

Titan SiliconServer



System Administration Manual

Publication Title	Titan SiliconServer - System Administration Manual
Publication Date	February 2006

Neither BlueArc Corporation nor its affiliated companies (collectively, “BlueArc”) makes any warranties about the information in this guide. Under no circumstances shall BlueArc be liable for costs arising from the procurement of substitute products or services, lost profits, lost savings, loss of information or data, or from any other special, indirect, consequential or incidental damages, that are the result of its products not being used in accordance with the guide.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). Some parts of ADC use open source code from Network Appliance, Inc. and Traakan, Inc.

The product described in this guide may be protected by one or more U.S. patents, foreign patents, or pending applications.

The following are trademarks licensed to BlueArc Corporation, registered in the USA and other countries: BlueArc™, the BlueArc™ logo and the BlueArc Storage System™.

Microsoft, MS-DOS, Windows, Windows NT, and Windows 2000/2003 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through The Open Group.

All other trademarks appearing in this document are the property of their respective owners.
Copyright © 2006 BlueArc Corporation. All rights reserved.

Other Related Documents

The documents, which are listed below, provide a full specification on how to configure and administer the storage enclosures in the Titan subsystem.

- ❑ **Hardware Guide:** This guide (in PDF format) provides an overview of the hardware, describes how to resolve any problems, and shows how to replace faulty components.
- ❑ **FC-14 User Manual:** This document (in PDF format) provides a full specification of the FC-14 Storage Enclosure and instructions on how to administer it.
- ❑ **FC-16 User Manual:** This document (in PDF format) provides a full specification of the FC-16 Storage Enclosure and instructions on how to administer it.
- ❑ **SA-14 User Manual:** This document (in PDF format) provides a full specification of the SA-14 Storage Enclosure and instructions on how to administer it.
- ❑ **AT-14 User Manual:** This document (in PDF format) provides a full specification of the AT-14 Storage Enclosure and instructions on how to administer it.
- ❑ **AT-42 User Manual:** This document (in PDF format) provides a full specification of the AT-42 Storage Enclosure and instructions on how to administer it.
- ❑ **Command Line Reference:** This guide (in HTML format) describes how to administer the system by typing commands at a command prompt.
- ❑ **Release Notes:** This document gives late-breaking news on the system.

About This Guide

The following types of messages are used throughout this guide. We recommend that these messages are read and clearly understood before proceeding.



Tip: A tip contains supplementary information that is useful in completing a task.



Note: A note contains information that helps to install or operate the system effectively.



Caution: A CAUTION INDICATES THE POSSIBILITY OF DAMAGE TO DATA OR EQUIPMENT. DO NOT PROCEED BEYOND A CAUTION MESSAGE UNTIL THE REQUIREMENTS ARE FULLY UNDERSTOOD.

Support

Any of the following browsers can be used to run the BlueArc SiliconServer System Management Unit (SMU) Web-based Graphical User Interface.

- ❑ Microsoft Internet Explorer: Version 6.0 or later.
- ❑ Mozilla Firefox: Version 1.0.4 or later.

The following Java Runtime Environment is required to enable some advanced functionality of the SiliconServer's Web UI.

- ❑ Sun Microsystems Java Runtime Environment: Version 5.0, update 6, or later.

A copy of all product documentation is included for download or viewing through the Web UI. The following software is required to view this documentation:

- ❑ Adobe Acrobat: Version 7.0.5 or later.

Table of Contents

- Chapter 1. The BlueArc Storage System 1**
 - Storage System Overview. 1
 - The Titan SiliconServer 2
 - Enterprise Virtual Servers 3
 - The Storage Subsystem 3
 - The System Management Unit (SMU) 4
 - The Private Management Network. 4
 - Titan SiliconServer Initial Setup 6
 - Managing the Titan SiliconServer 7
 - Using Web Manager. 7
 - Using the Command Line Interface 13
 - Using the Embedded Web UI 16
- Chapter 2. System Configuration. 17**
 - Configuring the System Management Unit (SMU) 17
 - Using the SMU Setup Wizard 18
 - Configuring Security Options. 19
 - SMTP Relay Configuration 20
 - Selecting Managed Servers. 21
 - User Management 24
 - Configuring the Management Network. 36
 - Configuring the Management Network. 38
 - Configuring Devices on the System Monitor 40
 - Configuring a System Power Unit 45
 - Configuring the Titan SiliconServer 47
 - Using the SiliconServer Setup Wizard. 47
 - Configuring Server Identification 52
 - Configuring Date and Time. 53
 - Controlling Direct Server Access 56
 - About License Keys 58
 - Using License Keys 59
- Chapter 3. Network Configuration 61**
 - Titan Networking Overview and Concepts 61
 - Gigabit Ethernet Data Interfaces 61
 - Jumbo Frames. 63
 - IP Address Assignments 63

Table of Contents

Network Statistics	64
Configuring the Gigabit Ethernet Interfaces	64
Link Aggregations (IEEE 802.3ad)	64
IP Network Setup	68
IP Routes	73
Static Routes	73
Default Gateways	74
Dynamic Host Routes	74
Routing Precedence	74
Managing the Server's Route Table	75
Configuring Name Services	76
Setting up the System to Work with a Name Server	76
Configuring Network Information Services	80
Chapter 4. Multi-Tiered Storage	91
Multi-Tiered Storage Overview and Concepts	91
Multi-Tiered Storage	91
Fibre Channel Fabric and Arbitrated Loop	93
Load Balancing and Failure Recovery	94
Fibre Channel Statistics	95
FC-14 and SA-14 Storage Subsystems	95
Storage Characteristics	95
Discovering and Adding Racks	96
Creating System Drives	99
Managing FC-14 and SA-14 Storage	102
Reviewing Events Logged	108
Monitoring Physical Disks	109
FC-16 Storage Subsystem	111
Storage Characteristics	112
Creating System Drives	112
Managing FC-16 Storage	117
Monitoring Physical Disks	122
AT-14 and AT-42 Storage Subsystem	126
Storage Characteristics	126
Creating System Drives	128
Configuring the Storage Enclosure	129
System Drives	133
Managing System Drives	133

Creating System Drives	133
Viewing System Drives	133
Chapter 5. Storage Management.	140
Introduction	140
System Drives	140
About Storage Pools	140
About Chunks	141
About Silicon File Systems	141
About Virtual Volumes	142
Using Storage Pools	142
Using Silicon File Systems	148
Expanding a Silicon File System	153
Relocating a Silicon File System	153
WORM File Systems	163
Controlling File System Usage	165
Setting Usage Quotas	167
Understanding Quotas	167
Managing Usage Quotas	169
Using Virtual Volumes	174
Understanding Virtual Volumes	174
Managing Virtual Volumes	175
Managing Quotas on Virtual Volumes	179
Retrieving Quota Usage through rquotad	186
The Quota Command	186
Implementing rquota on Titan	186
BlueArc Data Migrator	189
Data Migration Paths	190
Data Migration Rules	193
Data Migration Policies	205
Data Migration Schedules	209
Data Migration Reports	214
Reverse Migration	219
Considerations when using Data Migrator	219
Chapter 6. File Services	222
File Service Protocols	222
Enabling File Services	222
File System Security	223

Table of Contents

Mixed Security Mode	224
UNIX Security Mode	226
Security Mode Configuration	226
Mixed Mode Operation	232
File Locks in Mixed Mode	233
Configuring User and Group Mappings	235
Sharing Resources with NFS Clients	242
The Titan SiliconServer and NFS	242
Configuring NFS Exports	243
Using CIFS for Windows Access	249
The Titan SiliconServer and CIFS	249
Dynamic DNS	251
Configuring CIFS Security	252
Configuring Local Groups	257
Configuring CIFS Shares	259
Controlling Access to Shares	263
Using Windows Server Management	265
Transferring files with FTP	270
The Titan SiliconServer and FTP	270
Configuring FTP Preferences	270
Setting up FTP Mount Points	272
Setting Up FTP Users	274
Setting Up FTP Audit Logging	277
Block-Level Access through iSCSI	279
The Titan SiliconServer and iSCSI	280
Configuring iSCSI	281
Setting up iSCSI Logical Units	283
Setting Up iSCSI Targets	288
iSCSI Security (Mutual Authentication)	292
Accessing iSCSI Storage	294
Chapter 7. Data Protection	300
Data Protection Overview	300
Checkpoints	300
Protecting the Data from Failures	300
Using Snapshots	302
Snapshots Concepts	302
Accessing Snapshots	302
Latest Snapshot	303

Quick Snapshot Restore	303
Snapshot Rules	303
Managing Snapshots	306
Performing NDMP Backups	308
Configuring NDMP	309
NDMP Backup Devices	312
NDMP and Snapshots	315
Backing Up Virtual Volumes and Quotas	318
Clearing the Backup History or Device Mappings	319
Using Storage Management Applications	320
Compatibility with Other SiliconServers	330
Policy-Based Data Replication	332
Incremental Data Replication	332
Incremental Block-Level Replication	333
Configuring Policy-Based Replication	333
Creating Replication Policies	334
Choosing the type of Destination SiliconServer	334
Replication Policies	335
Replication Rules	340
Replication Files to Exclude Syntax	346
Replication Schedules	346
Scheduling Incremental Replications	351
Replication Status & Report	351
Troubleshooting Replication Failures	354
Virus Scanning	356
Virus Scanning Overview	357
Configuring Virus Scanning	357
Forcing Files to be Rescanned	361
Chapter 8. Scalability and Clustering	362
Scalability and Clustering Overview	362
Enterprise Virtual Servers	362
Shared Storage Pool	362
High Availability Clusters	363
Server Farms	363
Using Enterprise Virtual Servers	365
EVS Management	368
Titan High Availability Clusters	370
Clustering Concepts	370

Table of Contents

Creating a Cluster	372
Managing a Cluster	375
Cluster Name Space.	379
CNS Topology	380
Creating a Cluster Name Space	381
Editing a Cluster Name Space	382
Considerations when using CNS	384
Migrating an EVS.	384
Migrating an EVS within an HA Cluster.	384
Migrating an EVS within a Server Farm	387
Chapter 9. Status & Monitoring	391
BlueArc Storage System Status	391
Checking the System Status	393
Checking the Status of a Server Unit	396
Checking the Status of a Power Unit	397
Checking the Status of a Storage Unit	398
Checking the Status of the SMU	403
Monitoring Multiple Servers	405
Titan SiliconServer Statistics	406
Ethernet Statistics	406
TCP/IP Statistics	410
Fibre Channel Statistics	414
File and Block Protocol Statistics	417
Data Access and Performance Statistics	426
Management Statistics	428
Event Logging and Notification	434
Using the Event Log.	435
Setting up Event Notification.	438
Setting Up an SNMP Agent	448
The Management Information Base.	448
Chapter 10. Maintenance Tasks.	454
Checking Version Information.	454
Saving and Restoring the Server's Configuration.	457
Saving and Restoring the SMU's Configuration	459
Standby SMU	459
Upgrading System Software and Firmware.	462

Table of Contents

Upgrading SMU Software 462

Upgrading Titan Server Firmware 463

Providing an SSL Certificate 467

 Requesting and Generating Certificates 467

 Acquiring a SSL Certificate from a Certificate Authority (CA) 469

 Installing and Managing Certificates 469

 Accepting Self-Signed Certificates 470

Shutting Down / Restarting the System 472

 Shutting Down / Resetting the Titan SiliconServer 472

 Shutting Down / Restarting the SMU 474

Default Username and Password 475

1 The BlueArc Storage System

Storage System Overview

The BlueArc Storage System is a highly scalable and modular Network Attached Storage (NAS) server with multi-gigabit throughput from network to disk.

The Titan SiliconServer has a patented architecture structured around bi-directional data pipelines and a hardware-based file system. This allows the storage capacity to scale to 256 Terabytes, and sustain higher access loads without compromising performance. The storage system can be configured as a single server or as a dual-server, high-availability cluster.

Titan supports BlueArc's Multi-Tiered Storage (MTS), which can simultaneously connect multiple diverse storage subsystems behind a single server unit (or cluster). Using MTS, Titan can be customized to match the storage requirements of your applications. In this way, Titan provides a solution that can meet your performance and scaling goals.

The BlueArc Storage System consists of the following elements:

- ❑ [The Titan SiliconServer](#). The SiliconServer technology is the core of the BlueArc Storage System.
- ❑ [Enterprise Virtual Servers \(EVS\)](#). The EVS are the file serving entities of the Titan SiliconServer.
- ❑ [The Storage Subsystem](#). The storage subsystem consists of devices that store the data managed by the Titan SiliconServer.
- ❑ [The System Management Unit \(SMU\)](#). The SMU provides server administration and monitoring tools. In addition, it supports clustering, data migration, and replication.
- ❑ [The Private Management Network](#). The management network consists of auxiliary devices required for operation of the BlueArc Storage System, such as RAID storage subsystems, FC switches, and Uninterruptible Power Supply (UPS) units.

The Titan SiliconServer

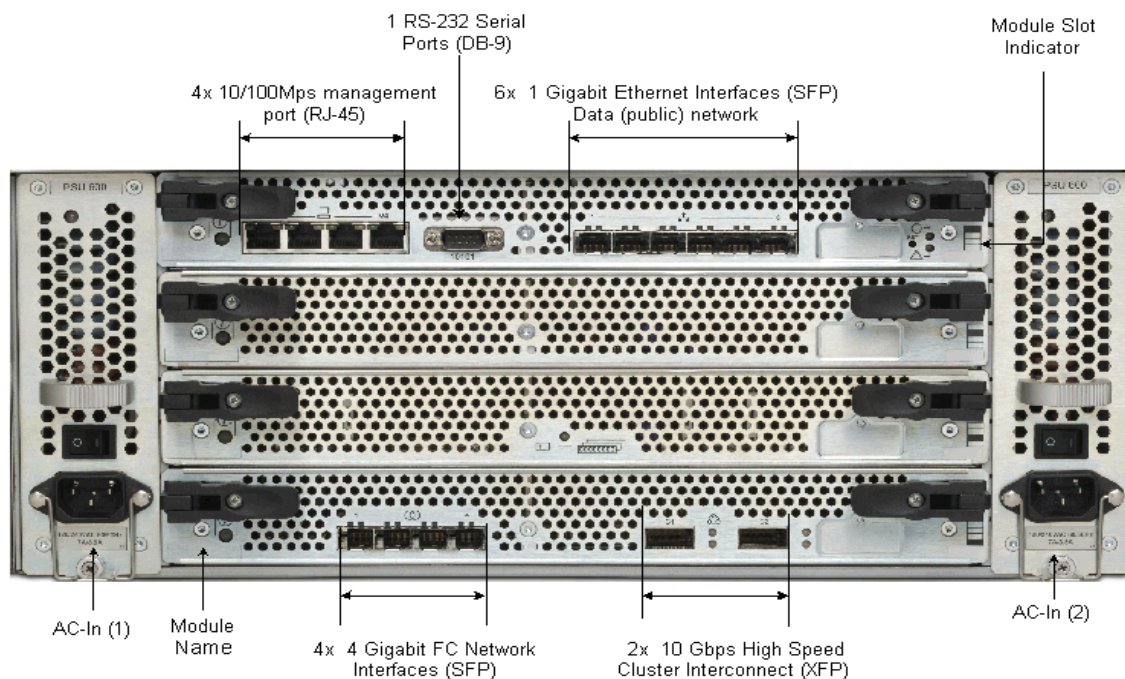
Titan is a high-performance, enterprise-class Network Attached Storage (NAS) server, which services file access requests issued by network clients through Gigabit Ethernet. Titan satisfies these requests by reading and writing data located on one or more storage devices, connected through two or four Fibre Channel (FC) links. The storage system can be configured with a single Titan SiliconServer or with multiple servers clustered together, sharing the same storage devices.

Titan can be configured as an Active/Active (A/A) cluster, so network requests can be distributed between two Cluster Nodes. Should a Cluster Node fail, its file services and server administration functions are transferred to the other server.

The Titan SiliconServer chassis is 4U (7") high, 48.3 cm (19") rack mountable and a maximum of 63.5 cm (25") deep, excluding the fascia. It consists of a passive backplane (that is not removable), three hot swappable fan trays and two hot swappable redundant power supplies.

The front panel shows system status through two LEDs (a green *power* LED and an amber *fault* LED). The only Field Replaceable Units (FRUs) accessible from the front of the Titan SiliconServer chassis are its cooling fans.

The unit is serviced from its rear panel, which includes additional status LEDs, connectors (power, Ethernet, Fibre Channel, RS-232), and FRUs, such as the power supplies and server modules. See the *Titan SiliconServer Hardware Guide* for more information on the Titan SiliconServer hardware.



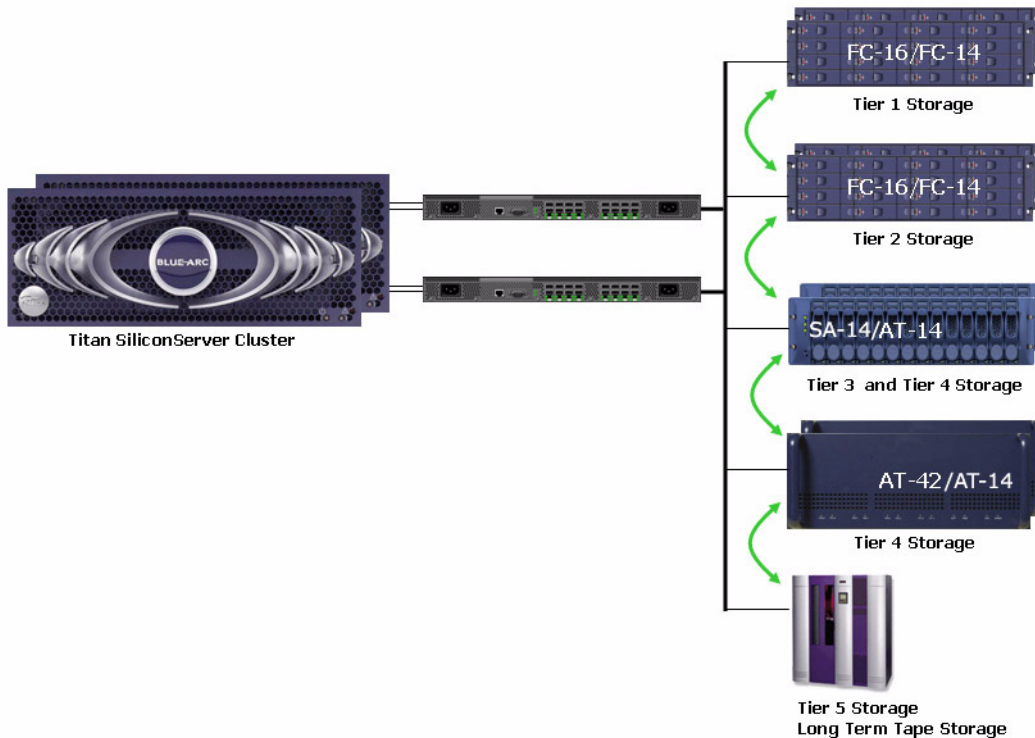
Enterprise Virtual Servers

All file services are provided by logical server entities referred to as Enterprise Virtual Servers (**EVS**). A Titan SiliconServer or High Availability (HA) cluster supports up to eight EVS. Each EVS is assigned unique network settings and storage resources. In a **HA cluster**, EVS are automatically migrated between servers when faults occur to ensure maximum availability. When multiple servers or clusters are configured with a **shared storage pool**, they are referred to as a **Server Farm**. EVS can be manually migrated between servers in a Server Farm based on performance and availability requirements.

The Storage Subsystem

The storage subsystem consists of storage devices and the Fibre Channel (FC) infrastructure (such as FC switches and cables) used to connect these devices to Titan.

Titan supports BlueArc's Multi-Tiered Storage (MTS), which can simultaneously connect multiple diverse storage subsystems behind a single server or cluster.



MTS supports 4-tiers of disk based storage subsystems with different disk technologies and performance characteristics. A fifth tier is used for FC or Ethernet attached Tape Library Systems (TLS).

MTS usage can be optimized by using Data Migrator with Titan. With Data Migrator, routinely accessed data can be retained on primary storage, while older data can be migrated to cost-

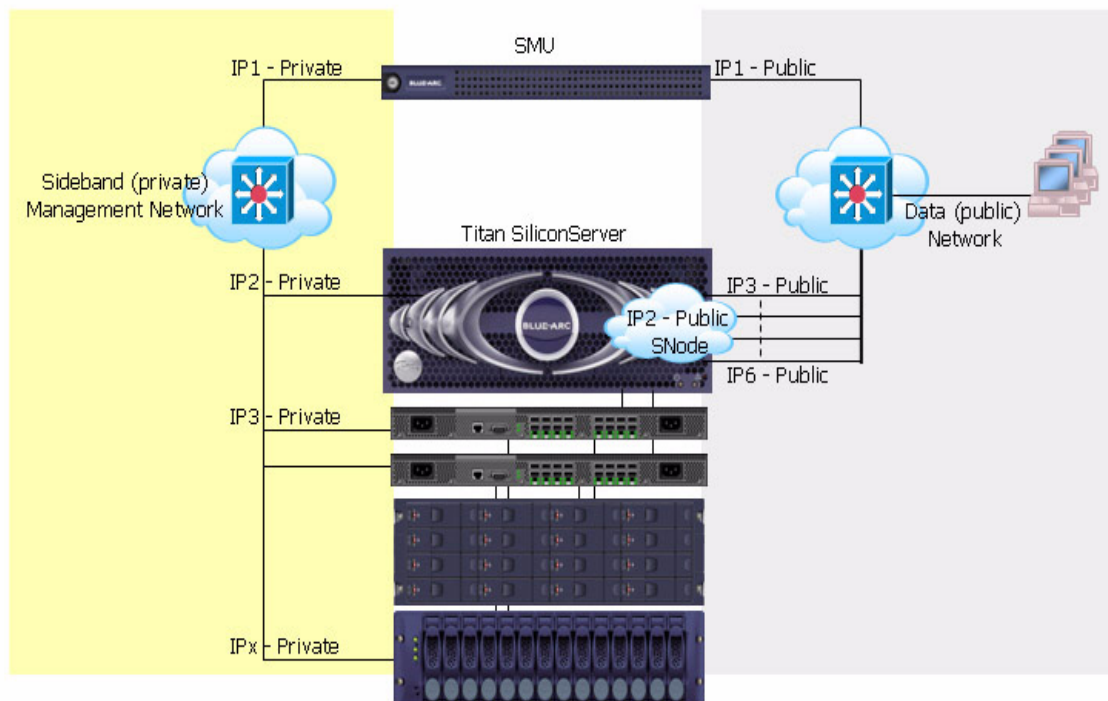
efficient secondary storage. Titan can monitor a file's size, type, duration of inactivity, access history, etc., and migrate the files based on pre-defined rules that are triggered by any of the mentioned criteria reaching a specific threshold. Migrations from primary to secondary storage are handled as automated background tasks with minimal impact on server performance. To the client workstation, it is indistinguishable whether the file's contents have been migrated or still remain on primary storage. Refer to the [Data Migrator](#) section for more detailed information.

The System Management Unit (SMU)

Titan is managed from the System Management Unit (SMU) through its Web Manager interface. The SMU also supports data replication and data migration and acts as the Quorum Device in a Titan cluster. Although the SMU is an integral component of the BlueArc Storage System, it is not involved in any data movement between the network client and Titan. All network clients communicate directly with the Titan SiliconServer.

The Private Management Network

Titan operates in conjunction with a number of auxiliary devices such as RAID storage subsystems, Fibre Channel switches, and UPS units. Most of these devices are managed through Ethernet.



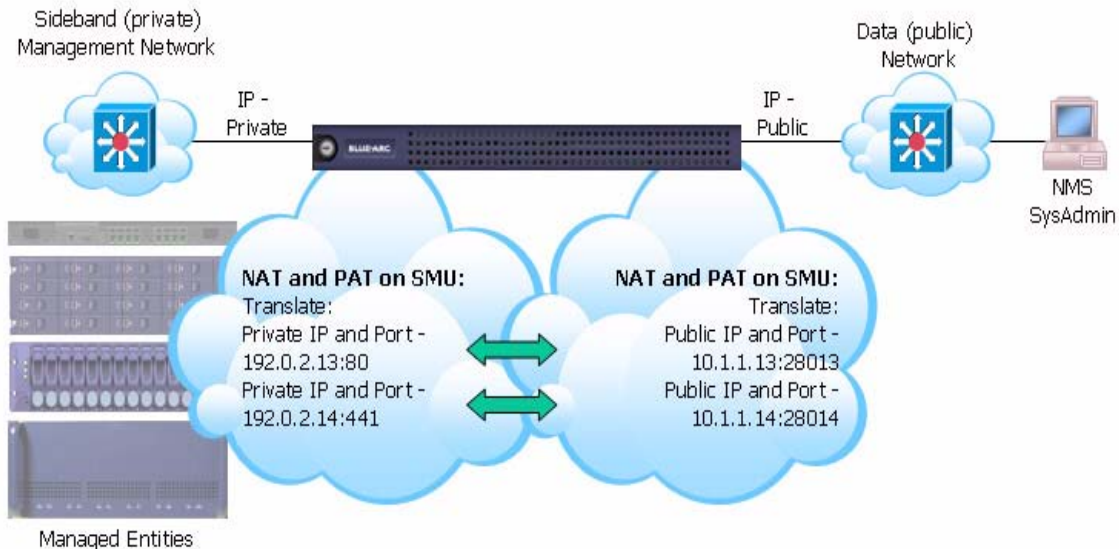
In order to minimize the impact on the enterprise network, Titan's physical management

structure is divided into two discrete components:

- ❑ **A public data network (i.e. the enterprise network).** The public management interface from the BlueArc Storage System perspective consists of the first Ethernet port on the SMU (the public Ethernet interface). In addition, management access can be enabled on individual Gigabit Ethernet (GE) interfaces on Titan.
- ❑ **A private (sideband) management network.** The private management network is a small network used to connect Titan's auxiliary devices and is isolated from the main network through the SMU using *Network Address Translation (NAT)* technology. It consists of the private management interface of the SMU, the 10/100 Mbps Ethernet management interface on the server, and all the Ethernet managed devices that comprise the Titan Storage Subsystem.

The private management network manages the storage subsystem, including auxiliary devices. Devices on this network are only accessible from the public (data) network through the SMU, which provides NAT, NTP, and email relay services. The SMU has two 10/100/1000 Mbps Ethernet interfaces. The first interface (eth0) connects to the public (data) network, while the second interface (eth1) resides on the private management network.

The diagram below shows how NAT isolates the private management network. The example shows a device with the IP address **192.0.2.13:80** accessible through HTTP, and a second device with IP address **192.0.2.14:443** accessible through HTTPS. These devices appear on the enterprise network as **10.1.1.13:28013** and **10.1.1.13:28014**.



Titan SiliconServer Initial Setup

The BlueArc Storage System is normally installed and pre-configured by BlueArc Global Services.

Follow these steps to configure Titan:

1. Configure the SMU through its serial interface. When the SMU is first installed, the following settings will need to be configured:
 - ❑ **A server (or host) name.** This is the name by which the SMU is identified on the network.
 - ❑ **An IP address and subnet mask.** These are used to access the SMU.
 - ❑ **A gateway IP address.**
 - ❑ **A DNS domain name.**
 - ❑ **Passwords** for the *root* and *manager* accounts ([default password](#) is *bluearc*).
2. Perform the initial configuration of the Titan SiliconServer using the serial interface. When Titan is first installed, it requires the following configuration settings:
 - ❑ **An admin name.** This is the server name. It should be unique as it will be used to identify this specific server.
 - ❑ **An administrative IP address and subnet mask.** These are assigned to the 10/100 management port, which is typically connected to the private management network.



Note: The subnet mask should be the same as that used for the private management network on the SMU (i.e. 255.255.255.0), and the IP address should correspond to that network (i.e. 192.0.2.x).

- ❑ **A file serving IP address and subnet mask.** These are assigned to the first Gigabit Ethernet (GE) interface on the server. Once the initial configuration has been completed, additional GE ports can be aggregated together to share these settings, and further IP addresses can be assigned.



Tip: These settings should NOT correspond to the private management network.

- ❑ **The IP address of the default gateway.**

Completing the setup

1. Complete the setup of the SMU by running the [SMU Setup Wizard](#).
2. Add Titan to the [Managed Servers List](#) in the SMU. Use the [default administration account](#) with user name **supervisor** and password **supervisor**.

3. [Enter License Key\(s\)](#) for the server.
4. Run the [SiliconServer Setup Wizard](#).
5. Complete Titan setup:
 - ❑ [Network interface](#)
 - ❑ [Storage management](#)
 - ❑ [File services](#)
 - ❑ [Data protection](#)
6. Optionally, configure Titan as part of a [high availability cluster](#).

Managing the Titan SiliconServer

Titan and its storage subsystem is managed through Web Manager, a Web-based administration tool. This tool allows most administrative tasks to be performed from any client on the network using a suitable Web browser (Microsoft Internet Explorer 6.0 or later, or Firefox 1.0.4, or later). Web Manager can be configured to support multiple Titan SiliconServers.

As an alternative to the Web Manager, use the [Command Line Interface](#) (CLI), which is documented in the *Command Line Reference Guide*.

Using Web Manager

The Web Manager is used to set up, operate, and monitor Titan and its storage subsystem. Web Manager can be configured to support multiple Titan SiliconServers. However, only one server can be managed at a time. This is referred to as the *currently managed server*.



Tip: Use the drop-down page in the Server Status console to select a different server from the managed servers list.

The Web Manager's home page shows the [Server Status Console](#), the top-level page, and shortcuts to commonly used functions.

Starting Web Manager

1. Open a Web browser.
2. In the **Address** or **Location** field, type the **https://** prefix, followed by the name (or IP address) assigned to the SMU. For example:
https://10.1.6.104/
3. Click **ENTER**.
4. When the login page appears, type the *user name* and *password*. Note that user names and passwords are case-sensitive and that there is a [default user account](#) with the user name **admin** and password **bluearc**.



Note: BlueArc recommends that this password be changed as soon as possible.

Once the login procedure is completed, the **Web Manager** home page is displayed.

Using the Server Status Console

Summary Status information pertaining to the *currently managed server* can be viewed from the Web Manager's server console, in Titan SiliconServer's home page.

The screenshot shows the 'Server Status Console' interface. At the top, there is a header bar with the title 'Server Status Console' and a 'Status' button. Below the header, there is a dropdown menu showing 'Titan - 10.2.21.113' and a green LED indicator. The main content area is divided into several sections: 'Volume Nearest Capacity' showing a green LED and '2 %' with a 'View' button; 'Current Data Throughput' showing 'Rx' and 'Tx' values for 'Net' and 'FC' in 'Mbps'; and 'Alerts' showing 'Critical', 'Severe', and 'Warning' counts with corresponding colored LEDs (red, orange, and yellow). Callout boxes provide detailed explanations for each of these elements.

Server name and IP address of the *currently managed server*.
This drop-down box can be used to select another managed server.

Summary server status.
Clicking the LED loads the **System Monitor** page.

Volume Nearest Capacity:
The LED shows how close this File System is to its configured size limits:
☐ **Green** = File System within limits
☐ **Yellow** = File System reached / crossed warning threshold
☐ **Orange** = File System reached / crossed critical threshold
 Clicking **View** loads the **Silicon File Systems**

Current data throughput from both the network and the Fibre Channel links.
These are instantaneous values (in MB/s) sampled every 60 seconds.

Alerts:
Critical: 0
Severe: 1
Warning: 30

Critical errors, in the past 24 hours, in the event log.
Clicking the red LED loads the **Event Log** page, showing all critical errors.

Severe errors, in the past 24 hours, in the event log.
Clicking the orange LED loads the **Event Log** page, showing all severe errors.

Warnings, in the past 24 hours, in the event log.
Clicking the yellow LED loads the **Event Log** page, showing all warnings.

When displaying status using a colored LED, the following conventions apply:

Color	Status	Means that the item is
	Information	Is operating normally and not displaying an alarm condition
	Warning	Needs attention, but does not necessarily represent an immediate threat to the operation of the system
	Severe Warning	Has failed in a way that poses a significant threat to the operation of the system
	Critical	Requires immediate attention. The failure that has occurred is critically affecting system operation

Web Manager and Server Management

Web manager provides support for multiple levels of server management. Please see [User Management](#) section for more details.

Understanding Web Manager Pages

The Web manager uses a two-level page structure. The Home page includes page categories including shortcuts to commonly used functions. The following page categories are all associated with the *currently managed server*:

- **Status & Monitoring** – System Monitor, Event Log, Email Alerts Setup, SNMP, Statistics, etc.
- **SiliconServer Administration** – EVS Management, SiliconServer Setup Wizard, Cluster Configuration, etc.
- **Storage Management** – Silicon File Systems, Virtual Volumes, Quotas, System Drives, Data Migration, etc.
- **Data Protection** – Virus Scanning, Replication, Snapshots, NDMP backup, etc.
- **File Services** – NFS, CIFS, iSCSI, FTP, User Mapping, Group Mapping, etc.
- **Network Configuration** – IP Addresses, Name Services, NIS/LDAP Configuration, IP Routes, Link Aggregation, etc.

Additional categories:

- **SMU Administration** – used to manage the SMU itself (currently managed server selection, security, private management network, etc.).
- **Online Documentation** – used to access documentation (like this manual) from the SMU.

Clicking on any of the shortcuts, such as **Silicon File Systems** and **NFS Exports**, starts the desired function. Clicking on the page categories loads a page, such as the **Data Protection** page shown below:

The screenshot shows the BlueArc Titan web interface. The top header features the BlueArc logo, a status bar indicating 'Titan - 192.0.2.2', and navigation links for Help, About, and Sign Out. Below the header, a breadcrumb trail shows 'Home > Data Protection'. The main content area is titled 'Data Protection' and lists several categories with their respective functions:

- Data Protection**
 - [Virus Scanning](#): Enable and configure virus scanning
 - [Virus Statistics](#): View virus scanning statistics
 - [Snapshots](#): List current Snapshots, take a Snapshot
 - [Snapshot Rules](#): Schedule automatic Snapshots
- Replication**
 - [Replication](#): List Replication Policies and Schedules
 - [Replication Rules](#): List Replication Rules
 - [Replication Status & Reports](#): List Replication Status and Reports
- NDMP Configuration**
 - [Backup Status](#): Running, enabled/disabled, abort
 - [Backup User](#): NDMP username, password to access this SiliconServer
 - [Backup History](#): Clear backup history, clear device mappings
 - [Backup SAN Management](#): Discover tape devices and autochangers on SAN and mark them for use (i.e. "Allow Access")
 - [Backup Snapshot Options](#): Automatically use snapshots for backups

At the bottom, a 'Categories:' section provides a grid of links to other parts of the system:

Status & Monitoring	Storage Management	Data Protection	File Services
Network Configuration	SiliconServer Admin	SMU Administration	Documentation

Understanding Web Manager Tables

Some of the pages in the Web Manager interface include tables, such as the one shown below.

Each column heading is a hyperlink, with which the table can be sorted. Each time the link is clicked, the order of the sort will alternate between ascending and descending, as indicated by the small arrow.

Some tables' contents may be filtered. In this example, the filter has selected only those quotas whose usage exceeds 300 MB.

BLUE-ARC

?

Help

i

About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management

Home > Storage Management > Virtual Volumes

Virtual Volumes

EVS / File System

EVS01 / All File Systems

change...

