the IP address of the DXi V-Series will not change. Otherwise, if the system is powered down and is unable to renew its DHCP lease, it could be assigned a new IP address the next time it is powered up. If a new IP address is assigned, NAS and replication services must be updated for the new IP address.

3   For each device, select the MTU (Maximum Transmission Unit) frame size in the **Jumbo Frame MTU Size** drop-down box.

   • **1500 MTU** - The standard (STD) MTU frame size of 1,500 bytes is used.

   • **9000 MTU** - The jumbo MTU frame size of 9,000 bytes is used.

4   Click **Update** to save the changes you made to the **Interface Details** table. (Clicking **Update** does not yet apply the new network settings to the DXi V-Series.)

Click **Undo** to revert to all current Interface Details changes to the last update.

Configuring Interface IP Addresses

Under **IP Address Configuration > IP Address Table**, configure one or more network interfaces for each port or device (virtual Ethernet port or bonded device) (see Figure 103):

Note: If DHCP is enabled for the device, you cannot specify network information. Instead, all IP address information is automatically assigned by the DHCP server.

Figure 103 Network Page: IP Address Table

1 Click **Add IP** to add a network interface to a device.

Or select an interface to edit the IP address, netmask, gateway and traffic type. (To select an interface, click the radio button next to the interface index name, for example, **bond0:2**.)

Note: A maximum of 10 IP addresses are allowed per device. All IP addresses in the IP Address Table (added or modified) must be valid and unique, and must have a valid gateway and netmask.

2 Select the check box to enable VLAN tagging for the interface. (Or clear the check box to disable VLAN tagging for the interface.)

VLAN tagging allows you to assign an interface to a virtual local area network (VLAN). With VLAN tagging, you can route different traffic types (management, data, and replication) over different VLANs, making sure traffic types do not mix.

If VLAN tagging is enabled, enter the **VLAN Tag ID** for the interface. (Valid values are **2** to **4094**. You can assign only one tag ID to an interface.)

Quantum DXi V-Series User's Guide

> **Note:** The maximum allowed number of VLAN tag IDs is 64. If you attempt to add more than 64 VLAN tag IDs, an error displays.

> **Note:** To maintain connectivity, the switch ports connected to the DXi must be configured to accept the correct VLAN tag ID.

> **Caution:** If VLAN tagging is enabled for an interface, DXi Advanced Reporting is unable to collect and record statistics for traffic moving over the VLAN interface (for example, eth1.400). Statistics are still collected for the base device (for example, eth1.)

3 Enter the following network information as provided by your network administrator (all fields are required):

- **IP Address** - The IP address of the interface.
- **Netmask** - The network mask of the interface.
- **Gateway** - The gateway of the DXi V-Series. (This is usually not the same as the default gateway.)

4 Select the check box for each type of network traffic allowed on the interface (segmentation):

> **Note:** At least one interface must allow management traffic.

> **Note:** If the DXi is configured for source or target replication, you should configure at least one interface to allow replication traffic (select **Repl** or **Any**) before applying changes to network settings.

> **Note:** If you configure segmentation for non-bonded interfaces (Ethernet ports) that are on the same subnet, all traffic will use the lowest numbered Ethernet port first, no matter how segmentation is configured. To avoid this issue, create bonded interfaces, and then select the desired traffic type for each bonded interface.

- **Mgmt** - Select to allow management traffic.

- **Repl** - Select to allow replication traffic.
- **Data** - Select to allow data traffic.
- **Any** - Select to allow all types of traffic (management, replication, and data).

5 Click **Update** to save the changes you made to the **IP Address** table. (Clicking **Update** does not yet apply the new network settings to the DXi V-Series.)

Click **Delete** to remove IP address information for the selected interface. Or click **Undo** to revert all current IP Address Table changes to the last update.

Note: When you add a network interface, a default route (via the default gateway) is automatically created for the interface after network settings are applied and the DXi reboots. For example, if you add an interface with IP address 10.20.185.172, a route with the destination IP address 10.20.185.0 is automatically added. If you delete the default route, it is automatically added again the next time network settings are applied and the DXi reboots. For more information about interface routing, see Understanding Interface Routing on page 206.

Configuring Interface Routing

Some network configurations require that you specify routing details for an interface. You need to specify routing details if the host or client the interface connects to is on a different subnet that is not reachable using the default gateway. You also need to specify routing details if you have configured multiple network segments (replication, data, or management) on the same subnet. For more information and examples, see Understanding Interface Routing on page 206.

Under **IP Address Configuration > Routing Details**, enter routing information for one or more interfaces (see Figure 104):

Note: If DHCP is enabled for the device, you cannot specify routing information. Instead, all IP address information is automatically assigned by the DHCP server.

Figure 104 Network Page:
Routing Details

1 In the **IP Address Table** (above routing details), select an interface to add or modify routing data. (To select an interface, click the radio button next to the interface index name, for example, **bond0:2**.)

After selecting an interface in the **IP Address Table**, the **Routing Details** table below expands to display available routes (if any).

Note: A maximum of 8 routes per interface are allowed.

2 If necessary, click the **Show** link to show the routing details table.

3 Click **Add Route** to add a route to the selected interface.

Or select a route to edit its settings.

4 Enter the following network information as provided by your network administrator:

- **Destination** - The destination network for the route.

- **Dest Netmask** - The network mask for the route.

- **Dest Gateway** - The gateway IP address used for *outgoing* traffic sent from the interface to a host or client. (This is usually not the same as the default gateway.)

Note: The destination gateway of each route *must* match the subnet of at least one configured IP address listed in the **IP Address Table**. If no match is found, an error displays stating that the route's destination gateway is not reachable.

Note: In the example shown in , to reach a host on the 10.50.50.x subnet, you would enter 10.50.50.0 for destination network, 255.255.255.0 for the destination netmask, and 10.20.20.1 as the destination gateway.

5 Click **Update** to save the changes you made to the **Routing Details** table. (Clicking **Update** does not yet apply the new network settings to the DXi V-Series.)

Click **Delete** to remove IP routing information for the selected interface. Or click **Undo** to revert all current Routing Details changes to the last update.

Applying Network Settings

For network changes to take effect, you must apply the changes, finalize the confirmation, and reboot the system. To apply all changed settings on the **Network** page to the DXi V-Series, click **Apply** at the bottom of the page. Follow the prompts to confirm the changes and reboot the system.

Note: To revert all network settings to the initial state and undo all changes, click the **Reset** button.

Understanding Interface Routing

For a network on the interface to communicate with a host located on a different subnet, you must specify routing information in the **Routing Details** section. Routing is used to direct outgoing traffic from a network interface on the DXi to an IP address in another subnet by means of a destination gateway. Responses from the destination are routed back to the DXi using the gateway specified for the interface in the **IP Address Table** section.

In addition, when configuring segmented network interfaces, if the source DXi replication, data, and management interfaces are on the same subnet, you must add a host route on the source DXi to make sure the replication interface is correctly selected when replicating data to the target DXi.

See the following examples for details:

- Example 1: Segments and Target on Different Subnets
- Example 2: Segments and Target on the Same Subnet
- Example 3: Segments on the Same Subnet and Target on a Different Subnet

Example 1: Segments and Target on Different Subnets

In the example below (see Figure 105), the DXi has two segmented interfaces, one for management traffic and one for data traffic:

- The management interface is assigned to the 10.30.24.x subnet in the **IP Address Table** section. This subnet connects to the corporate network by mean of the default gateway (10.30.24.1).

- The data interface is assigned to the 10.20.20.x subnet in the **IP Address Table** section. This subnet connects to a gateway at 10.20.20.1.

- Using the data interface, the DXi needs to connect to a backup host that is on the 10.50.50.x subnet. Because this host is not on the same subnet as the data interface, the DXi cannot communicate with the host unless you specify routing information in the **Routing Details** section.

  In this example, you would specify 10.50.50.0 for destination network, 255.255.255.0 for the destination netmask, and 10.20.20.1 as the destination gateway.

Note: The gateway specified in the **IP Address Table** section is for *incoming* traffic to the interface. The gateway specified in the **Routing Details** section is for *outgoing* traffic from the interface.

Figure 105 Interface Routing:
Example 1

Example 2: Segments and Target on the Same Subnet

In the example below (see Figure 106), the DXi has two segmented interfaces, one for data and management traffic, and one for replication traffic:

- The source DXi management/data IP address, the source DXi replication IP address, and the target DXi IP address are all on the same subnet (192.168.10.x).

- To make sure the replication segment is used when communicating with the target DXi, you must add a host route in the **Routing Details** section on the source DXi.

  In this example, you would specify the following routing details for the replication interface on the source DXi:

- **Destination** - Use the IP address of the target DXi (192.168.10.200).

- **Dest Netmask** - Use 255.255.255.255.

- **Dest Gateway** - Use the replication IP address of the source DXi (192.168.10.100).

Figure 106 Interface Routing: Example 2

Source DXi

Target DXi

192.168.10.x subnet

Replication IP: 192.168.10.100

Management/Data IP: 192.168.10.101

IP: 192.168.10.200

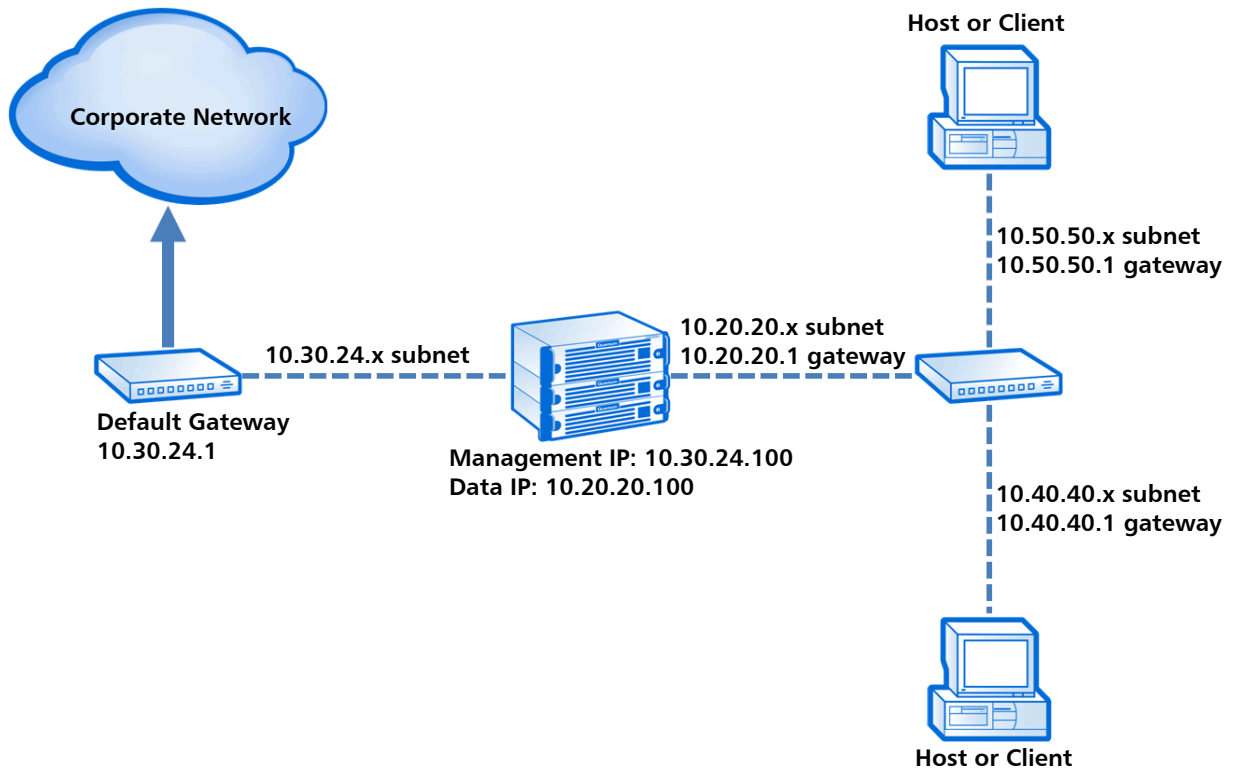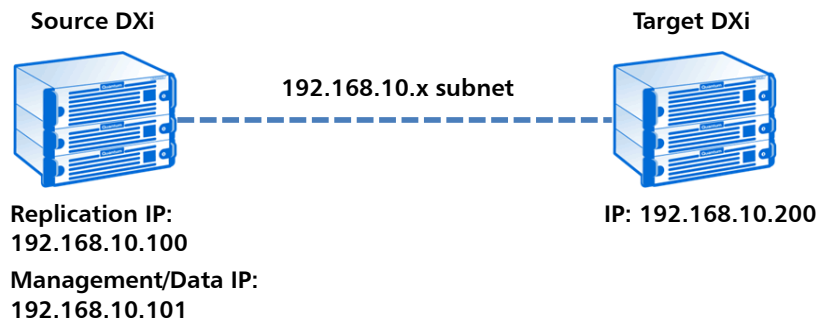**Example 3: Segments on the Same Subnet and Target on a Different Subnet**

In the example below (see Figure 107), the DXi has two segmented interfaces, one for data and management traffic, and one for replication traffic:

- The source DXi management/data IP address and the source DXi replication IP address are on the same subnet (192.168.10.x). The target DXi IP address is on a different subnet (192.168.20.x)

- To make sure the replication segment is used when communicating with the target DXi, you must add a network route in the **Routing Details** section on the source DXi.

In this example, you would specify the following routing details for the replication interface on the source DXi:

- **Destination** - Use the subnet of the target DXi (192.168.20.0).

- **Dest Netmask** - Use 255.255.255.0.

- **Dest Gateway** - Use the IP address of the gateway (192.168.10.1).

- In addition, to enable communication with the target DXi by means of the gateway, you must add a second host route in the **Routing Details** section on the source DXi.

    In this example, you would specify a second set of routing details for the replication interface on the source DXi:

    - **Destination** - Use the IP address of the gateway (192.168.10.1).

    - **Dest Netmask** - Use 255.255.255.255.

    - **Dest Gateway** - Use the replication IP address of the source DXi (192.168.10.100).