Filter

Name:

Path:

filter

viols 1-20 of 251 : Page: 1 2 3 4 5 >> >

Name	File System	Contact	Path	
☐ prj1	vol0	projectadmin@company.com	/prjVVol1	details
☐ prj10	vol0	projectadmin@company.com	/prjVVol10	details
☐ prj100	vol0	projectadmin@company.com	/prjVVol100	details
☐ prj101	vol0	projectadmin@company.com	/prjVVol101	details
☐ prj102	vol0	projectadmin@company.com	/prjVVol102	details
☐ prj103	vol0	projectadmin@company.com	/prjVVol103	details
☐ prj104	vol0	projectadmin@company.com	/prjVVol104	details
☐ prj105	vol0	projectadmin@company.com	/prjVVol105	details
☐ prj106	vol0	projectadmin@company.com	/prjVVol106	details
☐ prj107	vol0	projectadmin@company.com	/prjVVol107	details
☐ prj108	vol0	projectadmin@company.com	/prjVVol108	details
☐ prj109	vol0	projectadmin@company.com	/prjVVol109	details
☐ prj11	vol0	projectadmin@company.com	/prjVVol11	details
☐ prj110	vol0	projectadmin@company.com	/prjVVol110	details
☐ prj111	vol0	projectadmin@company.com	/prjVVol111	details
☐ prj112	vol0	projectadmin@company.com	/prjVVol112	details
☐ prj113	vol0	projectadmin@company.com	/prjVVol113	details
☐ prj114	vol0	projectadmin@company.com	/prjVVol114	details
☐ prj115	vol0	projectadmin@company.com	/prjVVol115	details
☐ prj116	vol0	projectadmin@company.com	/prjVVol116	details

Check All

Clear All

viols 1-20 of 251 : Page: 1 2 3 4 5 >> >

Actions:

delete

add

View Quotas

Download All Quotas

Tables consisting of large numbers of entries are displayed a page at a time. The page shown comprises 20 quotas out of a total of 251.
The pages can be navigated using the controls at the top and bottom of the list. Hovering the mouse over each control will display "screen tips" describing their purpose.

Using the Command Line Interface

The Titan SiliconServer and the System Management Unit (SMU) each have a command line interface (CLI) used for configuration and management. Both support secure connections, configurable passwords, and other security mechanisms.

SMU Command Line Interface

The SMU ships without a pre-configured network setup. The SMU must be accessed through a direct serial connection in order to perform the initial setup. Once configured, the SMU's CLI can be accessed directly through SSH or through a Java-enabled SSH session running through Web Manager.

To connect using a serial console

1. Attach an RS232 null-modem cable (DB-9 Female to DB-9 Female) to the serial port on the back of the SMU. Attach the other end of the serial cable to a computer (e.g. laptop).
2. Set up the terminal emulation program (such as Window's HyperTerminal) to the following settings:

115,200 b/s, 8 bits/byte, 1 stop bit, No parity



3. Log into the SMU.
 - If the SMU is being accessed to perform initial setup, log in as the user *setup* and perform the installation steps as directed.
 - Otherwise, login as the user *manager*. When prompted, enter the password for the user *manager*.
4. Once connected, select which Titan's CLI to access or enter "q" to access the SMU's shell. At the SMU's command line interface, the Titan's CLI may be accessed through Telnet or PSSC.

To connect with SSHTerm

For Windows and other users who do not have SSH available, the SMU can be accessed by using SSHTerm. SSHTerm is a Java SSH client (applet). It is developed by 3SP and is distributed under the General Public License (GPL). SSHTerm is provided as a convenient, cross-platform alternative to other SSH clients. Refer to 3SP's web site: <http://www.3sp.com/> for more information.

SSHTerm requires a recent version of Java (1.4.x or greater). Go to <http://www.java.com> to verify that the browser has the latest version of Java Plug-in installed.



Note: Java must be enabled on the browser.

1. From the **Home** page, click **SMU Administration**. Then, click **SSHTerm**.
2. Click **Launch SSHTerm** and a new window will pop up containing the SSH client applet. Accept the certificate registered to *3SP LTD*, and click **Always** or **Yes** when asked to allow the host.
SSHTerm will automatically connect to the SMU as the user *manager*.
3. When prompted, enter the password for the user *manager*.

Multiple SSHTerm windows may be used at once. Just click **Launch SSHTerm** for each new SSH session. When the SSH session has finished, just close the window.



Note: Once connected to the SMU's command line, use telnet or PSSC (Perl SiliconServer Control) to access the Titan Storage System.

SiliconServer Command Line Interface

The Titan SiliconServer implements a comprehensive command line interface (CLI), which is documented separately in the Titan SiliconServer Command Line Reference.

The Titan CLI can be accessed in the following ways:

- Using Secure Shell (SSH) to connect into the Titan SiliconServer through the SMU.
- Using SSH or Telnet to directly connect into the Titan SiliconServer.
- Using the SiliconServer Control (SSC) utility, available for Windows and Linux.
- Using the Perl SiliconServer Control (PSSC) utility, available for all other Unix operating systems.

In order to use SSH, Telnet, SSC, or PSSC to access the server's CLI directly through the public network, it is necessary to have a server administration [IP address](#) assigned to at least one of the Gigabit Ethernet interfaces. Titan supports access to its CLI through any administrative IP address. By default an administrative IP address is available on the private management network.

To connect using SSH via the SMU

The SMU supports SSH. After logging into the SMU, the SMU can proxy connections directly to the server's CLI. This can be useful for two reasons:

- It eliminates the need to assign a server administration IP address to the Gigabit interface of the Titan.

- It enhances the security of server by isolating administrative access to the private management network.

To SSH into the Titan, using the SMU as a proxy, do the following:

1. Connect to the SMU through SSH.
2. Log into the SMU as *manager*.
3. A list of servers will appear. Select the target server.
4. A connection to Titan's Command Line Interface will be automatically initiated.

To connect using SSH or Telnet

When connecting to a Titan SiliconServer through SSH or Telnet, use the server's administration name or IP address, and log in using the *supervisor* user account. Titan must be configured to accept SSH or Telnet connections over its Ethernet interfaces.

Titan's SSH implementation grants full access to the CLI. Connections can be made using DSS or RSA host key types.

To SSH into the Titan, run the following:

1. Connect to the server's administrative name or IP address:
`ssh supervisor@titan_name_or_IP`
2. When prompted, enter the *supervisor* user's password.

To Telnet into the Titan, run the following:

1. Connect to the server's administrative name or IP address:
`telnet titan_name_or_IP`
2. When prompted, enter the *supervisor* user's password.

To Connect using SiliconServer Control

SSC can be used to connect to Titan from the SMU, from Windows PCs, and from Linux/Unix workstations. SSC provides a secure connection using a modified version of the Arcfour cipher for encryption and Sha-1 for authentication. SSC comes in two varieties:

- SSC for Windows and Linux.
- PSSC, a Perl scripted version of SSC for Linux/Unix operating systems.

SSC is a utility for accessing the Titan's command line interface and is optimally used for scripting. Titan supports SSC access to its CLI through any administrative IP address. By default an administrative IP address is available on the private management network.

The syntax for SSC is:

```
ssc [-u <username>] [-p <password>] <host>[:<port>] [<command>]
```

The syntax for PSSC is:

```
pssc [-u <username>] [-p <password>] <host>[:<port>] [<command>]
```

Syntax	Description
Username	The user account used to log into Titan (typically <i>supervisor</i>)
Password	The password for this user account. If no user name or password is specified, SSC/PSSC will prompt for one.
Host	Titan's server administration IP address or host name.
Port	If the SSC/PSSC port number has been changed from its default of 206, then the port number configured for SSC must be specified in the command syntax.
Command	The command to execute. If no command is specified, SSC/PSSC allows interactive command entry.

Using the Embedded Web UI

Each Titan SiliconServer incorporates an embedded Web management tool. Although this is not the primary management interface for Titan, this tool can be used as an alternative to Web Manager, or if the SMU is offline.

To start the embedded Web UI

1. Open a Web browser.
2. In the **Address** or **Location** field, type the **http://** prefix, followed by an administrative IP address on the Titan, followed by **:81**. For example:
http://10.1.6.104:81
3. Click **ENTER**.
4. When the login page appears, type the user name and password. Note that the user name and password are case-sensitive. A [default user account](#) exists with the user name *supervisor* and password *supervisor*.

2 System Configuration

System Configuration Overview

This section describes how to configure the BlueArc Storage System, during or after installation. It includes setup instructions for the System Management Unit (SMU), for the Titan SiliconServer, and the private management network. Network configuration (including IP address selection), storage management, file services, data protection, and clustering are discussed in separate sections. To facilitate the setup, Web Manager provides setup wizards for both the SMU and Titan.

Security settings for Titan are an important part of the system configuration. These include user name and password for system administrators, and restrictions on which systems (or hosts) are allowed to access Titan.



Tip: BlueArc recommends that security settings be defined on the system as soon as possible, to prevent unauthorized access.

Configuring the System Management Unit (SMU)

The System Management Unit (SMU) is an integral component of the BlueArc Storage System. The SMU is used to manage Titan and to perform certain functions, such as data migration and replication. As a result, the SMU needs to be set up first so Web Manager can be used to perform other configuration steps required.



Note: The SMU is shipped with the [default user name](#) *admin* and password *bluearc*. BlueArc recommends that this password is changed as soon as possible.

Using the SMU Setup Wizard

This wizard performs the basic configuration of a new SMU. It changes the default password used to access the SMU, sets up name services for network operation, and configures the date and time.

To use the SMU Setup Wizard

From the **SMU Administration** page, click **SMU Setup Wizard**. The following screen will be displayed:



?

 Help

i

 About

+

 Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

SMU Administration | [Home](#) > [SMU Administration](#) > SMU Setup Wizard

SMU Setup Wizard

Change the password used to access the SMU

User Name: admin

Current Password:

New Password:

Confirm New Password:

back

next

cancel

For information on how to complete the wizard, see below:

Item /Field	Description
Passwords	Set up passwords to prevent unauthorized access to the system management facilities.
DNS Server Setup	Enter the IP addresses of the DNS servers and domain search orders that will be applied to the SMU.
SMTP Relay	Enter the host name (not the IP address) of the email server to which the SMU can send event notification emails.
Date & Time	Set the clock on the SMU and select one or more NTP servers.

Configuring the System Management Unit (SMU)

Private management network	Configure the private management network.

When the wizard is complete a page will be displayed showing the details entered. To complete the setup, click **finish**, and then click **OK** to reboot.

Configuring Security Options

The SMU can be configured to control which hosts have access to it, as well as other auxiliary devices managed by the SMU. To prevent the current managing workstation from being locked out, it must be included in the list of allowed hosts.

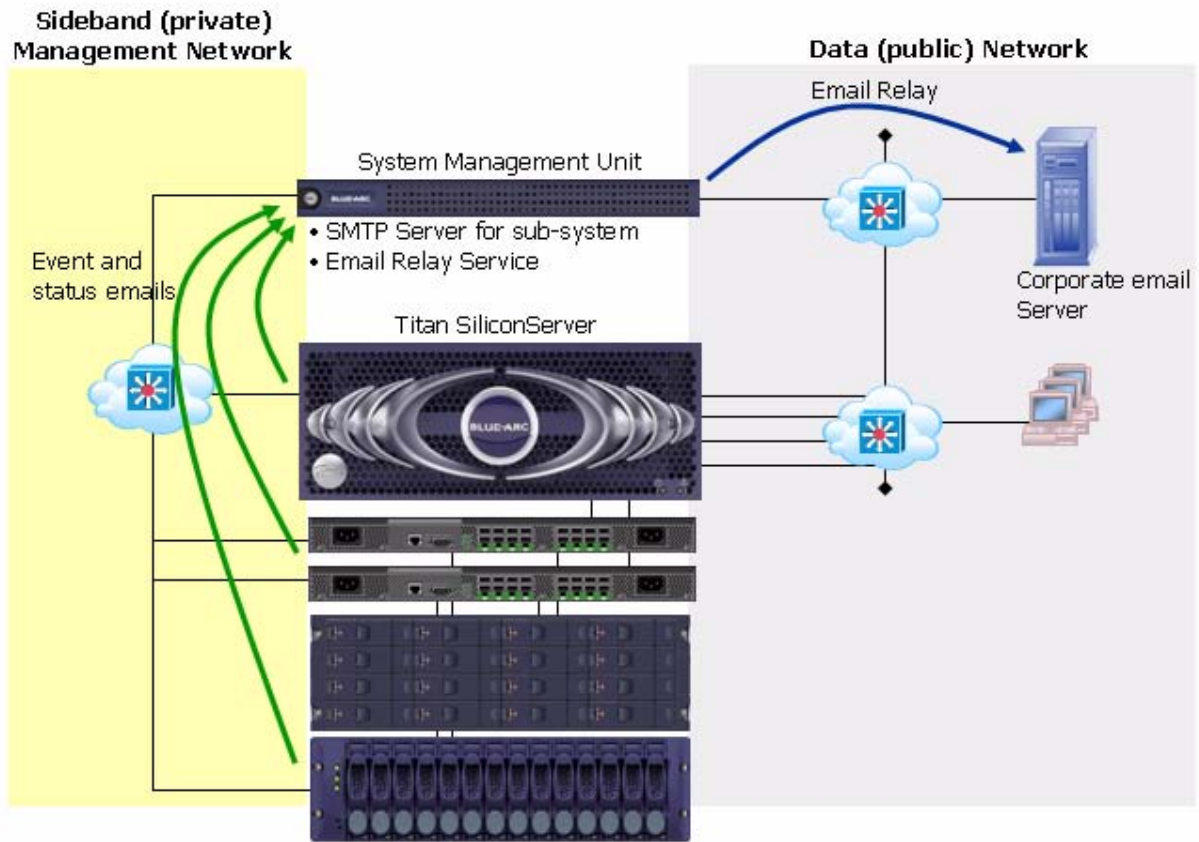
From the **SMU Administration** page, click **Security Options**.

The screenshot shows the BLUE ARC SMU Administration interface. The top navigation bar includes the BLUE ARC logo, a status indicator for 'TITAN - 192.0.2.2', and links for Help, About, and Sign Out. Below the navigation bar, the breadcrumb trail reads 'Home > SMU Administration > Security Options'. The main heading is 'Security Options'. A section titled 'Control which Hosts have Access to the SMU' contains a checkbox labeled 'Restrict Access To Allowed Hosts' which is checked. Below this, there is a list of 'Allowed Hosts' with the following IP addresses: 10.2.4.101, 10.2.2.63, 192.168.41.1, and 192.168.41.5. To the right of the list are 'Add' and 'Delete' buttons. At the bottom of the section is an 'apply' button.

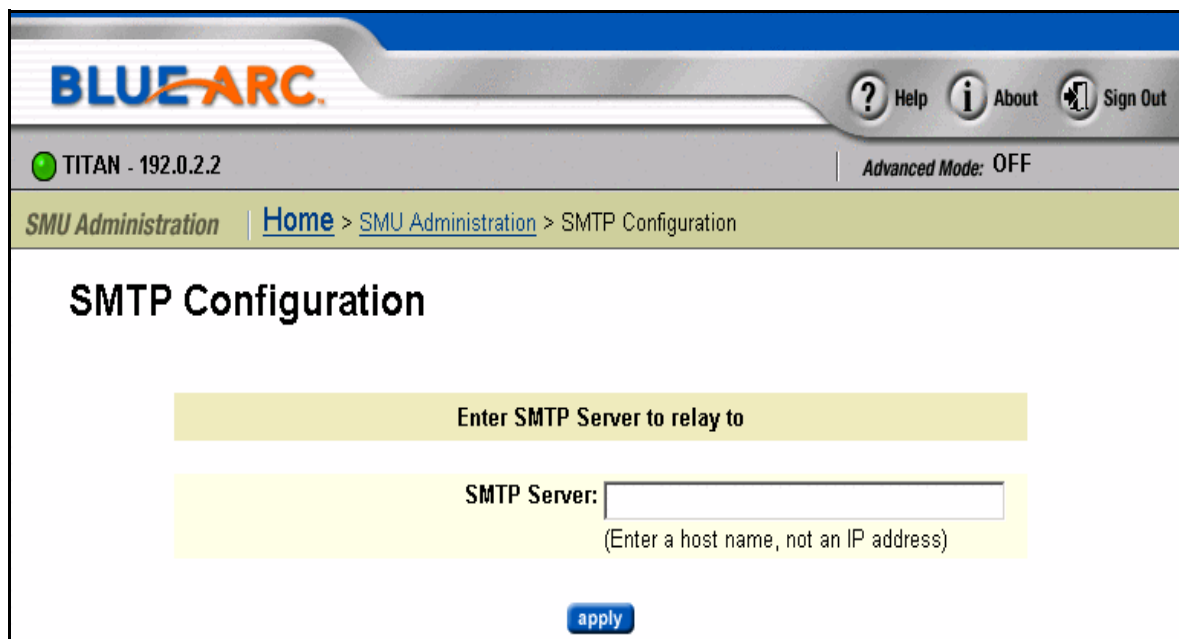
Enter the **IP address** of each allowed host and click the **Add** button. When the list is complete click the **OK** button.

SMTP Relay Configuration

The SMU can be configured to forward emails from Titan SiliconServers and auxiliary devices on the [private management network](#) to the public network.



From the **SMU Administration** page, click **SMTP Configuration**. The following screen will be displayed:



The screenshot shows the BlueArc Titan web interface. At the top, there is a header with the BlueArc logo and navigation links: Help, About, and Sign Out. Below the header, a status bar shows 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF'. The main navigation bar includes 'SMU Administration' and a breadcrumb trail: 'Home > SMU Administration > SMTP Configuration'. The central area is titled 'SMTP Configuration' and contains a yellow box with the text 'Enter SMTP Server to relay to'. Below this, there is a label 'SMTP Server:' followed by a text input field. A note below the input field says '(Enter a host name, not an IP address)'. At the bottom of the form is a blue 'apply' button.

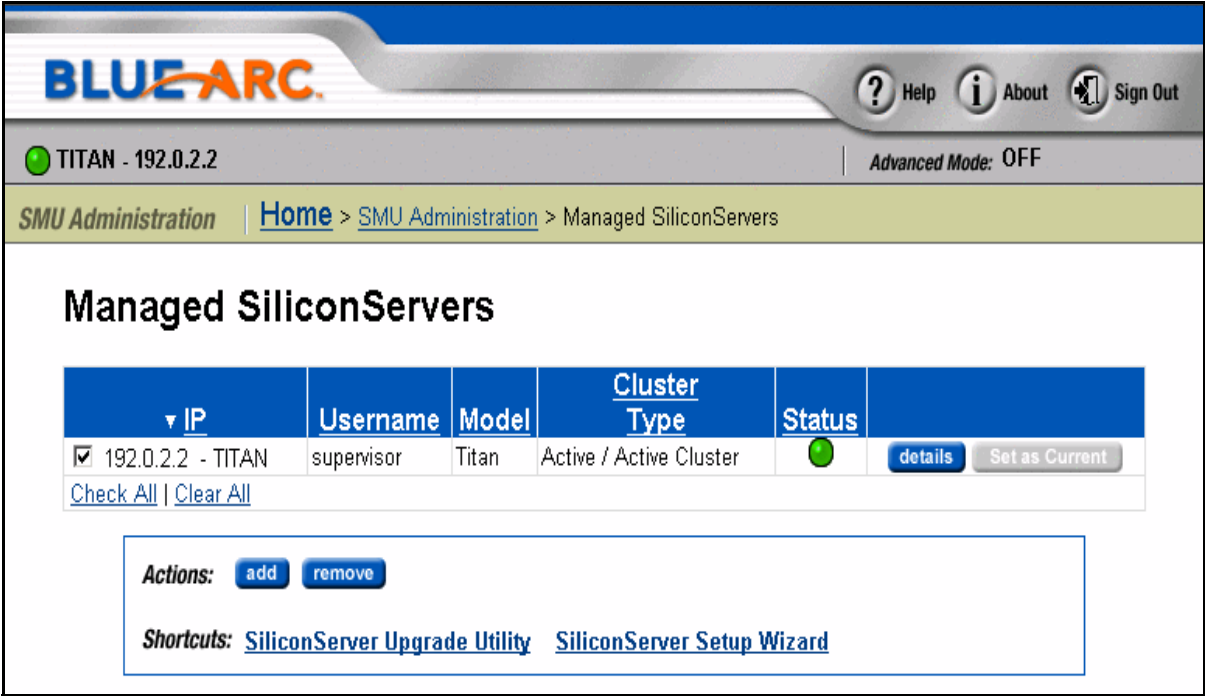
Enter the **host name** of an SMTP Server on the public network. The SMU will then relay e-mails from the Titan servers on the private network to the public network. Ensure that the SMTP server on Titan's [Email Alert Configuration](#) page is set to be the SMU's **eth1** IP address.

Titan's email configuration can be viewed through the **Email Alerts Setup** link found on the **Status & Monitoring** page.

Selecting Managed Servers

The SMU can manage multiple Titan SiliconServers and their associated storage subsystems. Information about each server should be added to the **Managed Servers** page. The SMU needs to know the IP Address and username/password of the server to be managed. Only one server may be managed at a time. This server is known as the *currently managed server*. From the list, any server can be selected as the *currently managed server*.

To display the servers managed by the SMU, from the **SMU Administration** page, click **Managed SiliconServers**.



The screen displays the following:

Item / Field	Description
IP Address	The IP address of the server.
Username	The username used to access the server.
Model	The model type, e.g. Titan.
Cluster Type	The cluster type, e.g. Single Node, Active/Active Cluster.
Status	The current status of the SiliconServer:  Green indicates that the server is operating normally (i.e. not showing an alert condition)  Amber is displaying a warning (e.g. operating normally, however, action should be taken to maintain normal operation)  Red indicates a critical condition (e.g. the server is no longer functioning).
Details	A link to a page displaying detailed information used to contact or to manage the server.

Set as Current	Select the server as the <i>currently managed server</i> .

In the Actions frame it is possible to **add** or **remove** managed servers from the displayed list.

To remove one or more servers, make a selection by putting a tick in the appropriate checkbox, or click **check all** to remove all servers. Then, click **remove**.



Tip: To change the current managed server, click **Set as Current** on this page or use the drop-down box in the Server Status Console.

To add a server, click **add**. The following screen will be displayed:

This screen requires the following:

Item/Field	Description
SiliconServer IP Address	Enter the IP address of the server to be added. For Titan, this is the IP address used for server administration, typically assigned to the 10/100 management port.
SiliconServer Username	Enter the username needed to access this server, e.g. supervisor.
SiliconServer Password	Enter the password needed to access this server.

When all the details have been entered, click **OK**.

When the Titan is added to the SMU as a *Managed SiliconServer*, the following actions will

occur:

- ❑ If the server is managed through the private management network, the SMU's eth1 IP address will be added to the server's list of [NTP](#) servers.
- ❑ If the server is managed through the private management network, the SMU's eth1 IP address will be configured as the server's Primary SMTP server. If Titan was already configured to use a mail server, this server will automatically be made the Backup SMTP server.
- ❑ Titan's user name and password will be preserved on the SMU. This ensures that when selecting this server as the current managed server, or when connecting to the Titan's Command Line Interface via SSH, the server does not prompt for an additional authentication of its user name and password.

User Management

Web Manager provides support for multiple levels of server management. Administrators can create accounts in Web Manager and assign different administrative functions or "roles" to the accounts. These roles grant the ability to manage specific elements such as networking or storage of any server or servers in a [Server Farm](#).

Once a user has been created and assigned a role, this account can be used to log into the Web Manager. Available servers and administrative functions will be presented in the user interface based on the permissions granted by the role. Only the links for menu pages for which the role permits will be visible in the Web Manager.

Administrative Roles

Titan can be configured with multiple user accounts and each user account can be assigned one of the following "roles":

- **Global Administrator** - in this role administrators have full privileges on all servers managed from the SMU. Global Administrators also have administrative control of the SMU including the ability to create new user accounts.
- **Storage Administrator** - in this role the administrator can configure storage devices, manage files systems, virtual volumes and allocate them to specific servers, but cannot manage other settings of the server such as the network settings.
- **Server Administrator** - in this role the administrator manage one or more servers or HA clusters, and may be able to manage IP addresses and exports, allocate storage and be given or denied access to manage the subsystem of those servers.

Management roles are controlled by the SMU. The information relating to administrative accounts like name, password, role or server list is maintained in the SMU's configuration database.

Administrative Functions

The following table shows the Web Manager functions for the different administrative roles listed

for each type of user. The information contained in this table also shows a list of the SMU functions that are available to each user. Only the Web Manager menu pages for which access is allowed will be displayed for each administrator.



Note: The table does not show the Global Administrator, as this role has access to everything.

System Management Unit Interface			Server Administrator with Storage	Server Administrator without Storage	Storage Administrator Only Role
Status and Monitoring					
	Status		Yes	Yes	No
	Event Notification		Yes	Yes	Yes
	Server Load Graphics		Yes	Yes	Yes
	Server Statistics		Yes	Yes	Yes
	Files Services Statistics		Yes	Yes	No
	Management Access Statistics		Yes	Yes	No
	Diagnostics Logs (Advanced)		Yes	Yes	Yes
SiliconServer Admin					
	Server				
		SiliconServer Setup Wizard	Yes	Yes	No
		Clone SiliconServer Settings	Yes ¹	Yes ¹	No
		Server Identification	Yes	Yes	No
		Date and Time	Yes	Yes	No
		Version Information	Yes	Yes	Yes
	EVS				
		EVS Management	Yes	Yes	No
		EVS Migrate	Yes ¹	Yes ¹	No
	Cluster				

		Cluster Configuration	Yes	Yes	No
		Physical Nodes	Yes	Yes	No
		Cluster Wizard	No	No	No
	Power Management		Yes	Yes	No
	Maintenance Tasks				
		Reset/Shutdown	Yes	Yes	No
		Configuration Backup & Restore	Yes	Yes	No
		Upgrade firmware	No	No	No
		Manage Packages	No	No	No
		Licensing Keys	Yes	Yes	No
	Management Access		Yes	Yes	No
	Management Access Statistics (Advanced)		Yes	Yes	No
Storage Management					
	Silicon File Server Management				
		Silicon File Systems	Yes	Yes ²	Yes
		Storage Pools	Yes	No	Yes
		Virtual Volumes & Quotas	Yes	Yes	No
		Quotes by File System	Yes	Yes	No
		File System Relocation	Yes	Yes	Yes
	MTS		Yes	No	Yes
	Policy Based Data Migration				
		Data Migration	Yes	Yes	No
		Data Migration Rules	Yes	Yes	No
		Data Migration Paths	Yes	Yes	No
		Complete Data Migrations	Yes	Yes	No
	Storage Graphics		Yes	Yes	Yes

Data Protection					
	Data Protection				
		Virus Scanning	Yes	Yes	No
		Virus Statistics	Yes	Yes	No
		Replication	Yes ³	Yes ³	No
		Snapshots	Yes	Yes	No
		Snapshot Rules	Yes	Yes	No
	NDMP Configuration		Yes	Yes	No
File Services			Yes	Yes	No
Network Configuration			Yes	Yes	No
SMU Administration					
	SMU		No	No	No
	Managed Servers				
		Managed SiliconServers	Yes ⁴	Yes ⁴	Yes ⁴
		Management Network	No	No	No
	Management Access		No	No	No
Documentation Access			Yes	Yes	Yes
	Notes: (1) Access is limited to relevant servers. (2) Cannot create/expand a File System. (3) Replication activity is limited to relevant servers. (4) Read only access allowed.				

Using Advanced Mode Functions

Advanced Mode controls the visibility of hidden links to advanced configuration options and pages. Advanced Mode functions could potentially degrade system performance and cause disruption to the existing services.



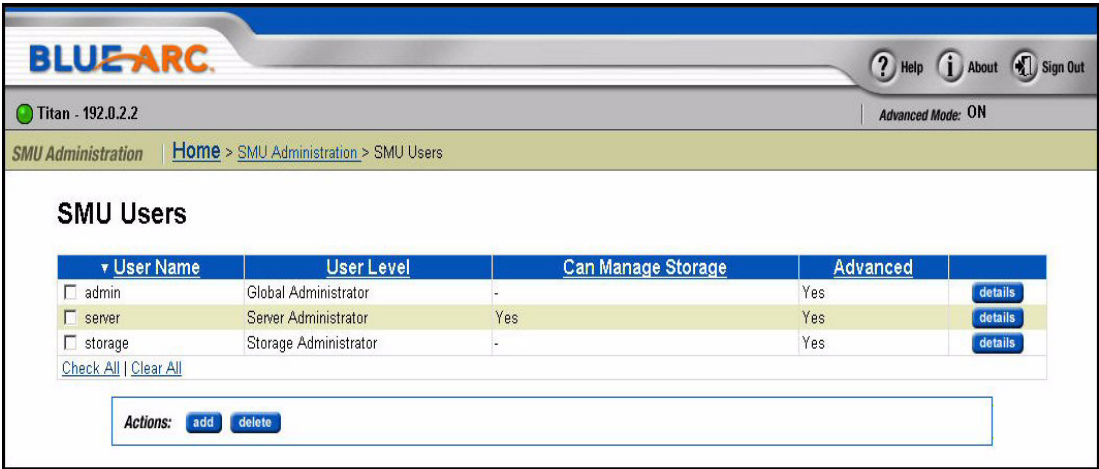
Caution: Advanced Mode functions should only be used after consulting BlueArc Global Services.

When Advanced Mode is off, links to advanced configuration pages are *invisible*. To view these

links, which are typically found on the category page, turn Advanced Mode on for the desired SMU user.

To Add an SMU User

From the **Home** page, click **SMU Administration**. Then, click **SMU Users**. From this page the administrator can setup additional user roles for any Titan server on the network.



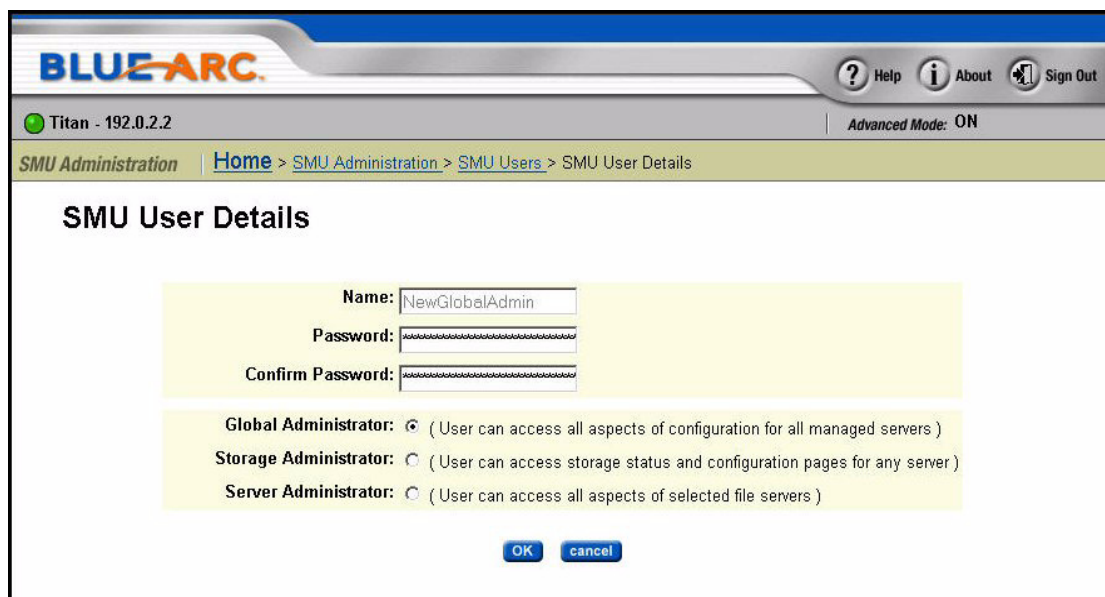
The fields on this screen are described in the table below:

Item / Field	Description
User Name	Administrator's user name.
User Level	Displays the user level or type of administrative role.
Can Manage Storage	Displays if the user Can Manage Storage systems.
Advanced	Displays if Advanced functions are available to this user.

To Edit a SMU User's Information

From the **Home** page, click **SMU Administration**. Then, click **SMU Users**.

Next, click **details** next to the desired SMU user.



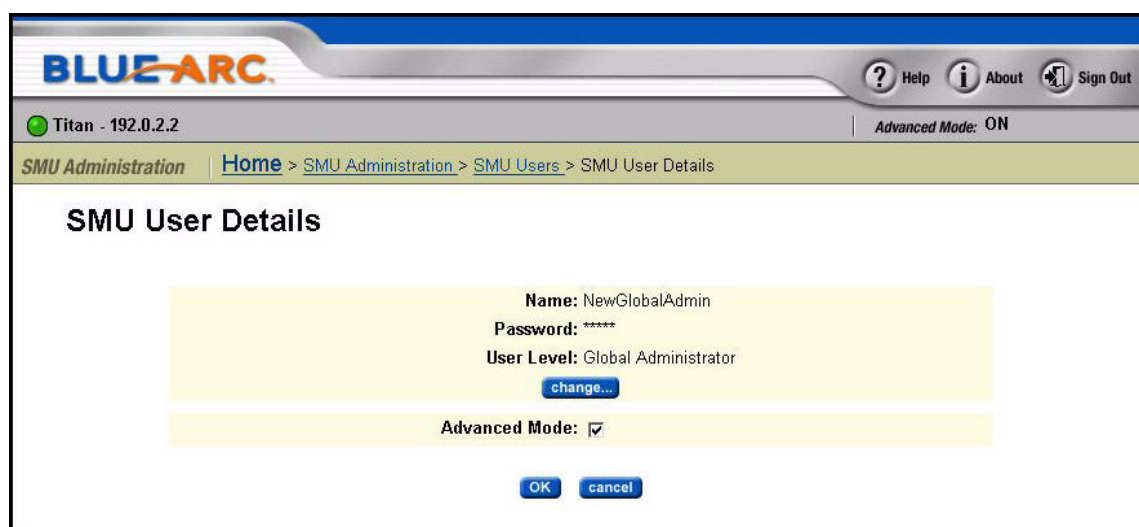
The screenshot shows the BlueArc web interface. The top navigation bar includes the BlueArc logo, a status bar with 'Titan - 192.0.2.2' and 'Advanced Mode: ON', and links for Help, About, and Sign Out. The breadcrumb trail is 'Home > SMU Administration > SMU Users > SMU User Details'. The main heading is 'SMU User Details'. Below it is a form with the following fields:

- Name:** NewGlobalAdmin
- Password:** [masked with asterisks]
- Confirm Password:** [masked with asterisks]
- Global Administrator:** ☒ (User can access all aspects of configuration for all managed servers)
- Storage Administrator:** ☐ (User can access storage status and configuration pages for any server)
- Server Administrator:** ☐ (User can access all aspects of selected file servers)

At the bottom of the form are 'OK' and 'cancel' buttons.

From the **SMU User Details** Screen:

1. Click **change**.
2. Change the SMU user's password or role.
3. Click **OK** to return to main **SMU User Details** page.



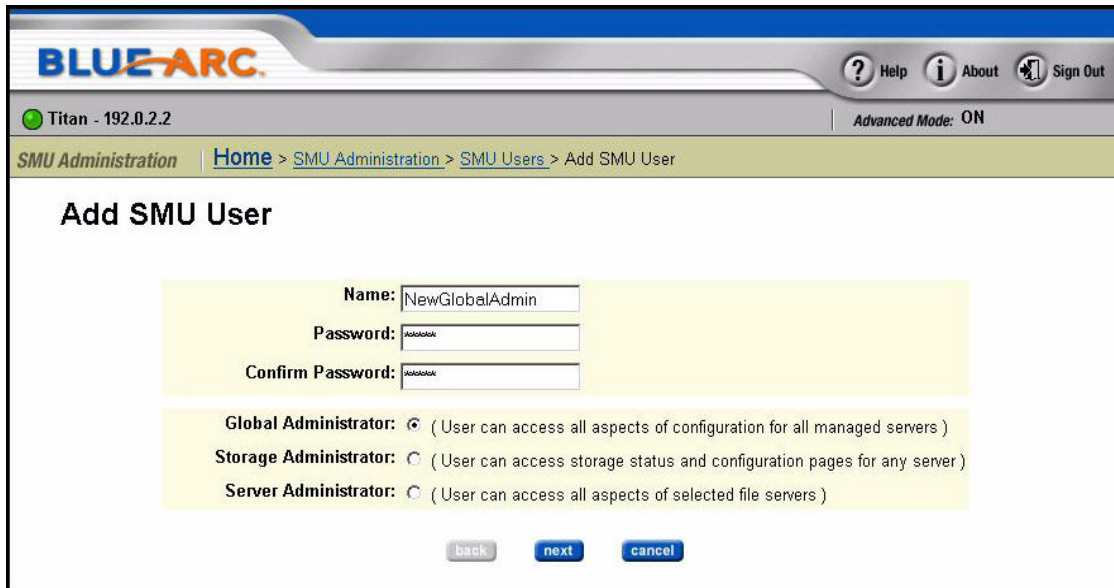
This screenshot shows the same 'SMU User Details' form, but after clicking the 'change' button. The fields are now read-only and display the current values:

- Name:** NewGlobalAdmin
- Password:** *****
- User Level:** Global Administrator

Below these fields is a 'change...' button. At the bottom of the form, there is a checkbox for **Advanced Mode:** which is currently checked. 'OK' and 'cancel' buttons are at the very bottom.

To add an SMU User - Global Administrator, follow these steps:

1. Click the **"Add"** button. The following page is displayed.



BLUE ARC

Titan - 192.0.2.2 | Advanced Mode: ON

SMU Administration | [Home](#) > [SMU Administration](#) > [SMU Users](#) > Add SMU User

Add SMU User

Name:

Password:

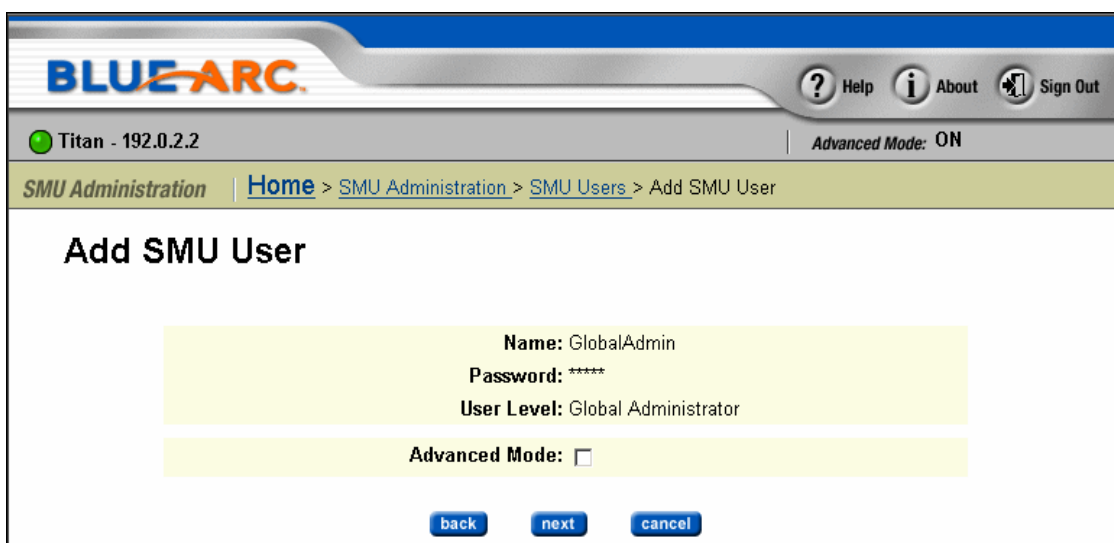
Confirm Password:

Global Administrator: ☒ (User can access all aspects of configuration for all managed servers)

Storage Administrator: ☐ (User can access storage status and configuration pages for any server)

Server Administrator: ☐ (User can access all aspects of selected file servers)

2. Enter a **User Name** for this SMU User.
3. Enter a **Password** for this SMU User, and confirm the password.
4. Click the **Global Administrator** option.
5. Click **next** to continue. The following screen is displayed.



BLUE ARC

Titan - 192.0.2.2 | Advanced Mode: ON

SMU Administration | [Home](#) > [SMU Administration](#) > [SMU Users](#) > Add SMU User

Add SMU User

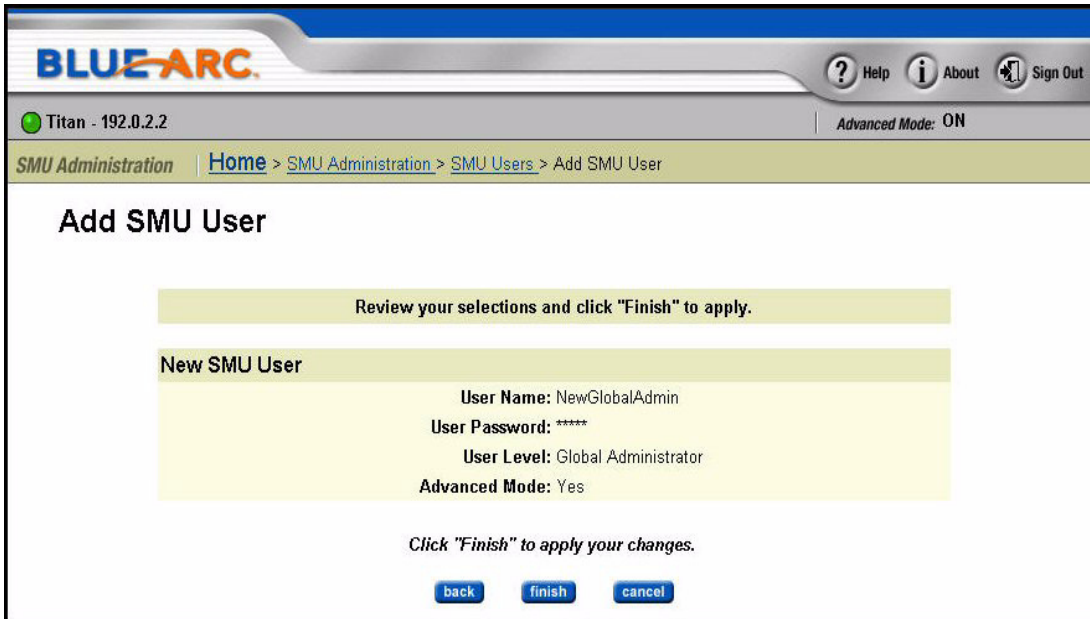
Name: GlobalAdmin

Password: *****

User Level: Global Administrator

Advanced Mode: ☐

This page displays the new SMU user's profile. Click the **Advanced Mode** checkbox if this SMU user needs to have access to the advanced functions. Click **next** to continue. The following confirmation screen is displayed.

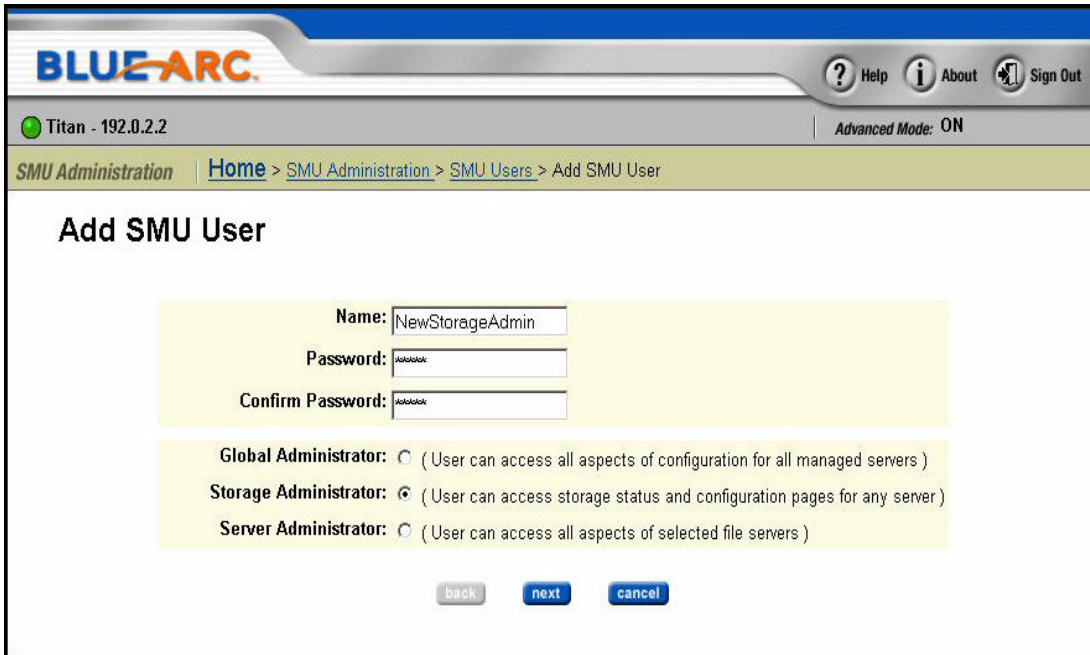


The screenshot shows the BLUE ARC web interface for SMU Administration. The top navigation bar includes the BLUE ARC logo, a status bar showing 'Titan - 192.0.2.2' and 'Advanced Mode: ON', and links for Help, About, and Sign Out. The breadcrumb trail is 'Home > SMU Administration > SMU Users > Add SMU User'. The main heading is 'Add SMU User'. A yellow box contains the text 'Review your selections and click "Finish" to apply.' Below this, another yellow box titled 'New SMU User' displays the following details: 'User Name: NewGlobalAdmin', 'User Password: *****', 'User Level: Global Administrator', and 'Advanced Mode: Yes'. At the bottom, it says 'Click "Finish" to apply your changes.' and provides three buttons: 'back', 'finish', and 'cancel'.

Verify that the New SMU User's profile is correct and click **finish** to apply your changes. The SMU Users screen is displayed listing the newly created SMU User.

To add an SMU User - Storage Administrator, follow these steps:

1. Click the **Add** button. The following page is displayed.



The screenshot shows the BLUE ARC web interface for SMU Administration. The top navigation bar includes the BLUE ARC logo, a status bar showing 'Titan - 192.0.2.2' and 'Advanced Mode: ON', and links for Help, About, and Sign Out. The breadcrumb trail is 'Home > SMU Administration > SMU Users > Add SMU User'. The main heading is 'Add SMU User'. The form contains three input fields: 'Name' (containing 'NewStorageAdmin'), 'Password' (masked with asterisks), and 'Confirm Password' (masked with asterisks). Below these are three radio button options: 'Global Administrator' (unchecked), 'Storage Administrator' (checked), and 'Server Administrator' (unchecked). Each option has a descriptive text in parentheses. At the bottom are three buttons: 'back', 'next', and 'cancel'.

BLUE ARC

Titan - 192.0.2.2 | Advanced Mode: ON

SMU Administration | [Home](#) > [SMU Administration](#) > [SMU Users](#) > Add SMU User

Add SMU User

Name:

Password:

Confirm Password:

Global Administrator: ☐ (User can access all aspects of configuration for all managed servers)

Storage Administrator: ☒ (User can access storage status and configuration pages for any server)

Server Administrator: ☐ (User can access all aspects of selected file servers)

2. Enter a **User Name** for this SMU User.
3. Enter a **Password** for this SMU User, and confirm the password.
4. Click the **Storage Administrator** option.

- Click **next** to continue. The following screen is displayed.

BLUE-ARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

SMU Administration | Home > SMU Administration > SMU Users > Add SMU User

Add SMU User

Name: NewStorageAdmin
 Password: *****
 User Level: Storage Administrator
 Advanced Mode: ☒

Available Servers		Selected Servers
Titan 192.0.2.2	➡	All Servers
	⬅	

back next cancel

- Highlight the servers that this SMU User has rights and privileges to manage from the **Available Servers** list and move them to the **Selected Servers** list.
- Click **next** to continue. The following page is displayed.

BLUE-ARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

SMU Administration | Home > SMU Administration > SMU Users > Add SMU User

Add SMU User

Review your selections and click "Finish" to apply.

New SMU User

User Name: NewStorageAdmin
 User Password: *****
 User Level: Storage Administrator
 Advanced Mode: Yes

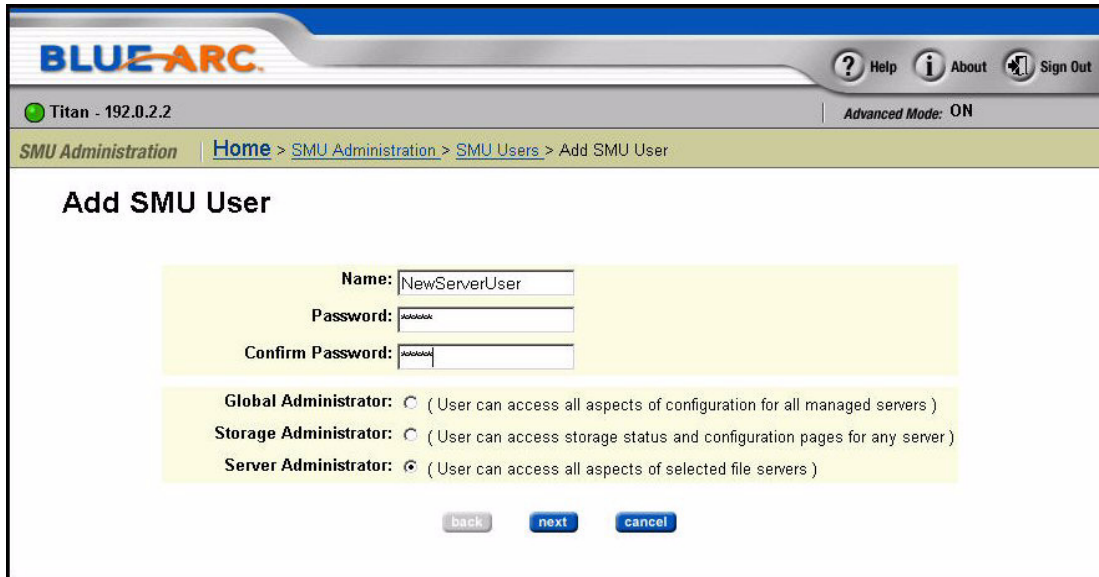
Click "Finish" to apply your changes.

back finish cancel

- Click **finish** to apply your changes.

To add an SMU User - Server Administrator, follow these steps:

1. Click the **Add** button. The following page is displayed.

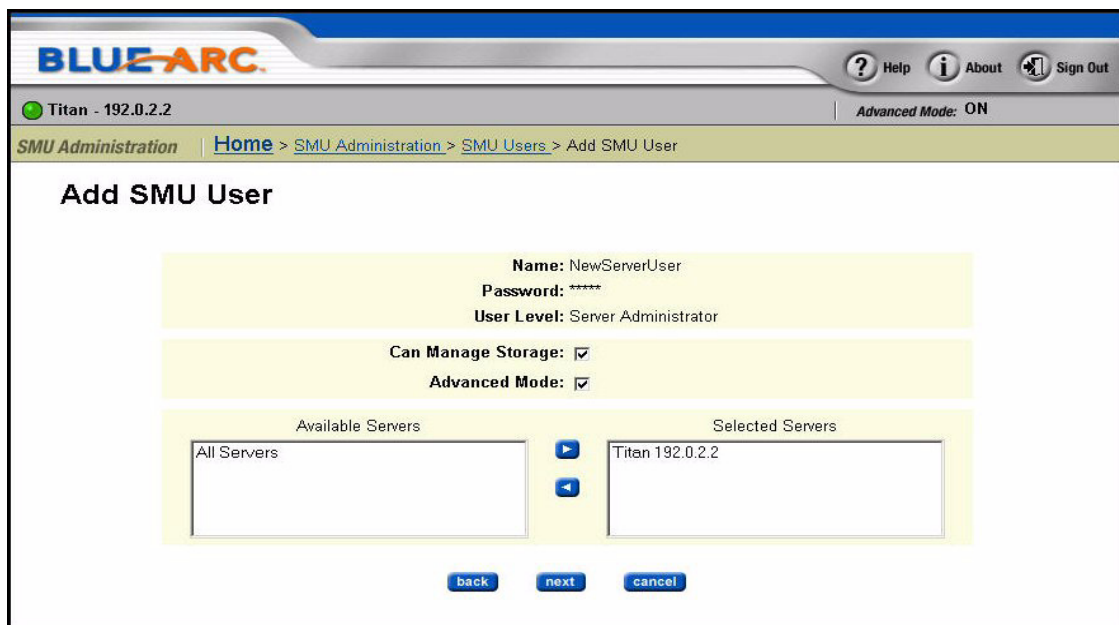


The screenshot shows the 'Add SMU User' form in the BLUE-ARC web interface. The breadcrumb trail is 'Home > SMU Administration > SMU Users > Add SMU User'. The form contains the following fields and options:

- Name:** NewServerUser
- Password:** [masked]
- Confirm Password:** [masked]
- Global Administrator:** ☐ (User can access all aspects of configuration for all managed servers)
- Storage Administrator:** ☐ (User can access storage status and configuration pages for any server)
- Server Administrator:** ☒ (User can access all aspects of selected file servers)

At the bottom are three buttons: 'back', 'next', and 'cancel'.

2. Enter a **User Name** for this SMU User.
3. Enter a **Password** for this SMU User, and confirm the password.
4. Click the **Server Administrator** option.
5. Click **next** to continue. The following screen is displayed.

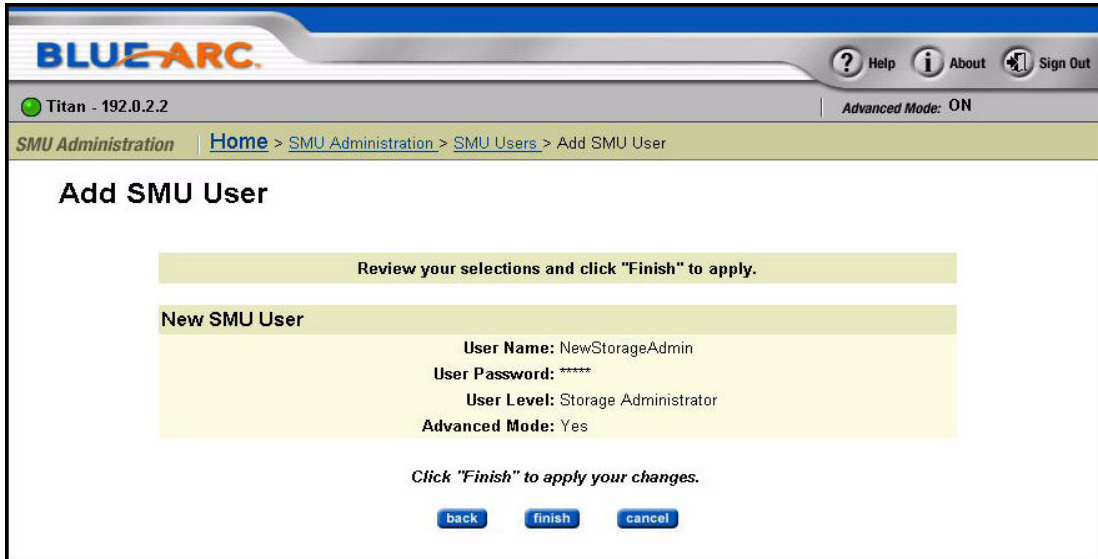


The screenshot shows the 'Add SMU User' form after clicking 'next'. The breadcrumb trail remains 'Home > SMU Administration > SMU Users > Add SMU User'. The form now displays the following information and options:

- Name:** NewServerUser
- Password:** *****
- User Level:** Server Administrator
- Can Manage Storage:** ☒
- Advanced Mode:** ☒
- Available Servers:** A list box containing 'All Servers'.
- Selected Servers:** A list box containing 'Titan 192.0.2.2'.

Between the 'Available Servers' and 'Selected Servers' list boxes are two arrow buttons: a right-pointing arrow and a left-pointing arrow. At the bottom are three buttons: 'back', 'next', and 'cancel'.

6. Highlight the servers that this SMU User has rights and privileges to manage from the **Available Servers** list and move them to the **Selected Servers** list.
7. Click the **Can Manage Storage** checkbox for users who have the necessary right and privileges to manage storage devices on the network.
8. Click the **Advance Mode** checkbox to allow the user to access to advanced functions.
9. Click **next** to continue. The following page is displayed.

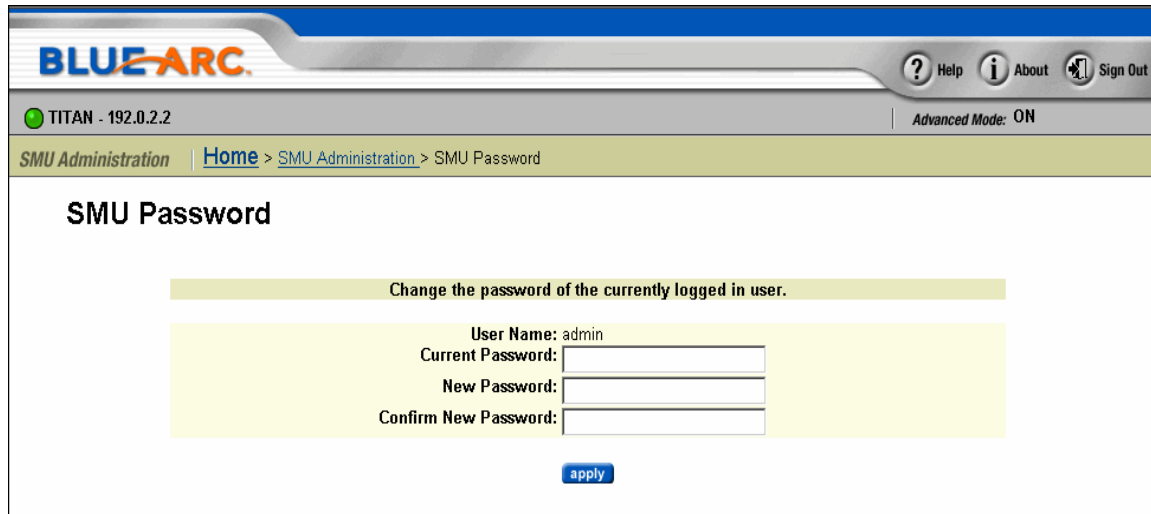


The screenshot shows the BLUE ARC SMU Administration web interface. The top navigation bar includes the BLUE ARC logo, a status bar showing 'Titan - 192.0.2.2' and 'Advanced Mode: ON', and links for Help, About, and Sign Out. The breadcrumb trail is 'SMU Administration > Home > SMU Administration > SMU Users > Add SMU User'. The main heading is 'Add SMU User'. Below it, a yellow box contains the instruction: 'Review your selections and click "Finish" to apply.' Another yellow box titled 'New SMU User' displays the following details: 'User Name: NewStorageAdmin', 'User Password: *****', 'User Level: Storage Administrator', and 'Advanced Mode: Yes'. Below this box, a message states 'Click "Finish" to apply your changes.' At the bottom, there are three buttons: 'back', 'finish', and 'cancel'.

10. Click **finish** to apply the changes.

To change the password for the currently logged in user

1. From the **SMU Administration** page, click **SMU Password**.



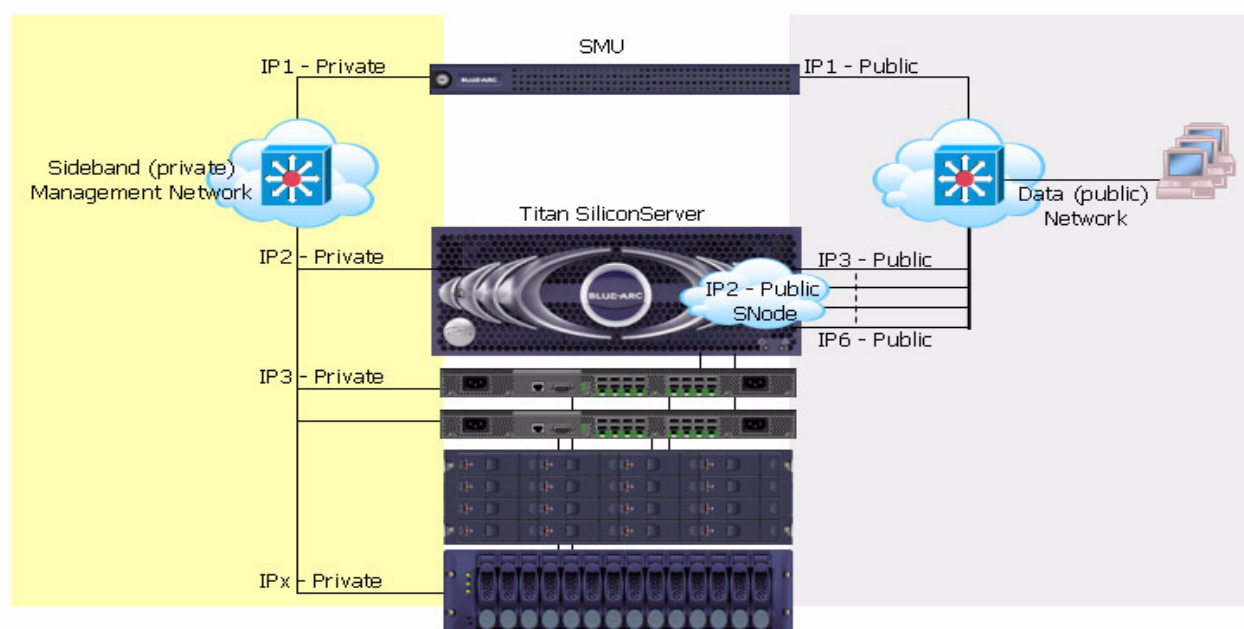
The screenshot shows the BlueArc SMU Administration web interface. The top header features the BlueArc logo, a status bar with 'TITAN - 192.0.2.2' and 'Advanced Mode: ON', and navigation links for Help, About, and Sign Out. The breadcrumb trail indicates the path: Home > SMU Administration > SMU Password. The main content area is titled 'SMU Password' and contains a form for changing the password of the currently logged-in user. The form includes a label 'User Name: admin' and three input fields for 'Current Password', 'New Password', and 'Confirm New Password'. An 'apply' button is located at the bottom of the form.

2. Enter the **current password** followed by the **new password and** confirmation.
3. Click **Apply** when you are finished.

Configuring the Management Network

The BlueArc Storage System operates in conjunction with a number of auxiliary devices, such as RAID storage subsystems, Fibre Channel switches, and power management units. Most of these devices are managed through Ethernet. In order to minimize the impact on an enterprise network, the Titan SiliconServer's physical management structure is divided into two distinct components:

1. A private (sideband) management network. This is a small network used to connect Titan and auxiliary devices, and is isolated from the main network through the SMU (using Network Address Translation - NAT).
2. A public (data) management network (i.e. the enterprise network).



There are significant advantages to having a private management network:

- Network traffic required for normal SMU monitoring of Titan and auxiliary devices will not be on the enterprise network.
- Devices on the private management network will not take up valuable IP addresses on the enterprise network.
- The SMU is able to discover all devices on the private management network, aiding setup.

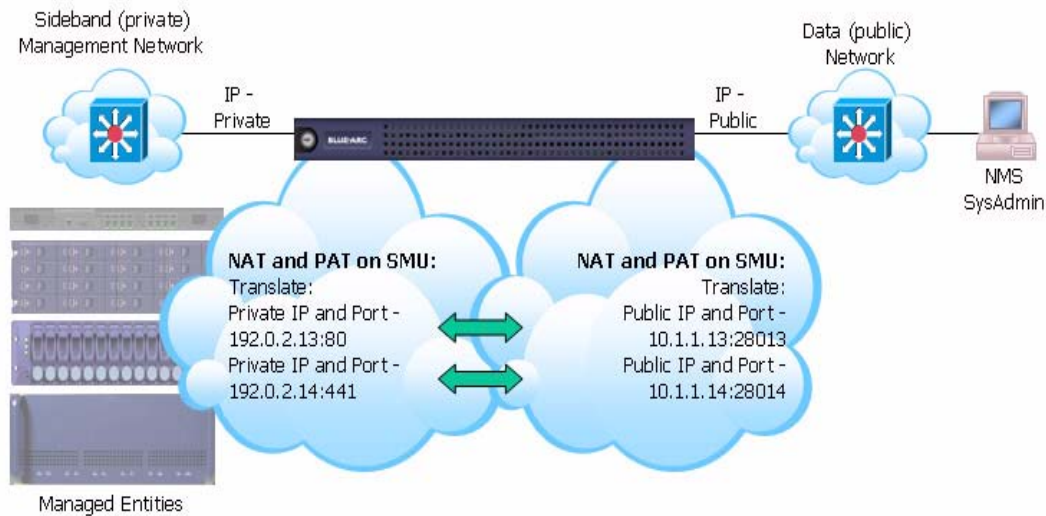
The alternative to using the private management network is to place all of the auxiliary devices onto the enterprise data network. These devices will need to be issued permanent IP addresses within the network. It is possible to have a mixed system, in which some of the auxiliary devices are isolated on the private management network, while others remain on the enterprise network.

Network Address Translation (NAT) Port Range

In order to isolate the private management network from the enterprise network completely, the SMU uses **Network Address Translation (NAT)** and **Port Address Translation (PAT)**. For instance, an HTTP request for a device in the private network would actually be made to the *public* IP address on the SMU's eth0 interface, on a *NATed* port (e.g. **192.168.1.124:28013**). This request will be translated by the SMU to the *private* IP address and *actual* HTTP port of the device on the private network (e.g. **192.0.2.13:80**). This is referred to as the **NAT Port**.

Devices on the Management Network

The IP address range of the private management network includes only those IP addresses sharing the first three octets of the SMU's private (**eth1**) IP address. For example, if the SMU's private IP address is **192.0.2.1** then the devices on the private management network must have addresses in the range of **192.0.2.2 – 192.0.2.254** in order to work on the private management network.



Configuring the Management Network

From the **SMU Administration** page, click **Management Network**.

BLUEARC

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

SMU Administration | [Home](#) > [SMU Administration](#) > Management Network

Management Network

SMU Public IP Address (eth0): 192.168.41.20

SMU Private IP Address (eth1):

Subnet Mask (eth1): 255.255.255.0

NAT Port Range: 28002 - 28254

Devices on Management Network: 4

apply

The **Management Network** page configures the private management network on the SMU's **eth1** interface. An address of **192.0.2.1** will be suggested. This address will not be seen on the enterprise network, but must fall in a distinctly different range to the SMU's public address (i.e. the address on **eth0**). This private IP address is also required to end with **.1** so that the management relationship the SMU has with secondary devices can be maintained more easily.

Once the IP address has been defined, click **apply**.

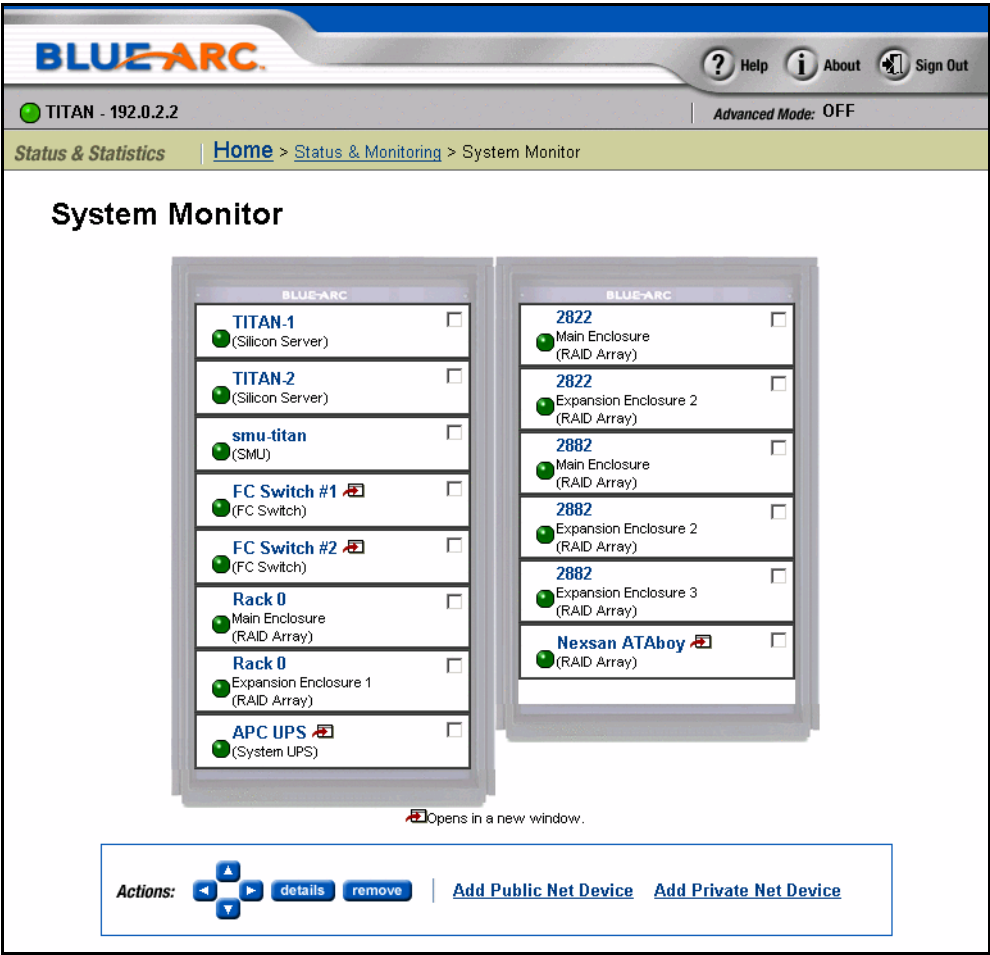


Note: Remember the settings defined for this network so that they may be referenced when configuring Titan's Administration Services IP address and subnet mask.

The NAT Port range is provided for information only. It is rare that these values will ever need to be known.

Configuring Devices on the System Monitor

From the **Status & Monitoring** page, click **System Monitor**.



A system can contain the following basic components:

Component	Description	Action when clicking the <i><u>component</u></i>	Action when clicking the <i><u>details</u></i> button
Titan SiliconServer	This component provides multiple Gigabit Ethernet interfaces to the network and multiple Fibre Channel interfaces to the main enclosure. In high availability configurations, there are two servers.	Loads the Server Status page.	