Figure 107 Interface Routing: Example 3

Source DXi

192.168.10.x subnet

192.168.20.x subnet

Target DXi

Replication IP:
192.168.10.100

Gateway IP:
192.168.10.1

IP: 192.168.20.200

Management/Data IP:
192.168.10.101
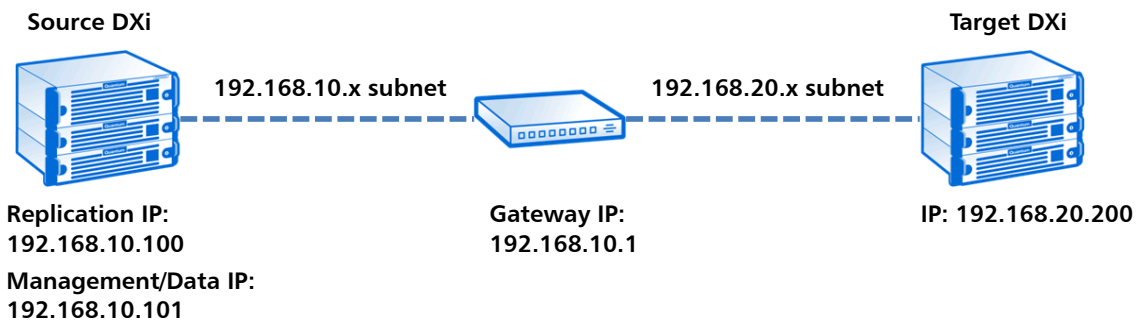
Backpanel Locations

The **Backpanel Locations** section at the bottom of the **Network** page displays a graphical representation of the virtual Ethernet ports.

The diagram indicates the current bonding configuration and connectivity status for all Ethernet ports.

- Ports that are bonded together in an interface are shaded the same color.

- A green border indicates a port is connected to a network.

- A red border indicates a port is configured but is not connected to a network.

- Click **Update Port View** to update the information on the diagram.

Date & Time

The **Date & Time** page allows you to set the system date and time of the DXi V-Series. You can specify a Network Time Protocol (NTP) server to synchronize the system time with, or you can manually enter the date and time.

Caution: The DXi V-Series uses VMware Tools time management services. Quantum recommends that you do *not* configure NTP on the DXi V-Series. Instead, you should configure NTP on the ESXi server.

Caution: Changing the date and time settings requires a system reboot immediately after the changes are applied. Wait for at least 15 minutes before logging back in.

Note: If you intend to join the DXi V-Series to a Windows network using Active Directory for NAS storage, Quantum recommends using an NTP Server to set the system date and time (see Windows Domain on page 135).

To access the **Date & Time** page, on the **System** page, click the **Date & Time** tab (see Figure 108).
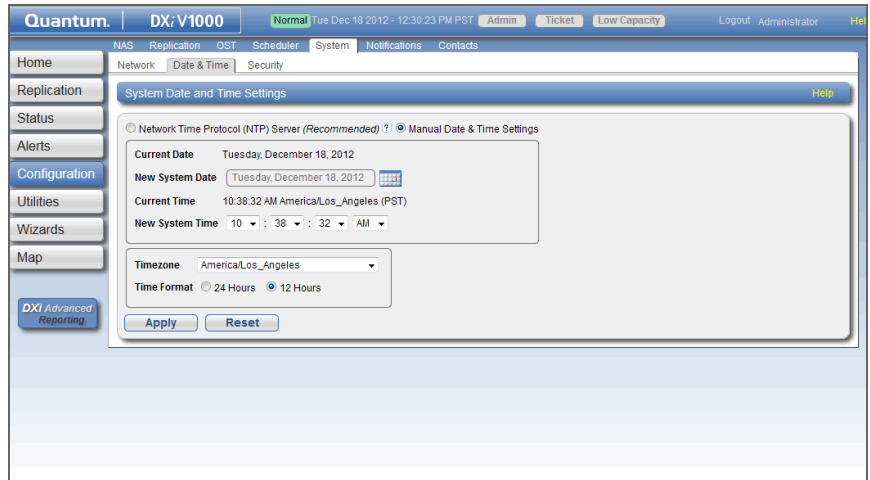
To set the system date and time:

1 Select one of the following options:

- **Network Time Protocol (NTP) Server** - Select this option to synchronize the DXi V-Series with an NTP timeserver or pool. Then select or specify a timeserver or pool.

  - **Select a Timeserver Pool** - (Recommended) Select one of the well-known, geographically-based NTP timeserver pools in the drop-down box.

    Note: To select a timeserver pool, you must first specify at least one DNS IP address on the **Network** page (see Network on page 193). Otherwise, you must specify the IP address of the timeserver pool.

  - **Specify a Timeserver or Pool** - Type the name or IP address of the NTP server or pool. (See http://support.ntp.org for information about publicly available NTP servers)

  To verify that the DXi V-Series can communicate with the NTP server or pool, click **Test NTP**.

- **Manual Date & Time Settings** - Select this option to manually set the system date and time.

  Specify the **New System Date** by clicking the calendar icon. Specify the **New System Time** using the drop-down boxes.

2   In the **Timezone** drop-down box, select the time zone where the
DXi V-Series is located.

3   Next to **Time Format**, select the format to use when displaying
times (**24 hours** or **12 hours**).

4   Click **Apply**.

Security

The **Security** page allows you to configure security settings for the
DXi V-Series, including access passwords, SSL settings, and the inactivity
timeout.

To access the **Security** page, click the **Configuration** menu, and then
click the **Security** tab.

The **Security** page contains the following tabs:

- Web & CLI Passwords

- SSL

- Login Session

- Security Notice

Web & CLI Passwords

The **Web & CLI Passwords** page allows you to change the account
passwords for the remote management console (Web) and the
command line interface (CLI). You can also enable or disable the CLI
account.

The DXi V-Series has two access levels for logging onto the remote
management console or the CLI:

- **Monitor** - Allowed to view information on the DXi V-Series remote
  management console or the CLI but cannot make changes.

- **Administrator** - Allowed to view and change information on the
  DXi V-Series remote management console or the CLI.

To access the **Web & CLI Passwords** page, on the **Security** page, click
the **Web & CLI Passwords** tab (see Figure 109).

Figure 109 Web & CLI
Passwords Page
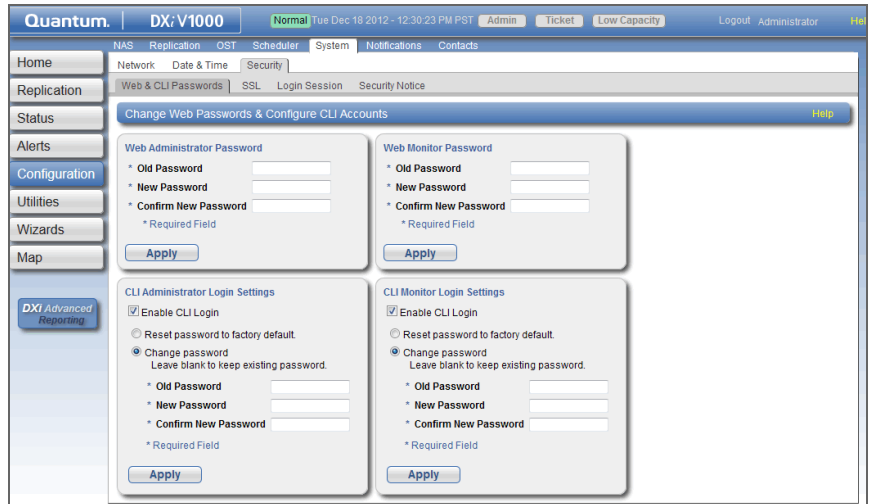
Use the **Web & CLI Passwords** page to perform the following tasks:

- Change the administrator or monitor password for Web access (see Changing Web Passwords on page 214).

- Enable or disable CLI access for the administrator or monitor account (see Enabling CLI Accounts on page 215).

- Change the administrator or monitor password for CLI access (see Changing CLI Passwords on page 215).

- Reset the CLI administrator or monitor password to the factory default (see Resetting CLI Passwords on page 216).

Changing Web Passwords

Use the Web passwords when logging onto the remote management console as an administrator or monitor (see Accessing Remote Management on page 16).

To change the Web passwords:

1 Under **Web Administrator Password** or under **Web Monitor Password**, enter the following information:

- **Old Password** - Enter the old password.

- **New Password** - Enter the new password.

- **Confirm New Password** - Enter the new password again to confirm it.

Note: The default password is **password**.

Note: Passwords are limited to 15 characters. All alphanumeric
characters are allowed, as well as underscores (**_**) and
hyphens (**-**).

---

2 Click **Apply**.

Enabling CLI Accounts

The CLI accounts provide access to the DXi V-Series command line
interface as an administrator or monitor.

Note: For more information about using the CLI, see the *DXi V-Series
Command Line Interface (CLI) Guide*.

To enable or disable the CLI accounts:

1 Under **CLI Administrator Login Settings** or under **CLI Monitor
Login Settings**, do one of the following steps:

  • Select the **Enable CLI Login** check box to enable the CLI
    account.

  • Clear the **Enable CLI Login** check box to disable the CLI
    account.

2 Click **Apply**.

Changing CLI Passwords

Use the CLI passwords when logging onto the command line interface
as an administrator or monitor.

To change the CLI passwords:

1 Under **CLI Administrator Login Settings** or under **CLI Monitor
Login Settings**, select the **Change password** option.

2 Enter the following information:

  • **Old Password** - Enter the old password.

  • **New Password** - Enter the new password.

  • **Confirm New Password** - Enter the new password again to
    confirm it.

> **Note:** The default password for the CLI Administrator account is **cliadmin**. The default password for the CLI Monitor account is **cliviewer**.

> **Note:** Passwords are limited to 15 characters. All alphanumeric characters are allowed, as well as underscores (**_**) and hyphens (**-**).

3 Click **Apply**.

Resetting CLI Passwords

The default password for the CLI Administrator account is **cliadmin**. The default password for the CLI Monitor account is **cliviewer**.

To reset the CLI account passwords to their default values:

1 Under **CLI Administrator Login Settings** or under **CLI Monitor Login Settings**, select the **Reset password to factory default** option.

2 Click **Apply**.

SSL

The **SSL** page allows you to enable or disable SSL on the DXi V-Series. You can also install a new SSL certificate to replace the Quantum default SSL certificate.

To access the **SSL** page, on the **Security** page, click the **SSL** tab (see Figure 110).

Figure 110 SSL Page
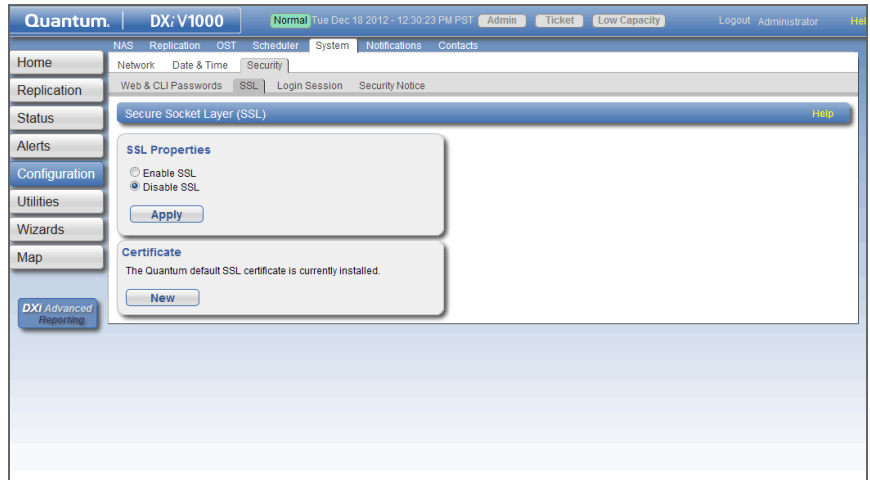
Use the **SSL** page to perform the following tasks:

* Enable or disable SSL on the DXi V-Series (see Enabling SSL on page 217).

    Note: If you enable SSL, see Server Authentication Warnings on page 218 for important information about Web browser settings.

* Install a new SSL certificate (see Installing an SSL Certificate on page 218).

Enabling SSL

SSL (Secure Sockets Layer) is a protocol that provides security and privacy over the Internet by negotiating encryption keys before transmitting data between a client and a server.

To establish a secure connection, the DXi V-Series must have an encryption key assigned to it by a Certification Authority in the form of a certificate file, private key file, and pass phrase. After you install these components, you can establish a secure connection using the SSL protocol. The DXi V-Series comes with a Quantum default SSL certificate.

To enable or disable SSL:

1 Under **SSL Properties**, select the **Enable SSL** option to enable SSL.

Or select the **Disable SSL** option to disable SSL.

Note: The default setting is disabled.

2 Click **Apply**.

Server Authentication Warnings

Enabling SSL with the default Quantum certificate allows you to securely communicate with the DXi V-Series Web-based interface using SSL encryption. However, you may receive a warning from your Web browser stating that the server you are attempting to connect to does not match the server embedded within the certificate.

This is expected behavior because the default certificate can only be used for encryption and not server authentication. You can install your own custom certificate in order to take advantage of server authentication in addition to encrypted communication.

To suppress server authentication warnings for the default certificate:

- **Internet Explorer** - If a dialog box displays warning you of a possible certificate error, add the IP address for the DXi V-Series to the **Trusted Sites** list (**Tools > Internet Options > Security > Trusted Sites**). If subsequent warning pages display along with an option to close your Web browser or continue to the Web site, click **Continue**. This suppresses the warnings until you restart your Web browser.

- **Firefox** - If the **Secure Connection Failed** dialog box displays, click the link at the bottom of the dialog box and follow the instructions to add an exception for your DXi V-Series.

Installing an SSL Certificate

You can purchase and install your own custom SSL certificate in order to take advantage of server authentication in addition to encrypted communication on the DXi V-Series.

To install an SSL certificate:

1 Under **Certificate**, click **New**.

The **Install New Certificate** page displays (see Figure 111).

Figure 111 Install New
Certificate Page
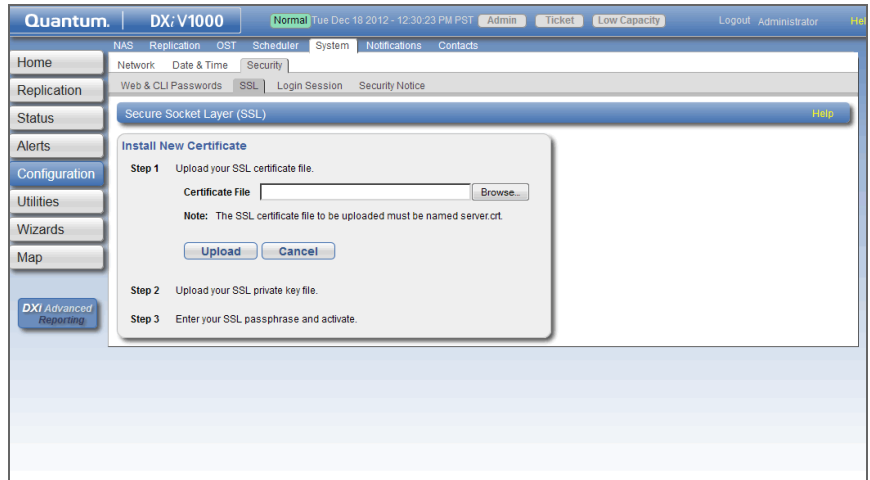
2 In the **Certificate File** box, type the location and filename of the new SSL certificate file.

Or click **Browse** to browse the system and locate the SSL certificate file. The SSL certificate file must be named **server.crt**.

3 Click **Upload**.

4 Type your SSL private key and press **<Enter>**.

5 Type your SSL passphrase and press **<Enter>**.

A **Successful Upload** page displays stating that the SSL certificate file has been installed on the system.

6 Click **OK**.

The certificate displays in the **Certificate** section.

Login Session

The **Login Session** page allows you to specify the inactivity timeout for the DXi V-Series remote management console. The default timeout is 30 minutes.

When the remote management console is inactive for the specified period of time, the user is automatically logged off and must log back on to continue (see Accessing Remote Management on page 16).

To access the **Login Session** page, on the **Security** page, click **Login Session** (see Figure 112).

Figure 112 Login Session Page
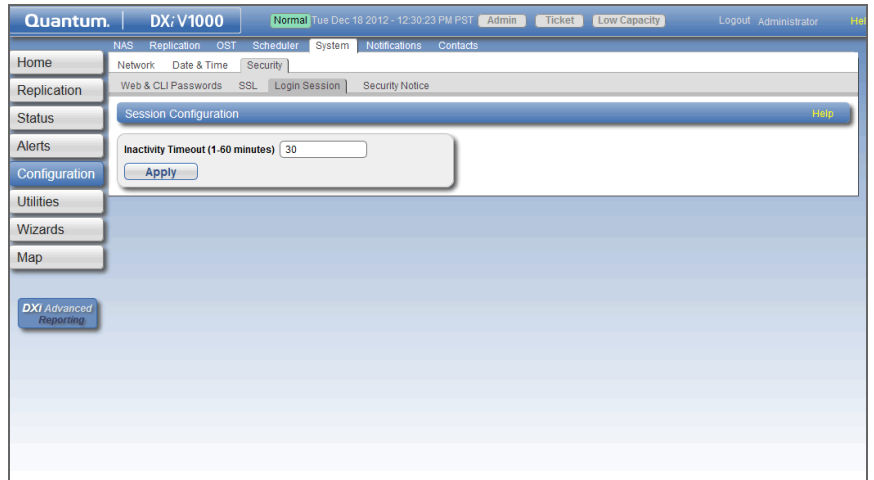
To specify the inactivity timeout:

1 In the **Inactivity Timeout** box, enter the number of minutes of inactivity before a user is automatically logged off (1–60 minutes).

2 Click **Apply**.

Security Notice

The **Security Notice** page allows you to specify a message that will appear to all users when logging on to the remote management console or the CLI (command line interface).

If a security notice message has been specified, the user must accept the message in order to begin using the system. If no security notice has been specified, the user can use the system immediately after logging on.

To access the **Security Notice** page, on the **Security** page, click **Security Notice** (see Figure 113).

Figure 113 Security Notice
Page
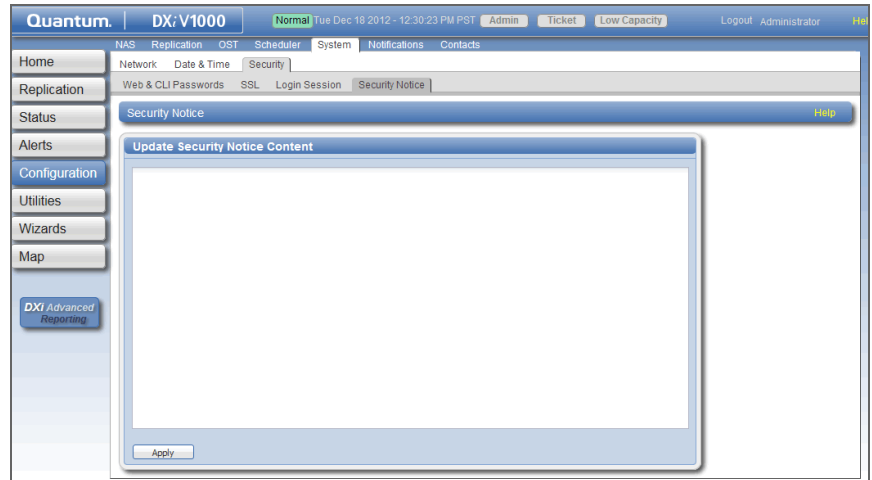
To add or update a security notice message, enter the message in the
box and click **Apply**.

Notifications

The **Notifications** page allows you to manage the methods the
DXi V-Series uses to send notifications. The DXi V-Series can send
notifications by e-mail, or using SNMP (Simple Network Management
Protocol).

To access the **Notifications** page, click the **Configuration** menu, and
then click the **Notifications** tab.

The **Notifications** page contains the following tabs:

• Email

• SNMP

Email

The **Email** page allows you to specify the recipients to notify by e-mail
when administration alerts or service tickets occur. You can specify e-
mail recipients, notification levels, and information about your e-mail

configuration. You can also configure the DXi V-Series to generate and send configuration and status reports.

Note: For more information about administration alerts and service tickets, see DXi V-Series Alerts on page 115.

To access the **Email** page, on the **Notifications** page, click the **Email** tab.

The **Email** page contains the following tabs:

- Recipients
- Server
- Test
- Email Reports

Recipients

The **Recipients** page allows you to manage the e-mail recipients the DXi V-Series sends notifications to. You can add, edit, and delete e-mail recipients, and you can specify the types of notifications to send.

Note: To enable the DXi V-Series to send e-mail, you must specify an outgoing e-mail server (see Server on page 227).

To access the **Recipients** page, on the **Email** page, click the **Recipients** tab (see Figure 114).

Figure 114 Recipients Page
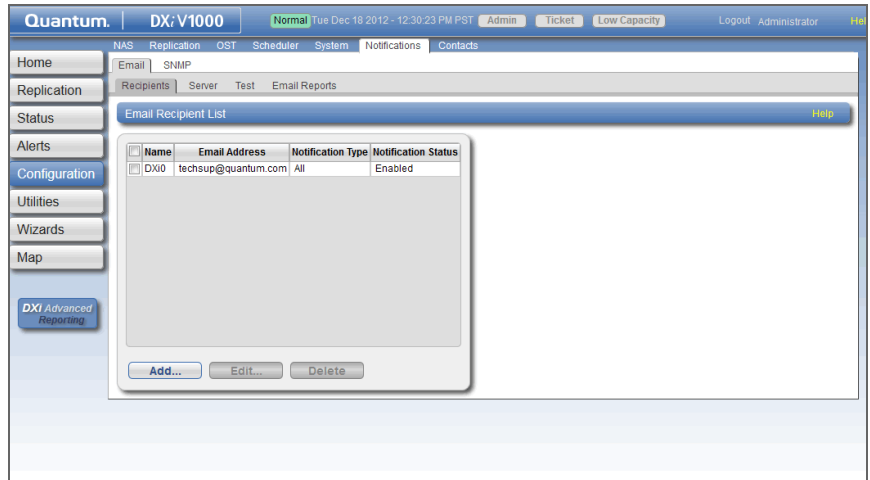
Use the **Recipients** page to perform the following tasks:

- View information about e-mail recipients (see Email Recipient List on page 223).

- Add an e-mail recipient (see Adding an E-mail Recipient on page 224).

- Edit an e-mail recipient (see Editing an E-mail Recipient on page 225).

- Delete an e-mail recipient (see Deleting an E-mail Recipient on page 226).

Email Recipient List

The **Email Recipient List** displays the following information about e-mail recipients:

- **Name** - The name of the recipient.

- **Email Address** - The e-mail address of the recipient.

- **Notification Type** - The types of notifications sent to the recipient (**High**, **High and Medium**, or **All**).

- **Notification Status** - The status of e-mail notifications for the recipient (**Enabled** or **Disabled**).

Adding an E-mail Recipient
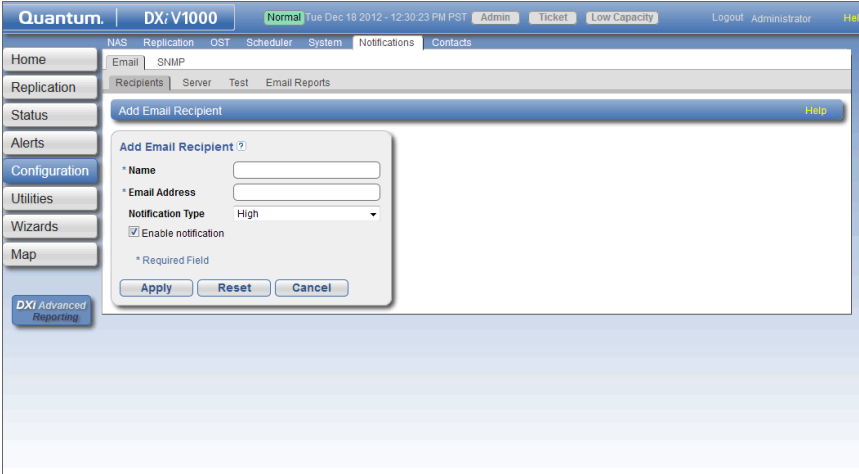
Add an e-mail recipient to send notifications about administration alerts or service tickets to the recipient by e-mail.

To add an e-mail recipient:

1 Click **Add**.

The **Add Email Recipient** page displays (see Figure 115).

Figure 115 Add Email
Recipient Page

2 Enter information about the recipient:

- **Name** - The name of the recipient.

- **Email Address** - The e-mail address of the recipient.

- **Notification Type** - Select the types of notifications to send to the recipient:

  - **High** - Send e-mail notifications for High service tickets.

    High service tickets indicate that a critical problem has occurred and needs to be resolved immediately. The operation and performance of the DXi V-Series are degraded, and there is a risk of system failure or data loss.

  - **High and Medium** - Send e-mail notifications for High and Medium service tickets.

    Medium service tickets indicate that a serious problem occurred and needs to be resolved, but it does not

necessarily need to be fixed immediately. The operation and performance of the DXi V-Series may be degraded.

- **All** - Send e-mail notifications for High, Middle, and Low service tickets, as well as any administration alerts.

   Low service tickets indicate that a minor problem occurred and needs to be resolved, but the operation and performance of the DXi V-Series are not significantly affected.

3 Select the **Enable notification** check box to enable sending of notifications to the recipient.

Or clear the **Enable notification** check box to disable sending of notifications to the recipient.

4 Click **Apply**.

Editing an E-mail Recipient

Edit an e-mail recipient to change the recipient's e-mail address or the types of notifications sent to the recipient. You can also enable or disable sending of notifications to the recipient.

To edit an e-mail recipient:

1 Click **Edit**.

The **Edit Email Recipient** page displays (see Figure 116).

Figure 116 Edit Email Recipient Page
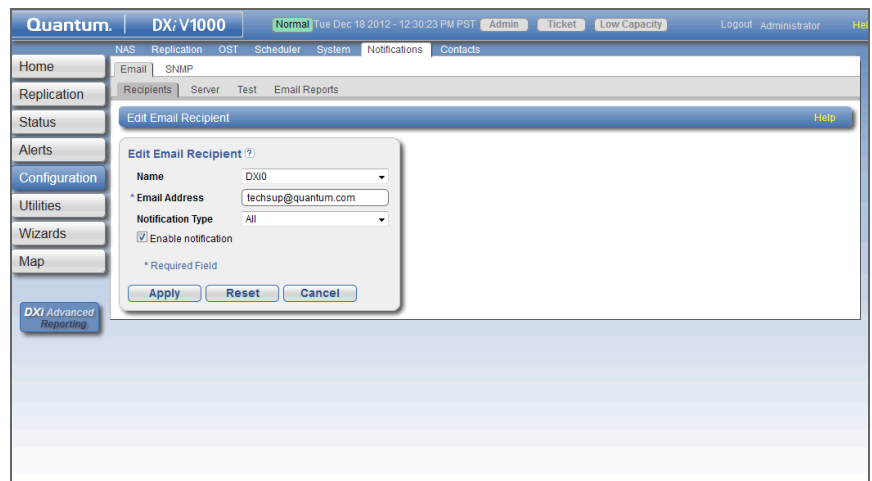
2 Enter information about the recipient:

> **Note:** If you are editing an e-mail recipient, you cannot change the **Name**.

- **Name** - (Optional) Select a different e-mail recipient to edit.
- **Email Address** - The e-mail address of the recipient.
- **Notification Type** - Select the types of notifications to send to the recipient:
  - **High** - Send e-mail notifications for High service tickets.

    High service tickets indicate that a critical problem has occurred and needs to be resolved immediately. The operation and performance of the DXi V-Series are degraded, and there is a risk of system failure or data loss.
  - **High and Medium** - Send e-mail notifications for High and Medium service tickets.

    Medium service tickets indicate that a serious problem occurred and needs to be resolved, but it does not necessarily need to be fixed immediately. The operation and performance of the DXi V-Series may be degraded.
  - **All** - Send e-mail notifications for High, Middle, and Low service tickets, as well as any administration alerts.

    Low service tickets indicate that a minor problem occurred and needs to be resolved, but the operation and performance of the DXi V-Series are not significantly affected.

3 Select the **Enable notification** check box to enable sending of notifications to the recipient.

Or clear the **Enable notification** check box to disable sending of notifications to the recipient.

4 Click **Apply**.

Deleting an E-mail Recipient

Delete an e-mail recipient if you no longer want the DXi V-Series to send e-mail notifications to the recipient.

To delete an e-mail recipient, select the recipient and click **Delete**.

Note: You can select multiple recipients to delete at once.

Server

The **Server** page allows you to specify the server for outgoing e-mail. The DXi V-Series cannot send e-mail notifications until you specify the outgoing e-mail server.