Main Enclosure	An FC-14 , SA-14 , or FC-16 main enclosure contains disk slots, dual power supplies, and dual RAID controllers.	Loads the enclosure status page.	Loads the System Drives page.
Expansion Enclosure	An FC-14 , SA-14 , or FC-16 expansion enclosure does not contain any RAID controllers.	Loads the enclosure status page.	Loads the System Drives page.
SMU	The System Management Unit	Loads the SMU System Status page.	
System Power Unit	This component is also known as an <i>uninterruptible power supply</i> (UPS).	Loads the UPS Status page.	Loads the UPS Configuration page.
NDMP Backup Devices	Titan monitors its FC links every 60 seconds, and automatically detects the presence of backup devices and adds them to the system monitor. Since Titan could be connected into a FC network shared with other servers, it does not automatically make use of backup devices found on its FC links. Backup devices are added to the configuration through the SAN Management (for backup devices) page.	Loads the NDMP Devices page.	Loads the Backup SAN Management page.
Other Components	Any component can be added to the system monitor. If the device supports a web-based management interface, the management interface can be launched directly from the server management interface.	Loads the embedded management utility for the device. For example, for an AT-14 or AT-42 storage enclosure, it loads the Home page for the device.	Loads either the Add Public Net Device or the Add Private Net Device page. Settings for the component can be changed from this page.

To change the position of any of the items on this screen, select the item (place a tick in the checkbox) and use the **arrows** in the **Action** box.

To display details of the selected item, select the item (place a tick in the checkbox) and click **Details**.

To remove any of the displayed items, select the item (place a tick in the checkbox) and click **Remove**.

Devices residing on either the public (data) or private (sideband) management networks may be

added to the System Monitor, by clicking **Add Public Net Device** or **Add Private Net Device**. Devices on the private management network are "hidden" from the data network through Network Address Translation (NAT).

Once a device has been added, clicking on its **name** will open its embedded management utility from the Web browser, using either HTTP, HTTPS, or telnet. In addition, the SMU can be configured to receive SNMP traps from the device. The SMU will periodically check if the device is still active and connected to the Titan SiliconServer. If a device is no longer responding to network "pings", the device's color will change to red and an alert will be issued.

Adding a device to the public (data) network

From the **Status Monitor** page, click **Add Public Net Device** link. The following screen will be displayed:

The screenshot shows a web browser window with the BLUE-ARC logo at the top. The page title is "Add Public Net Device". The form contains the following fields and controls:

- Device Name:** A text input field.
- Device IP Address:** A text input field.
- Device Type:** A dropdown menu with "Silicon Server" selected.
- Monitor SNMP Traps:** A checked checkbox with the text "If checked, the SiliconServer listens for traps sent from the device."
- Management UI:** A section with a dropdown set to "http" and a text box with "80", followed by the text "Use http and port 80 when opening the Device's management UI."
- Buttons:** "OK" and "cancel" buttons at the bottom.

The table below describes the fields on this screen:

Item / Field	Description
Device Name	A descriptive name to be displayed in the System Monitor to represent this device. Any name may be chosen by the administrator.
Device IP Address	The IP address for the device.
Device Type	Select a device type that best describes the device. This is used purely to help distinguish components in the System Monitor, and does not affect any functionality. Examples include FC switch and System UPS.

Monitor SNMP Traps	If checked, then Titan will <i>listen</i> for SNMP Traps being sent from the device. Enable this option if the device being added is a Nexsan or APC device. Whenever Titan receives traps from these devices, an Event will be logged, and an Email alert may be generated depending on how event logging and notification is configured for the Titan SiliconServer.  Note: The SMU can also be configured to listen for SNMP Traps from supported storage devices. For more details, refer to Receiving SNMP Traps in SMU.
Use Protocol and Port	Specify a protocol (e.g. HTTP) and port number (e.g. 80) to be used for accessing the device's management UI. If the device is to be directly accessed for management by clicking on it is name in the System Monitor, then select HTTP, HTTPS, or telnet and enter the corresponding port number. This information will be used to generate a URL to the device.

Adding a device to the private (sideband) management network

From the **System Monitor** screen, click **Add Private Net Device**.



The screenshot shows the BLUE ARC System Monitor interface. The top navigation bar includes the BLUE ARC logo, a status bar showing 'TITAN - 192.0.2.2', and buttons for Help, About, and Sign Out. The main content area displays the 'Add Private Net Device' dialog box. The dialog box contains the following fields and options:

- Device Name:** Vixel
- Device IP/NAT Mapping:** <Device IP>:<Public NAT Port> (Vendor)
192.0.2.5:28005 (Vixel)
- Device Type:** Silicon Server (dropdown menu)
- Monitor SNMP Traps:** ☒ If checked, the SiliconServer listens for traps sent from the device.
- Use:** http (dropdown menu) and port 80 (text input) when opening the Device's management UI.

At the bottom of the dialog box are 'OK' and 'cancel' buttons.

The table below describes the fields on this screen:

Item / Field	Description
Device Name	A descriptive name displayed in the System Monitor to represent this device. Any name may be chosen by the administrator
Device IP/NAT Mapping	Devices the SMU <i>discovers</i> on the management network are displayed here, excluding devices displayed in the System Monitor. The following Information is displayed for these devices: <i>IP Address:</i> The private IP Address of the device. (This IP address is not directly visible on the public side of the SMU). <i>Public NAT Port:</i> This port on the SMU interface eth0 is used through the public network to access the management port on the device. <i>Vendor:</i> Name of vendor corresponding to the device's MAC address. If the vendor is recognized then a Device Type is recommended (i.e. pre-selected). "Generic" is used if the SMU does not recognize the MAC address. Failure to recognize a Vendor or MAC address does not affect any functionality.
Device Type	Select a device type that best describes the device. This is used purely to help distinguish components in the System Monitor, and does not affect any functionality. Examples include FC switch and System UPS.
Monitor SNMP Traps	If checked, then Titan will <i>listen</i> for SNMP Traps being sent from the device. Enable this option if the device being added is a Nexsan or APC device. Whenever Titan receives traps from these devices, an Event will be logged, and an Email alert may be generated depending upon the configuration of Titan. The SMU can also be configured to listen for SNMP Traps from supported storage devices.
Use Protocol and Port	Specify a protocol (e.g. HTTP) and port number (e.g. 80) to be used for accessing the device's management UI. If the device is to be directly accessed for management by clicking on its name in the System Monitor, then select HTTP, HTTPS, or telnet and enter the corresponding port number. This information will be used to generate a URL to the device.



Note: BlueArc recommends adding the SMU's eth1 IP to the device's list of [NTP](#) servers. Also, if the device supports email notification, and if [email forwarding](#) is configured on the SMU, the SMU's eth1 IP can also be configured as the device's mail server.

Receiving SNMP Traps through the SMU

SNMP traps are alert messages sent by storage devices on the network. These traps provide information about failures or other conditions on those devices. Set the SMU's eth1 IP address as the receiving target for SNMP traps sent by managed devices on the private management network. When a supported storage device sends a trap, the SMU decodes and registers it in each managed server's [event log](#), detailing the trap's name and the contents of the trap's variable binding list.

The SMU supports, and can decode traps from, devices that support the following MIB modules:

- Fibre Alliance
- Brocade Silkworm
- Nexsan



Note: Devices that do not support the SMU's list of supported MIB modules can register traps in the Titan server's Event Log by setting a Titan Administrative IP address as the receiving target for SNMP Traps. Traps registered from Nexsan or APC devices will be properly decoded. Traps from any other device will be registered in unencoded form.

Configuring a System Power Unit

A system power unit, also known as an Uninterruptible Power Supply (UPS), isolates Titan from loss of power, by providing power from a battery. Should the loss of power last long enough for the batteries to drain, the UPS will notify Titan, which can then conduct an orderly shutdown before power runs out. Titan only supports Ethernet-connected APC SMART UPS and the APC Symmetra UPS devices.



Note: Each Titan has its own [NVRAM](#), which it uses to buffer file system writes. In the event of a loss of power, Titan will use its NVRAM to complete any disk transactions that were not saved to disk.

To check the status of the system power unit at any time, refer to the section, [Checking the Status of a Power Unit](#) where the current status is described in detail.

To view system power units configured

From the **SiliconServer Admin** page, click **UPS Configuration**.

The screenshot shows the 'System Power Unit' configuration page in the BLUE-ARC SiliconServer Admin interface. The page has a header with the BLUE-ARC logo and navigation links (Help, About, Sign Out). Below the header, it shows the current user 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF'. The breadcrumb trail is 'SiliconServer Admin > Home > SiliconServer Admin > UPS Configuration'. The main content area is titled 'System Power Unit' and contains a table with one entry: IP address 192.0.2.23. To the right of the table are buttons: Add>>, Properties>>, Delete, and Reset Default. Below the table are form fields for Name, User name (set to 'apc'), and a checkbox for 'Withstand single UPS failure'. Under the heading 'On power failure', there are four checked options with input fields: 'Shutdown after being on battery for 180 seconds', 'Shutdown 0 seconds after power supply reports low battery', 'Shutdown when estimated runtime < 300 seconds', and 'Tolerate power supply being on battery for up to 0 seconds'. At the bottom are 'Apply' and 'Cancel' buttons.

To add a System Power Unit

For the server to be able to monitor the UPS, it must be registered with the UPS as a PowerChute client. In a cluster, if the UPS is on the same subnet, then only one IP address (the Administrative IP) needs to be registered; otherwise each server must be registered individually.

1. From the **UPS Configuration** page, click **Add**.
2. Enter the **IP address** of the power unit.
3. Enter a **user name** for the UPS, e.g. *apc*.
4. Enter the **authentication phrase** for the UPS.
5. **Confirm** the authentication phrase.
6. Check the **Enable SNMP Traps** box if the Titan SiliconServer is to receive traps from the UPS. The UPS must also be configured to send SNMP traps to the Titan SiliconServer.
7. Click **Apply**.

To configure a system power unit

1. If there is more than one UPS, and each UPS generates sufficient power, Titan can be configured **NOT** to shutdown when one of the power units fails. This is done by selecting the **Withstand Single UPS Failure** checkbox. This option will only appear after the first UPS has been added.
2. Identify what the server should do in the event of a power failure by customizing the settings in the **On power failure** fields:
 - Shut down the server if it has been running on UPS power for a specified number of seconds.
 - Shut down the server after a low battery event has been detected. The duration between the event and the shutdown can be specified in a number of seconds.
 - Shut down the server before UPS runs out of power. The server can estimate the amount of power remaining in the UPS and shutdown within a specified number of seconds before this occurs.
 - Do not take any action on power failure for a specified number of seconds. This may be used to prevent unintended shutdowns due to UPS battery tests or maintenance.
3. Click **Apply**.

Configuring the Titan SiliconServer

The Titan SiliconServer is at the heart of the BlueArc Storage System. Titan requires a number of configuration settings, such as system name, date and time, etc. License keys also need to be installed for the protocols and services purchased with the Titan SiliconServer.

Using the SiliconServer Setup Wizard

This wizard performs the basic configuration of a new Titan. The wizard steps through the setup of a new password, setting the server identification, email alerts, name services, etc. At the end of the SiliconServer Setup Wizard, a confirmation screen will appear allowing all the changes to be reviewed.



Note: An IP address must be assigned to Titan before the setup wizard can be used. In addition, Titan must be configured as a Managed Server. For more information, see [Titan SiliconServer Initial Setup](#).

From the **SiliconServer Admin** page, click **SiliconServer Setup Wizard**. The following screen will be displayed:



The screenshot shows a web interface for the SiliconServer Setup Wizard. At the top, there is a blue header with the "BLUE ARC" logo on the left and navigation links for "Help", "About", and "Sign Out" on the right. Below the header, a grey bar displays "TITAN - 192.0.2.2" and "Advanced Mode: OFF". A green breadcrumb trail shows the path: "SiliconServer Admin" > "Home" > "SiliconServer Admin" > "SiliconServer Setup Wizard - Clone SiliconServer Settings". The main content area has a title "SiliconServer Setup Wizard - Clone SiliconServer Settings". Below the title, a yellow box contains the text "Clone the selected configuration from:" followed by a drop-down menu showing "SMU". Below the drop-down menu, it says "to: TITAN". At the bottom of the yellow box, there are three buttons: "back", "next", and "cancel".

If this is the first Titan to be configured, settings defined on the SMU can be cloned to ease the setup of the new server. To clone settings from the SMU, select **SMU** from the drop-down menu and click **next**. See [Cloning from the SMU](#) for more information about cloning settings from the SMU.

If the SMU is already managing other Titan SiliconServers and the selected server is being added to an existing server farm, an expanded list of settings can be cloned to the new server. Proceed to [Cloning from another Titan SiliconServer](#) for more information about cloning settings from another server.

Cloning from the SMU

Check or uncheck the boxes next to configuration items to determine whether these settings will be cloned.

BLUE ARC

TITAN - 192.0.2.2 | Advanced Mode: OFF

SiliconServer Admin | Home > SiliconServer Admin > SiliconServer Setup Wizard - Clone SiliconServer Settings

SiliconServer Setup Wizard - Clone SiliconServer Settings

Clone the selected configuration from: SMU
to: TITAN

Configuration Item	Source Configuration (SMU)	Dest. Configuration (TITAN)
☒ Time	Time: 08:58:54 Date: 02/15/2005	Time: 08:58:51 Date: 02/15/2005
☒ NTP	NTP Servers: 192.0.2.1 10.2.1.7	NTP Servers: No NTP Servers set
☒ DNS Servers	DNS Servers: 192.168.41.1 192.168.41.2 192.168.41.5	DNS Servers: No DNS Servers set
☒ DNS Search order	DNS Search Order: shire.bluearc.com terastack.bluearc.com	DNS Search Order: No DNS Searches set
☒ SMTP servers	Primary SMTP Server: 192.0.2.1 Secondary SMTP Server:	Primary SMTP Server: 192.0.2.1 Secondary SMTP Server:

[Check All](#) | [Clear All](#)

[back](#) [next](#) [cancel](#)

The selected configuration will be applied to the SiliconServer before continuing with the wizard.

The following is a list of configuration items that can be cloned from the SMU:

- Time
- NTP
- DNS Servers
- DNS Search order
- SMTP servers

Cloning from another Titan SiliconServer

Check or uncheck the boxes next to items to determine whether these settings will be cloned. The following is a list of configuration items that can be cloned from another Titan:

- Time
- NTP
- Time Zone
- DNS Servers
- DNS Search order
- WINS
- NIS
- NS Ordering
- NFS Users
- NFS Groups
- CIFS Domains
- FTP Configuration
- SMTP Profiles
- SMTP Servers
- SNMP Alerts
- Windows Popup Alerts
- Syslog Alerts
- HTTP Access
- HTTPS Access
- SNMP Access
- Routes
- NDMP Information

Configuring the Titan SiliconServer

Proceed with the SiliconServer Setup Wizard to complete the setup of the following settings on Titan:

Screen	Description
Password	Configure a custom password to secure access to Titan's management functions.
Server Identification	Set the system name and other identifying information used protocols such as <i>SNMP</i> and <i>SMTP</i> (email).
Name Services	Configure Titan to work with one or more name services , such as DNS, WINS, and NIS. Name services are used to convert server or host names into IP addresses.
SMTP	Configure primary and secondary SMTP servers to be used for sending Email Alerts. During this stage of the Wizard, a default profile that will alert BlueArc Support will be recommended. It is strongly recommended that this profile be created so BlueArc can respond quickly should a failure occur. Additional email profiles for administrative notification of failures can be setup once the Wizard is complete.
Date & Time	Set the server's clock. Synchronize the clock with one or more NTP servers. Since Titan is typically setup on the private management network, add the SMU to the server's list of NTP servers.

Configuring Server Identification

The configuration parameters listed on this page are used to identify Titan. This information is used by protocols such as *SNMP* and *SMTP* (email). To configure the server identification:

From the **SiliconServer Admin** page, click **Server Identification**.



?

 Help

i

 About

Logout

 Sign Out

Titan - 192.0.2.2

Advanced Mode: OFF

SiliconServer Admin | [Home](#) > [SiliconServer Admin](#) > Server Identification

Server Identification

Enter descriptive server information.

Server Name: Titan

Description:

Company Name:

Department:

Location:

Street 1:

Street 2:

City:

State: -

Zip Code / Post Code:

Country:

Contact 1:

First Name:

Surname:

Tel. No.:

Email:

Contact 2:

First Name:

Surname:

Tel. No.:

Email:

apply

Enter the details that will identify the server: **Server Name**, **Description**, **Company Name**, **Department**, **Location**, and **Contacts 1** and **2**. When all fields have been completed, click **apply**.



Note: If Titan is configured for Microsoft Windows networking, then the value used for Description will also serve as the server's comment for all configured [CIFS names](#).

Configuring Date and Time

Titan's current date, time, and time zone can be configured. The NTP Server from which Titan may synchronize its time can also be configured.

Keeping Titan's time in sync with a reliable time source is an important part of keeping the server operating properly. The current time is used in Kerberos authentication which is required when operating with [Active Directory](#). Clock drifting may also cause file access and modification times to be misreported resulting in unexpected results in [Data Migrations](#). Using NTP is the best and most reliable method for keeping Titan's time accurate.

From the **SiliconServer Admin** page, click **Date and Time**.

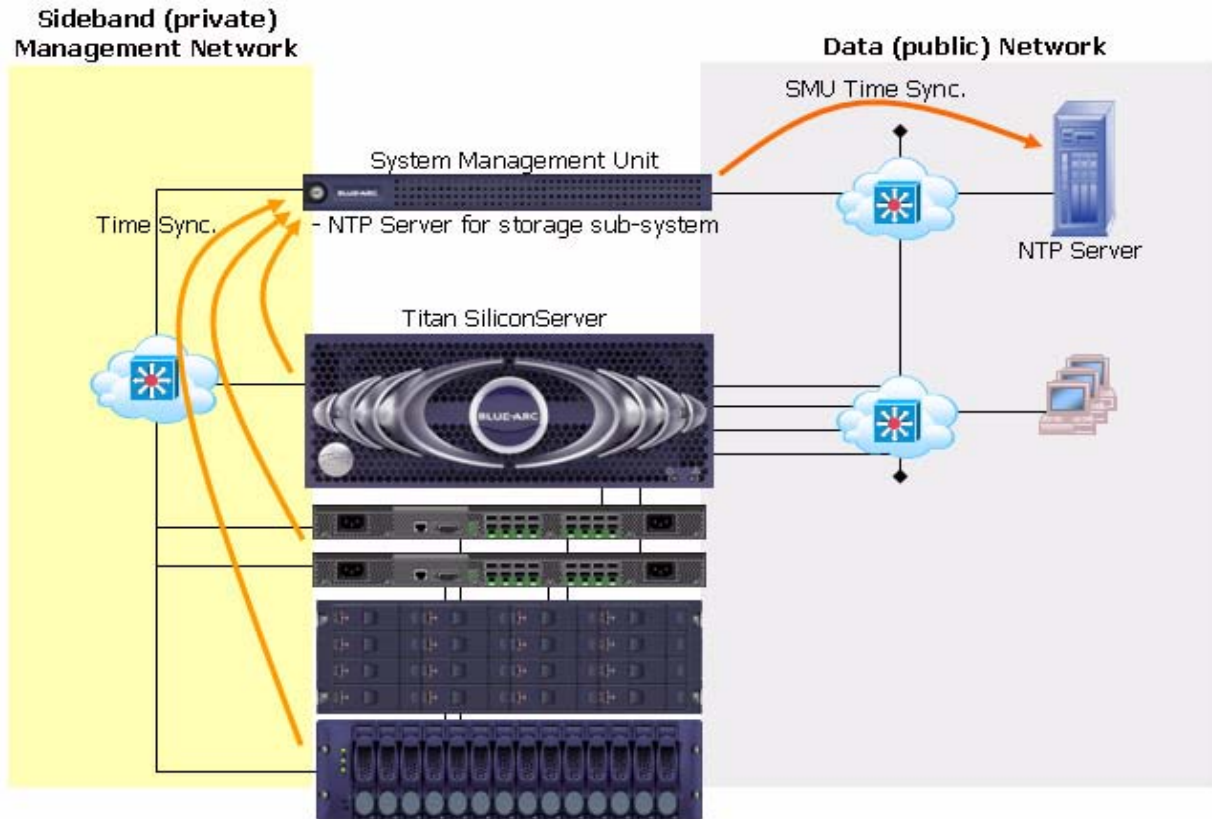
The following table describes the fields on this screen:

Item / Field	Description
Time	Set the time in the 24-hour format .
Date	Select the date from the calendar popup utility.

Time Zone	Select a time zone from the list. For guidance on which zone to select, see http://www.worldtimeserver.com/ .
Daylight Savings	Select whether or not to adjust the server clock automatically when daylight saving time changes.  Note: Never try to compensate for daylight saving by changing the time zone or the time.
Set Time at Boot	NTP is used to align Titan's time with the configured time server <i>gradually</i> . However, if the time is off by more than 15 minutes, NTP updates will not register. If Set Time at Boot is enabled, the time is synchronized with the configured NTP servers when the NTP service starts, typically when the server is rebooted. The NTP service can also be restarted through the CLI. If this option is enabled when the NTP service starts, then the time is set immediately, not gradually, and without regard for the current time offset.
NTP Server	To synchronize the server time with one or more NTP servers on the network, enter the IP address of the NTP server. The system will then qualify and compare all the NTP servers and use the results to set the most accurate time.  Note: If the server is setup on the private management network, the SMU's eth1 IP address should be added to the list of NTP servers.

Using the SMU for NTP

The SMU is configured as an NTP server so that every device on the private management network can be configured to synchronize with at least one NTP server. The SMU itself can synchronize with an NTP server on the public network. The following diagram illustrates this process:



NTP Server Interaction

If using NTP, Titan checks that the specified servers are legitimate NTP servers and then, over a period of a few hours, gradually adjusts the clock to the NTP time. This gradual adjustment is normal and is designed to minimize the effects on utilities that use file timestamps.

If there are more than 15 minutes difference between the time initially set on Titan and the time returned by the NTP servers, Titan does not try to synchronize to the NTP time. Instead, it records a *Warning* event in the Event Log indicating that the date and time must be manually changed to within 15 minutes of the NTP time.

Controlling Direct Server Access

The Titan SiliconServer is primarily managed using Web Manager. In certain circumstances, however, it can also be managed directly through the following mechanisms:

- ❑ The [command line interface](#) (CLI), accessible through SSH and Telnet.
- ❑ The SSC utility, available for both Windows and Linux/Unix.
- ❑ [SNMP](#).

To protect the server from unauthorized access, various safeguards have been included. The following sections detail the configuration options that exist to *lock down* the management interfaces and ports of the Titan SiliconServer.

[Statistics](#) are available to monitor access through these various methods.



Note: To prevent unauthorized access to the storage system, BlueArc recommends that Titan be configured only to respond to predefined (authorized) management hosts on the network, based on the management access method (Telnet, SSC, and SNMP) and defined port number.

Setting the SiliconServer Password

The SiliconServer password is used to authenticate direct management connections to the Titan. This password is required when adding Titan to the SMU's list of managed servers, or when accessing Titan directly through its command line interface.

1. From the **SiliconServer Admin** page, click **Change Password**.
2. Enter the **current password** followed by the **new password** and **confirmation**. This will change the access password for the currently selected server only.
3. Click **Apply**.

Configuring Server Access

In addition to the user name and password required for logon, Titan allows the system administrator to configure the following security settings:

- Specify which *ports* should be used for management communications.
- Specify which *devices* (hosts) can access the management interface.
- Disable unused management interfaces.

To configure server access

From the Home page, click **SiliconServer Admin**. Then, click one of the items in the **Management Access** section, i.e. **Telnet**, **SSC**, or **SNMP**.

The screenshot shows the 'SSC Access Configuration' page. At the top, there's a header with the BLUE ARC logo and links for Help, About, and Sign Out. Below the header, it shows 'TITAN - 192.0.2.2' and 'Advanced Mode: ON'. The main content area is titled 'SSC Access Configuration'. It contains two main sections. The first section has a checked checkbox 'Enable SSC Access', a 'Port Number' field with the value '206', and a 'Maximum Number Of Connections' field with the value '5'. The second section has an unchecked checkbox 'Restrict Access To Allowed Hosts', an 'Allowed Hosts' list box, and 'Add' and 'Delete' buttons. An 'apply' button is at the bottom.

For each facility used to manage the system, do one or more of the following:

Item/Field	Description
Enabled checkbox	To enable or disable the facility, select or clear the Enabled checkbox.
Port number	To change the default port number that the system uses for the facility, type the new number in the field.
Maximum number of connections	To specify the maximum number of users who can simultaneously access the facility, type the new number in the field.
Restrict Access to Allowed Hosts	To specify which users can use the facility, select the checkbox. Then type the IP address of a chosen user in the Allowed Host field and click Add .
Delete	To delete a host, select it from the list and click Delete .

If the system has been setup to work with a [name server](#), the name of the host can be used as well as the IP address. When all fields have been completed, click **apply**.

About License Keys

License keys add powerful services to the Titan SiliconServer and can be purchased and added whenever needed. A BlueArc License Certificate identifies all of the purchased services and should be kept in a safe place. The License Certificate is included in the User Documentation Wallet that was shipped with the system.

The following table lists all licensed services:

Service	Description
CIFS	Common Internet File System. This is a message format used by Windows and MS-DOS to share files, directories, and devices.
NFS	Network File System. This is Sun's distributed file system that enables users of UNIX workstations (including Windows NT systems running an NFS emulation program) to access remote files and directories on a network as if they were local.
iSCSI	Internet Small Computer System Interface. This license enables iSCSI Initiators to communicate at block level with the servers' iSCSI targets.
IBR	Incremental Block-Level Replication. This enables the highly efficient block-level transfer of files during replications.
WORM	Write Once Read Many file systems. These are used to store crucial company data in an unalterable state for a specific duration.
EVS	Enables the migration of Enterprise Virtual Servers between servers in a Server Farm.
Data Migrator	BlueArc Data Migrator. This enables efficient use of primary storage space by transferring older, less performance critical data to secondary storage.
CNS	Cluster Name Space. Used to create a virtual name space through which multiple file systems can be made accessible through a single mount point.
Snapshot Restore	A tool for rolling back one or more files to a previous version without actually copying the data from a snapshot.
FS Rollback	File System Rollback. A tool for restoring a Silicon File System to the state of the last successful replication.
Storage Pools	Allows Storage Pools to host more than one Silicon File System.
Cluster	Allows Titan SiliconServers to be configured as Active/Active, High-availability Clusters.
TB	The amount of licensed storage in Terabytes.

Expiration of License Keys

Licensed features that have been purchased from BlueArc have no expiration date. License keys may be obtained from BlueArc that enable features for use on a trial basis. When used for the purpose of a trial, the features will have a predefined expiration date.

Five days before the expiration of a trial license, a daily warning event will be logged in the server's event log to indicate that the license is about to expire. When two days are left, severe events are logged. When a trial license has expired, the features that were enabled by the license will be disabled.

Using License Keys

Keys for licensed services are managed from the **License Keys** page. It shows the status of each key, the features enabled by the keys, and provides controls for adding and deleting keys.

At the top of the License Keys page is a scroll box containing all the keys. Keys which are appended with a "V" character indicate that they are valid on the server, and keys appended with the "O" character indicate that they are valid on another server. The licensed services that are associated with a specific key can be seen by selecting a key from the list.

License Keys

ddf7-b936-944d-5987-5f14-f2e7-5377-6de2-16c8-8d5b-V

Service	Selected key
CIFS	Enabled
NFS	Enabled
iSCSI	Enabled
IBR	Enabled
DataMigrator	Enabled
EVS	Enabled
Storage Pools	Enabled
FS Rollback	Enabled
Snapshot Restore	Enabled
CNS	Enabled
TB	256 TB
Expires	
MAC ID	3e-b6-bb-62-d8-ed

Total Number of TB licensed : 256 TB

Add a new license key

New Key

Import license keys from a file

To Add a License Key

1. Move to the SMU **Home** page.
2. Click on the **SiliconServer Admin** heading to view the SiliconServer Admin page.
3. From the **Maintenance Tasks** heading, click on **License Keys** to view the License Key page.
4. Do one of the following to add the key:
 - ☐ Type the key number into the **New Key** field, and then click **Add Key**.
 - ☐ If a file that contains the license key has been supplied, use the **Browse** button to select the key file, then click **Import File**.

After all the keys have been entered, follow the instructions to reset the system.

To Delete a License Key

1. Move to the SMU **Home** page.
2. Click on the **SiliconServer Admin** heading to view the SiliconServer Admin page.
3. From the **Maintenance Tasks** heading, click on **License Keys** to view the License Key page.
4. From the scroll box at the top of the page, select a key.
5. Click the **Delete** Key button to delete the key.

3 Network Configuration

Titan Networking Overview and Concepts

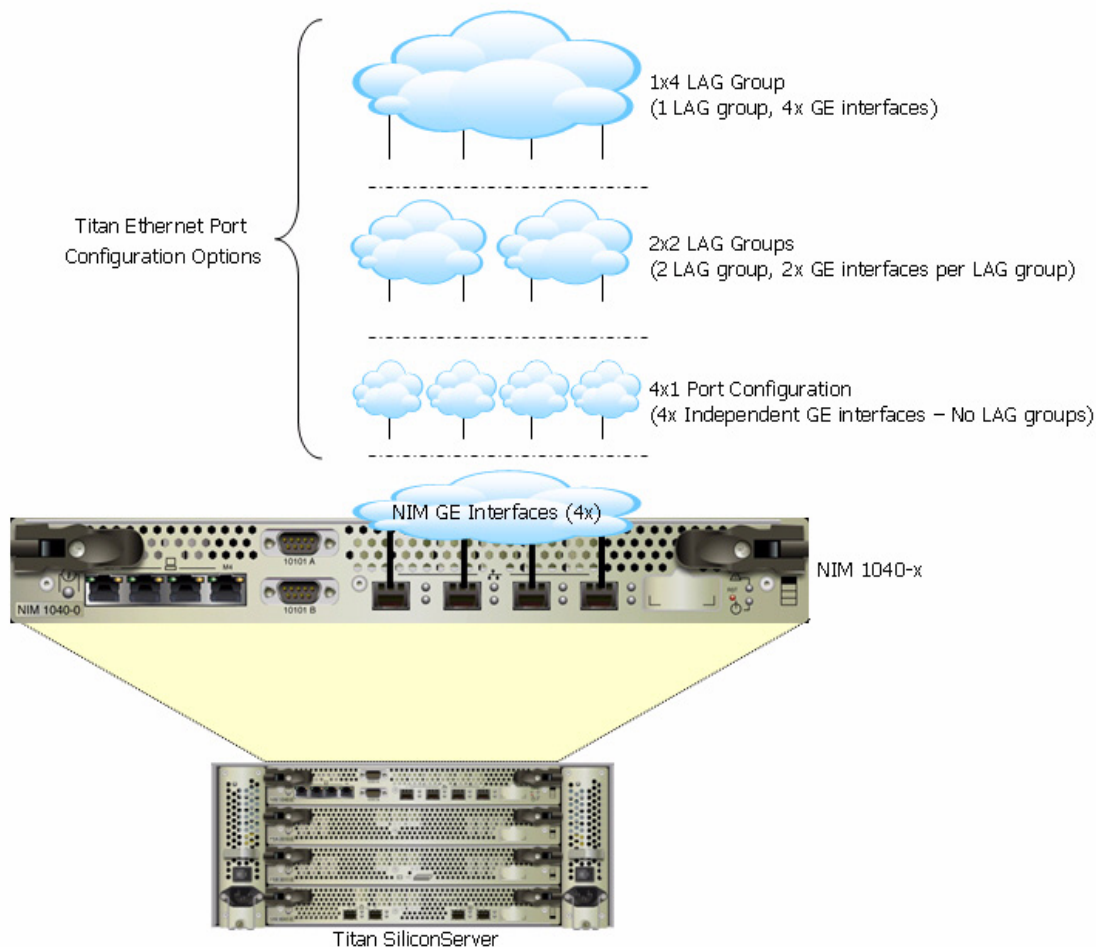
The network interfaces of the BlueArc Storage System, used for data access and management, are explained in this section.

Each Titan SiliconServer provides the following networking ports:

- Six Gigabit Ethernet (GE) ports that support copper and fiber SFPs. The GE ports are intended for high performance data access and support jumbo frames. They can be configured individually or trunked together using IEEE 802.3ad link aggregation.
- A 10/100 Ethernet management port, which is typically used to connect Titan to the [private management network](#). The physical connection to be used is any one of the four externally accessible RJ-45 ports. These four ports are internally wired to a 10/100 Ethernet switch, which is embedded inside the server unit.

Gigabit Ethernet Data Interfaces

Gigabit Ethernet data interfaces are used by network clients to access the Titan SiliconServer.



The GE ports can be configured for either diverse routing or link aggregation.

- Diverse routing allows each port to be configured to support an IP subnet, so that a Titan SiliconServer can be physically connected to a maximum of four separate IP subnets.
- Link aggregation (or trunking) allows multiple GE ports to share a single IP address on the same IP subnet. Any combination of GE ports can be trunked together. Link aggregation increases the bandwidth of a network interface, and isolates the server from failures in the networking infrastructure. For example, if there is a network link failure, the other links in the aggregation will assume all the traffic. Link aggregation is based on the IEEE 802.3ad standard.



Note: Titan supports Link Aggregation Control Protocol (LACP). LACP is used to automatically configure link aggregation settings defined for Titan on the switch to which it is connected. To use LACP, the switch to which the Titan GE interfaces are connected must also support LACP.

Jumbo Frames

Jumbo frames allow transmissions of MAC frames of a size greater than the Ethernet standard of 1,518 bytes. Networking equipment lacking this extension simply drop any jumbo frames received and record an oversize packet error. The use of Jumbo frames allows increased transfer rates by reducing the number of MAC frames required for large transfers.

Jumbo frames co-exist with standard frames on an Ethernet network. To use jumbo frames, correctly configured equipment between the end-points supporting jumbo frames must be provided. The configured equipment offers a MTU maximum of 9000 bytes.

All the GE interfaces of a Titan SiliconServer support jumbo frames.

- Jumbo frames are received unconditionally on all GE interfaces without any configuration changes.
- Jumbo frames can be transmitted by a GE interface by configuring its MTU size to a value less than or equal to 9000.

IP data transmission using jumbo frames depends on the destination IP address or sub-network. The maximum MTU size for a destination IP address or sub-network is configured as an attribute in the IP routing table.

IP Address Assignments

IP addresses are assigned to Titan for three different purposes:

- **File services.** Network clients access Titan's [File Services](#) through Titan's configured file service IP addresses. File services are only accessible through the GE ports. Multiple IP addresses can be assigned for file services. The IP addresses assigned may be on the same or different networks, but must be unique.
- **Administration Services.** These IP addresses are used when [managing Titan](#), through Web Administration Manager or using Titan's embedded management interfaces. Titan requires at least one IP address, which is assigned to the 10/100 Ethernet port connected to the [private management network](#). Additional IP addresses can be assigned to GE ports, so that management functions (such as telnet or SSC) may be performed directly on these network ports.



Note: When configuring an Administration Services IP address for use on the private management network, verify that its subnet mask matches that of the SMU's private management network (eth1) i.e. 255.255.255.0. Also, choose an IP address that resides within the management network's range e.g. 192.0.2.2-254. This should be the same IP address that is used when configuring Titan as the managed server on the SMU.