To access the **Server** page, on the **Email** page, click the **Server** tab (see Figure 117).

Figure 117 Server Page
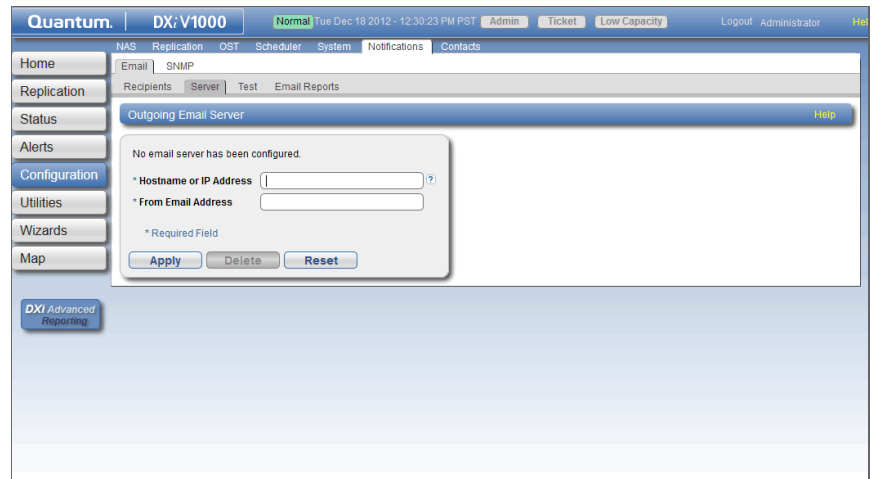
To specify the outgoing e-mail server:

1 In the **Hostname or IP Address** box, enter the hostname or IP address of the outgoing e-mail server.

Note: When entering IP addresses, never use an address that is in a reserved IP address range. To see a list of reserved IP address ranges, click the quick tip icon **[?]** located near the IP address field.

Note: To use hostname format, you must specify at least one DNS IP address on the **Network** page (see Network on page 193).

> **2** In the **From Email Address** box, enter the return e-mail address displayed in e-mails sent by the DXi V-Series.
>
> Specify a return address that lets you easily identify the system that generated the e-mail (for example, `systemname@any-domain.com`). The return address must contain an @ symbol and a valid domain name, including a period.
>
> **3** Click **Apply**.

Test

The **Email Test** page allows you to send a test e-mail to verify that e-mail notifications are correctly configured on the DXi V-Series.

To access the **Email Test** page, on the **Email** page, click the **Test** tab (see Figure 118).

Figure 118 Email Test Page
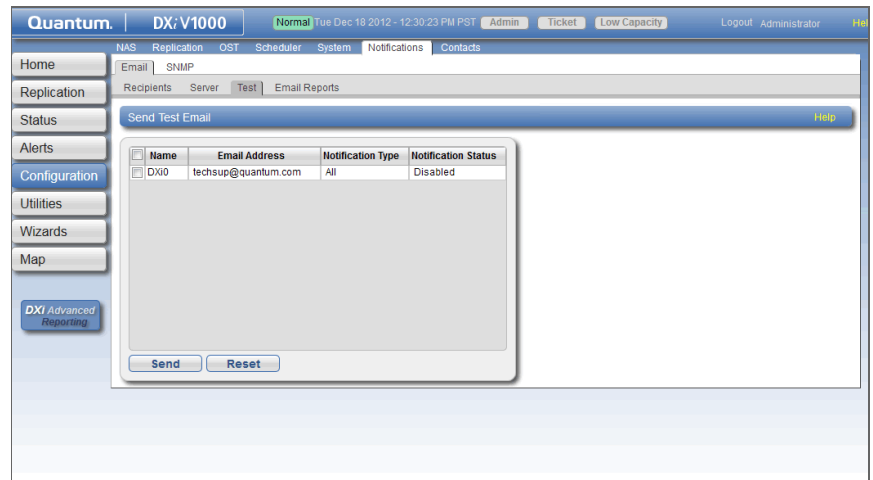
To send a test e-mail, select a recipient in the list and click **Send**. If the recipient does not receive the e-mail, make sure that the recipient's e-mail address is correct (see Editing an E-mail Recipient on page 225). Also make sure that the outgoing e-mail server is correct (see Server on page 227).

Email Reports

The **Email Reports** page allows you to specify the e-mail recipients for automatically generated reports. You can also generate reports on demand.

The system can generate a report with system status data or with configuration data. Each report also includes the system serial number, date and time, and a message that informs the recipient that the e-mail is automated and they should not respond to it.

Note: To enable the DXi V-Series to send e-mail, you must specify an outgoing e-mail server (see Server on page 227).

To access the **Email Home** page, on the **Email** page, click the **Email Home** tab.

The **Email Home** page contains the following tabs:

- Recipients
- On Demand

Recipients

The **Recipients** page allows you to specify the e-mail recipients who will receive all scheduled status data and configuration data reports.

Note: To configure the schedule when e-mail reports are sent, use the **Configuration > Scheduler** page (see Scheduling E-mail Reports on page 189).

To access the **Recipients** page, on the **Email Home** page, click the **Recipients** tab (see Figure 119).

Figure 119 Recipients Page
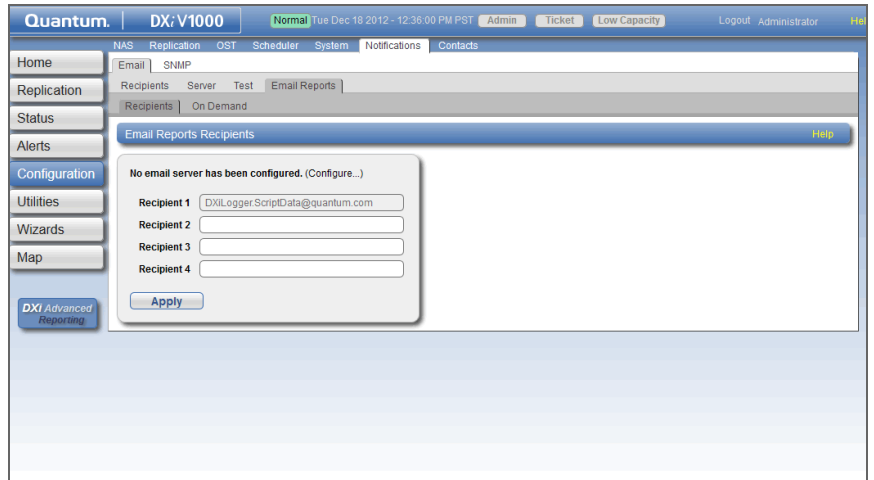
Enter the e-mail addresses of up to three recipients in the boxes, and then click **Apply**. When the DXi generates scheduled e-mail reports, they will be sent to the specified addresses.

Note: You cannot edit the first recipient.

On Demand

The **On Demand** page allows you to manually generate a status data or configuration data report. The report is immediately sent to the specified e-mail recipient. You can also view configuration data.

To access the **On Demand** page, on the **Email Home** page, click the **On Demand** tab (see Figure 120).

Figure 120 On Demand Page
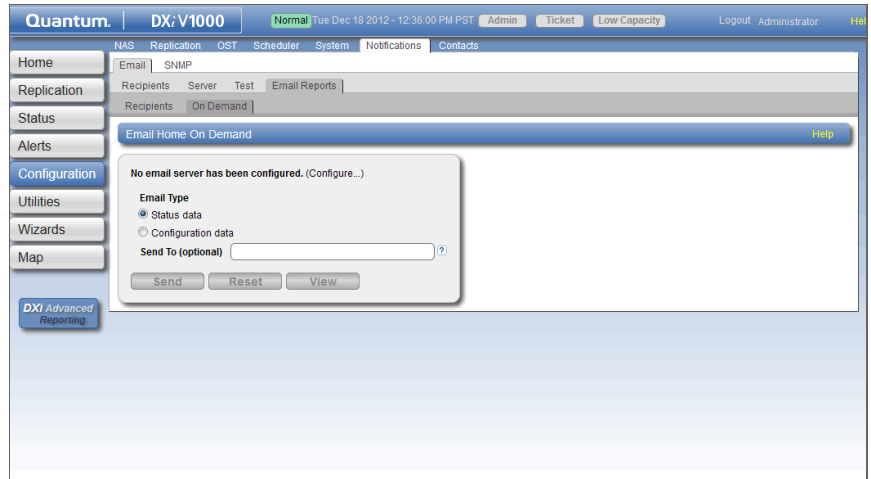
Use the **On Demand** page to perform the following tasks:

- Manually send a status data or configuration data report (see Sending a Report on page 231).

- View a configuration data report (see Viewing Configuration Data on page 231).

Sending a Report

To manually send a status data or configuration data report:

1 Under **Email Type**, select the type of report to send (**Status data** or **Configuration data**).

2 In the **Send To** box, enter the e-mail address of the recipient.

   An e-mail address is required for sending **Configuration data**. For **Status data**, if you do not enter an e-mail address, the report is sent to **DXiLogger.ScriptData@quantum.com**.

3 Click **Send**.

Viewing Configuration Data

To view a configuration data report:

1 Under **Email Type**, select **Configuration data**.

2 Click **View**.

   The **System Configuration Report** window displays.

3 (Optional) Click **Save** to save a local copy of the report in TXT format.

SNMP

The **SNMP** page allows you to configure the DXi V-Series to send status messages using SNMP (Simple Network Management Protocol). The DXi V-Series supports SNMP v1 and v2c.

SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network, or communities. SNMP compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

You can configure the DXi V-Series to act as an agent and send traps to a specified destination. You can also add SNMP community information.

To access the **SNMP** page, on the **Notifications** page, click the **SNMP** tab.

The **SNMP** page contains the following tabs:

- Destinations
- Community
- Test

Destinations

The **Destinations** page allows you to manage the destinations the DXi V-Series sends SNMP traps to. You can add, edit, and delete SNMP destinations, and you can specify the types of traps to send.

To access the **Destinations** page, on the **SNMP** page, click the **Destinations** tab (see Figure 121 on page 233).

Figure 121 Destinations Page
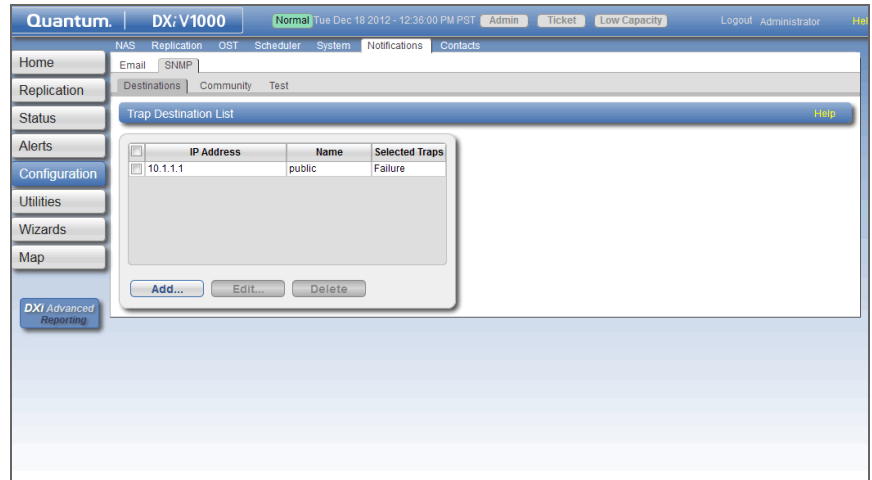
Use the **Destinations** page to perform the following tasks:

- View information about SNMP destinations (see Trap Destination List on page 233).

- Add an SNMP destination (see Adding a Destination on page 233).

- Edit an SNMP destination (see Editing a Destination on page 235).

- Delete an SNMP destination (see Deleting a Destination on page 236).

Trap Destination List

The **Trap Destination List** displays the following information about SNMP destinations:

- **IP Address** - The IP address of the destination.

- **Name** - The name of the destination.

- **Selected Traps** - The traps the DXi V-Series sends to the destination (**Failure**, **Warning**, **Informational**, **Available**, or **Unavailable**).

Adding a Destination

Add an SNMP destination to send traps from the DXi V-Series to the destination.

Note: You can add up to 5 destinations.

To add a destination:

1 Click **Add**.

The **Add Trap Destination** page displays (see Figure 122).

Figure 122 Add Trap
Destination Page
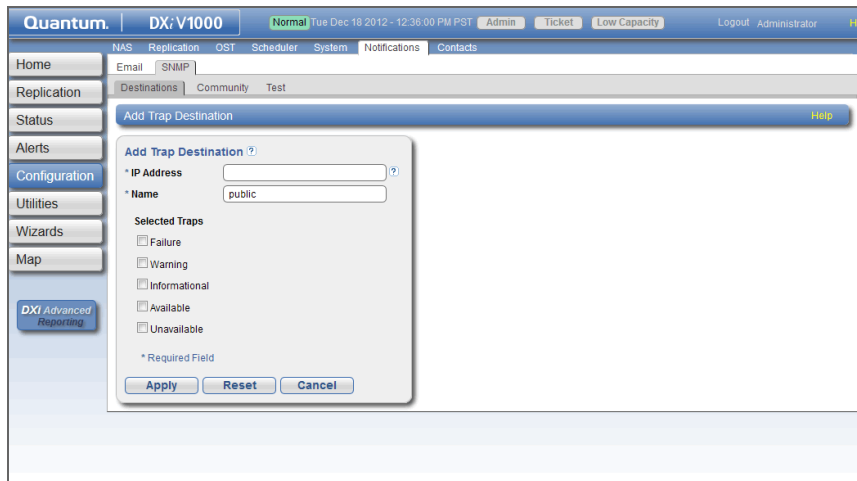
2 Enter information about the destination:

- **IP Address** - Enter the IP address of the system that will receive the traps generated by the DXi V-Series.

  Note: When entering IP addresses, never use an address that is in a reserved IP address range. To see a list of reserved IP address ranges, click the quick tip icon **[?]** located near the IP address field.

  Note: To use hostname format, you must specify at least one DNS IP address on the **Network** page (see Network on page 193).

- **Name** - Enter the name of the destination.

3 Select one or more traps to send to the destination:

- **Failure** - Sends failure traps.

- **Warning** - Sends warning traps.

- **Informational** - Sends informational traps.

- **Available** - Sends a trap when the system transitions from an unavailable to an available state.

- **Unavailable** - Sends a trap when the system transitions from an available to an unavailable state.