- **Clustering.** When configured as a [cluster](#), each Titan needs an IP address for the 10/100 management port connected to the private management network. This is used for communication between Cluster Nodes and between the Cluster Nodes and Quorum Device (QD).

At least two IP addresses are required to configure Titan for access through the public network.

These are:

- A public IP address on the [System Management Unit \(SMU\)](#) for server administration.
- A public File Services IP address on at least one of the GE interfaces. If link aggregation is used on all the GE ports, only a single IP address is required for all four ports in a 4x1 link aggregation group. If diverse routing is configured (independent configurations per GE interface), each interface must have its own IP address.

Network Statistics

[Ethernet](#) and [TCP/IP](#) statistics for Titan are available to monitor the activity since the last reboot or since the point when the statistics were last reset. Both per-port and overall statistics are available. The statistics are updated every ten seconds.

A histogram of bytes/second received and transmitted during the most recent few minutes is also available. The Ethernet History is a graphical display of the Ethernet traffic on Titan. Both per-port and overall histograms are available.

Configuring the Gigabit Ethernet Interfaces

Configuring the GE ports on Titan requires the following steps:

1. Creating an aggregation with one or more GE ports assigned to it.
2. Assigning IP addresses. Add the IP addresses necessary to access file and block services provided by the server.

Link Aggregations (IEEE 802.3ad)

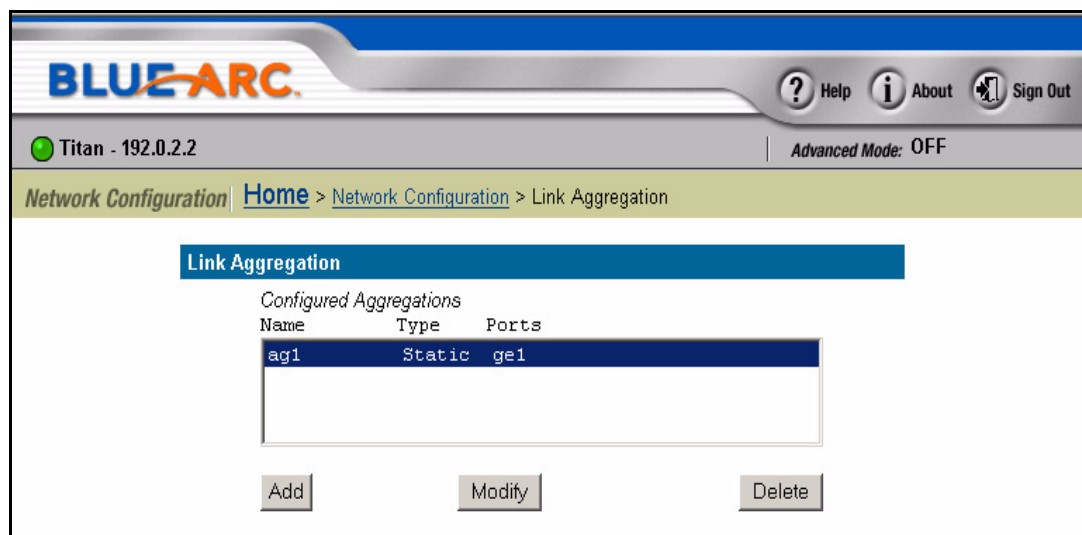
The Titan SiliconServer supports aggregation of multiple GE ports into logical links. This allows connection into the server with all of Titan's GE links in parallel. Link aggregation, also called trunking, provides two key benefits:

- It increases the bandwidth of a single connection.
- It provides increased fault resiliency – if one link is broken, the other links share the traffic for that link.

Aggregated GE ports share a single MAC address and a single set of IP addresses. GE ports can be aggregated in arbitrary sets for all ports in a trunk. The Titan SiliconServer is initially configured with a single port aggregation containing GE port 1.

To view Link Aggregation Groups (LAGs)

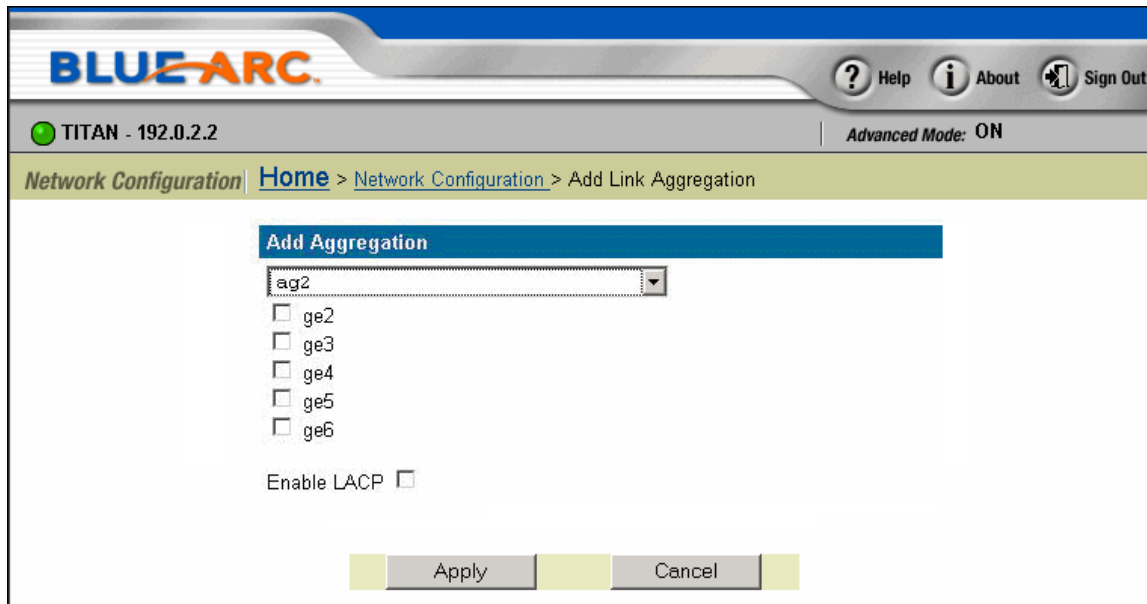
From the **Network Configuration** page, click **Link Aggregation Configuration**.



Item /Field	Description
Name	Name of the aggregation (ag1, ag2, ag3, ag4, ag5, ag6).
Type	Configuration Type of the aggregation: Static: the switch to which the aggregated links are connected must be configured to match the link aggregation settings defined on the Titan. LACP: the Link Aggregation Control Protocol (LACP) will be used to automatically negotiate the Aggregation between the Titan and its network switch. For this to function appropriately, the network switch in use must support LACP. Furthermore, the switch must be configured to use LACP on all of its ports that will be physically connected to the Titan GE interfaces.
Ports	Gigabit Ethernet Port to which the aggregation is linked (ge1, ge2, ge3, ge4, ge5, ge6).

To Add Link Aggregation Groups (LAGs)

1. Click **Add**.



The screenshot shows the BLUE ARC web interface for network configuration. The top navigation bar includes the BLUE ARC logo, a status bar showing 'TITAN - 192.0.2.2' and 'Advanced Mode: ON', and links for Help, About, and Sign Out. The breadcrumb trail is 'Network Configuration > Home > Network Configuration > Add Link Aggregation'. The main content area is titled 'Add Aggregation' and features a drop-down menu with 'ag2' selected. Below the menu are five checkboxes for interfaces: ge2, ge3, ge4, ge5, and ge6. At the bottom of the form is an 'Enable LACP' checkbox, which is currently unchecked. 'Apply' and 'Cancel' buttons are at the bottom right.

2. Select the aggregation from the drop-down list.
3. Check the box next to the GE interfaces to be added to the aggregation.
4. If supported by the Ethernet switch, check to **Enable LACP**.



Note: Titan supports Link Aggregation Control Protocol (LACP). LACP is used to automatically configure link aggregation settings defined for Titan on the switch to which it is connected. To use LACP, the switch to which the Titan GE interfaces are connected must also support LACP. In addition, the switch must be configured to use LACP on the ports linked to the Titan SiliconServer..

5. Click **Apply**.

To View / Modify Configured Aggregations

1. Select the aggregation from the list.
2. Click **Modify**.
3. Select the GE interfaces that should function as a part of the aggregation.
4. If supported by the Ethernet switch, check **Enable LACP**.
5. Click **Apply**.

To Delete an Aggregation

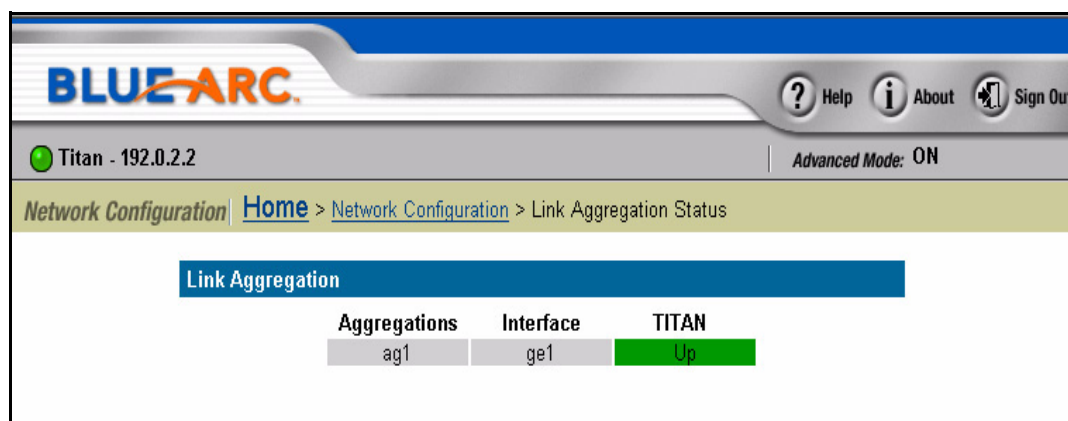
1. Select the aggregation from the list.
2. Click **Delete**.



Note: In order to delete a link aggregation group, all IP addresses and GE ports associated with the LAG must first be removed.

To View an Aggregation's Status

From the **Network Configuration** page, click **Link Aggregation Status**.



Item / Field	Description
Aggregations	Name of the aggregation (ag1, ag2, ag3, ag4, ag5, ag6).
Interface	The list of GE ports. They will appear next to their configured aggregation.
<server name>	• Up: The port on Titan is physically connected to the switch and is able to send and receive incoming data. • Attached (LACP only): The port on Titan is physically connected to the switch. Traffic not passing across the link. Ports in this mode are typically running as the standby ports in 3+3 or 5+1 groups. • Detached (LACP only): The port on Titan is physically connected to the switch. Traffic not passing across the link. This state is a transient LACP state and may be seen prior to a port becoming attached. • Down: There is no physical connection between the port on Titan and the switch.

IP Network Setup

Titan SiliconServer IP addresses are assigned to various interfaces and used for the following purpose:

- **File services** (CIFS, NFS, FTP, and iSCSI). IP addresses used to access file services using GE aggregations are assigned to an [Enterprise Virtual Server \(EVS\)](#). Each EVS can have multiple IP addresses assigned to the same GE interface.
- **Server administration**. Typically, the 10/100 management port is assigned an IP address on the private management network. However, in order to access Titan on the public network using telnet or SSC, an *Admin Services* IP address must be assigned to one or more of the GE interfaces.
- **Clustering**. When Titan is configured in a cluster, the 10/100 management port on each Cluster Node is assigned an IP address on the private management network for communications between the Cluster Nodes and the QD.

From the **Network Configuration** page, click **IP Addresses**.

?

 Help

i

 About

Logout icon

 Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Network Configuration | [Home](#) > [Network Configuration](#) > IP Addresses

IP Addresses

▼ IP Address	Subnet Mask	EVS	Port	Type	Cluster Node
☐ 192.0.2.2	255.255.255.0	Titan	mgmnt1	Admin Services	TITAN-1
☐ 192.0.2.3	255.255.255.0		mgmnt1	Cluster Node	TITAN-1
☐ 192.0.2.4	255.255.255.0		mgmnt1	Cluster Node	TITAN-2
☐ 192.168.38.100	255.255.240.0	EVS01	ag1	File Services	TITAN-2
☐ 192.168.38.101	255.255.240.0	EVS02	ag1	File Services	TITAN-2
☐ 192.168.38.102	255.255.240.0	EVS03	ag1	File Services	TITAN-2
☐ 192.168.38.103	255.255.240.0	EVS04	ag1	File Services	TITAN-2
☐ 192.168.38.104	255.255.240.0	EVS05	ag1	File Services	TITAN-1
☐ 192.168.38.105	255.255.240.0	EVS06	ag1	File Services	TITAN-1
☐ 192.168.38.106	255.255.240.0	EVS07	ag1	File Services	TITAN-1
☐ 192.168.38.107	255.255.240.0	EVS08	ag1	File Services	TITAN-1
☐ 192.168.38.108	255.255.240.0	Titan	ag1	Admin Services	TITAN-1

[Check All](#) | [Clear All](#)

Actions:

add

delete

Shortcuts: [EVS Management](#)

Item / Field	Description
IP Address	The IP Address of the services or Cluster Node.
Subnet Mask	The subnet mask of the services or Cluster Node.
EVS	One of the following: - The label of the Enterprise Virtual Server on which the File Services IP is bound. - If the server name is displayed, then the IP address is an administrative IP for the server.
Port	The interface used by the IP address: agX identifies one of the GE aggregations mgmnt1 identifies the 10/100 management port
Type	Type of services or configuration of the server (Admin Services , File Services , or Cluster Node).
Cluster Node	If configured as a cluster, the name of the Cluster Node to which the IP address is assigned.

Adding an IP Address

To add an IP address to an interface, click **add**.

The screenshot shows the BlueArc TITAN web interface. At the top, there's a header with the BlueArc logo and navigation links: Help, About, and Sign Out. Below the header, a status bar shows 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF'. The main navigation area includes 'Network Configuration', 'Home', 'Network Configuration', 'IP Addresses', and 'Add IP Address'. The central content area is titled 'Add IP Address' and contains a form with the following fields:

- EVS:** A dropdown menu currently showing 'Titan - Admin Services'.
- Port:** A dropdown menu currently showing 'ag1'.
- IP Address:** A text input field.
- Subnet Mask:** A text input field.

At the bottom of the form are two buttons: 'OK' and 'cancel'.

1. Select from the drop-down list the EVS to which the IP will be assigned. Alternatively, specify that the IP address should be used for Administrative services.

- 2. Select from the drop-down list the port: **agX** or **mgmt1**. If the IP address is being assigned to an EVS, an Ag port must be specified.
- 3. Enter the **IP address**.
- 4. Enter the **Subnet Mask**.
- 5. Click **OK**.

Removing an IP Address

When an IP address has been added to the server it is immediately available for use. To ensure IP addresses are not in use when they are removed, the EVS to which the IP is assigned must be disabled. When the EVS is disabled the IP address assigned to the EVS may be deleted. Once the IP address has been removed, the EVS should be enabled.

Disable the EVS

- 1. From the **SiliconServer Admin** page, click **EVS Management**.

BLUE ARC

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

SiliconServer Admin | [Home](#) > [SiliconServer Admin](#) > EVS Management

EVS Management

Type	Label	First IP Address	Status	Enabled	Cluster Node
Admin Services	Titan	192.0.2.2	online	Yes	TITAN-1
File Services	EVS01	192.168.38.100	online	Yes	TITAN-1
File Services	EVS02	192.168.38.101	online	Yes	TITAN-1
File Services	EVS03	192.168.38.102	online	Yes	TITAN-2
File Services	EVS04	192.168.38.103	online	Yes	TITAN-2
File Services	EVS05	192.168.38.104	online	Yes	TITAN-1
File Services	EVS06	192.168.38.105	online	Yes	TITAN-2

Modify Label

Disable EVS

Restart EVS

Add EVS

Delete EVS

- 2. Select the **EVS** to which the **IP** is assigned.
- 3. Click **Disable EVS**.

Delete the IP Address

1. From the **Network Configuration** page, click **IP Addresses**.
2. Select the **IP Address** to delete.
3. Click **delete**.

Enable the EVS

1. From the **SiliconServer Admin** page, click **EVS Management**.
2. Select the **EVS** that needs to be reactivated.
3. Click **Enable EVS**.

Advanced IP Network Setup

To access additional configuration settings for the IP Network configuration, turn the **Advanced Mode: ON**. Then, on the **Network Configuration** page, click **Advanced IP Setup**.

The screenshot displays the BLUE ARC Network Configuration interface. At the top, the status bar shows 'TITAN - 192.0.2.2' and 'Advanced Mode: ON'. The breadcrumb trail indicates the path: 'Network Configuration > Home > Network Configuration > Advanced IP Setup'. The main section is titled 'IP Configuration' and is divided into two parts: 'Global Settings' and 'Per-port Settings (These values override the defaults for the specified port)'. The 'Global Settings' section includes fields for 'IP reassembly timer - seconds' (15), 'Ignore ICMP echo requests' (unchecked), 'IP MTU for off-subnet transmits - bytes' (1500), 'TCP Keep alive' (checked), 'TCP Keep alive timeout' (7200), 'TCP MTU' (1500), and 'Other Protocol MTU' (1500). The 'Per-port Settings' section shows a dropdown menu for 'Ports' set to 'ag1', with corresponding fields for 'Ignore ICMP echo requests' (unchecked), 'IP MTU for off-subnet transmits - bytes', 'TCP Keep alive' (unchecked), 'TCP Keep alive timeout', 'TCP MTU', and 'Other Protocol MTU'. At the bottom of the 'Per-port Settings' section are buttons for 'Restore default settings' and 'Create'. At the very bottom of the form are 'Apply' and 'Cancel' buttons.

The default settings for this page are detailed below:

Global Settings		Default Settings
IP reassembly timer (seconds)		15
Ignore ICMP echo requests		No
IP MTU for off-subnet transmits - bytes	Server and clients on same IP sub-network	1500
	Clients that reside on a different subnet than the server	576
TCP Keep alive		Yes
TCP Keep alive timeout (seconds)		7200
TCP MTU		1500
Other Protocol MTU		1500

The Advanced IP Network settings are applied at a global level - i.e. the values supplied as Global Settings are initially used for all aggregations (and the GE interfaces that they use). After that, individual configuration settings may be defined for each defined Aggregation (Port) on the server.

Use the **Create** button to build a new record of settings for the currently selected Aggregation, as indicated by the Aggregation name selected via the **Ports** field. Enter the details using the fields that follow, and click **Apply**.

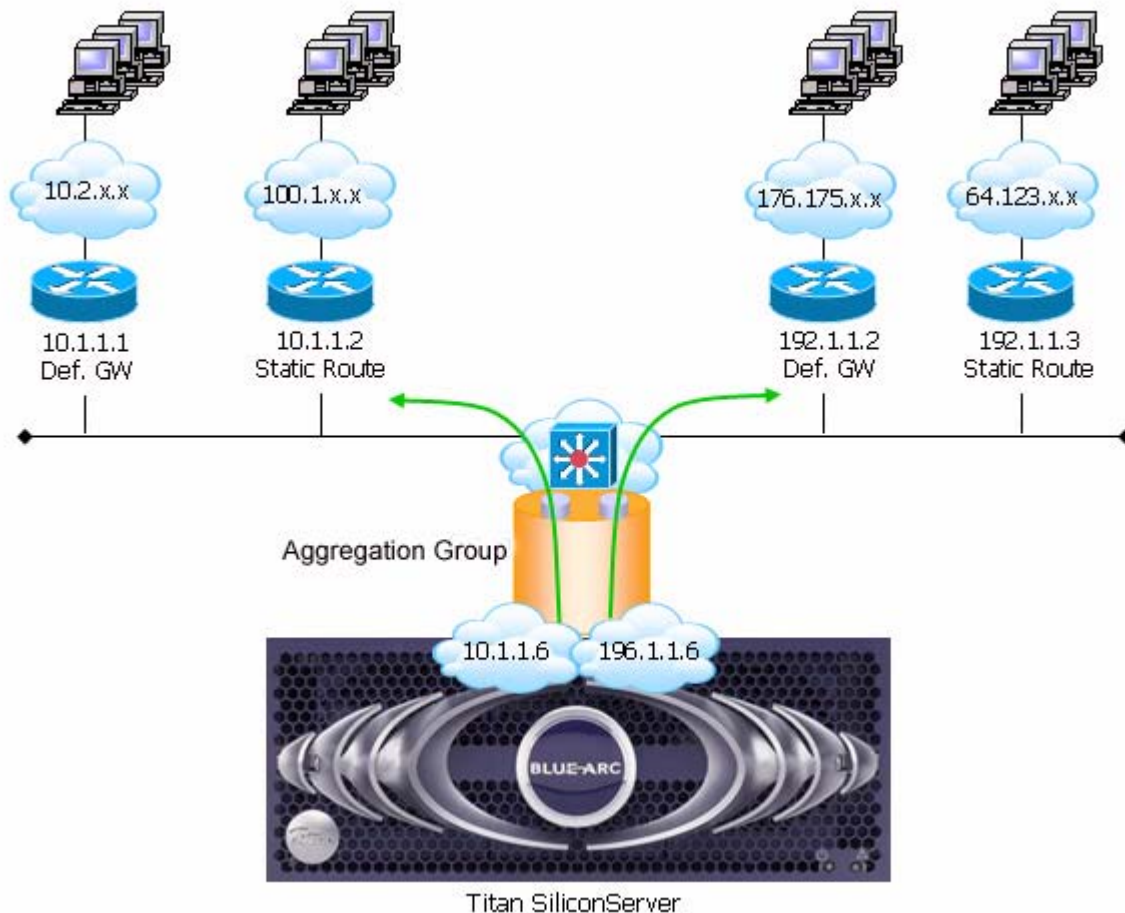
To delete the settings for a specific Aggregation, select the particular Aggregation from the Ports field and then click **Delete**. The settings applied to the aggregation (and all of the interfaces (GEs) it uses) will revert to the defaults as defined by the *Global Settings*.

The **Restore default settings** button may be used to restore the default settings in the *Global Settings* box.

After completing the IP network settings, follow the instructions to reset the server if instructed.

IP Routes

Titan can be configured to route IP traffic in three different ways: through Static Routes, Default Gateways, and Dynamic Routes. The illustration below shows how a Titan may be configured to communicate with various IP networks through routes.



The following sections discuss Static Routes, Default Gateways, and Dynamic Host Routes in more detail.

Static Routes

Static routing provides a means to forward data in a network through a fixed path. If a server is attached to a network, and that network is connected to additional networks through a router, communication between the server and the remote network can be enabled by specifying a static route to each network.

Static routes are set up by specifying their details in a *routing table*. Each entry in the table

consists of a destination network ID, a gateway address, and sometimes a subnet mask. The entries in the table are persistent. If the server is restarted, the table preserves the static routing entries.

Titan supports both network and host-based static routes. Select the **Network** option to set up a route to address all the computers on a specific network. Select the **Host** option to address a specific computer that is on a different network than the router through which it is normally addressed. The maximum possible static routes is 128. Note that default gateways also count against the total number of static routes.

Default Gateways

Titan supports multiple default gateways for routing IP communication. When connected to multiple IP networks, add a default gateway for each network to which the Titan is connected. When configured in this way, Titan will direct traffic through the appropriate default gateway by matching the source IP address specified in outgoing packets with the gateway on the same subnet.

With multiple default gateways, Titan routes IP traffic logically and reduces the need to specify static routes for every network with which Titan needs to communicate.

Dynamic Host Routes

Titan also supports *ICMP redirects*, an industry standard which provides a means for routers to convey routing information back to the server. When one router detects that another router offers a better route to a destination, it sends a redirect that temporarily overrides the system's routing table. Being router-based, dynamic redirects do not require any configuration, but they can be viewed in the routing table.

Titan stores dynamic host routes in its route cache for ten minutes. When the time has elapsed, packets to the selected destination use the route specified in the routing table until the server receives another ICMP redirect.

Titan's route cache can store a maximum of 65,000 dynamic routes at a time.

Routing Precedence

Titan's routing options follow an order where the most specific route available for the outgoing IP packet will be chosen. The host route is the most specific since it targets a specific computer on the network. The network route is the next most specific since it targets a specific network. A gateway is the least specific route and hence the third routing option for Titan.

Therefore, if Titan finds a host route for the outgoing IP packet, it will choose that route over a network route or gateway. Similarly, when a host route is not available, Titan will choose a corresponding network route or, in the absence of host and network routes, Titan will send the packet to a default gateway.

Managing the Server's Route Table

The routing table on the **IP Routes** page displays all the routes configured on the server. Any additions or modifications to the routes can be made on this page.

To View/Modify the Route Table

From the **Network Configuration** page, click **IP Routes**.

BLUE-ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Network Configuration Home > Network Configuration > IP Routes

IP	Netmask	Gateway	Type
0.0.0.0	0.0.0.0	192.168.46.1	Gateway

☒ Static Routes ☒ Dynamic Routes

Delete Delete All

IP ☐ Host
Netmask ☒ Network
Gateway ☐ Gateway

Add

Flush cache after making changes
Flush

Item/Field	Description
Host/ Network/ Gateway	Select the route type: Host , Network , or Gateway .
IP Address Netmask Gateway	Enter the IP address for the static route. - For host-based static routing, enter the IP address of the destination device and the Gateway through which the host should be accessed. The Netmask will always be 255.255.255.255 for host-based routes. - For network-based static routing, specify the target network based on the IP and Netmask, and the Gateway through which the host should be accessed. - To define a gateway, enter the IP address of the gateway.
Add	The Add button will add the route.
Delete	To remove a route, select it from the drop-down list. Then, click Delete . To remove all routes, click Delete All .
Flush	Click Flush to flush the cache immediately.

Configuring Name Services

The Titan SiliconServer supports standard name services. Name services are used to convert server or host names into IP addresses. In addition to the Domain Name System (DNS), Titan supports WINS (used by CIFS clients) and NIS (used by NFS clients).

Setting up the System to Work with a Name Server

Titan can be set to work with a local name server and to support four name resolution methods:

1. Domain Name System (DNS)
2. Windows Internet Naming Service (WINS)
3. Network Information Service (NIS)
4. Lightweight Directory Access Protocol (LDAP)

These name resolution methods associate computer identifiers (e.g. IP addresses) with computer names. This will allow computer names rather than IP addresses in dialog boxes (for example, the NFS Export Properties dialog box).

In addition to name services, NIS provides the following functionality:

- Administering the names and IDs of UNIX [users and groups](#) if CIFS and NFS clients are accessing Titan.
- Authenticating [FTP](#) users.

From the **Network Configuration** page, click **Name Services**.

The screenshot shows the BlueArc Titan web interface. The top navigation bar includes the BlueArc logo, a status indicator for 'Titan - 192.0.2.2', and links for Help, About, and Sign Out. Below the navigation bar, the breadcrumb trail reads 'Network Configuration > Home > Network Configuration > Name Services'. The main heading is 'Name Services'. A yellow box contains the instruction 'Specify Name Service information where applicable'. Below this, there are three sections: 'DNS Servers' with two input fields containing '192.168.41.1', 'Domain Search Order' with a large text area and 'Add', 'Up', 'Down', and 'X' buttons, and 'WINS Servers' with two input fields labeled 'Primary' and 'Secondary'. An 'apply' button is at the bottom.

Item /Field	Description
DNS Servers	Enter the IP addresses of a maximum of three DNS servers. If more than one DNS server is entered, the search will be performed in the order listed.

Domain Search Order	Enter a Domain suffix to use as a search keyword. Click add to append it to the list of suffixes displayed. The order of the suffixes in the list box can be changed by using the <i>up</i> and <i>down</i> arrows. A suffix can be deleted by selecting it from the list and then, clicking the X button. The suffix (e.g. <i>ourcompany.com</i>), combined with a computer's host name, makes a fully qualified domain name. When a search for a computer name is performed, the DNS server searches for it in the order in which the suffixes are listed. For example, if the box contains the entries <i>uk.ourcompany.com</i> and <i>us.ourcompany.com</i>, a request for the IP address of <i>author</i> generates a query for <i>author.uk.ourcompany.com</i> and then for <i>author.us.ourcompany.com</i>. However, the system does not search the parent Domain <i>ourcompany.com</i>.
WINS Servers	To setup a primary WINS server, type the IP address in the Primary field. If there is a secondary WINS server, then type the address in the Secondary WINS server field.

Specifying the Order in which to Use Name Services

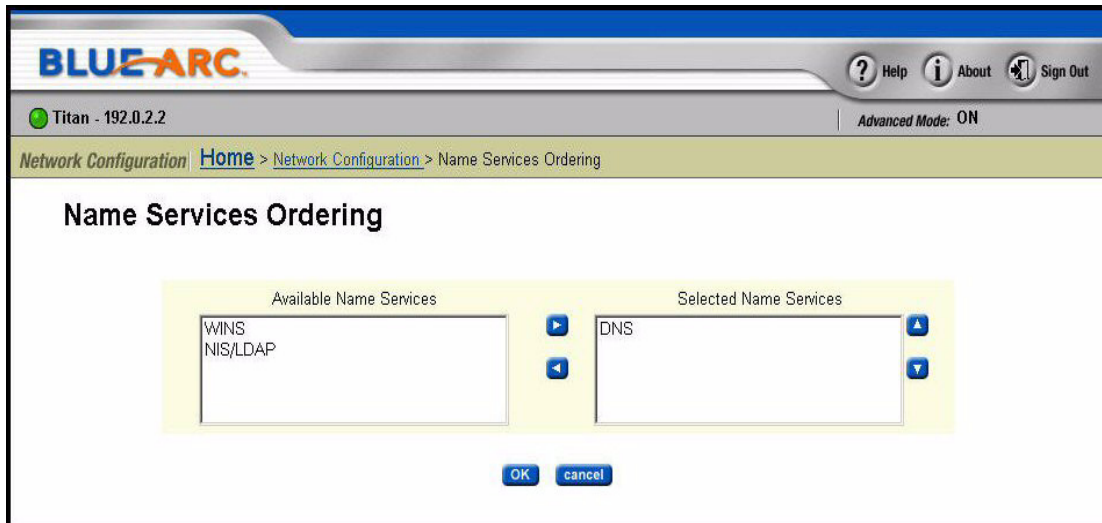
If Titan has been configured to work with multiple name services, the order in which those services should be used must be specified.



Note: If only one name service is used, verify that the name service appears in the **Name Services Order** configuration page.

Changing the Name Service Order

- From the **Network Configuration** page, click **Name Services Ordering**.
The **Name Services Ordering** page displays a list of Available Name Services and the Selected Name Services in separate boxes.



2. Select a Name Service that you wish to use from the Available Name Services box and move it to the Selected Name Services box using the right arrow button.
3. If necessary repeat Step 2 for all the Name Services that should be used.
4. Change the order that the system will use for the Name Services by selecting a service in the Selected Name Services box and clicking the **Up** or **Down** buttons.
5. If necessary repeat step 4 until the desired order has been achieved.
6. Remove any services which are not required by selecting the service and then moving it from the Selected Name Services box using the left arrow button.
7. Click OK or Cancel to commit or decline the changes.

Configuring Network Information Services

Network Information Services are databases that provide simple management and administration of Unix-based networks. These databases can provide details about users and groups. They also can contain information about individual client machines, along with their IP address and host name which facilitates authentication for users that log into clients on the network. LDAP and NIS, formerly known as Yellow Pages (YP), are both capable of providing Network Information Services.

Titan can utilize Network Information Services and easily integrate into environments running either LDAP or NIS. Using the Network Information Services, Titan can perform the following:

- Retrieve NFS user and group account information
- Name services for resolving host names to IP addresses
- (FTP) authentication

Benefits of Using LDAP

Many organizations are moving towards LDAP and replacing their existing NIS infrastructure with the more reliable, scalable and secure system that LDAP provides. Using LDAP instead of NIS to provide Network Information Services can provide the following advantages:

- Better information accuracy because of LDAP's more frequent data synchronization of current and replicated data.
- Encryption of communication using Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
- Authentication of connection to the LDAP database, as opposed to NIS, which allows anonymous access to its database.



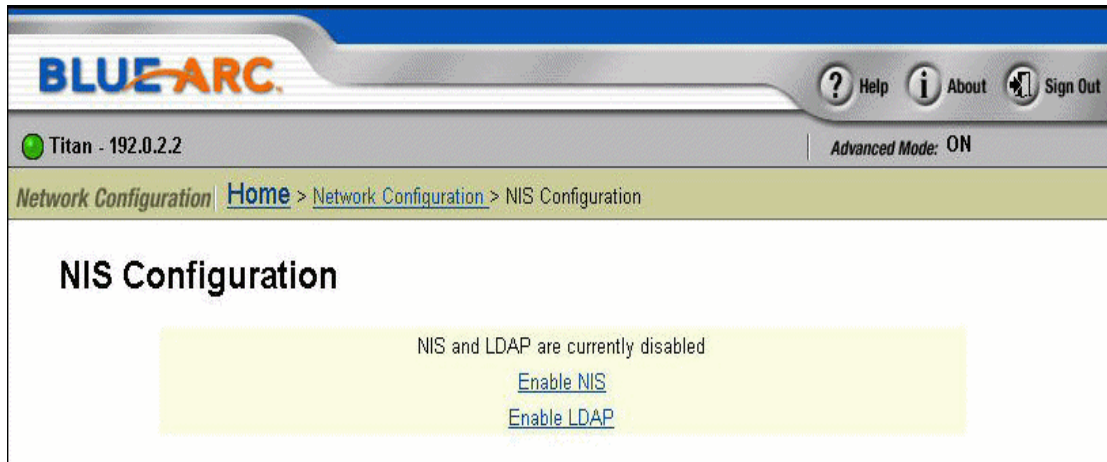
Note: LDAP cannot be used to resolve NIS Netgroups. If Netgroups are required, local Netgroups must be used.

The next section discusses how to enable and configure NIS and LDAP services using the Web Manager.

Enabling Network Information Services

After deciding which network information service to use, enable the service using the following instructions.

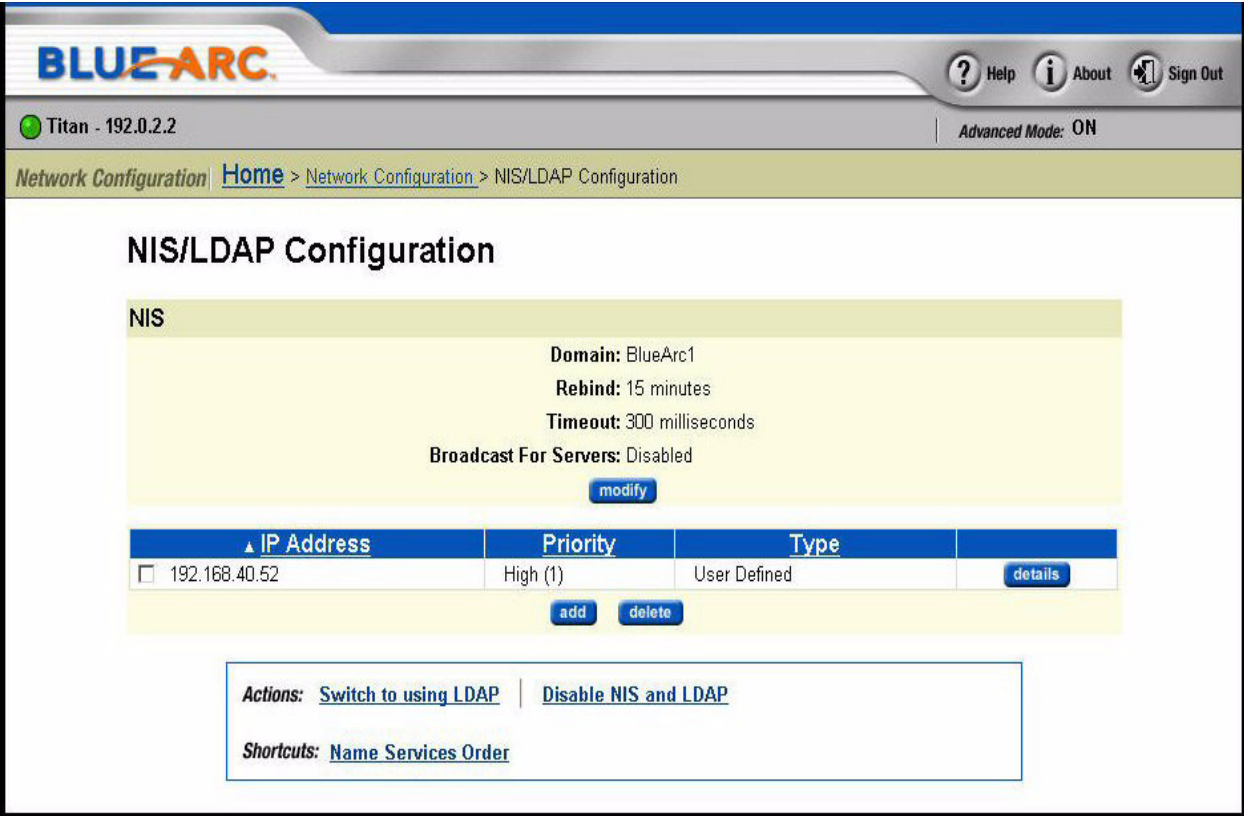
From the **Network Configuration** page, click **NIS/LDAP Configuration**. The following screen is displayed:



- **Enable NIS** - click this link to enable NIS.
- **Enable LDAP** - click this link to enable LDAP.

Configuring NIS Settings

If NIS has been selected to provide Network Information Services, then from the **Network Configuration** page, click **NIS/LDAP Configuration**.



From the NIS Configuration screen the following tasks may be performed:

- switch between NIS and LDAP configurations
- add or delete servers
- view server details
- modify the NIS configuration
- disable NIS

Item/Field	Description
Domain	The name of the NIS Domain for which the system is a client.
Rebind	The frequency with which Titan attempts to connect to its configured NIS servers. Enter a value from 1 to 15 minutes.

Timeout	The period of time for a response from an NIS server when checking the Domain for servers. Enter a value from 100 to 10000 milliseconds. The default value is 300 milliseconds.
Broadcast For Servers	This option allows Titan to discover available NIS servers on the network. Servers must be in the same NIS domain and be present on the same network as Titan in order to be found.
IP Address	Displays the IP address of the NIS servers to which the server is currently bound.
Priority	The priority level for the server. The lowest value is the highest priority level. If the NIS Domain contains multiple servers, the system will try to bind to the server with the highest priority level whenever it performs a rebind check. Priority Levels • High - Level 1 • Medium - Level 2 • Low - Level 3
Type	This section displays the type of NIS server. Servers can be automatically discovered through the broadcast for servers option or added manually.

Actions

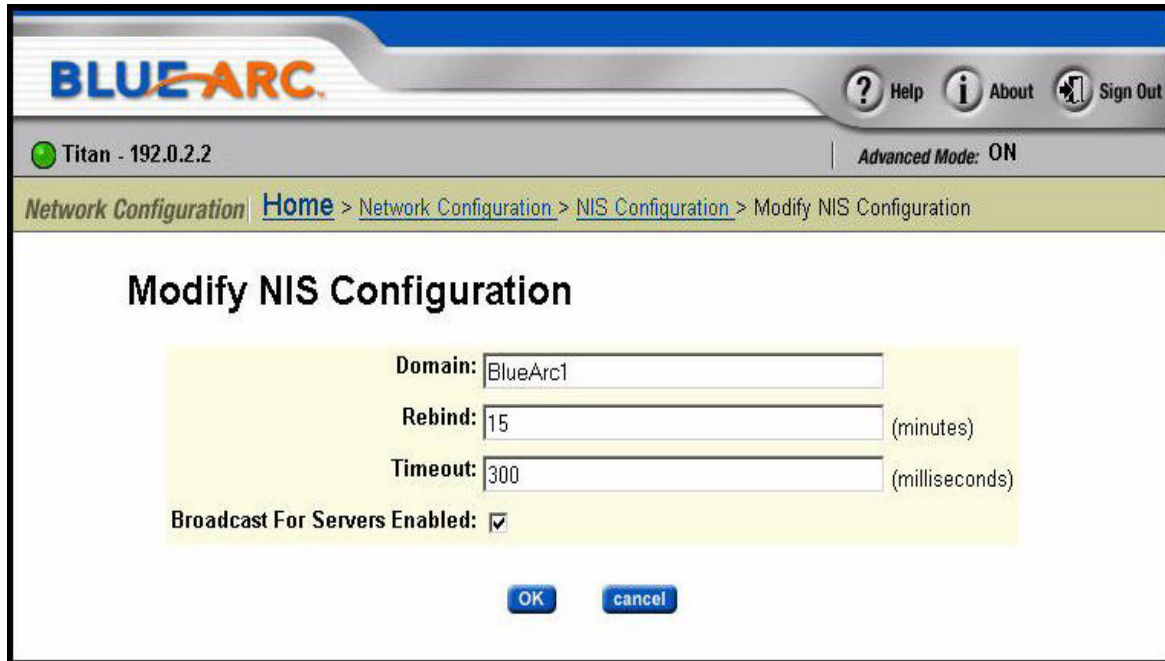
- **Switch to using LDAP:** Click this link to change to using LDAP for Network Information Services.
- **Disable NIS and LDAP:** Click this link to disable Network Information Services.

Shortcuts:

- **Name Services Order:** Clicking this shortcut navigates to the Name Services page where NIS/LDAP can be selected to provide host name resolution.

Changing the NIS Configuration

To make changes to the NIS configuration, click the **modify** button on the NIS Configuration page. The following screen will be displayed.



1. Enter the **Domain** Name.
2. Enter the **Rebind** time in minutes.
3. Enter the **Timeout** in milliseconds.
4. Check the broadcast checkbox if you want the server to be listed in NIS/Configuration page.
5. Click **OK** to continue.

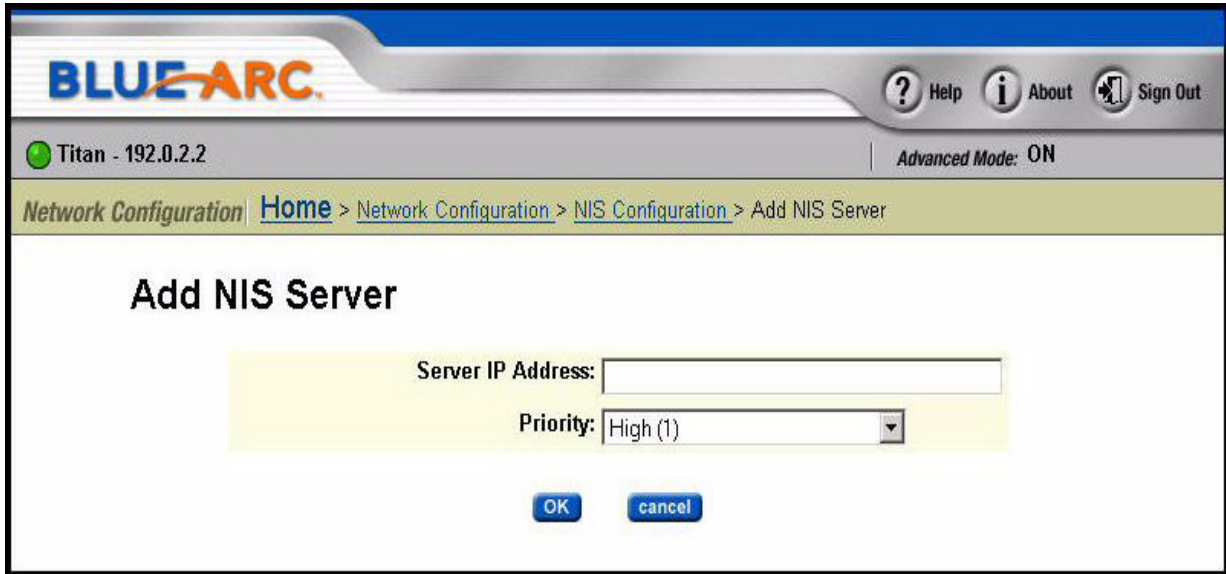
Configuring NIS Servers

A list of the servers to which the Titan may be bound can be specified. This list can contain a maximum of 16 NIS servers.

To add server by IP Address

1. From the **Home** page, click **Network Configuration-> NIS Configuration**.

- Click the **add** button. The following screen is displayed.



The screenshot shows the BlueArc Titan web interface. The top header includes the BlueArc logo, a status bar showing 'Titan - 192.0.2.2' and 'Advanced Mode: ON', and navigation links for Help, About, and Sign Out. The breadcrumb trail is 'Network Configuration > Home > Network Configuration > NIS Configuration > Add NIS Server'. The main content area is titled 'Add NIS Server' and contains a form with two fields: 'Server IP Address' (a text input field) and 'Priority' (a drop-down menu currently set to 'High (1)'). Below the form are 'OK' and 'cancel' buttons.

- Enter the **IP address** of the **NIS** server in the **Server IP Address** field.
- In the Priority field, assign a **priority** level from the drop-down list. The lowest value is the highest priority level. If the NIS Domain contains multiple servers, the system will try to bind to the server with the highest priority level whenever it performs a rebind check.
- Click **OK** to add this NIS server.

Broadcast For Servers

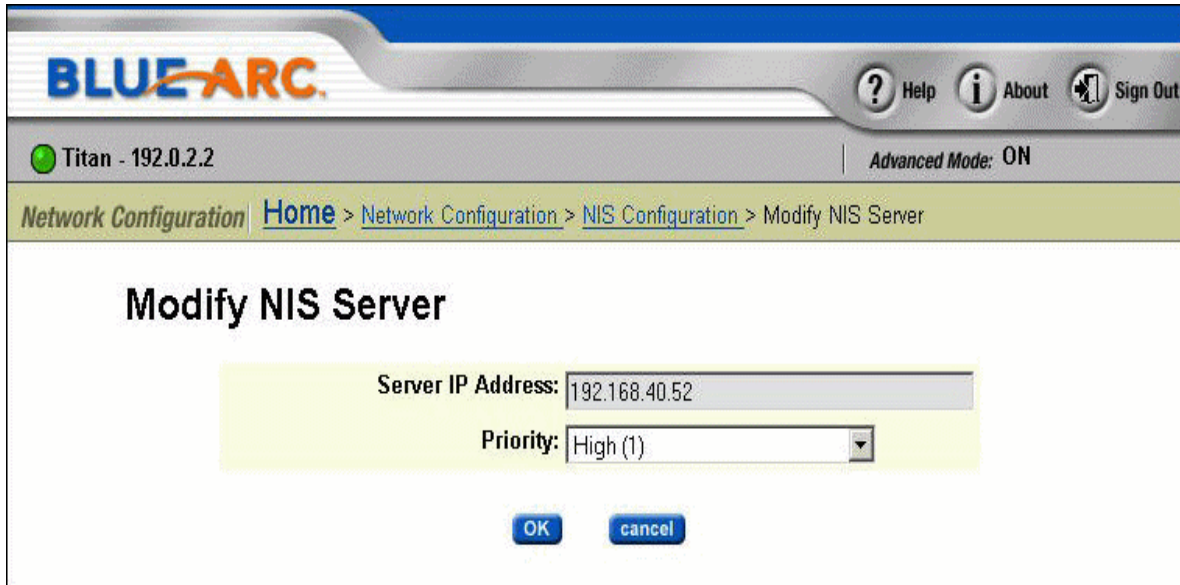
Once NIS settings have been configured, "Broadcast for Servers" can be enabled. If enabled, Titan will search for NIS servers on the network that are in its configured NIS domain. These servers are found by broadcast and therefore must be on the same logical network as the Titan. NIS servers found by broadcast are regularly pooled for responsiveness. When a request for NIS lookup is made, the most responsive server will be selected.

To remove NIS servers found by broadcast, disable "Broadcast for Servers". Attempting to remove NIS servers found by broadcast will result in the following error message.



To change the priority of a configured NIS Server

1. From the **Home** page, click **Network Configuration-> NIS Configuration**.
2. Click **details** button next to the server. The following screen is displayed.

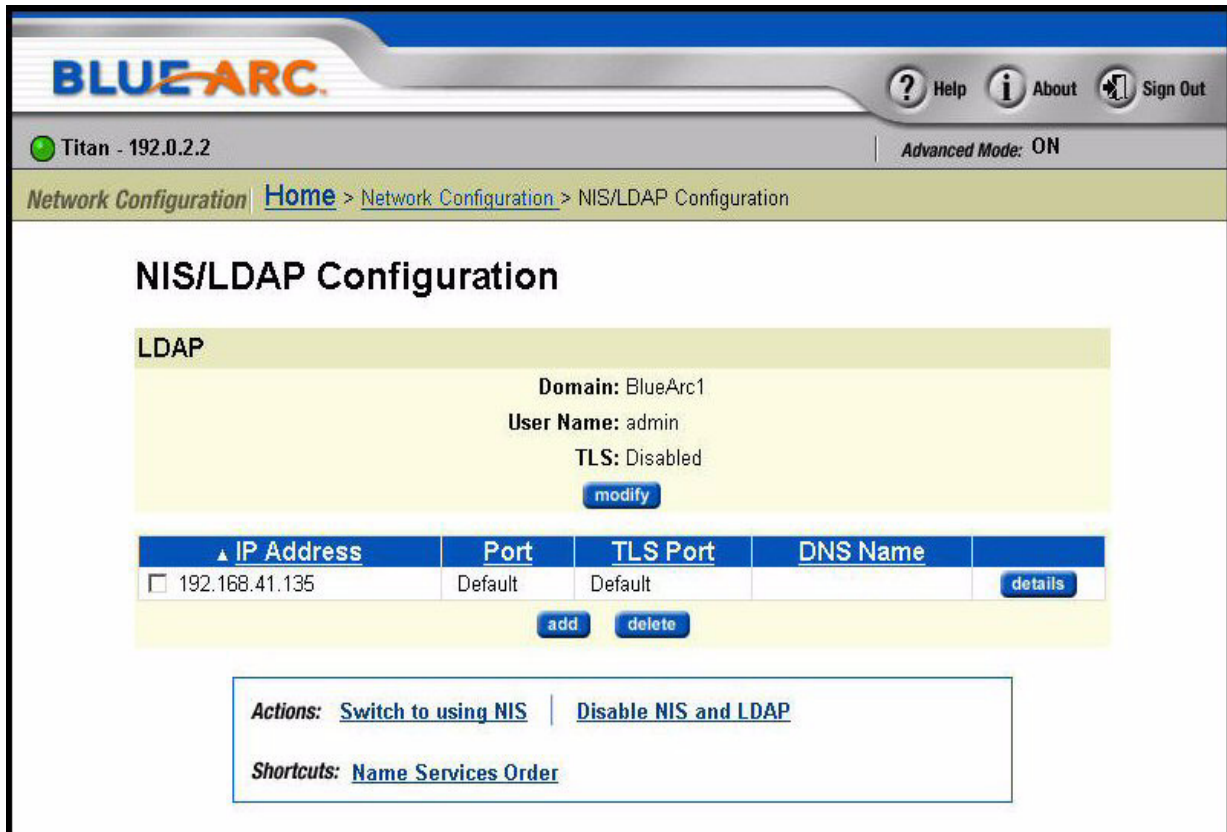


The screenshot shows a web browser window with the BlueArc logo in the top left. The top navigation bar includes links for Help, About, and Sign Out. Below this, a status bar shows 'Titan - 192.0.2.2' and 'Advanced Mode: ON'. The breadcrumb trail reads: 'Network Configuration > Home > Network Configuration > NIS Configuration > Modify NIS Server'. The main content area is titled 'Modify NIS Server' and contains a form with two fields: 'Server IP Address' with the value '192.168.40.52' and 'Priority' with a dropdown menu showing 'High (1)'. At the bottom of the form are 'OK' and 'cancel' buttons.

3. Change the priority of a configured NIS server by selecting one of the available options listed in the drop down box.
4. Click **OK** to continue.

Configuring LDAP Settings

If LDAP has been selected to provide Network Information Services, then from the **Network Configuration** page, click **NIS/LDAP Configuration**.



BLUE ARC

Help About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Network Configuration Home > Network Configuration > NIS/LDAP Configuration

NIS/LDAP Configuration

LDAP

Domain: BlueArc1
 User Name: admin
 TLS: Disabled
[modify](#)

IP Address	Port	TLS Port	DNS Name	
☐ 192.168.41.135	Default	Default		details

[add](#) [delete](#)

Actions: [Switch to using NIS](#) | [Disable NIS and LDAP](#)

Shortcuts: [Name Services Order](#)

From this screen you can perform the following tasks:

- switch between NIS and LDAP configurations
- add or delete servers
- view server details
- modify the LDAP configuration
- disable LDAP

Item/Field	Description
Domain	The name of the LDAP Domain for which the system is a client. For example: bluearc.com

User Name	The user name of the administrator who has rights and privileges for this LDAP server. For example: cn="Directory Manager",dc=bluearc,dc=com
TLS	Use this option to enable/disable the SSL connection.
IP Address	Displays the IP address of the NIS servers to which the server is currently bound.
Port	The standard port that is configurable by the administrator. The default port is 389
TLS Port	The secure port that is configurable by the administrator. The default port is 636
DNS Name	The fully qualified hostname of the LDAP server.

Actions:

- **Switch to using NIS:** Click this link to change to using NIS for Network Information Services.
- **Disable NIS and LDAP:** Click this link to disable Network Information Services.

Shortcuts:

- **Name Services Order:** Clicking this shortcut navigates to the Name Services page where NIS/LDAP can be selected to provide host name resolution.

Modifying the LDAP Configuration

To make changes to the LDAP configuration, click **modify**. The following screen is displayed. Administrators can use this screen to directly manage LDAP configuration for specific users.



Note: This option supports both registered and anonymous login of users.

BLUE ARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Network Configuration [Home](#) > [Network Configuration](#) > [NIS Configuration](#) > Modify LDAP Configuration

Modify LDAP Configuration

Domain:

User Name:

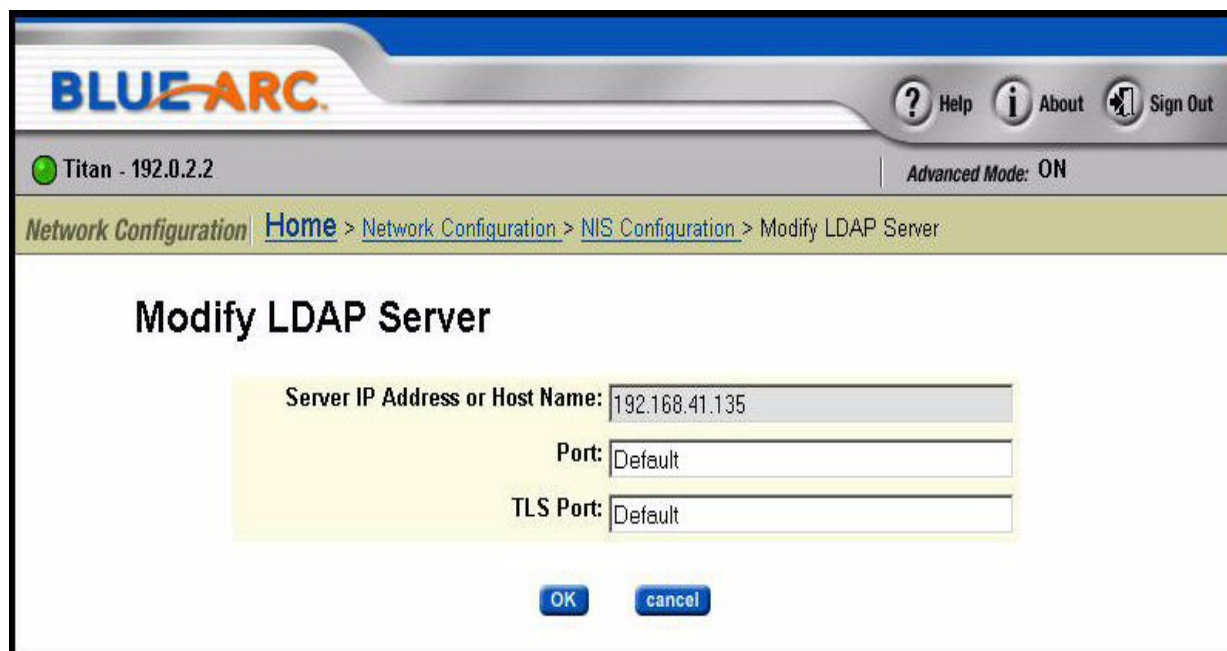
Password:

TLS Enabled: ☐

- ❑ Change or modify the **Domain** Name.
- ❑ Change or modify the **User Name**.
- ❑ Enter the **Password**.
- ❑ Specify if **TLS** is **Enabled/Disabled**.
- ❑ Click **OK** to continue.

Modifying the LDAP Server

To modify the LDAP server, select **Network Configuration->NIS Configuration->Modify LDAP Server**. The following screen is displayed.



The screenshot displays the BlueArc Titan web interface. At the top, the BlueArc logo is on the left, and navigation links for Help, About, and Sign Out are on the right. Below the header, a status bar shows 'Titan - 192.0.2.2' and 'Advanced Mode: ON'. A breadcrumb trail reads: 'Network Configuration > Home > Network Configuration > NIS Configuration > Modify LDAP Server'. The main content area is titled 'Modify LDAP Server' and contains three input fields: 'Server IP Address or Host Name' with the value '192.168.41.135', 'Port' with the value 'Default', and 'TLS Port' with the value 'Default'. At the bottom of the form are 'OK' and 'cancel' buttons.

1. Modify or change **Port** entry.
2. Modify or change **TLS Port** entry.
3. Click **OK** to continue.

4 Multi-Tiered Storage

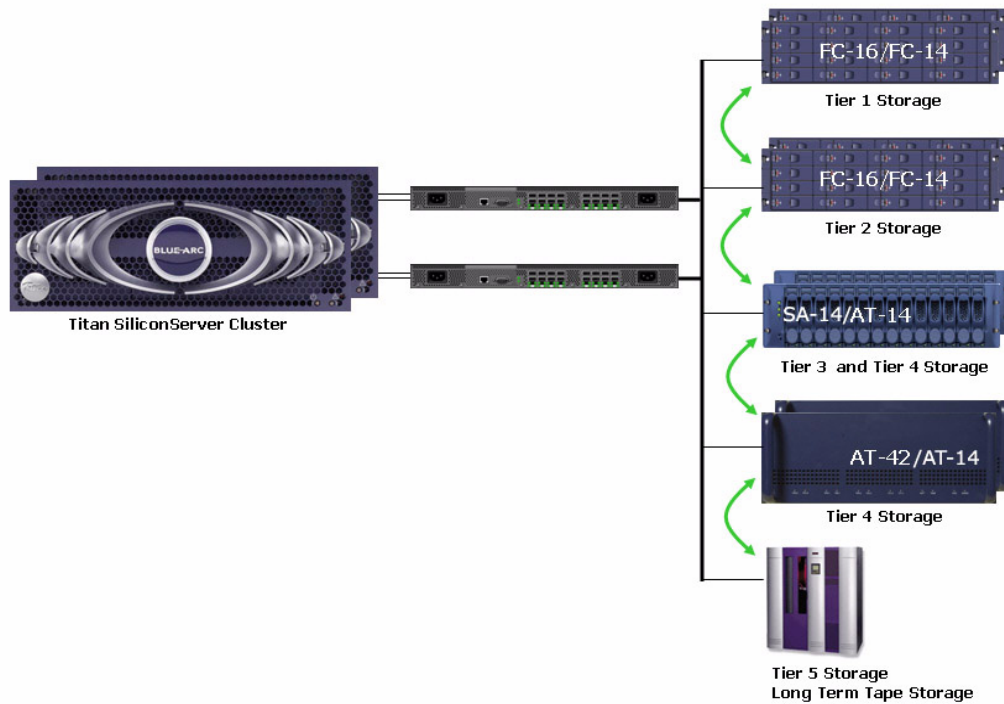
Multi-Tiered Storage Overview and Concepts

Configuring the Multi-Tiered Storage (MTS) of the Titan SiliconServer is explained in this chapter. The storage subsystem consists of storage devices and the Fibre Channel (FC) infrastructure (such as FC switches and cables) used to connect these devices to Titan. Each Titan provides four (4) Fibre Channel (FC) ports, independently configurable for either 1, 2 or 4 Gigabit operation.

Multi-Tiered Storage

MTS allows you to install various types of storage technologies behind a Titan. Through MTS, the storage that best meets the requirements for applications can be selected. BlueArc supports four tiers of networked storage, including NDMP Tape Library Systems (TLS) that can be Ethernet or FC attached. All the storage that resides behind Titan is managed as a single system

through an integrated network management interface.



RAID Storage Subsystems

Titan supports the following RAID storage subsystems:

- FC-14 storage enclosures used for Tier 1 and Tier 2 storage
- FC-16 storage enclosures used for Tier 1 and Tier 2 storage
- SA-14 storage enclosures used for Tier 3 storage
- AT-14 storage enclosures used for Tier 3 and Tier 4 storage
- AT-42 storage enclosures used for Tier 4 storage

The five subsystems listed above have different capacity and performance characteristics. If one or more of the storage subsystems are configured, the server combines the storage resources into one or more File Systems.

Storage Tier	Supported Enclosures	Storage Technology	Disk RPM	RAID Technology	Performance Characteristics
Tier 1	FC-14, FC-16	Dual ported FC disks	15,000	RAID 1/5; RAID 1/5/10	Very high performance
Tier 2	FC-14, FC-16	Dual ported FC disks	10,000	RAID 1/5; RAID 1/5/10	High performance
Tier 3	SA-14, AT-14	SATA disks PATA disk	7,200	RAID 5	Nearline performance
Tier 4	AT-14, AT-42	PATA disks	5,400	RAID 5	Archival
Tier 5	N/A	Tape	NA	N/A	Long term storage

Fibre Channel Fabric and Arbitrated Loop

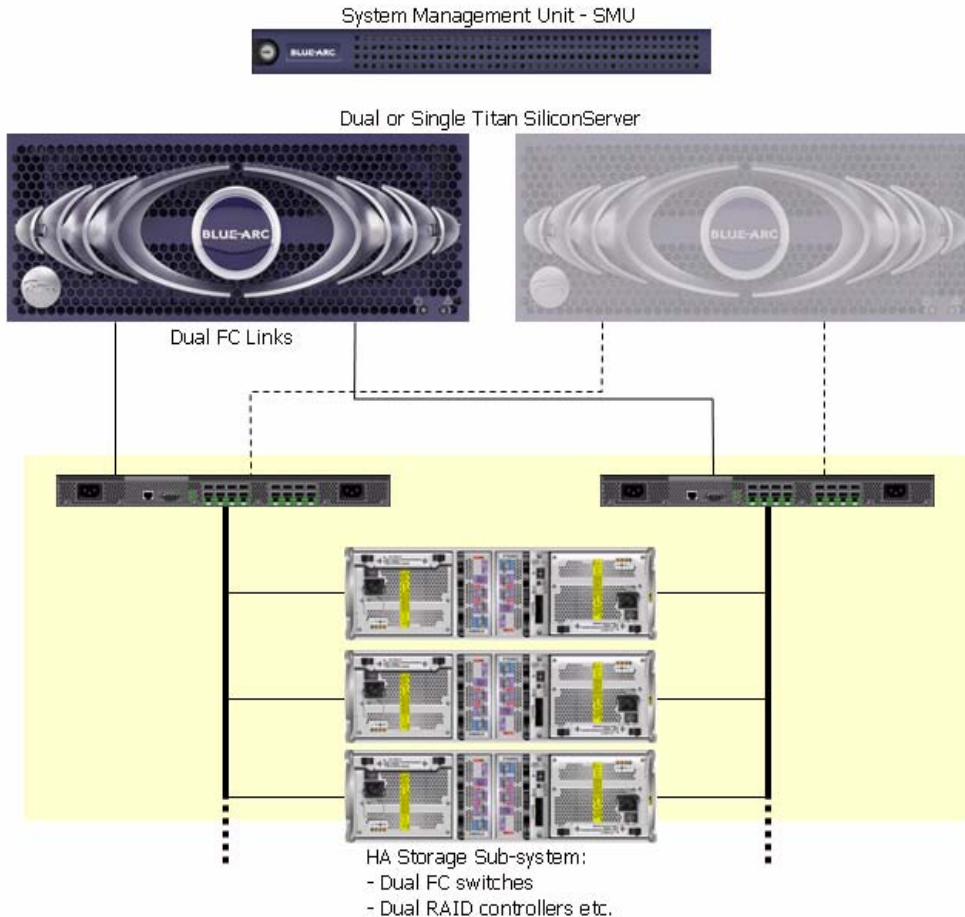
Titan supports both fabric and private loop Fibre Channel (FC) attachments. Fabric is supported on all Brocade switches and private loop is supported on the Vixel 9x00 series switches.

When connecting to a Brocade FC switch	The server must be configured for N_Port operation.
When connecting to a Vixel 9x00 FC switch	The server must be configured to NL_Port operation.

FC links are configured from the [Command Line Interface](#) (CLI), using the `fc-link`, `fc-link-type` and `fc-link-speed` commands. For more information about each command, run `man <command>` at the CLI.

Load Balancing and Failure Recovery

The following diagram illustrates a simplified storage configuration, showing how each storage subsystem can be used through one of two FC paths.



The server automatically routes FC traffic to individual System Drives over either of the two FC paths, thus distributing the load across the two FC switches and, when possible, across dual active/active RAID controllers. Load balancing can also be configured by identifying a “preferred FC path” for each System Drive. Should a failure occur in one of the two FC paths from the server to the RAID storage subsystem, the server can recover automatically by moving all of the disk I/O activity to the other FC link. Should the FC link become active again, the server will automatically redistribute the load.

Load balancing is configured from the [Command Line Interface \(CLI\)](#), using the `sdp` command. For more information, run `man sdp`. This command can also be used to determine what FC path is used to communicate to each System Drive.

Fibre Channel Statistics

Statistics are available to monitor the FC activity since Titan was last started or the statistics were reset. Both per-port and overall statistics are available. The statistics are updated every ten seconds. In addition, a Fibre Channel histogram which shows the number of bytes/second received and transmitted over the last few minutes is also available.

FC-14 and SA-14 Storage Subsystems

The FC-14 storage subsystem supports **Tier 1** (15,000 RPM) and **Tier 2** (10,000 RPM) FC disks. Each storage enclosure can house up to 14 FC disks.

The SA-14 storage subsystem supports **Tier 3** (7,200 RPM) SATA disks. Each storage enclosure can house up to 14 SATA disks.

The FC-14 and SA-14 storage subsystems consist of the following elements:

- **Storage Controller Enclosure (SCE)**. The SCE consists of the FC-14C or SA-14C storage enclosures and dual RAID controllers. Each RAID controller has dual RAID host ports, and a single cascade port. The cascade port is used to connect to the Environmental Services Monitoring (ESM) modules in the storage expansion enclosure (SEE). A single SCE can support a maximum of seven FC-14Es or SA-14Es.
- **Storage Expansion Enclosure (SEE)**. The SEE consists of the FC-14E or SA-14E storage enclosures fitted with dual ESM modules. Each ESM module has two interfaces on it that are used to *Loop in* and *Loop Out* of the SEE. Wiring is diversely routed so that the SCE routes down one path to the first SEE and down the other path to the last SEE.



Note: Different tiers of storage and drive capacities cannot be mixed behind a RAID controller.

Storage Characteristics

Both the FC-14 and SA-14 storage enclosures use hardware RAID controllers, but the FC-14 uses Fibre Channel (FC) disk technology while the SA-14 uses SATA disks. The RAID controllers provide complete RAID functionality and enhanced disk failure management. The number of controllers in the system depends on its storage capacity.

The FC-14 and SA-14 RAID controllers are integrated as a pair of controllers into a FC-14C or SA-14C storage enclosure, and each RAID storage controller enclosure supports a maximum of seven FC-14E or SA-14E expansion enclosures respectively (a maximum of 112 disks). One or more FC-14E or SA-14E storage enclosures connected to a storage controller enclosure is referred to as a RAID rack.

Active/Active RAID Controllers

The RAID controllers operate as an Active/Active (A/A) pair within the same rack. Both RAID controllers can actively process disk I/O requests. Should one of the two RAID controllers fail, Titan re-routes the I/O transparently to the other controller, which starts processing disk I/O requests for both controllers.

System Drives

System Drives are the basic storage element used by the Titan SiliconServer. A System Drive comprises a number of *physical disks*. The size of the System Drive depends on multiple factors such as the RAID level, the number of disks, and their capacity. RAID 5 is the only supported RAID level for the FC-14 and SA-14. Titan assigns each System Drive a unique identifying number (ID).

Hot Spare Disk

A hot-spare disk is a physical disk that is configured for automatic use in the event that another physical disk fails. Should this happen, the system automatically switches to the hot-spare disk and rebuilds on it the data that was located in the failed disk. The hot-spare disk must have at least as much capacity as the other disks in the System Drive. The hot-spare disk is a global hot-spare, meaning that only one hot-spare disk is required per RAID rack.

When the failed disk is replaced, the RAID controller's CopyBack process will automatically move the reconstructed data from the disk that was the hot spare to the replacement disk. The hot spare disk will then be made available for future use.

If it is necessary to remove and replace disks, it is possible to perform hot swap operations. In other words, an offline or failed disk can be removed and a new disk inserted while the power is still on and the system is still operating. Sixty seconds should be allowed between disk removal and replacement to allow the management system to recognize the change.

Discovering and Adding Racks

FC-14 and SA-14 RAID racks must be discovered and added to a Managed SiliconServer before system drives can be created. Discovered racks may be added to the list of RAID Racks for the currently selected Managed Server.

To add a RAID Rack

1. From the **Home** page, click **Storage Management**. Then, click **RAID Racks**.

BLUEARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > RAID Racks

RAID Racks

Name	Controller 0 (A) Status	Controller 1 (B) Status	Firmware	Rack Status	
☐ 2822	Online	Online	05.42.10.00 / 05.42.10.00	OK	details
☐ 2882	Online	Online	06.10.05.90 / 06.10.05.90	OK	details
☐ Rack 0	Online	Online	8.50.00 / 8.50.00	OK	details

[Check All](#) | [Clear All](#)

Actions: [delete](#) [Discover Racks](#) | [View Physical Disks](#) [View Active Tasks](#)

Shortcuts: [System Drives](#)

2. Click **Discover Racks**. This may take some time to complete.

BLUEARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > [RAID Racks](#) > Discover Racks

Discover Racks

Choose racks to monitor

Rack Name	IP Address(es)	Rack Password
☒ 2882	192.168.38.33 / 192.168.38.34	
☒ 2822	192.168.38.35 / 192.168.38.36	

[OK](#) [cancel](#)

3. A list of the discovered RAID Racks will be displayed.
 - If no racks appear, the SMU was unable to find any FC-14 or SA-14 RAID Racks on its network. Verify that the RAID racks have their network settings properly configured.
 - RAID Racks that have already been added to the Currently Managed Server will not be present in the list of discovered RAID Racks.
4. Check the boxes of the RAID Racks to be added to the currently managed server's list of monitored RAID Racks.
5. If the discovered Racks have configured passwords, enter those passwords in the **Rack Password** field.
6. Click **OK** to add the RAID Racks.