4 Click **Apply**.

Editing a Destination

Edit an SNMP destination to change the name of the destination or the types of traps the DXi V-Series sends to the destination.

To edit a destination:

1 Click **Edit**.

The **Edit Trap Destination** page displays (see Figure 123).

Figure 123 Edit Trap Destination Page
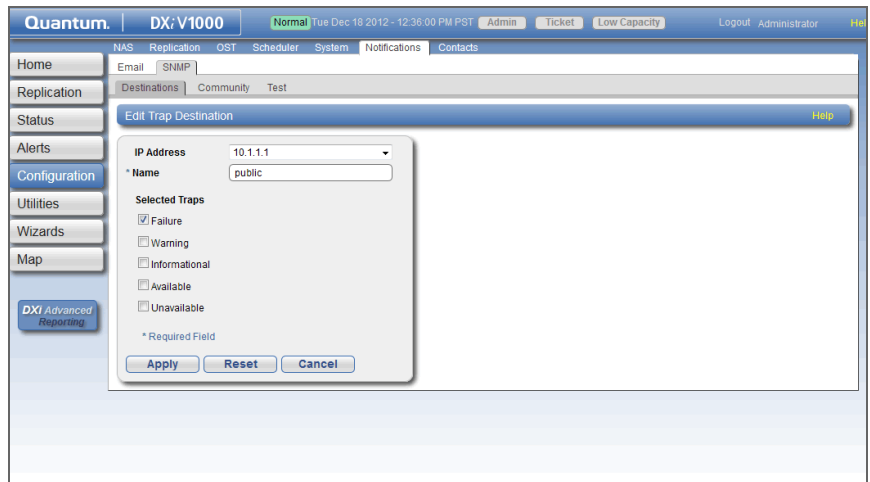
2 Enter information about the destination:

> **Note:** If you are editing a destination, you cannot change the **IP Address**.

- **IP Address** - (Optional) Select a different destination to edit.

- **Name** - Enter the name of the destination.

3 Select one or more traps to send to the destination:

- **Failure** - Sends failure traps.

- **Warning** - Sends warning traps.

- **Informational** - Sends informational traps.

- **Available** - Sends a trap when the system transitions from an unavailable to an available state.

- **Unavailable** - Sends a trap when the system transitions from an available to an unavailable state.

4 Click **Apply**.

Deleting a Destination

Delete an SNMP destination if you no longer want the DXi V-Series to send traps to the destination.

To delete a destination, select the destination and click **Delete**.

Note: You can select multiple destinations to delete at once.

Community

The **Community** page allows you to manage SNMP community information for the DXi V-Series. You can add, edit, and delete communities, and you can specify the community access type.

To access the **Community** page, on the **SNMP** page, click the **Community** tab (see Figure 124).

Figure 124 Community Page
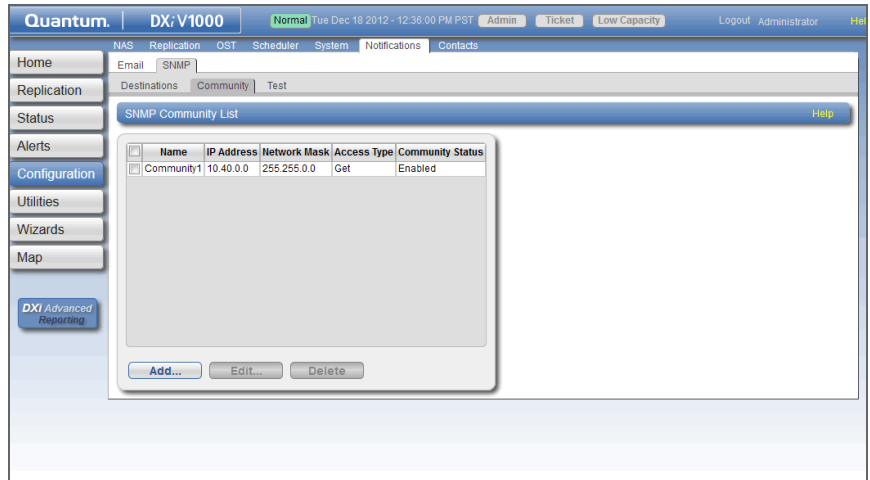
Use the **Community** page to perform the following tasks:

- View information about SNMP communities (see SNMP Community List on page 237).

- Add an SNMP community (see Adding a Community on page 237).

- Edit an SNMP community (see Editing a Community on page 239).

- Delete an SNMP community (see Deleting a Community on page 241).

SNMP Community List

The **SNMP Community List** displays the following information about SNMP communities:

- **Name** - The name of the community.

- **IP Address** - The IP address of the community.

- **Network Mask** - The network mask of the community.

- **Access Type** - The access type of the community (**Get** or **Get/Set**).

- **Community Status** - The status of the community (**Enabled** or **Disabled**).

Adding a Community

Add an SNMP community to include the DXi V-Series in a group of devices that are monitored by a common management station.

> **Note:** If no communities are defined, the SNMP agent is not accessible.

To add a community:

1 Click **Add**.

The **Add SNMP Community** page displays (see Figure 125).

Figure 125 Add SNMP Community Page
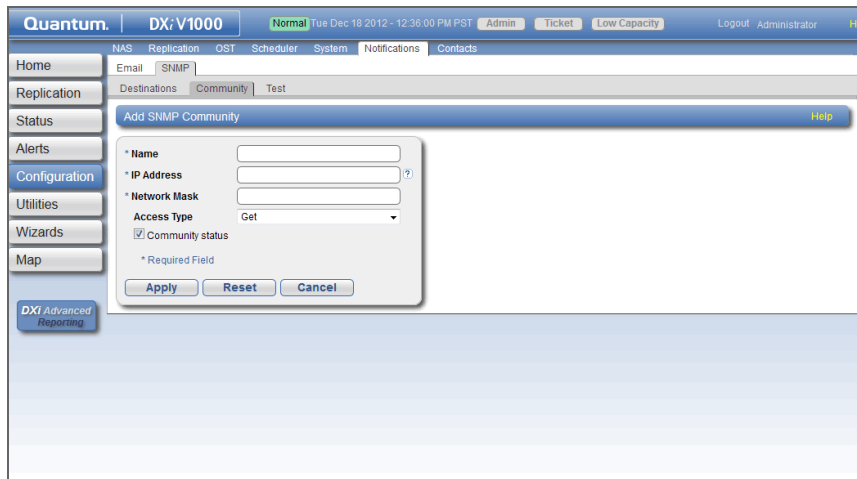
2 In the **Name** box, enter a unique **Name** for the community (up to 20 characters).

Valid characters are letters, numbers, hyphens, and underscores.

3 Enter a valid **IP Address** and **Network Mask** pair.

A pair is valid if performing a logical bitwise **AND** operation on the IP address and the network mask results in the IP address. See the table below for examples:

IP Address / Network Mask	Result
10.40.166.87 255.255.255.255	Allows access only from 10.40.166.87
10.40.166.87 10.40.166.87	Allows access only from 10.40.166.87

IP Address / Network Mask	Result
10.40.166.87 10.40.166.0	Invalid because the logical bitwise operation (address **AND** mask) is not equal to the address
10.40.166.87 255.255.0.0	Invalid because the logical bitwise operation (address **AND** mask) is not equal to the address
10.40.0.0 255.255.0.0	Allows access from any client with address 10.40.xx.xx

Note: If you define a single community and set both the IP address and network mask to 0.0.0.0 (or leave both blank), then IP address-based access control is disabled. In this case, the SNMP agent is accessible from any IP address.

Note: When entering IP addresses, never use an address that is in a reserved IP address range. To see a list of reserved IP address ranges, click the quick tip icon **[?]** located near the IP address field.

4 In the **Access Type** drop-down box, select the access type for the community:

- **Get** - Allows SNMP get operations.
- **Get/Set** - Allows both SNMP **get** and **put** operations.

5 Select the **Community status** check box to enable the community.

Or clear the **Community status** check box to disable the community.

6 Click **Apply**.

Editing a Community

Edit an SNMP community to change the IP address or access type for the community. You can also enable or disable the community.

To edit a community:

1 Click **Edit**.

The **Edit SNMP Community** page displays (see Figure 125).
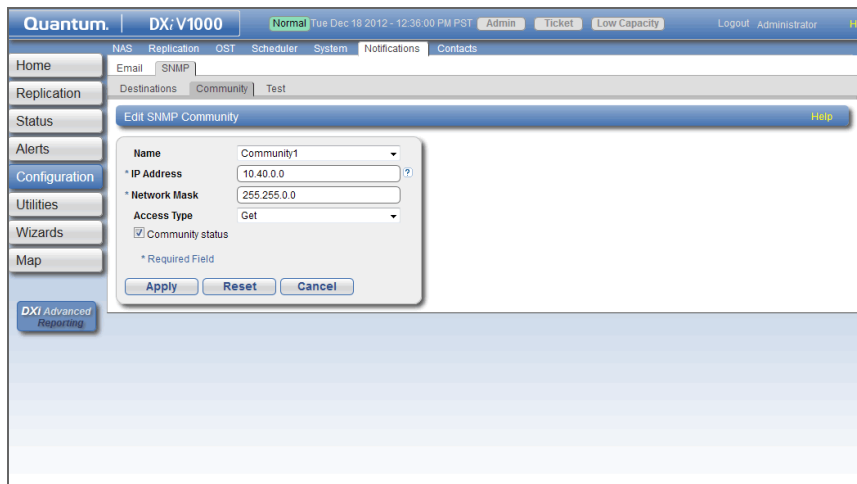
2 (Optional) In the **Name** box, select a different community to edit.

3 Enter a valid **IP Address and Network Mask** pair.

A pair is valid if performing a logical bitwise **AND** operation on the IP address and the network mask results in the IP address. See the table below for examples:

IP Address / Network Mask	Result
10.40.166.87 255.255.255.255	Allows access only from 10.40.166.87
10.40.166.87 10.40.166.87	Allows access only from 10.40.166.87
10.40.166.87 10.40.166.0	Invalid because the logical bitwise operation (address **AND** mask) is not equal to the address

IP Address / Network Mask	Result
10.40.166.87 255.255.0.0	Invalid because the logical bitwise operation (address **AND** mask) is not equal to the address
10.40.0.0 255.255.0.0	Allows access from any client with address 10.40.xx.xx

Note: If you define a single community and set both the IP address and network mask to 0.0.0.0 (or leave both blank), then IP address-based access control is disabled. In this case, the SNMP agent is accessible from any IP address.

Note: When entering IP addresses, never use an address that is in a reserved IP address range. To see a list of reserved IP address ranges, click the quick tip icon **[?]** located near the IP address field.

4 In the **Access Type** drop-down box, select the access type for the community:

- **Get** - Allows SNMP get operations.

- **Get/Set** - Allows both SNMP **get** and **put** operations.

5 Select the **Community status** check box to enable the community.

Or clear the **Community status** check box to disable the community.

6 Click **Apply**.

Deleting a Community

Delete an SNMP community if you no longer want the DXi V-Series to belong to a group of devices that are monitored by a common management station.

To delete a community, select the community and click **Delete**.

Note: You can select multiple communities to delete at once.

Test

The **SNMP Test** page allows you to send a test SNMP trap to verify that SNMP is correctly configured on the DXi V-Series.

To access the **SNMP Test** page, on the **SNMP** page, click the **Test** tab (see Figure 127).

Figure 127 SNMP Test Page
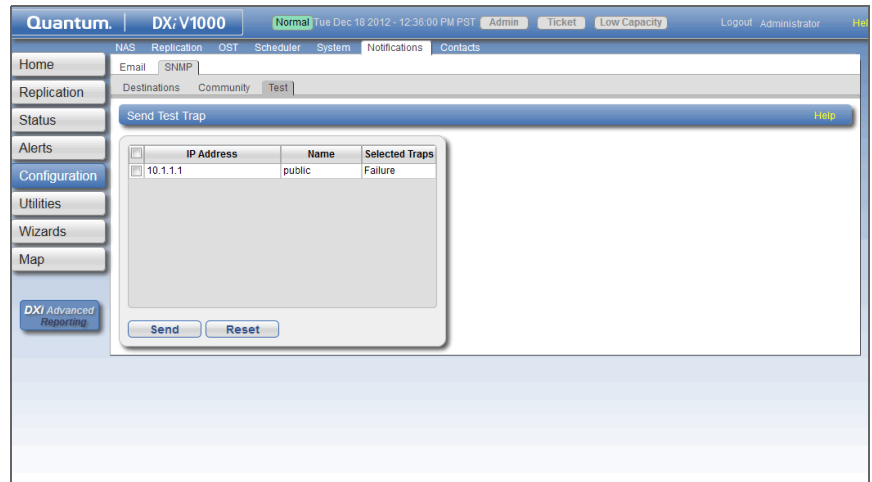
To send a test SNMP trap, select a destination in the list and click **Send**. If the destination does not receive the SNMP trap, make sure that the destination IP address is correct (see Editing a Destination on page 235). Also make sure that the community information is correct (see Community on page 236).

Contacts

The **Contacts** page allows you to enter company information. You can also enter individual contact information for primary and secondary contacts.

To access the **Contacts** page, click the **Configuration** menu, and then click the **Contacts** tab.

The **Contacts** page contains the following tabs:

*   [Company](#)

*   [Primary and Secondary](#)

Company

The **Company** page allows you to enter information about the company and location of the DXi V-Series.

To access the **Company** page, on the **Contacts** page, click the **Company** tab (see Figure 128).

Figure 128 Company Page

To enter company information:

1 Enter the following information:

*   **Company Name** - Enter the company name.

*   **Street** - Enter the company street address.

*   **City** - Enter the company city.

*   **State** - Enter the company state.

*   **Postal Code** - Enter the company postal code.

*   **Country** - Enter the company country.

*   **DXi V-Series Location** - Enter the physical location of the DXi V-Series (for example, data center).