The selected RAID Racks should appear on the RAID Racks' list page.



Note: If the SMU is managing multiple servers and if the RAID rack can be accessed by more than one server, then it should be added to all the Titans that can access it.

Once a Rack is added, a number of events will occur:

- The Rack will appear on the System Monitor (for the *currently* selected Managed Server).
- The SMU will begin logging Rack events, which can be viewed through the Event Log link on the **RAID Rack Details** page.
- The RAID Racks' **Severe Events** will be forwarded to the Managed Server to be included in its event log. The RAID Racks' Critical Events will be forwarded to each Managed Server that has discovered the Rack. These events will be included in each server's event log. This will trigger the server's Alert mechanism, possibly resulting in emails, traps, etc.
- The RAID Racks' time will be synchronized with the SMU's time daily.
- If System Drives are present on the RAID Rack, then the Racks' "cache block size" will be set to 16 KB.

Partially Discovered RAID racks

When discovering RAID racks, it is possible that only one of the controllers' IP addresses may be discovered (e.g. if only one controller is online). In this instance, the RAID Rack is considered only "partially discovered". The RAID Rack can still be added; however, it will appear on the RAID Rack list page with an amber status.

When both controllers are back online, the RAID Rack should be removed and rediscovered. Rediscovery will allow each of the controllers' IP addresses to be **fully** discovered. Having both IP addresses allows the SMU to maintain contact with the RAID Rack even if one of the controllers fails.



Note: Deleting a RAID Rack only removes it as a device managed by the SMU. It will not affect any configured System Drives or File Systems.

Creating System Drives

The storage system has been pre-configured by BlueArc. However, additional System Drives can be configured. A System Drive comprises a number of *physical disks* and has a unique identifying number (ID).



Caution: Before creating System Drives, set aside at least one disk to be used as a hot spare.

To Create a System Drive

1. From the **Home** page, select **Storage Management**. Then, click **System Drives**.

BLUE ARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Storage Management | [Home](#) > [Storage Management](#) > System Drives

System Drives

Licensing
Current capacity used: 3.07 TB
Limit: 256.00 TB

Filter
Filter By Access:
☐ Hide System Drives which are Secondary in a mirror [filter](#)

ID	Capacity	Manufacturer	Label	Comment / Rack Name	Storage Pool	Allow Access	Status	Mirror Status	Mirrored to	
☐ 0	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐ 1	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐ 2	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐ 3	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐ 4	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐ 5	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐ 6	393.39 GB	MYLEX		Rack 0		Allowed	OK			details
☐ 7	393.39 GB	MYLEX		Rack 0		Allowed	OK			details

[Check All](#) | [Clear All](#)

Actions: [allow access](#) [deny access](#) [forget](#) | [create](#) [Discover System Drives](#)

Shortcuts: [RAID Racks](#) [Storage Pools](#) [Active Tasks](#)

- 2. Click **create**.
- 3. On the **Select RAID Rack** page, select a rack on which the System Drive will be created. Then, click **next**.
- 4. On the **RAID Level** page, select the type of RAID array to create. RAID 1 and RAID 5 are the available options.

RAID Level	System Drive size	Notes
1	2 to 32 disks, up to 2 TB	Mirroring and duplexing. Data written to one disk is duplicated to a second for maximum data protection, but with 50% usable capacity. If a physical disk fails and a hot spare disk is available, the controller automatically inserts the spare and builds onto it the contents of the failed disk
5	up to 2 TB	Independent data disks with distributed parity blocks. Employs a combination of striping and parity checking. The use of parity checking provides redundancy without the overhead of having to double the disk capacity. If a physical disk fails and a hot spare disk is available, the controller automatically inserts the spare and builds onto it the contents of the failed disk from data and parity information on the remaining disks. For many applications, RAID 5 offers the best compromise between capacity, reliability, and speed.

5. Click **next**.

BLUE-ARC

TITAN - 192.0.2.2 | Advanced Mode: OFF

Storage Management | Home > Storage Management > System Drives > Select RAID Rack > Create a System Drive - rack 2822

Create a System Drive - rack 2822

Create System Drive from an existing Disk Array. | Create System Drive in a new Disk Array.

Capacity	Number of Physical Disks
<i>There is no unallocated space in existing Disk Arrays.</i>	
☐ 466.515 GB	3
☐ 699.773 GB	4
☐ 933.031 GB	5
☐ 1166.289 GB	6
☐ 1399.546 GB	7
☐ 1632.804 GB	8
☐ 1866.062 GB	9
☒ 2036.000 GB	10

System Drive Label:

System Drive Capacity: GB

Do not alter this value without guidance from BlueArc. If the capacity is less than the available capacity of the selected disk array, then a region of unallocated free space will remain in the disk array.

Unallocated Space: GB

6. On the **Create a System Drive** page, select the System Drive's size by clicking the appropriate button in the **Capacity** column. The System Drive's size relies on the number of physical disks specified in the **Number of Physical Disks** column.



Caution: To ensure optimal performance of the Storage Subsystem, do not change the value specified next to **System Drive Capacity** except under the direction of BlueArc Global Services.

7. Enter a name for the new System Drive in the **System Drive Label** field.
8. Click **create**.

A RAID 5 system drive will now have been created, with background initialization in progress, a stripe size of 32 K and **Media Scan** enabled.

The RAID controller performs an initialization of the System Drive to check for bad sectors and set up the RAID parity. The lights on the disks flicker during the process and the Active Tasks dialog box shows the progress of the initialization.

After the background initialization (BGI) has started, the new System Drive can be used. The new System Drive will be initialized non-destructively after other initializations and rebuilds are complete. While the BGI is in progress, the newly created System Drives are protected against a single disk failure.

To Verify the System Drive

From the **Home** page, click **Storage Management** page. Then, click **System Drives**.

On the **System Drives** page, the newly added System Drive should appear. Under the Status Column, the status of the System Drive displays if it is formatting or initializing.

Once the System Drive has been initialized, a file system can be created. For more information on how to set up a file system, see "[To Create a Silicon File System](#)".

Managing FC-14 and SA-14 Storage

FC-14 and SA-14 RAID racks can be managed using Web Manager. Common operations are:

- Changing the name, password, media scan period, or cache block size settings.
- Checking the status of media scan and other operations.
- Reviewing events logged by the RAID rack.
- Determining the status of physical disks.

To view a list of installed RAID racks

Click on the **Storage Management** page, then click **RAID Racks**.

BLUE ARC TITAN - 192.0.2.2 Advanced Mode: ON

Storage Management | [Home](#) > [Storage Management](#) > RAID Racks

RAID Racks

Name	Controller 0 (A) Status	Controller 1 (B) Status	Firmware	Rack Status	
☐ Rack 0	Online	Online	05.40.04.00 / 05.40.04.00	OK	details
☐ Rack 1	Online	Online	8.60.00 / 8.60.00	OK	details
☐ Rack 2	Online	Online	8.60.00 / 8.60.00	OK	details

[Check All](#) | [Clear All](#)

Actions: [delete](#) [Discover Racks](#) | [View Physical Disks](#) [View Active Tasks](#)

Shortcuts: [System Drives](#)

Item /Field	Description
Name	The name of the RAID Rack.
Controller A/B Status	Status of each controller in the RAID rack: Online or Offline .
Firmware	Firmware level in the RAID controllers.
Rack Status	Global status for all enclosures and RAID controllers in the RAID rack.

The **delete** button removes the RAID rack from the list. Deleting the rack just removes the rack as a managed rack, it does not affect the system drives configured on the storage enclosures in the rack.

The **Discover Racks** link allows Titan to check for additional RAID racks. Titan searches for FC-14 and SA-14 storage devices connected to both the public and private management networks. Once a RAID rack has been found, then it can be managed.

The **System Drives** link brings up the **System Drives** page in which a System Drive can be managed.

The **View Physical Disks** link shows the status of the physical disks associated with a RAID rack.

The **View Active Tasks** link shows the status of operations, such as media scans, which are in progress for a RAID rack.

The **details** button brings up a **RAID Rack Details** page. This page provides information on the RAID rack.

BLUE-ARC

?

 Help

i

 About

✕

 Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > [RAID Racks](#) > RAID Rack Details

RAID Rack Details

Identification

Name:

2822

Rack WWN:

60:0a:0b:80:00:12:df:a4:00:00:00:41:fe:89:b7

Configuration

Media Scan Period:

14

days

Cache Block Size:

4 KB

16 KB

Controllers

Controller A (192.168.38.35):

Status

Online

Mode

Active

Firmware

05.42.10.00

Controller B (192.168.38.36):

Status

Online

Mode

Active

Firmware

05.42.10.00

Batteries

Battery 0

Status:

OK

Location:

Controller Slot A

Age:

264 Day(s)

Life Remaining:

455 Day(s)

Battery 1

Status:

OK

Location:

Controller Slot B

Age:

264 Day(s)

Life Remaining:

455 Day(s)

Power Supplies

PSU 0:

OK

PSU 1:

OK

PSU 2:

OK

PSU 3:

OK

Temperature Sensors

Temperature Sensor 0:

OK

Temperature Sensor 1:

OK

Temperature Sensor 2:

OK

Fans

Fan 0:

OK

Fan 1:

OK

Fan 2:

OK

Fan 3:

OK

Physical Disks

Overall Physical Disk Status:

OK

Actions:

apply

Change Password

Shortcuts:

[Physical Disks](#)

[Active Tasks](#)

[Event Log](#)

[System Drives](#)

Item/Field	Description
Identification	• Name of the RAID Rack. Enter a new RAID Rack name which is used to identify the RAID Rack. • WWN: Worldwide name for the RAID Rack. • Media Scan Period: The number of days over which a complete scan of the system drives will occur. • Cache Block Size: 4 KB or 16 KB. By default, the cache block size is 16 KB. Setting the cache block size to 4 KB may result in reduced performance with file systems configured with 32 KB block size. Click the OK button to apply any changes to the RAID Rack Identification.
Controllers	The information for each RAID Controller: • Status: The Status of the RAID Controller. • Mode: The mode will report the RAID controller as running in either Active or Passive mode. By default, both controllers will be Active. • Firmware: The firmware version installed on the RAID Controllers.
Batteries	The information for each battery within the RAID Rack: • Status: The status of the batteries. Green - OK, Amber - Warning, Red - Severe. • Location: The location of the batteries within the RAID Rack. • Age: The number of days which the batteries have been in the RAID Rack. • Life Remaining: The number of days until the batteries should be replaced.
Power Supplies	The status of the Power Supply Units (PSU) within the RAID Rack.
Temperature Sensors	The temperature (Temperature Sensor) within the RAID Rack.
Fans	The Status of the Fans within the RAID Rack.
Physical Disks	The summary of the Physical Disks within the RAID Rack.

Performing a Media Scan on a System Drive

Media Scan is intended to provide an early indication of an impending System Drive failure and to reduce the possibility of encountering a media error during host operations. A typical file system is a mixture of frequently used files, rarely used files, and free space. If a disk develops bad spots in sectors that are not often accessed, this failure could remain undetected. To prevent a disk failure during a rebuild, which could lead to data loss, it is necessary to detect

unreliable disks promptly, thus preventing the RAID controller from failing them at a critical time.

Media Scan can detect drive media errors before they are found during a normal read or write to the System Drive. The Media Scan operation is performed as a background task and scans all data and parity information on the configured system drives. It will run on all System Drives that are *optimal* (meaning are operating without known failures) and have no modification operations in progress. Errors detected during a media scan will be reported to the Event Log.

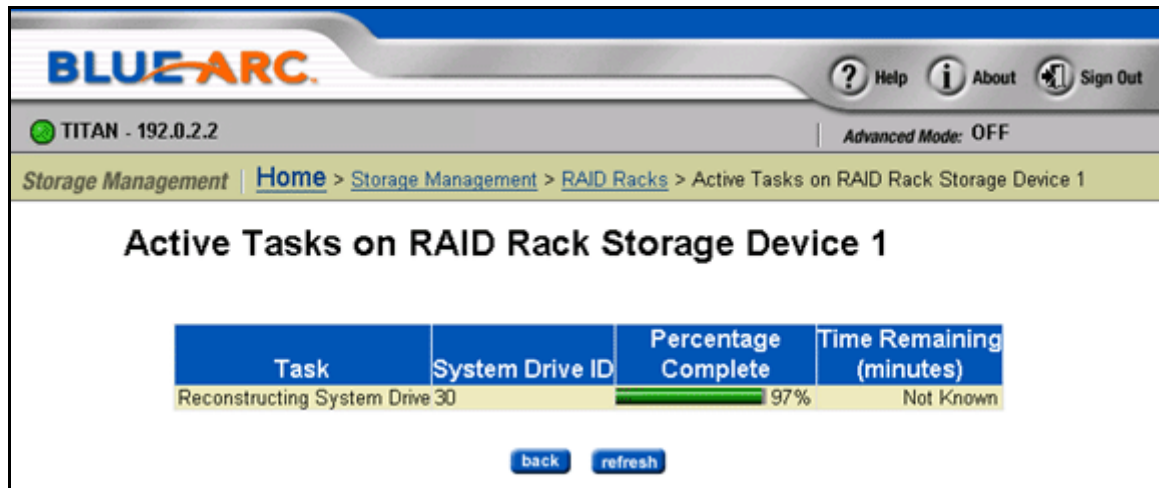
Media scan runs at a lower priority on the RAID controller than normal storage access. However, performance can be maximized by increasing the time allowed for the media scan to complete. To increase the duration of the media scan and, as a result reduce the cycles used by the RAID controller, the **Media Scan Period** can be increased to up to 30 days on the **RAID Rack Details** page.

Checking the Status of Active Tasks

You can view the status of on-going activity (Media Scan, CopyBack, initializing, etc.) within the RAID Rack on the **Active Tasks** page.

1. From the **Home** page, click **Storage Management**. Then, click **RAID Racks**.
2. Check the check box next to the RAID Rack on which to view the Active Tasks.

3. Click **View Active Tasks**.



Item/Field	Description
Task	The Active Tasks (on-going activity) on the RAID Rack.
Component	The System Drive on which the Active Task is occurring.
Percentage Complete	The percentage of completion (%) for the Active Task. Not all Active Tasks will have a percentage complete shown.
Time Remaining (minutes)	The time remaining (minutes) for the Active Task to be completed.  Note: Some tasks will report a Percentage Complete but not a Time Remaining. In this case, Time Remaining will be shown as Not Known.

The **back** button will bring up the **RAID Racks** list page.

The **refresh** button will update the status of the Active Tasks. All on-going activity on the RAID Rack are displayed on this page. This page will automatically refresh every 60 seconds.

Reviewing Events Logged

The SMU monitors events, such as failure conditions, logged by the RAID rack. The SMU is connected to the FC-14 or SA-14 through an “out-of-band” Ethernet link (the [private management network](#) is typically used for this purpose). Severe events are immediately forwarded to the Titan SiliconServer’s [event log](#). This will trigger alert notifications (e.g. email or SNMP traps) if Titan is configured to do so. In addition, if the SMU is unable to connect to the RAID racks, a severe alert will be triggered on Titan.

To review events logged by the RAID Rack

- 1. From the **Home** page, click **Storage Management**. Then, click **RAID Racks**.
- 2. Click the **details** button corresponding to the RAID Rack on which to view the details page.
- 3. Click **Event Log**.

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: ON

Storage Management

Home > Storage Management > RAID Racks > Rack Event Log

Rack Event Log

Details

Filter

Rack Name: Rack 0

Severity: All

filter

Current Controller A Time: Sep 15, 2004 7:23:51 AM

Current Controller B Time: Sep 15, 2004 7:23:48 AM

Events 1-20 of 1000 : Page: 1 2 3 4 5 >> >

Severity	Date/Time	Message	ID / Location
Info	Sep 15, 2004 7:11:18 AM	Controller return status/function call for requested operation	5023 / UNKNOWN
Info	Sep 15, 2004 7:11:18 AM	Change name of storage array	5016 / UNKNOWN
Info	Sep 15, 2004 6:45:58 AM	Controller return status/function call for requested operation	5023 / UNKNOWN
Info	Sep 15, 2004 6:45:58 AM	Change name of storage array	5016 / UNKNOWN
Info	Sep 13, 2004 4:42:23 PM	Controller return status/function call for requested operation	5023 / UNKNOWN
Info	Sep 13, 2004 4:42:22 PM	Assign volume ownership	502A / Volume label: LSI-vold
Info	Sep 13, 2004 4:41:10 PM	Drive tray path redundancy restored	282C / ESM tray: 1
Info	Sep 13, 2004 4:41:10 PM	Drive tray path redundancy restored	282C / ESM tray: 2
Info	Sep 13, 2004 4:41:08 PM	Drive tray path redundancy restored	282C / ESM tray: 1
Info	Sep 13, 2004 4:41:08 PM	Drive tray path redundancy restored	282C / ESM tray: 2
Info	Sep 13, 2004 4:40:54 PM	Fibre channel link up	1018 / Drive Channel index: 1 slot: 1
Info	Sep 13, 2004 4:40:53 PM	Fibre channel link down	1017 / Drive Channel index: 1 slot: 1
Info	Sep 13, 2004 4:40:52 PM	Fibre channel link up	1018 / Drive Channel index: 1 slot: 2
Info	Sep 13, 2004 4:40:51 PM	Fibre channel link down	1017 / Drive Channel index: 1 slot: 2
Info	Sep 13, 2004 4:37:56 PM	Fibre channel link down	1017 / Drive Channel index: 1 slot: 1
Info	Sep 13, 2004 4:37:56 PM	Fibre channel link up	1018 / Drive Channel index: 2 slot: 1
Info	Sep 13, 2004 4:37:55 PM	Fibre channel link up	1018 / Drive Channel index: 1 slot: 1
Info	Sep 13, 2004 4:37:55 PM	Fibre channel link down	1017 / Drive Channel index: 2 slot: 1
Info	Sep 13, 2004 4:37:54 PM	Fibre channel link down	1017 / Drive Channel index: 1 slot: 2
Info	Sep 13, 2004 4:37:53 PM	Fibre channel link up	1018 / Drive Channel index: 2 slot: 2

Events 1-20 of 1000 : Page: 1 2 3 4 5 >> >

Actions:

refresh

download

clear all

The Event Log is updated every three minutes or when a **severe** event occurs on the RAID Rack.

The **Event Log** page will display a maximum of 1000 events (**info** or **severe**). Up to 3000 events are archived on the SMU and will be available for download by using the **download** button.

This table can also be filtered to view the event log based on the **severity** level: **All**, **Info**, or **Severe**.

Item /Field	Description
Severity	The level of severity is displayed by: Green - Info, Red - Severe
Date/Time	The date and time at which the event was logged.
Message	The details about the event.
ID/Location	The ID and the location within the FC-14 RAID Rack that the event type has occurred.

The **Details** section provides the Rack Name and the **Current (RAID) Controllers Date and Time**.

The **refresh** button will refresh the **Event Log** page. The **Event Log** page will automatically refresh every 60 seconds.

Clicking **download** will allow the archived events to be downloaded in a comma separated values (.csv) provided in a ZIP file. Even though the SMU displays only the most recent 1,000 events, many more are archived on the SMU's hard drive. Approximately 2 MB (about 4,000) of the most recent events are archived.

The **clear all** button will clear all the events in the RAID Rack.



Caution: Using the clear log button will permanently delete all the events from the SMU and the RAID Rack itself.

Monitoring Physical Disks

The status of the physical disks associated within a FC-14 or SA-14 RAID Rack can be determined by using Web Manager. Also, the status of the physical disks can be changed if a physical disk needs to be removed or a new hot spare disk has been added.

Checking and Changing the Status of Physical Disks

1. From the **Home** page, click **Storage Management**. Then, click **RAID Racks**.
2. Check the check box next to the RAID Rack on which to view the Physical Disks.

3. Click **View Physical Disks**.
- The status of the physical disks are displayed.

?

 Help

i

 About Sign Out

TITAN-ST - 192.0.2.2

Advanced Mode: ON

Storage Management

 | [Home](#) > [Storage Management](#) > [RAID Racks](#) > Physical Disks on RAID Rack Engenio-1

Physical Disks on RAID Rack Engenio-1

Enclosure	Slot	Capacity	Type	Span	Status	Hot Spare	Available	Off Line	Manufacturer	Firmware
	1	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	2	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	3	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	4	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	5	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	6	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	7	136.73 GB	FIBRE	engenioFC		☒	☐	☐	SEAGATE	MS11
	8	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	9	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	10	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	11	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	12	136.73 GB	FIBRE	engenioFC		☐	☐	☐	HITACHI	MS04
	13	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	14	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	1	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	2	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	3	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	4	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	5	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	6	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	7	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	8	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	9	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	10	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	11	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	12	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	13	136.73 GB	FIBRE	engenioFC		☐	☐	☐	SEAGATE	MS11
	14	136.73 GB	FIBRE	engenioFC		☒	☐	☐	SEAGATE	MS11

Actions: [Assign as Hot Spare\(s\)](#) [Unassign as Hot Spare\(s\)](#)

Item /Field	Description
Manufacturer	The name of the disk manufacturer.
Slot	The slot number in the storage enclosure in which the physical disk resides.

Capacity	The storage capacity of the disk.
Type	The type of physical disk in the enclosure, typically either Fibre (Channel) or SATA.
Span	The label of the Storage Pool, if the physical disk is in use within a Storage Pool.
Status	The current status of the physical disks within the RAID Rack.
Hot Spare	The box will be checked if it is assigned as a hot spare.
Available	The box will be checked if the physical disk is available.
Offline	The box will be checked if the physical disk is offline.
Manufacturer	The name of the disk manufacturer.
Firmware	The firmware version on the physical disk.

Within the Physical Disk page, hot-spares can be assigned or unassigned from physical disks which are checked as **available**.



Note: BlueArc requires that at least one disk be marked as a hot spare by the time the first System Drive is created.

FC-16 Storage Subsystem

The FC-16 storage subsystem supports **Tier 1** (15,000 RPM) and **Tier 2** (10,000 RPM) FC disks, where each storage enclosure can house up to 16 FC disks. The FC-16 storage enclosure can be configured to support one of the following configurations:

Storage Controller Enclosure (SCE).

The SCE consists of the FC-16 storage enclosure and, typically, two RAID controllers. Each RAID controller has dual RAID host ports, and a single cascade port. The cascade port is used to connect to the LRC's in the storage expansion enclosure. A single SCE can support up to three Storage Expansion Enclosures.

Storage Expansion Enclosure (SEE).

The SEE consists of the FC-16 storage enclosure and two LRC modules. Each LRC module has four interfaces on it that are used to *Loop In* and *Loop Out* of the SEE. The 1st SEE connects directly to the SCE; the rest connect indirectly, through another SEE.



Note: Different tiers of storage and drive capacities should not be mixed behind a RAID controller.

Storage Characteristics

The FC-16 storage enclosures use Fibre Channel disk technology and hardware RAID controllers, which provide complete RAID functionality and enhanced drive failure management. The number of controllers in the system depends on its storage capacity and the resilience level that it supports. A RAID controller (or controller pair) inserted in a storage enclosure supports up to three expansion enclosures, for a total of up to 64 disks. One or more FC-16 storage enclosures sharing a single RAID controller (or controller pair) are referred to as a RAID rack.

Active/Active RAID Controllers

The RAID controllers operate as an Active/Active pair within the same rack. Both RAID controllers can actively process disk I/O requests. Should one of the two RAID controllers fail, Titan re-routes the I/O transparently to the other controller, which starts processing disk I/O requests for both controllers.

System Drives

System Drives are the basic storage element used by the Titan SiliconServer. A System Drive comprises a number of *physical disks*. The size of the System Drive depends on multiple factors, such as the RAID level, the number of disks, and their capacity. The RAID controller supports RAID levels 1, 5, and 10 (a combination of striping and mirroring).

The Titan SiliconServer assigns each System Drive a unique identifying number (ID).

Hot Spare Disk

A hot-spare disk is a physical disk that is configured for automatic use in the event that another physical disk fails. Should this happen, the system automatically switches to the hot-spare disk and rebuilds on it the data that was located in the failed disk. The hot-spare disk must have at least as much capacity as the other disks in the System Drive. The hot-spare disk is a global hot-spare, meaning that only one hot-spare disk is required per RAID rack.

If it is necessary to remove and replace disks, it is possible to perform hot swap operations. In other words, an offline or failed disk can be removed and a new disk inserted while the power is still on and the system is still operating. Sixty seconds should be allowed between disk removal and replacement to allow the management system to recognize the change.

Creating System Drives

The Storage System has been pre-configured by BlueArc. However, additional System Drives can be created and configured. A System Drive comprises a number of *physical disks* and has a unique identifying number (ID).

Before creating a system drive, the storage system must be configured to initialize new System Drives in the foreground or the background.

To configure foreground/background initialization options

1. From the **Home** page, click **Storage Management**. Then, click **RAID Racks**.
2. Click **details** at the end of the row of the RAID Rack to which to view the initialization configuration.

BLUE ARC

TITAN - 192.0.2.2 Advanced Mode: ON

Storage Management | Home > Storage Management > RAID Racks > RAID Rack Configuration

RAID Configuration

ID	Name	RAID Racks		Firmware	Monitor
		Controller 0	Controller 1		
0	20000050CC00688A	Online	Not Present	8.50	Yes

Show

RAID cache size

Rack Name

Background Initialization ☒

By default, the box is checked for **background initialization (BGI)**.

BGI sets up RAID parity non-destructively so the new System Drive used as soon as it has been created. When using BGI, it is not necessary to wait for initialization to complete.

To use foreground initialization instead, remove the checkmark from the **Background Initialization** check box and click **Set Background Initialization**.

To create a System Drive

- 1. On the **Storage Management** page, click **System Drives**.

BLUE ARC

?

Help

i

AboutSign Out

Titan - 192.0.2.2

Advanced Mode: ON

Storage Management

|

[Home](#)

>

[Storage Management](#)

>

System Drives

System Drives

Licensing

Current capacity used: 3.07 TB

Limit: 256.00 TB

Filter

Filter By Access:

Show All

☐ Hide System Drives which are Secondary in a mirror

filter

	ID	Capacity	Manufacturer	Label	Comment / Rack Name	Storage Pool	Allow Access	Status	Mirror Status	Mirrored to	
☐	0	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐	1	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐	2	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐	3	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐	4	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐	5	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐	6	393.39 GB	MYLEX		Rack 0		Allowed	OK			details
☐	7	393.39 GB	MYLEX		Rack 0		Allowed	OK			details

Check All

|

Clear All

Actions:

allow access

deny access

forget

create

Discover System Drives

Shortcuts:

[RAID Racks](#)

[Storage Pools](#)

[Active Tasks](#)

2. Click **create**.
3. On the **Select RAID Rack** page, select the RAID rack on which the System Drive will be created. Then, click **next**.

The screenshot shows the BlueArc TITAN web interface. The top navigation bar includes the BlueArc logo, a status indicator for 'TITAN - 192.0.2.2', and links for Help, About, and Sign Out. Below the navigation bar, the breadcrumb trail reads 'Storage Management > Home > Storage Management > Create System Drive'. The main content area is titled 'Create system drive on RAID rack 0'. It features a 'Raid level' dropdown menu set to 'Raid 1', and radio buttons for 'Optimize for' with 'Speed' selected and 'Size' unselected. Below this, a table titled 'Available configurations' displays the following data:

Disks	Hot spares	Capacity	Efficiency
2	0	134276 MB	50%

At the bottom of the configuration area is a large 'Create System Drive' button.

4. Select the **RAID level** from the drop-down list.
5. Select **Speed** or **Size** for Optimization.

RAID Level	System Drive size	Notes
1	2 to 32 disks, up to 2 TB	Mirroring and duplexing. Data written to one disk is duplicated to a second for maximum data protection, but with 50% usable capacity. If a physical disk fails and a hot spare disk is available, the controller automatically inserts the spare and builds onto it the contents of the failed disk

5	up to 2 TB	Independent data disks with distributed parity blocks. Employs a combination of striping and parity checking. The use of parity checking provides redundancy without the overhead of having to double the disk capacity. If a physical disk fails and a hot spare disk is available, the controller automatically inserts the spare and builds onto it the contents of the failed disk from data and parity information on the remaining disks. For many applications, RAID 5 offers the best compromise between capacity, reliability, and speed.
10	up to 2 TB	Mirrored Stripes. Combines RAID levels 1 (mirroring) and 0 (striping): disks are mirrored for redundancy, and data is striped across multiple disks. However, only half the total capacity of the physical disks is used for the System Drive. If a physical disk fails and a hot spare disk is available, the RAID controller automatically inserts the spare and builds onto it the contents of the failed disk from the mirrored data.

- 6. Select the system drive configuration (e.g. the number of physical disk to use) from the drop-down list.
- 7. Click **Create System Drive**.

The controller performs a low-level disk initialization to check for bad sectors and set up the RAID parity. The lights on the disks flicker while this process occurs, and the Active Tasks dialog box shows the progress of the initialization.

If using background initialization (BGI), it is possible to use the new System Drive immediately. The new System Drive will be initialized non-destructively as soon as any other initializations, consistency checks, and rebuilds are complete. However, until BGI has finished, RAID parity will not be correct, and the data on the System Drive will be lost if a disk should fail. Performance will be lower than usual while BGI is in progress.

If the BGI is not enabled, the system will immediately start to initialize the new System Drive. It is possible to use other System Drives as normal, but the new System Drive cannot be used until initialization is complete.

To Verify the System Drive

From the **Home** page, click **Storage Management** page. Then, click **System Drives**.

On the **System Drives** page, the newly added System Drive should appear. Under the Status Column, the status of the System Drive displays if it is formatting or initializing.

Once the System Drive has been initialized, a file system can be created. For more information on how to set up a file system, see ["To Create a Silicon File System"](#).

Managing FC-16 Storage

You can manage FC-16 RAID racks using Web Manager. Common operations are:

- Performing consistency checks on System Drives.
- Checking the status of consistency checks and other operations.
- Determining the status of physical disks.

On the **Storage Management** page, click **RAID Racks**.

BLUEARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: ON

Storage Management | [Home](#) > [Storage Management](#) > RAID Racks

RAID Racks

Name	Controller 0 (A) Status	Controller 1 (B) Status	Firmware	Rack Status	
☐ Rack 0	Online	Online	05.40.04.00 / 05.40.04.00	OK	details
☐ Rack 1	Online	Online	8.60.00 / 8.60.00	OK	details
☐ Rack 2	Online	Online	8.60.00 / 8.60.00	OK	details

[Check All](#) | [Clear All](#)

Actions: [delete](#) [Discover Racks](#) | [View Physical Disks](#) [View Active Tasks](#)

Shortcuts: [System Drives](#)

Item / Field	Description
Name	RAID rack identifier.
Controller A/B Status	Status of each controller in the RAID rack.
Firmware	Firmware level in the RAID controllers.
Rack Status	The status for all enclosures and RAID controllers in the RAID rack.



Note: FC-16 storage enclosures will appear automatically in the list of RAID Racks. They do not need to be “discovered” and cannot be “forgotten” unless they are first physically removed from the server.

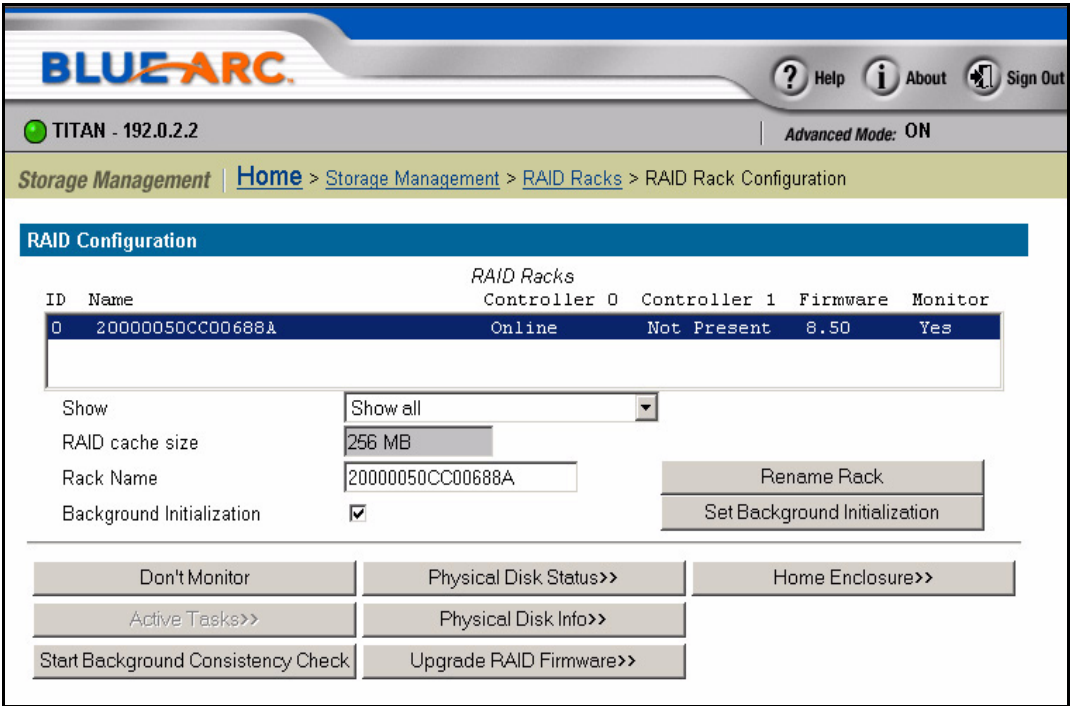
Multi-Tiered Storage

The **View Physical Disks** link shows the status of the physical disks associated with a RAID rack.

The **View Active Tasks** link shows the status of operations, such as system drive initialization, which are in progress for a RAID rack.

The **System Drives** shortcut brings up the **System Drives** page on which System Drives can be managed.

Clicking the **details** button will bring up a **RAID Rack Details** page. This page provides information about the selected RAID rack.



Item /Field	Description
RAID Racks	RAID Rack Details: • ID: The identifying number of the RAID Rack. • Name: The name of the RAID Rack. • Controller: The status of the RAID Controller – Online or Offline. • Firmware: The firmware number. • Monitor: Yes or No.
Show	The drop-down list allows the list to be displayed by: Show all (all of the RAID Racks are displayed), Show monitored RAID racks , and Show NOT monitored RAID racks .

RAID cache size	The size of the RAID cache.
Rack Name	The name of the RAID Rack.
Background Initialization	By default, the box will be checked for background initialization (BGI). For foreground initialization, remove the check-mark and click Set Background Initialization .

To rename the RAID Rack, enter a new **Rack Name** and click **Rename Rack**.

The **Set Background Initialization** button will set the initialization preference (BGI or FGI), depending on how the checkbox is marked.

RAID Monitoring allows a Titan to monitor a RAID Rack's health. If the storage subsystem is accessible by multiple Titan SiliconServers, it may not be desirable to allow each Titan to monitor every RAID Rack. Typically, Titan should only monitor RAID Racks that contain file systems owned by that Titan. To stop monitoring a RAID Rack, select it from the list and click **Don't Monitor**. To re-enable monitoring of the RAID Rack, use the CLI command `mylex-rack-ignore off`. For more information, refer to the *Command Line Reference Guide*.