> • **Support Contract** - Enter the support contract number for the DXi V-Series.
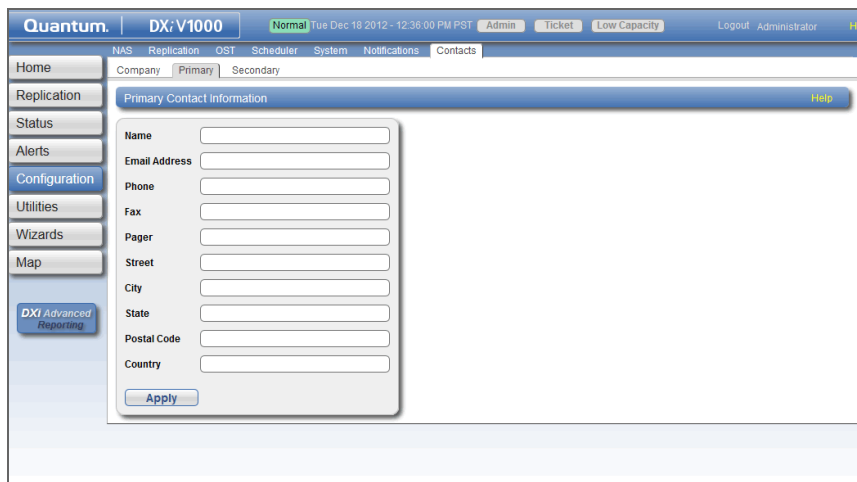
2 Click **Apply**.

Primary and Secondary

The **Primary** and **Secondary** pages allow you to enter information about the primary and secondary contacts for the DXi V-Series.

To access the **Primary** or **Secondary** page, on the **Contacts** page, click the **Primary** or **Secondary** tab (see Figure 129).

Figure 129 Primary and Secondary Pages

To enter primary or secondary contact information:

1 Enter the following information:

> • **Name** - Enter the contact name.
>
> • **Email Address** - (Required) Enter the contact e-mail address.
>
> • **Phone** - Enter the contact phone number.
>
> • **Fax** - Enter the contact fax number.
>
> • **Pager** - Enter the contact pager number.
>
> • **Street** - Enter the contact street address.
>
> • **City** - Enter the contact city.
>
> • **State** - Enter the contact state.

- **Postal Code** - Enter the contact postal code.
- **Country** - Enter the contact country.

2 Click **Apply**.

Chapter 9
DXi V-Series Utilities

The **Utilities** pages to perform maintenance tasks on the DXi V-Series, such as generating and downloading diagnostic files, analyzing disk and network performance, managing space reclamation, and securely erasing the system. You can also install license keys, upgrade the system software, and reboot or shut down the DXi V-Series.

To access the **Utilities** pages, click the **Utilities** menu.

The **Utilities** pages contain the following tabs:

- Diagnostics
- Analyzer
- Space Reclamation
- Secure Shred
- License Keys
- Software Upgrade
- Reboot & Shutdown

Diagnostics

The **Diagnostics** page allows you to generate and download diagnostic files. You can also perform healthchecks to verify the health and integrity of the data deduplication blockpool.

The diagnostic files are helpful when troubleshooting problems on the DXi V-Series. Generate and download the diagnostic files before contacting Quantum customer support.

To access the **Diagnostics** page, click the **Utilities** menu, and then click the **Diagnostics** tab.

The **Diagnostics** page contains the following tabs:

- System Diag File
- Healthchecks

System Diag File

The **System Diag File** page allows you to generate and download a system diagnostics file. This file contains the diagnostic logs for all of the system components.

To access the **System Diag File** page, on the **Diagnostics** page, click the **System Diag File** tab (see Figure 130).

Figure 130 System Diag File
Page
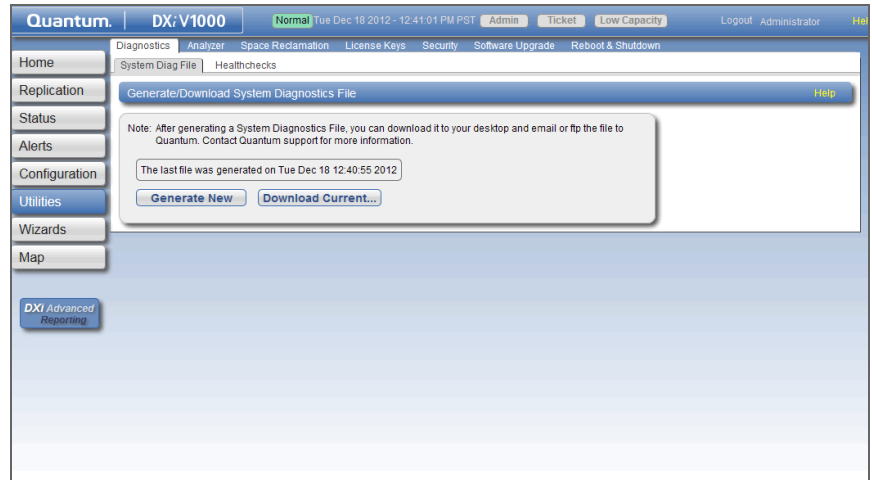
To generate and download a system diagnostics file:

1 Click **Generate New** to generate a new system diagnostics file.

The system generates a new diagnostics file. This can take several minutes.

2 After the file finishes generating, click the link to enable the **Download Current** button.

3 To download the generated diagnostics file, click **Download Current**.

A dialog box displays asking if you want to open or save the file.

4 Click **Save** or **OK** to download the file.

Healthchecks

The **Healthchecks** page allows you to perform tests that verify the health and integrity of the data deduplication blockpool. You can also enable and disable healthchecks.

Note: To configure the DXi V-Series to automatically run the healthchecks at specified intervals, use the **Configuration > Scheduler** page (see Scheduling Healthchecks on page 189).

To access the **Healthchecks** page, on the **Diagnostics** page, click the **Healthchecks** tab.

The **Healthchecks** page contains the following tabs:

- General

- Status

General

The **General** page allows you to start running the healthchecks or stop them if they are already running. When you start the healthchecks, only the healthchecks that are currently enabled are run (see Status on page 251).

To access the **General** page, on the **Healthchecks** page, click the **General** tab (see Figure 131).

Figure 131 General Page
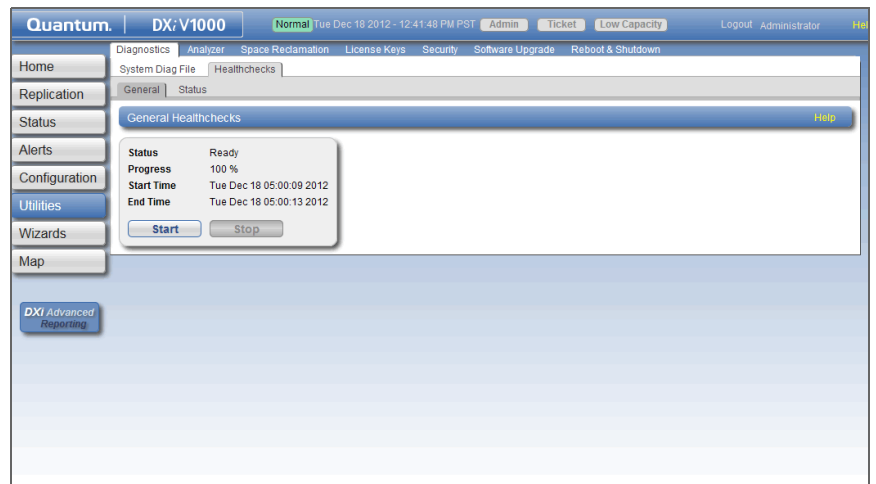
The **General** page displays the following information about the most recently run healthchecks:

- **Status** - The status of the healthchecks (**In Progress**, **Success**, **Failed**, or **Interrupted**).

- **Progress** - The percentage complete of the healthchecks.

- **Start Time** - The time the healthchecks started.

- **End Time** - The time the healthchecks ended.

Use the **General** page to perform the following tasks:

- To start all enabled healthchecks, click **Start**.

- To stop all healthchecks in progress, click **Stop**.

Status

The **Status** page allows you to view information about the most recent test results for each healthcheck. You can also enable or disable a healthcheck.

The following healthchecks are available:

- **De-Duplication** - Checks the overall health of the blockpool. This healthcheck verifies that the metadata in the namespace file and the data tags in the blockpool are correctly in sync.

- **Integrity** - Checks the integrity of data in the blockpool. This healthcheck examines a sample of data tags in the blockpool and verifies that the data has been properly stored without errors or corruption.

To access the **Status** page, on the **Healthchecks** page, click the **Status** tab (see Figure 132).

Figure 132 Status Page
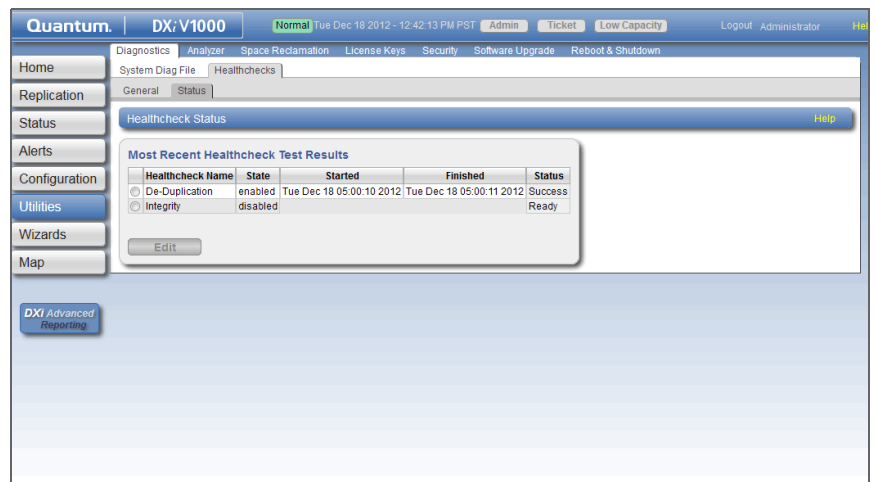
The **Status** page displays the following information about the most recently run test for each healthcheck:

- **Healthcheck Name** - The name of the healthcheck.

- **State** - The state of the healthcheck (**enabled** or **disabled**).
- **Started** - The time the healthcheck started.
- **Finished** - The time the healthcheck ended.
- **Status** - The status of the healthcheck (**Success** or **Failed**).

> **Note:** If running a healthcheck results in the Contact Support status, contact Quantum Customer Support for further assistance.

To enable or disable a healthcheck:

1 Select the healthcheck and click **Edit**.

The **Edit Healthcheck** page displays (see Figure 133).

Figure 133 Edit Healthcheck Page

2 Select the check box to enable the healthcheck.

Or clear the check box to disable the healthcheck.

3 Click **Apply**.

> **Note:** When healthchecks are run (manually or scheduled), only enabled healthchecks are run.

Caution: If a healthcheck fails when it is run, there may be a problem in the blockpool that could cause replication or restore operations to fail. Contact Quantum customer support if a healthcheck fails.

Analyzer

The **Analyzer** page allows you to analyze the network and disk performance of the DXi V-Series.

To access the **Analyzer** page, click the **Utilities** menu, and then click the **Analyzer** tab.

The **Analyzer** page contains the following tabs:

- Network
- Disk

Network

The **Network Analyzer** page allows you to analyze network performance by measuring network throughput between the DXi V-Series and another system (such as another DXi system).

To access the **Network Analyzer** page, on the **Analyzer** page, click the **Network** tab.

The **Network Analyzer** page contains the following tabs:

- Performance
- Settings

Performance

The **Performance** page allows you to perform network analysis with another system (the target). You can also view results from the most recently run test

To access the **Performance** page, on the **Network Analyzer** page, click the **Performance** tab (see Figure 134).
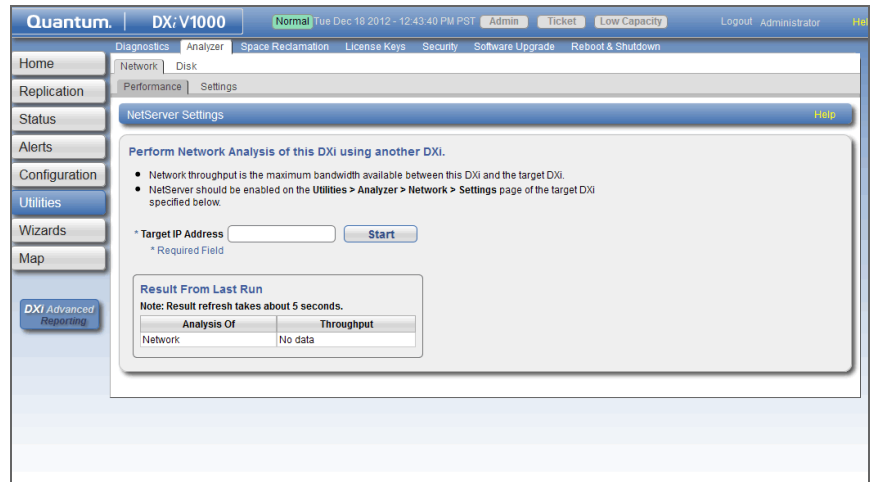
To perform network analysis:

1 In the **Target IP Address** box, enter the IP address of the system to perform network analysis with.

The target system must have NetServer enabled (see Settings on page 254).

2 Click **Start**.

The throughput result is displayed under **Result From Last Run** in MB/s.

Note: It takes approximately 5 seconds to refresh the results.

Settings

The **Settings** page allows you to enable or disable NetServer on the DXi V-Series. NetServer must be enabled on the target DXi system to perform network analysis with the system (see Performance on page 253).

To access the **Settings** page, on the **Network Analyzer** page, click the **Settings** tab (see Figure 135).

Figure 135 Settings Page

To enable or disable NetServer on the target DXi V-Series:

1 Select **Enable NetServer** to enable NetServer.

Or select **Disable NetServer** to disable NetServer.

2 Click **Apply**.

Note:	You should disable NetServer on the target system when you are done analyzing network performance.

Disk

The **Disk Analyzer** page allows you to analyze disk performance by measuring disk read and write throughput.

To access the **Disk Analyzer** page, on the **Analyzer** page, click the **Disk** tab (see Figure 136).

Figure 136 Disk Analyzer Page
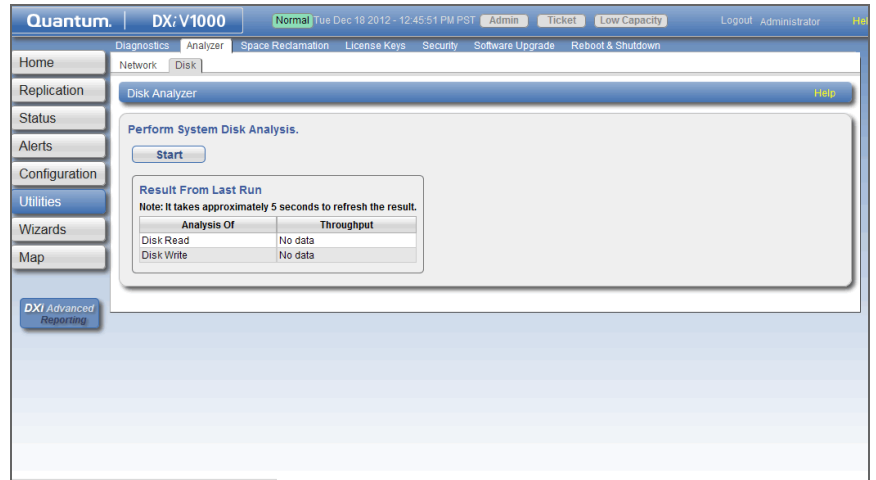
To perform disk analysis, click **Start**. The throughput result is displayed under **Result From Last Run** in KB/s.

Note: It takes approximately 5 seconds to refresh the results.

Space Reclamation

The **Space Reclamation** page allows you to manage space reclamation activity on the DXi V-Series. You can start or stop space reclamation. You can also monitor the progress of space reclamation activity.

During space reclamation, the DXi V-Series searches the blockpool for tags that are no longer referenced and then deletes the unneeded tags to free up space.

> **Caution:** For correct system operation, space reclamation *must* be run at regular intervals (at least once a week). Quantum recommends creating a schedule to automatically run space reclamation (see Scheduling Space Reclamation on page 190). Because space reclamation can affect system performance, avoid running space reclamation during known backup periods.

The space reclamation process can include up to four stages (see Space Reclamation Status on page 259).

- **New or Normal Mode** - To increase performance, when space reclamation is initiated on the **Space Reclamation** page or as a scheduled event, only Stage 2 (Calculating Deletion Candidates) and Stage 3 (Deleting New Candidates) are run.

  > **Note:** Stage 1 and 4 are not required in Normal mode because the DXi can automatically compact reclaimable space as needed and use it to store new deduplicated data.

- **Low Space or Legacy Mode** - When disk capacity is low, space reclamation is automatically started to free up disk space. In this case, all four stages of space reclamation are run.

To access the **Space Reclamation** page, click the **Utilities** menu, and then click the **Space Reclamation** tab (see Figure 137).
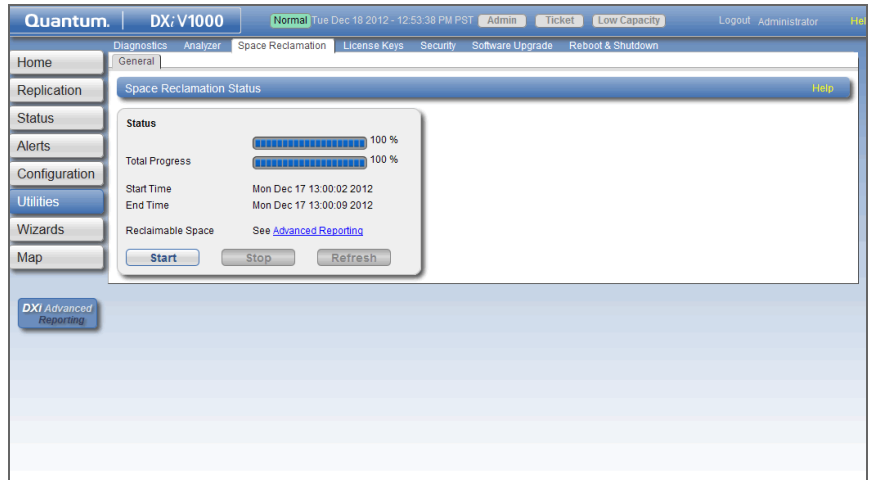
The **Space Reclamation** page displays the following information about the current or most recent space reclamation activity:

- **Status** - The status of space reclamation (see Space Reclamation Status on page 259).

- **Total Progress** - The progress of space reclamation activity.

- **Start Time** - The time space reclamation started.

- **End Time** - The time space reclamation ended.

- **Reclaimable Space/Space Reclaimed** - Displays **Pending** when space reclamation is running. When space reclamation is complete, click the link to view detailed statistics on the **Capacity Report - Disk Usage Graph** in DXi Advanced Reporting.

    Note: For help using the **Capacity Report**, click the help button on the upper right of the DXi Advanced Reporting window.

    Note: Because the DXi can automatically use reclaimable space to store new deduplicated data, space reclamation statistics may be affected (appear lower) if ingest occurs at the same time as space reclamation.

Use the **Space Reclamation** page to perform the following tasks:

- To start space reclamation, click **Start**.

- To stop space reclamation, click **Stop**.

- To update the display while space reclamation is running, click **Refresh**.

Space Reclamation Status

Space reclamation can have one of the following statuses:

- **Reclamation Completed** - Space reclamation completed without errors.

- **Reclamation Started by User** - Space reclamation was started manually by a user.

- **Reclamation Interrupted** - Space reclamation was interrupted and must be restarted.

- **Reclamation Interrupted by User** - Space reclamation was interrupted by a user and must be restarted.

- **Reclamation Interrupted - Error Encountered** - Space reclamation was interrupted because an error was encountered and must be restarted.

- **Reclamation Interrupt by User - Cannot be interrupted at this time** - Because the system is in a Low Space state, space reclamation cannot be stopped. Wait for space reclamation to finish freeing up disk space.

- **Reclamation Completed - No Candidates To Delete** - Space reclamation completed, but there were no candidates for reclamation.

- **Reclaim Existing Blockpool Freed Space** - The existing blockpool space has been reclaimed for use.

- **Stage 1 of 4** - Reclaim Disk Space (Initial).

- **Stage 2 of 4** - Calculating Deletion Candidates.

- **Stage 3 of 4** - Deleting New Candidates.

- **Stage 4 of 4** - Reclaim Disk Space.

License Keys

The **License Keys** page allows you to add a license key to the DXi V-Series to enable new functionality. You can also see the licenses that are installed on the system.

To access the **License Keys** page, click the **Utilities** menu, and then click the **License Keys** tab (see Figure 138).

Figure 138 License Keys Page
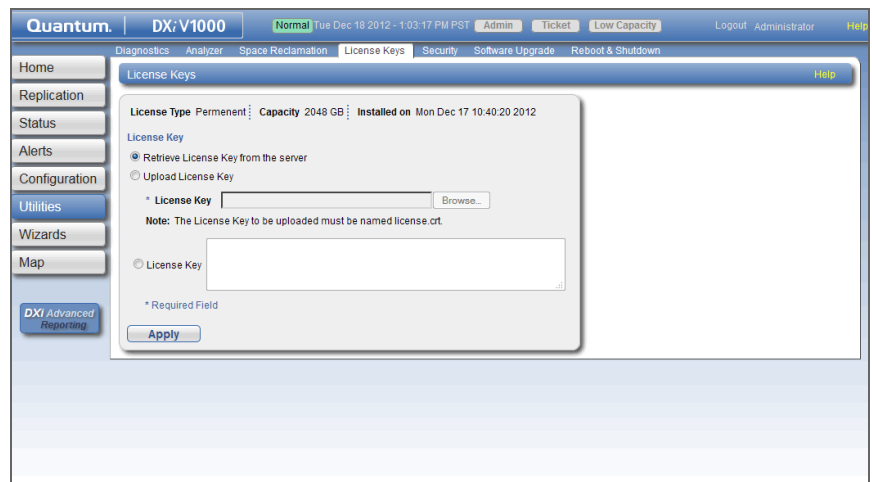
Use the **License Keys** page to perform the following tasks:

- View information about installed licenses (see License Key Information on page 260).

- Add a license key (see Adding a License Key on page 261).

License Key Information

The **License Keys** page displays the following information about the licenses that are installed on the DXi V-Series:

- **License Type** - The type of license currently installed on the DXi V-Series (**Permanent**, **Subscription**, or **Time-Based**).

> **Note:** For **Time-Based** licenses, the time remaining on the license is also displayed.

- **Capacity** - The current licensed capacity of the DXi V-Series.
- **Installed On** - The date a license was last installed.

Available Licenses

The following licenses are included with the DXi V-Series.

- **NAS** - Enables NAS (NFS, CIFS) connectivity.
- **Data Deduplication** - Enables data deduplication and compression.
- **Replication** - Enables replication to other DXi systems.
- **Storage Capacity** - Enables the purchased storage capacity for the system.
    - **DXi V1000 Trial Edition** - 256 GB of storage capacity.
    - **DXi V1000 Standard Edition** - 1 TB of storage capacity.
    - **DXi V1000 Enterprise Edition** - 1 TB of storage capacity, expandable to 2 TB.
    - **DXi V4000 Enterprise Edition** - 4 TB of storage capacity, expandable to 24 TB in 1 TB increments.

  If you purchase a storage capacity upgrade, you will receive a new Product Key certificate (see Adding a License Key on page 261).
- **OST** - Enables OpenStorage backup with Symantec OST.

Adding a License Key

Add a license key to enable new functionality on the DXi V-Series, for example, to add capacity or extend a Time-Based license.

> **Note:** Contact your Quantum sales representative to purchase a license. You will receive a License Certificate with instructions for obtaining and installing the license key.

There are three methods for adding a license key:

- (Recommended) Automatically Retrieving a License Key

- Uploading a License Key File
- Entering a License Key

Automatically Retrieving a License Key

The DXi V-Series automatically checks the license server each day to make sure the appropriate licenses are installed, based on your product serial number. If you have purchased a license but the DXi V-Series has not yet automatically retrieved the license, you can follow the procedure below to prompt the system to check for the new license and install it.

To automatically retrieve a license key from the license server:

1 On the **License Keys** page, select the **Retrieve License Key from the server** option.

2 Click **Apply**.

   The DXi V-Series automatically retrieves and installs the appropriate licenses based on the product serial number.

Note: To automatically retrieve license keys, the DXi V-Series must have access to the Internet. In addition, firewall port 443 (HTTPS) must be open on the network.

Uploading a License Key File

Use this method to install a license if Internet access via HTTPS (port 443) is not available and you have a **license.crt** file.

To manually upload a license key file:

1 Follow the instructions on the License Certificate you received to obtain the license key file.

2 On the **License Keys** page, select the **Upload License Key** option.

3 Click **Browse** to browse the system and locate the license key file. The license key file must be named **license.crt**.

4 Click **Apply**.

   The license key is installed on the system.

Entering a License Key

Use this method to install a license if Internet access via HTTPS (port 443) is not available and you have a license key.

To manually enter a license key:

1 Follow the instructions on the License Certificate you received to obtain the license key.

2 On the **License Keys** page, select the **License Key** option.

3 Copy the license key and then paste it into the **License Key** box.

4 Click **Apply**.

The license key is installed on the system.

Secure Shred

The **Secure Shred** page allows you to securely and permanently erase sensitive data stored on the DXi V-Series. To securely erase data, first delete files on NAS shares or storage servers, then start secure shred. During secure shred, all residual data associated with the deleted files is securely erased from the disk drives by performing a single-pass overwrite with zeros.

While secure shred is running, the DXi V-Series operates in limited mode. This means you cannot perform backups or restores, all scheduled jobs (including replication jobs) are stopped, and you cannot access or use any other features of the DXi. If necessary, you can cancel secure shred at any time and return the DXi to normal operation.

Caution: The secure shred process can take multiple days to complete.

Secure Shred and Virtual Machines

Secure shred behaves differently when it is run on a virtual machine compared to a physical system. Keep in mind the following information when running secure shred on a DXi V-Series:

• The secure shred function will zero out all empty space, up to a maximum of 2 TB (DXi V1000) or 24 TB (DXi V4000) of storage, regardless of the licensed capacity of the DXi V-Series. Make sure that the storage system has a full 2 TB (DXi V1000) or 24 TB (DXi V4000) of disk space available before running secure shred.

> **Note:** If the DXi V-Series is deployed on a thin-provisioned virtual disk, this will be converted to a thick-provisioned virtual disk if secure shred is run. (No capacity change will occur if the disk is already thick-provisioned.)

• The secure shred function is only effective on the current datastore location of the DXi V-Series. If the datastore has changed physical storage arrays since the DXi V-Series began operation, residual un-shredded data may be left in previously stored locations.

• For additional security, or in cases where the DXi V-Series may frequently migrate between physical storage arrays, you may choose to use VMware's virtual machine encryption option. While residual data would still be left after a migration, that data would be encrypted and unreadable without the appropriate password.

Running Secure Shred

To access the **Secure Shred** page, click the **Utilities** menu, and then click the **Security** tab (see Figure 139).

Figure 139 Secure Shred Page
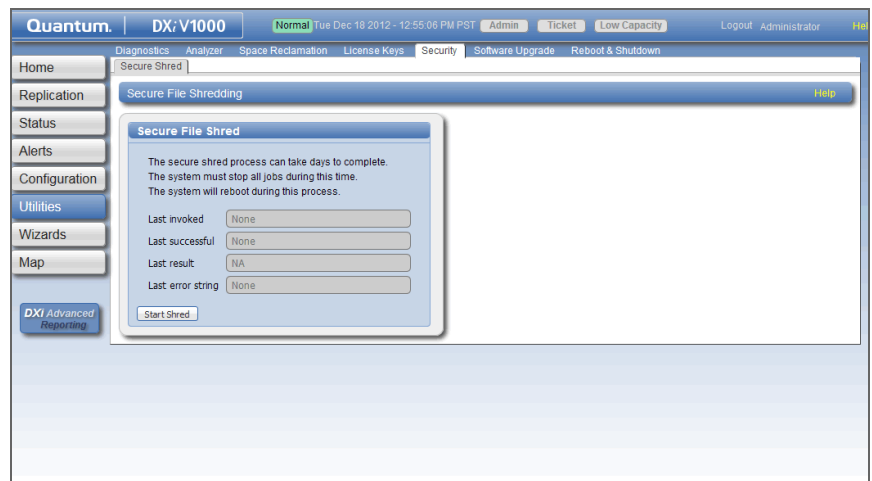
To securely erase data on the DXi V-Series:

1 Delete the data you want to securely erase:

- Delete files on NAS shares, or delete the shares (see <u>NAS</u> on page 127).

- Delete backup images on OST logical storage units (LSUs), or delete the LSUs and storage servers (see <u>OST</u> on page 151).

2 Run space reclamation from the **Utilities > Space Reclamation** page (see <u>Space Reclamation</u> on page 256).

3 If the DXi V-Series is *not* in Low Capacity condition (the **Low Capacity** indicator in the banner is not lit), then you must manually run space reclamation Stage 4 using the command line interface (CLI) console with the following command:

```
syscli --start compaction
```

Note: For more information about using the CLI console, see the *DXi-Series Command Line Interface (CLI) Guide* (6-67081).

Note: If the DXi V-Series is in Low Capacity condition (the **Low Capacity** indicator in the banner is lit), then you can skip this step.

4 Make sure all replication and backup jobs are completed (see <u>DXi V-Series Replication</u> on page 69).

5 On the **Secure Shred** page, click **Start Shred**.

A warning message displays.

6 Click **Yes**.

The system reboots and begins the secure shred process. This process can take multiple days to complete.

7 To check the status of secure shred, log onto the DXi V-Series to view the limited **Secure Shred Mode** interface (see <u>Figure 140</u>).

- The **Secure File Shred Log** displays details about the secure shred progress. Click **Hide** to hide the log.

- To cancel the secure shred process, click **Cancel**. The DXi reboots and resumes normal operation.

• When the secure shred process is complete, the **Reboot** button displays.

Note: You must log on as an Admin user to cancel secure shred or reboot the system.

Figure 140 Secure Shred Mode Interface

When secure shred is complete, Cancel changes to Reboot
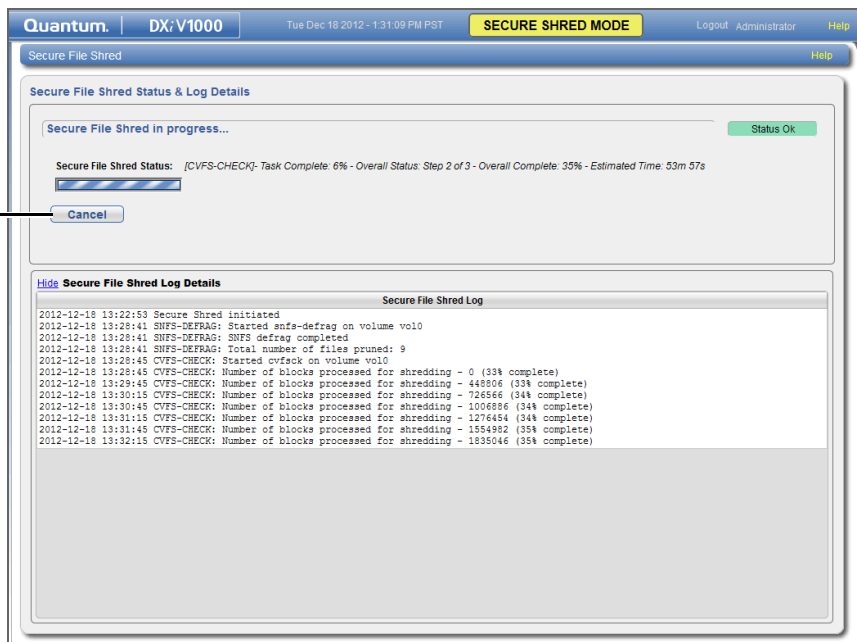
8 Click **Reboot** to finalize the secure shred process and reboot the DXi.

After the DXi finishes rebooting, you can resume normal system operation.

Software Upgrade

The **Software Upgrade** page allows you to upload a new software image to update the system software on the DXi V-Series.

Note: The system should be scheduled for downtime during a software upgrade.

To access the **Software Upgrade** page, click the **Utilities** menu, and then click the **Software Upgrade** tab (see Figure 141).

Figure 141 Software Upgrade Page

To upload a new system software image:

1 Make sure the following conditions are met before you continue:

- All replication and backup jobs are completed (see DXi V-Series Replication on page 69).

- All space reclamation tasks are completed without errors (see Space Reclamation on page 256).

- All outstanding administration alerts are deleted (see Admin Alerts on page 115).

- Healthchecks complete successfully without errors (see Healthchecks on page 249).

2 In the **Software Image File** box, type the location and filename of the new software image file.

Or click the **Browse** button to browse the system and locate the new software image. The software image file must end with the **.fw** extension.

3 Click **Upload**.

A **Warning** message displays.

4 Click **Start** to begin the upload process.

Do not close the window until the upload process is complete. An **Information** message displays stating the software image was uploaded successfully.

5 Click **OK**.

The **Activate/Remove Software Image** message displays (see Figure 142).

Figure 142 Activate/Remove
Software Image

Delete all Admin Alerts before activating the software image

6 Click **Activate** to activate the new software image.

> **Note:** To remove the software image from the system instead of activating it, click **Remove**.

A **Confirmation** message displays.

7 Click **Yes**.

A **Warning** message displays stating that activating the software will cause backup jobs to fail.

8 Click **Yes**.

An Information message displays stating that the system will restart.

The system automatically reboots two or more times during the software update process. Wait at least 15 minutes before attempting to log on to the system again.

Note: Clear your Web browser cache before logging on to the remote management console for the first time following the software upgrade. This will ensure the remote management console displays correctly.

Note: Following the software upgrade, the DXi V-Series will automatically contact the license server and install your product key and license. If the DXi V-Series does not have Internet access via HTTPS (port 443), it cannot contact the license server. In this case, you may not be able to ingest data until you have manually installed the product key and license. For more details, see Dark Site Upgrade Licensing on page 269.

Dark Site Upgrade Licensing

If you upgrade the DXi V-Series from software version 2.1.1 without Internet access, you *must* manually install a product key and license after completing the upgrade. You can obtain the product key and license from Quantum Support.

To apply the product key, access the DXi V-Series command line interface (CLI) console and log in as the **cliadmin** user. The default password is **cliadmin**, but your DXi administrator may have changed it. For more information about using the CLI console, see the *DXi-Series Command Line Interface (CLI) Guide* (6-67081).

After logging on to the CLI console, type the following command and press **<Enter>**:

```
syscli --activate --productkey XXXXX-XXXXX-XXXXX-XXXXX
```

where XXXXX-XXXXX-XXXXX-XXXXX-XXXXX is your product key.

If you entered the command correctly, the system responds with the following message: `Command completed successfully.`

You can now add the license using the **Utilities > License Keys** page in the remote management console (see Adding a License Key on page 261).

Reboot & Shutdown

The **Reboot & Shutdown** page allows you to reboot or shut down the DXi V-Series.

To access the **Reboot & Shutdown** page, click the **Utilities** menu, and then click the **Reboot & Shutdown** tab (see Figure 143).

Caution: Before shutting down the DXi V-Series, make sure that all backup and replication jobs are finished, and that space reclamation activity is complete.

Figure 143 Reboot & Shutdown Page

To reboot or shutdown the DXi V-Series:

1 Under **System Action**, select an option:

- **Reboot** - Reboots the DXi V-Series.

  Rebooting the system closes the Web browser connection. You must log on again after the system has rebooted.

- **Shutdown** - Shuts down the DXi V-Series.

- **Reset from diagnostic state** - (Only available when the node is in degraded mode) Restarts the services on the node without rebooting the system.

2 Click **Apply**.

3 Close the browser window.

Note: Shutting down the system can take up to 15 minutes. Only the node will completely shut down. When rebooting, the system can take approximately 30 minutes to start up, depending on the amount of installed storage capacity.

Troubleshooting

This appendix describes the status and problem reporting features of the DXi V-Series as well as problems you might encounter during setup and operation of the system. Corrective information is provided to help you resolve these problems.

For for information about troubleshooting the DXi V-Series, see the following sections:

* DXi V-Series Status and Problem Reporting
* General Troubleshooting Actions
* Common Problems and Solutions

DXi V-Series Status and Problem Reporting

To maintain system health and help you identify and correct problems that occur, the DXi V-Series constantly performs the following actions:

* Monitors the system software and hardware components.
* Detects system problems.
* Attempts to isolate each problem to a specific field replaceable component.

- Attempts to recover from the problem.

- Logs the problem.

- If the problem requires service, the system reports the problem in a service ticket associated with the field replaceable component.

General Troubleshooting Actions

For information about general troubleshoot actions you can take, see the following sections:

- Viewing Service Tickets

- Downloading a System Diagnostics File

Viewing Service Tickets

Service tickets include time and date information, status (open or closed), information about each error, and links to recommended troubleshooting procedures. The DXi V-Series generates service tickets according to the following scenarios:

- If the component associated with the problem does not have an open service ticket, the DXi V-Series opens a service ticket for the component and reports the problem in a service ticket.

- If the problem reoccurs, the DXi V-Series logs the number of times that it detects the problem in the existing report.

- If a different problem occurs with the same component, the DXi V-Series adds a new report to the same service ticket.

- If a problem occurs with a different component, the DXi V-Series uses the above scenario to open a new service ticket for the component or report the problem in an existing service ticket associated with the component.

To access the **Service Tickets** page, click the **Alerts** menu, and then click the **Service Tickets** tab.

For more information about working with service tickets, see Service Tickets on page 117.

Downloading a System Diagnostics File

The **System Diag File** page allows you to generate and download a system diagnostics file. This file contains the diagnostic logs for all of the system components.

To access the **System Diag File** page, on the **Diagnostics** page, click the **System Diag File** tab.

For information about downloading the system diagnostics file, see System Diag File on page 248.

Common Problems and Solutions

The troubleshooting information in this section covers the following topics:

- Start-up Problems
- Ethernet Network Problems
- Replication Problems

Start-up Problems

Table 1 describes problems that can occur during system start-up.

Table 1 Start-up Problems

Problem	Corrective Action
FATAL ERROR Unable to start SNFS! Message displays.	Contact your Quantum Customer Support representative (see Getting More Information or Help on page xxii).
FATAL ERROR Unable to start blockpool! Message displays.	Contact your Quantum Customer Support representative (see Getting More Information or Help on page xxii).

Ethernet Network Problems

Table 2 describes corrective actions for problems occurring with the Ethernet network.

Table 2 Ethernet Network Problems

Problem	Corrective Action
DXi V-Series system is not visible on the Ethernet network.	Try to ping the DXi V-Series system IP address from a host on the same network. If the ping reports round trip times, the DXi V-Series system is active. If not, check the cables, switches, or hubs for damaged components. If everything checks out, contact the Quantum Customer Support department (see Getting More Information or Help on page xxii).
DXi V-Series remote management pages are not visible.	IF you cannot connect to the DXi V-Series remote management pages, verify that the following network settings for the DXi V-Series are correct: • Hostname • IP addresses • Default gateway • Subnet mask • Domain name (optional)
An Ethernet cable is removed during normal operation.	The system will discontinue use of the associated Ethernet port. A Service ticket will be issued. The possibility of errors exist; data corruption will not occur. Reconnect the cable as soon as possible. It is not necessary to power the system off. Depending on the state of the system when the Ethernet cable was removed, replication, system management, or ingest may need to be restarted.

Replication Problems

Table 3 describes corrective actions for problems occurring with the replication.

Table 3 Replication Problems

Problem	Explanation/Corrective Action
The replication was paused, but the replication is still in process.	When you click **Pause**, the system will continue to replicate the current tag or block of information in process. The process of completing the current tag replication can take up to 15 minutes to complete. Once that tag has completed replication the system will pause and wait to resume.
The replication was paused and a **Failure** event was generated in the **Replication Events** page.	This is normal. When a replication is paused, a failure event is generated on the **Replication Events** page. They system will continue the replication when you click **Resume**.
Replication was disabled while a replication was in process and the replication completed.	If you click **Disable** during a replication in process, the system will complete the entire replication and then disable replication on the system. The system will be unable to replicate until you click **Enable**.
Enabled replication on a NAS share and received the following Event: No destination host is specified for replication.	You must configure the target system prior to configuring the source. If the target system is not configured first, you will not be able to designate the replication target.
Able to enable and schedule replication for NAS even though no target IP configured.	It is possible to enable and schedule a replication when a target system has not been configured. The replication will not start until a target system is configured.

Glossary

B

Blockpool   A pool of all unique data blocks that were captured during the data deduplication cycle. When backup jobs occur, the data deduplication engine searches for new data entering the DXi V-Series and uses a variable length compression type algorithm to compare this to existing data in the blockpool. Unique blocks are added to the blockpool and all known blocks are indexed.

Byte   The basic unit of computer memory which is large enough to hold one character.

C

Compress   A process of removing fine-grained redundancy from data prior to storing or transmitting it. The granularity may vary, but generally compression deals with redundancy in grains of a few bytes.

D

Data Deduplication   A process of removing coarse-grained redundancy from data prior to storing or transmitting it. The granularity may vary, but generally data deduplication deals with redundancy in grains of several kilobytes. When you select **Enable Data Deduplication** for a NAS share, data deduplication is running all of the time. Backup data is sent to

the DXi V-Series and data deduplication is performed on data as it is ingested.

Disk   A fixed set of sectors with sequential numbers starting from zero, directly and independently accessible and mutable by those numbers without affecting any other sector.

F

Filesystem   An abstraction layered over storage devices (typically disks) obscuring the physical details of the storage devices it supports in favor of a presentation oriented at storing and organizing files.

H

Host   The device or devices to which the system is connected.

I

Ingest   The throughput performance of data writes to the system.

L

LSU   Logical Storage Unit. A logical storage entity defined under the Symantec OpenStorage API.

N

NAS   Network Attached Storage is file-level computer data storage connected to a computer network providing data access to network clients.

NDMP   Network Data Management Protocol is a protocol meant to transport data between NAS devices, also known as filers, and backup devices. This removes the need for transporting the data through the backup server itself, thus enhancing speed and removing load from the backup server.

O

OST   OpenStorage API. An interface specific to Symantec NetBackup and Backup Exec for writing data to disk backup appliances, replicating it, and, in the case of NetBackup, writing data directly to disk, under control of the backup application.

R

RAID   Redundant Array of Independent Disks is a technology through which several physical storage disks are grouped into an array that appears to an operating system as one or more physical devices.

S

SNFS   StorNext® File System

SNMP   Short for *Simple Network Management Protocol*, a set of protocols for managing complex networks.

Sync ID   When you configure a share for Directory/File Based Replication, you specify a Sync ID for the share. The Sync ID associates the share on the source system with the share on the target system that will received the replicated data. The Sync ID of the source share and the target share *must* be identical.

T

Terabyte   A unit of measure for digital data equal to 1,000 gigabytes.