The **Physical Disk Status>>** button will display a status page on the physical disk in the RAID Rack.

The **Home Enclosure>>** button will display a graphic of the RAID Rack Enclosure. This page will automatically refresh every 60 seconds. The status of the FAN, Temperatures, and the physical disks are shown.

The **Battery Backup>>** button will display the status of the RAID Rack Battery Backup.

The **Active Task>>** button will display the on-going activity within the FC-16 RAID Rack.

The **Physical Disk Info>>** button will display the detailed information of the physical disk within the FC-16 RAID Rack.

The **Start Background Consistency Check** button will start consistency check on the FC-16 RAID Rack.

The **System Drives>>** button will display a **RAID Configuration** page. On the **RAID Configuration** page, System drives can be created, deleted, and initialized.

Performing a Consistency Check on a System Drive

A typical file system is a mixture of frequently used files, rarely used files, and free space. If a disk develops bad spots in sectors that are not often accessed, this failure could remain undetected. To prevent a disk failure during a rebuild, which could lead to data loss, it is necessary to detect unreliable disks promptly, thus preventing the RAID controller from failing them at a critical time.

It is possible to instruct a RAID controller to check, and optionally repair, the parity on any System Drive (SD) configured in RAID 1/5/10 (that is, any SD that can survive the failure of a single disk). The parity or mirrored data is used to rebuild the SD in the event of a disk failure.



Note: A RAID consistency check and a file system check are two distinct operations. The first checks, and optionally repairs, the RAID parity in a System Drive. However, it does not check the integrity of file system. That task is performed by a file system check.

It is possible to start a consistency check at any time from Web Manager or using the command line interface (CLI). It is not necessary to take the SD offline to run a consistency check. However, on each RAID rack, only one SD can be checked or rebuilt at a time. The performance of the host RAID controllers diminishes until the process ends. Other RAID racks are not affected.

To run a consistency check on a System Drive

1. From the **Storage Management** page, click **System Drives**.
2. Click **details** next to the System Drive on which to run the consistency check.
3. Click **Start Consistency Check**.



4. To start the consistency check, click **yes** to begin a check in which detected faults will be fixed. Click **no** to skip the repair of faults found. Click **cancel** to return to the **System Drive Details** page.



Note: If a RAID controller is replaced, the new RAID controller only becomes effective when the surviving RAID controller has completed a consistency check of all redundant System Drives.

During the consistency check, if parity errors are found, they will be logged in Titan's Event Log. If a check was initiated with fault correction enabled, the parity will be updated to match the

data.

Performing Background Consistency Checks

Consistency checks can be performed periodically on every System Drive (SD), from the [Command Line Interface](#) (CLI) using the `startbcc` command. This command runs a **background consistency check** (BCC) on a SD for each rack, allowing all SDs to be checked in a 'round robin' fashion. BCC is performed with fault correction disabled.



Note: BCC operations are conducted at a low-priority level to minimize the impact on system performance.

By default, the `mylex-sd-start-bcc` command is invoked periodically using `cron`. BCC will start at 1:00 a.m. every Saturday for one SD in each of the RAID racks. All SDs in a RAID rack will be checked in turn, one per week.

To disable a background consistency check, BCC can be disabled by running the `crontab list` command followed by "`crontab del <ID>`" where `<ID>` corresponds to the `mylex-sd-start-bcc` data shown by the `crontab list` command. Once BCC has been disabled, you can run `startbcc` directly from the CLI, or configure it to run automatically with cron settings of your choosing.

The `startbcc` command remembers each SD for which a BCC runs to completion. Every time the command is run, the next eligible SD in the rack is checked. If a BCC is aborted for any reason, or if it fails to complete, the same SD will be checked next time. Also, if an SD is skipped for any reason, an entry will be made in the [event log](#) describing why the SD has not been checked.

Because the aim of BCC is to detect unreliable disks, this operation will not start if there are potential conflicts, and will be interrupted under certain circumstances. Specifically, Titan cancels a BCC if one of the following events takes place:

- Any System Drive on the RAID rack becomes critical or fails.
- A command is issued to run a long operation that is not compatible with BCC, such as a rebuild, a BGI, or another consistency check.
- A `putconf` CLI command is issued, or new firmware is downloaded to disks or RAID controllers.
- The RAID controllers are reset.

Here are reasons for which BCC will skip a System Drive:

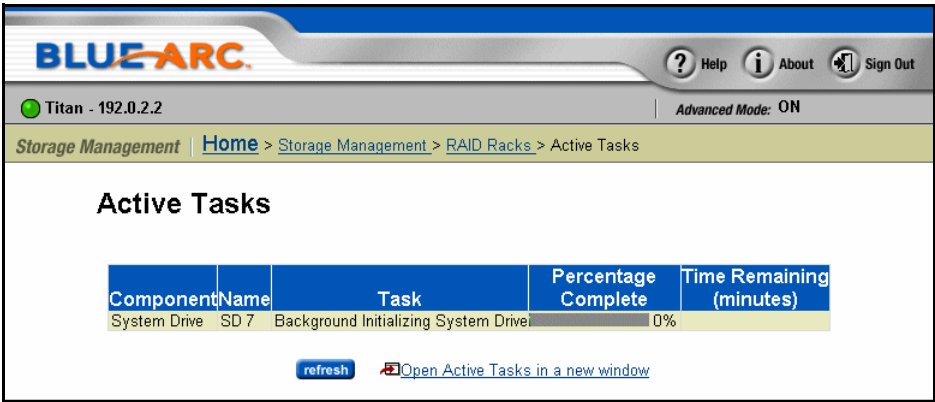
- There is another long operation is running, including disk firmware being loaded.
- There are recognizable problems with the RAID rack configuration, or the rack does not have a suitable *hot spare disk* with which to perform a rebuild, if necessary.
- More than one disk in the System Drive has experienced any disk errors, including PFA warnings.

- The controller in slot 0 is not online or there is a hardware fault on the rack, such as a failed PSU, fan or back-end channel.

Checking the Status of Active Tasks

The ongoing activity within the FC-16 RAID Rack can be viewed on the **Active Tasks** page.

1. From the **Storage Management** page, select **RAID Racks**.
2. Check the box of the target RAID Rack.
3. Click **View Active Tasks**.



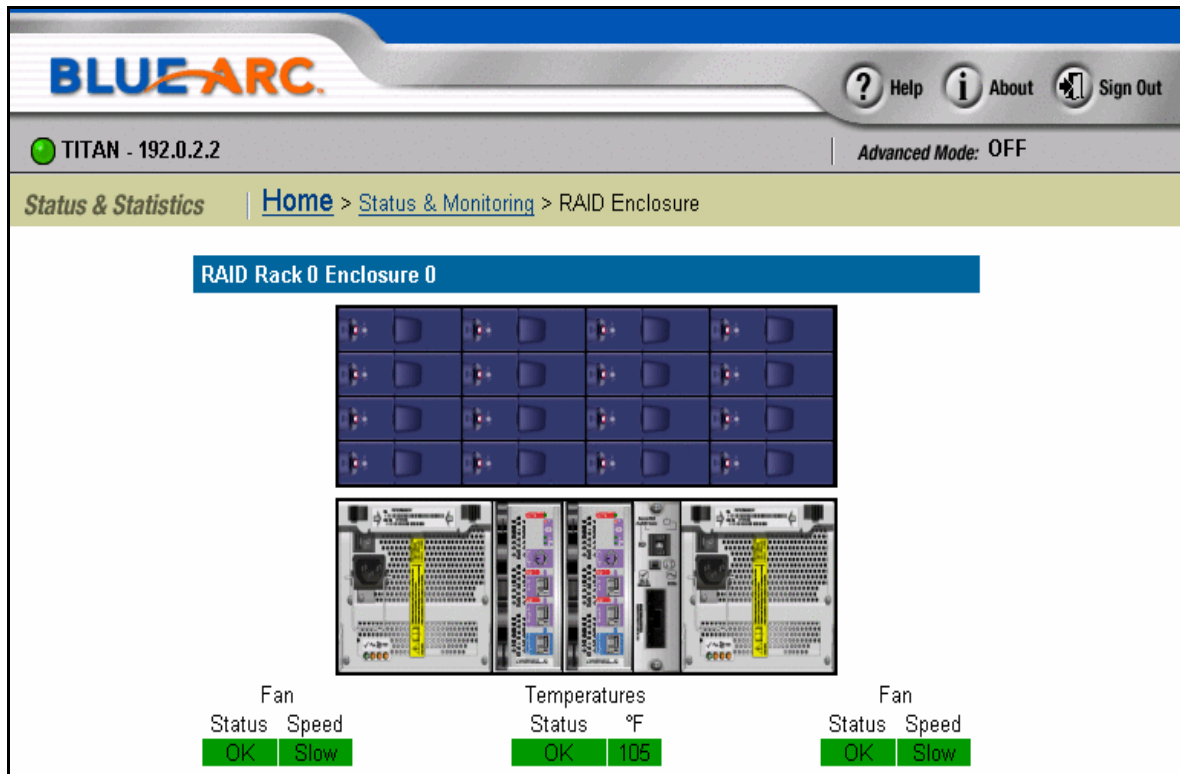
Item /Field	Description
Component	The System Drive or RAID Rack on which the task is being performed.
Task	The name, describing the running task.
Percentage Complete	An approximate indication of the status of the task.
Time Remaining	If available, the amount of time remaining before the task completes.

Monitoring Physical Disks

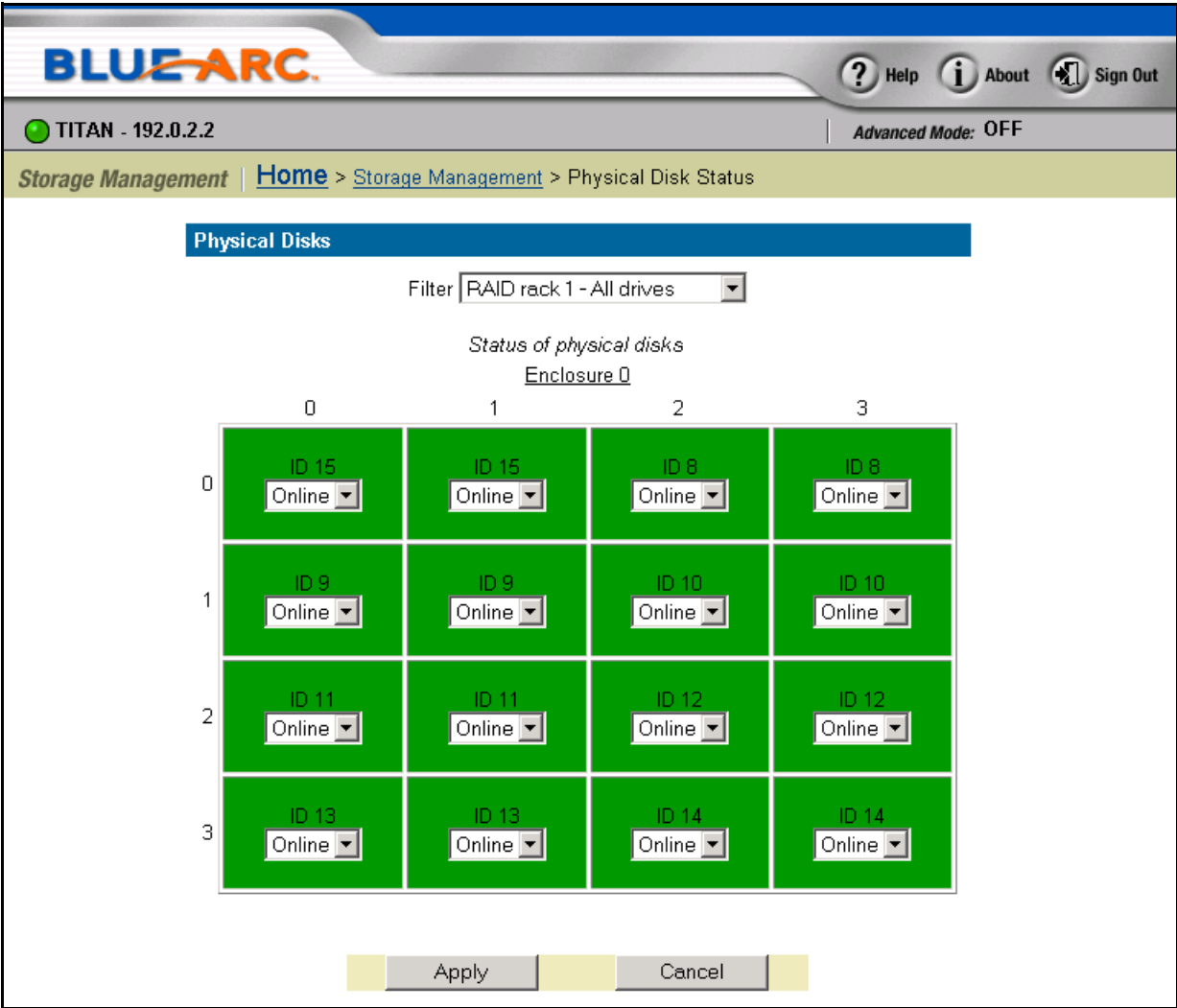
Using the Web Manager, it is possible to determine the status of the physical disks associated with a particular RAID Rack or System Drive. It is also possible to change the status of the disks in cases where, for example, a disk needs to be removed or a new hot spare disk has been added.

To check and change the status of the physical disks

1. From the **Status & Monitoring** page, click **System Monitor**. Then, click the FC-16 main enclosure.



2. Click on one of the disks to view all installed disk drives.

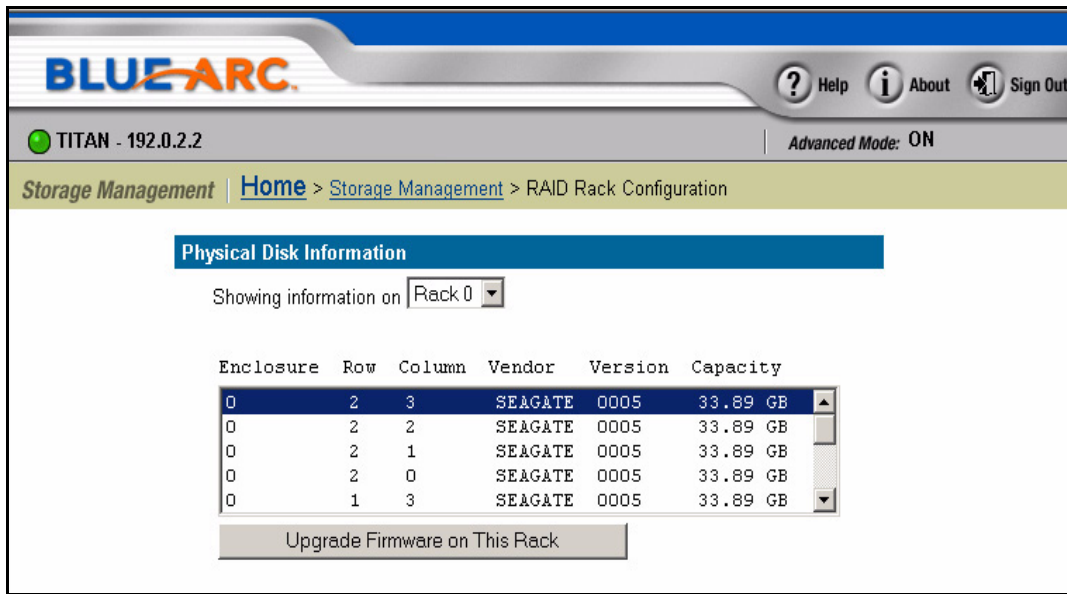


3. To change the status of one or more of the disks, select the new status from the drop-down list and then click **Apply**.

It is possible to view more information on physical disks associated with a particular RAID rack, such as their physical position and the name of their manufacturer.

To view more information on the physical disks

1. From the **Storage Management** page, click **RAID Racks**. Select the RAID Rack of interest and click **details**.
2. Click **Physical Disk Info>>**.



The table below describes the Item/Fields in this screen:

Item/Field	Shows
Showing information on...	Select a rack from the drop down list on which to view information.
Enclosure	The number of the storage enclosure that contains the physical disk.
Row	The vertical position of the physical disk. Rows are numbered 0 through 3, where 0 is the top-most row.
Column	The horizontal position of the physical disk. Columns are numbered 0 through 3, where 0 is the left-most column if looking at the front of the storage enclosure.
Vendor	The name of the disk manufacturer.
Version	The version number of the disk firmware.
Capacity	The storage capacity of the disk.

AT-14 and AT-42 Storage Subsystem

The AT-14 storage subsystem can support **Tier 3** (7,200 RPM) and **Tier 4** (5,400 RPM) PATA disks, where each storage enclosure can house up to 14 PATA disks per enclosure.

The AT-42 storage subsystem supports **Tier 4** storage (5,400 RPM PATA disks). Each storage enclosure can house up to 42 PATA disks per enclosure.

Neither the AT-14 nor the AT-42 storage enclosure support cascading, so each enclosure houses its own RAID controller. Each enclosure supports a single RAID controller, and each RAID controller supports dual FC host ports.



Note: This section describes how to configure the AT-14 and AT-42 storage systems. For instructions on how to define IP parameters, refer to the *AT-14 User Manual* or the *AT-42 User Manual*.

Storage Characteristics

The AT-14 and AT-42 storage enclosures use PATA disk technology and hardware RAID controllers, which provide complete RAID 5 functionality and tolerance of single disk failures.

System Drives

System Drives are the basic storage element used by the Titan SiliconServer. A System Drive comprises a number of physical disks. The size of the System Drive depends on the number of disks and their capacity. The AT-14 and AT-42 RAID controllers support RAID 5. Each System Drive has an identifying number (ID), which is unique to the Titan SiliconServer.

The *AT-14 User Manual* and *AT-42 User Manual* refer to System Drives as “volumes” (or “logical volumes”). These should not be confused with the file system volumes used by the Titan SiliconServer.



Note: Throughout this section, a “Volume” is equivalent to a “System Drive”.

Hot Spare Disk

A hot-spare disk is a physical disk that is configured for automatic use in the event that another physical disk fails. Should this happen, the system automatically switches to the hot-spare disk and rebuilds on it the data that was located in the failed disk. The hot-spare disk must have at least as much capacity as the other disks in the System Drive.

If it is necessary to remove and replace disks, it is possible to perform hot swap operations. In other words, an offline or failed disk can be removed and a new disk inserted while the power is still on and the system is still operating.

Background Consistency Checking

The AT-14 and AT-42 storage subsystems perform periodic consistency checks of all disks. This detects the presence of bad blocks, thus reducing the probability of a double failure, which could result in loss of data.

Managing the Storage Enclosures

AT-14 and AT-42 storage enclosures are managed using a Web management utility embedded in the storage subsystem.



On a properly configured Titan SiliconServer, this utility is accessible from the System Monitor page. In addition, the Titan SiliconServer tracks alerts issued by the storage subsystem through SNMP. To add an storage enclosure to the System Monitor, see [Configuring Devices on the System Monitor](#).

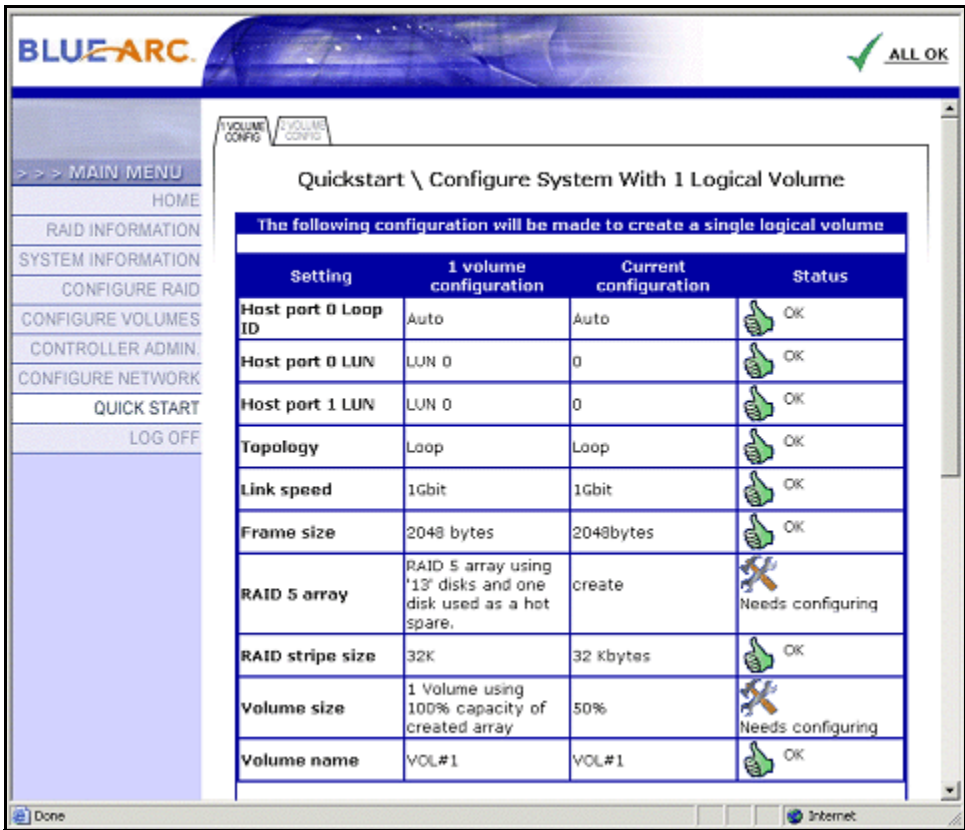
Creating System Drives

On AT-14 and AT-42 storage enclosures, System Drives are referred to as *volumes* and created when the storage unit is first set up. The storage enclosures are pre-configured as follows:

	Disk Arrays	Logical Volumes	Hot Spares
AT-14	1	2	1
AT-42	4	4	2

Configuring the AT-14 Storage Enclosure

1. From the **System Monitor** page, click on the AT-14 enclosure that has to be configured.
2. Click the **Quick Start** link on the left hand side of the page.

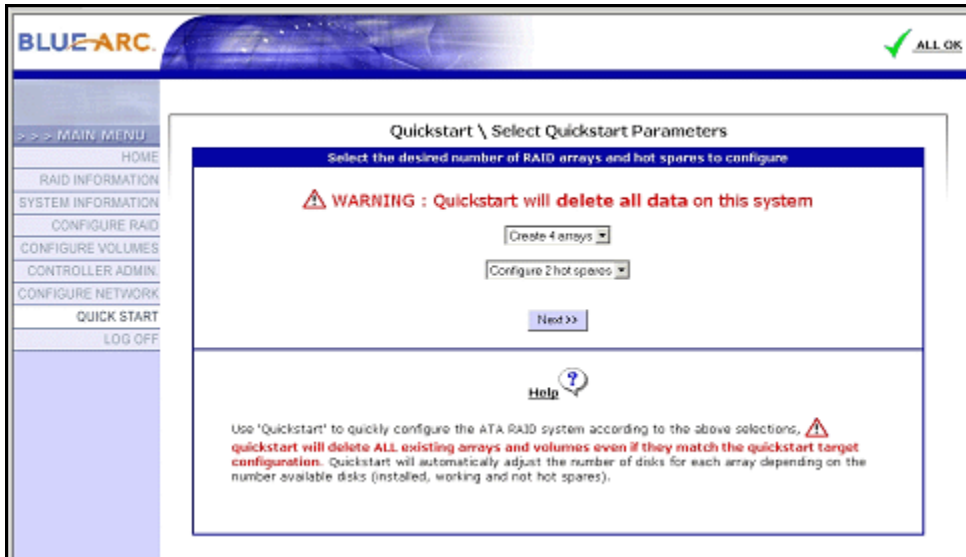


3. Select the **2 Volume Config** tab.
4. On the next screen, click the **Check this checkbox to confirm** box, and click the **Quickstart Configure for 2 Volumes** button.

- The next screen will show that the system is now initializing and will take several hours to complete (typically 3-4 hours).

Configuring the AT-42 Storage Enclosure

- From the **System Monitor** page, click on the AT-42 enclosure that has to be configured.
- Click the **Quick Start** link on the left hand side of the page.



- Select the **Create 4 arrays** option and **configure 2 hot spares** and click the **Next** button.
- On the next screen, click the **Check this checkbox to confirm** box, and click the **Quick Start** button.
- The next screen will show that the system is now initializing and will take several hours to complete (typically 3-4 hours).

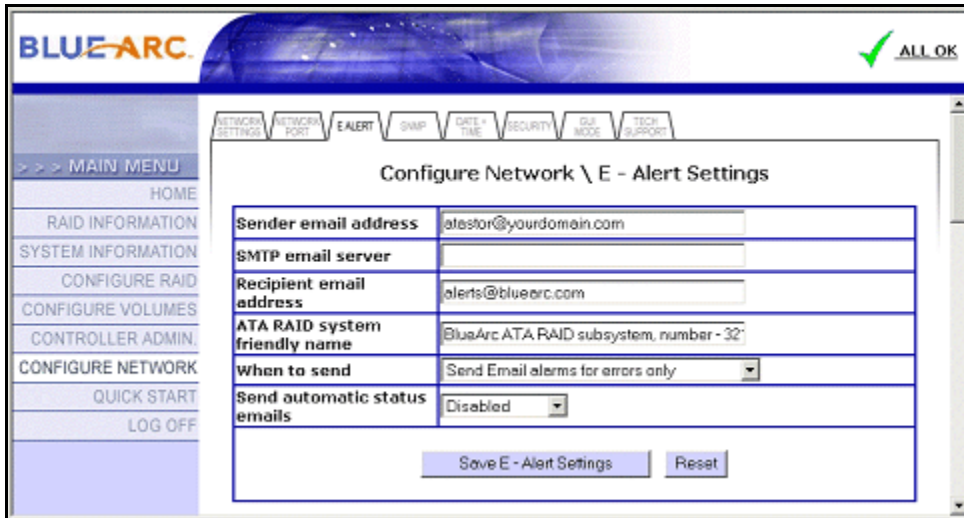
Configuring the Storage Enclosure

In order to ensure that an AT-14 or AT-42 storage enclosure is properly monitored, the following needs to be configured:

- Email alerts
- SNMP traps
- Date and time

Email Alerts

To setup Email Alerts, click the **Configure Network** on the left hand side of the page. Then, click the **E-Alert** tab.



The **Sender email address** should be set to an account that exists on the email server. Not all email servers will require this yet most will require the domain portion of this address to be correct, for example *'anyname@yourcorrectdomainname.com'*.

The **SMTP email server** can either be the Internet name (domain name) of the email server or the IP address of the email server. If the domain name is entered for the email server the DNS settings must be configured in the network settings page so that the domain name of the email server can be resolved. If the email server and/or the DNS is not located on the local network the gateway/router IP address will need to be set in the network settings page.



Note: If the SMU is configured to support email relay, and the AT-14 or AT-42 resides on the private management network, it is recommended to use the SMU's eth1 IP address as the configured mail server. The SMU will relay the email message to its configured SMTP server.

The **Recipient email address** is the standard email address of the person or account that wishes to receive email Alerts from the ATA RAID system. This is normally set to the email address of the network or system administrator.

The **ATA RAID system friendly name** is a descriptive name that will be included in all email alerts. It should be unique, allowing the RAID system to be easily identified. This is useful when there are more than one ATA RAID systems.

The **When to send** pull down menu will configure what type of email alerts need to be sent or, if required, this functionality can be switched off.

Send automatic status emails will send a ATA RAID system status email to the configured **Recipient email address**. The pull down menu allows the frequency of these emails to be configured. These emails provide assurance that the Email Alerts function is working and serve as a reminder of any existing problems.

The **Send test email now** button will attempt to send a test email using the settings entered. Note that to use the settings entered they must have been submitted using the **Save E-Alert Settings** button. There is NO notification that the email was successful, the email account must be checked to determine this.

SNMP Traps

On a properly configured system, SNMP traps alert the Titan SiliconServer of failures or other unusual conditions. These alerts, when received, are logged as events in Titan's event log. To setup SNMP traps click on the SNMP tab.

IP address to send SNMP trap to - This should be set to the IP address of the remote management station that will receive SNMP traps or the Administration Services IP address of Titan, if Titan is to display the AT-14 or AT-42 SNMP traps in its event log.

Community string - This must be set to the community string that the network management station is expecting to receive. If traps are being sent to Titan, they must match the **community name** of the Titan SiliconServer.



Note: The community string should be set to public.

Trap version - Select the trap version according to what version of trap the network management station is capable of receiving. Titan supports both Version 1 and Version 2c SNMP traps.

When to send a SNMP trap - Select under what conditions the ATA system will send an SNMP

trap.



Note: BlueArc recommends that the AT-14 and AT-42 storage enclosures be configured to send SNMP traps to the Titan SiliconServer for all levels. Also, Titan needs to be configured to accept these traps (see [Configuring Devices on the System Monitor](#)). When this is done, the SNMP traps will be registered as events, thus leveraging Titan’s event logging and notification functions.

When all settings have been set, click the **Save SNMP Settings** button.

Date and Time

- 1. To setup Date and Time select the **Date + Time** tab.

- 2. In the **Time Server IP address** field, enter the IP address for the [SMU’s eth1 interface](#) and ensure that the **Use entered IP address** option is selected.
- 3. When all settings have been entered click the **Save Settings** button.

System Drives

System Drives (SDs) are the basic storage elements used by Titan and are the foundation on which Silicon File Systems are created. With Parallel RAID Striping, multiple System Drives may be combined into large File Systems.

System Drives, which are also referred to as LUNs¹, are logical SCSI devices serviced by the RAID controllers in the storage subsystem.

Managing System Drives

System Drives are hosted by RAID storage subsystems attached to the server. Titan monitors its Fibre Channel (FC) links periodically and automatically detects the presence of System Drives (LUNs). Since Titan could be connected into a Storage Area Network (SAN) that is shared with other servers, Titan does not automatically make use of System Drives it detects on its FC links, unless:

- ❑ The System Drive was created using Web Manager or one of Titan's embedded UIs (like the Command Line Interface), or
- ❑ Access to the System Drive is marked as **Allowed** on the **System Drives** page.

The **System Drives** page lists all of the System Drives (SDs) that are part of the Titan SiliconServer configuration. This page is also used to set certain SD configuration parameters and to correlate file systems to System Drives.

Creating System Drives

Storage subsystems use RAID technology (typically RAID 5) to aggregate multiple disk storage devices into System Drives. The procedure for creating System Drives depends on the storage enclosure type. For more information, refer to the [FC-14](#), [FC-16](#), [SA-14](#), [AT-14](#), and [AT-42](#) Subsystem sections.

Viewing System Drives

The System Drives page lists all of the System Drives (SDs) that are created in Titan storage subsystems or SDs automatically *detected* by Titan on the Fibre Channel (FC) network. SDs are not used unless their access is marked as allowed.



Note: If a storage enclosure has been added, its SDs may not appear on the System Drives page. Click Discover System Drives to view the added SDs.

1. Technically, a Logical Unit Number (LUN) is a number that the RAID controller uses to identify a System Drive. Note that the LUN does not uniquely identify the System Drive on a Fibre Channel network, so the Titan SiliconServer uses an internally generated ID to track System Drives.

To View / Modify System Drives

From the **Home** page, click **Storage Management**. Then, click **System Drives**.

BLUE ARC

?

 Help

i

 About

✕

 Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

Storage Management

 | [Home](#) > [Storage Management](#) > System Drives

System Drives

Licensing

Current capacity used: 3.07 TB

Limit: 256.00 TB

Filter

Filter By Access:

Show All

☐ Hide System Drives which are Secondary in a mirror

filter

	ID	Capacity	Manufacturer	Label	Comment / Rack Name	Storage Pool	Allow Access	Status	Mirror Status	Mirrored to	
☐	0	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐	1	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐	2	393.39 GB	MYLEX		Rack 0	pool0	Allowed	OK			details
☐	3	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐	4	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐	5	393.39 GB	MYLEX		Rack 0	pool1	Allowed	OK			details
☐	6	393.39 GB	MYLEX		Rack 0		Allowed	OK			details
☐	7	393.39 GB	MYLEX		Rack 0		Allowed	OK			details

Check All | Clear All

Actions:

allow access

deny access

forget

create

Discover System Drives

Shortcuts:

RAID Racks

Storage Pools

Active Tasks

Item / Field	Description
Licensing	
Current capacity used	The storage capacity currently in use.
Limit	The amount of storage that is licensed on this Titan SiliconServer, measured in Terabytes.
Filter	
Filter by Access	Select a filter for viewing the System Drives list: Show All, Access Allowed, Denied Access, Not Present.
ID	The System Drive identifier.
Capacity	The capacity of the System Drive.
Manufacturer	The manufacturer of the RAID rack hosting the System Drive, as reported by the Fibre Channel network.

Label	On FC-14 or SA-14 Storage Enclosures, the label assigned to the System Drive when it was created. If the label says Not known, the System Drive is present on the Fibre Channel network but the RAID controller is not accessible through an Ethernet management network. It may be necessary to discover the RAID Rack.
Comment/Rack Name	FC-16 RAID racks are identified by their name or WWN. Other RAID racks are identified using the Comment field. If the label says Not known, the System Drive is present on the Fibre Channel network but the RAID controller is not accessible through an Ethernet management network. It may be necessary to discover the RAID Rack.
Storage Pool	If present, the label of the Storage Pool of which this System Drive is a part. Click on the Storage Pool label to view detailed information about that Storage Pool.
Allow Access	Indicates whether the System Drive is present and if Titan is allowed to access it.

Status	The current status of the System Drive. ❑ Grey: Not Present. The RAID controller has been out of contact since Titan was last booted (i.e. a Fibre Channel cable is loose, etc.) or the RAID controller (if in contact) reports that the SD has been deleted. ❑ Green: OK. The SD is present and operational.  Note: If the SD is “OK”, it can be performing other tasks (i.e. initializing in the background, rebuilding disks, etc.) The event log may provide more information. ❑ Amber: ❑ Initializing. The SD is undergoing a RAID initialization and cannot be used. ❑ Red: ❑ Disconnected. The SD is present but the RAID controller indicates that it is not available for use. ❑ Offline. The RAID controller was able to communicate with the SD when it was booted, but it is currently out of contact. ❑ Failed. The SD is present but it is unsuitable for use.
Mirror Status	If the System Drive is bound to another using Synchronous Volume Mirroring (SVM), the status of the mirrored System Drive is also shown.
Mirrored To	If mirrored using SVM the ID of the partner System Drive is displayed.

Titan keeps track of the SDs that are selected for access in its internal data structures, and assigns each SD a persistent System Drive ID.

If a SD goes off-line, it continues to appear in the **System Drives** page.

If a SD is permanently removed from the system, without having first been deleted, it must be explicitly removed from the **System Drives** table. From the **System Drives** page, click **details** for the SD which needs to be removed. Then, from the **System Drives Detail** page, click **forget**.

To find System Drives which are not listed in **System Drives** table and to refresh the system drive list, click **Discover System Drives**.

System Drive Details

The **System Drive Details** page displays the details for a single System Drive (SD). From the **Storage Management** page, click **System Drives**. Then, click **details** next to the System Drive on which to view the additional details.

BLUEARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Storage Management | [Home](#) > [Storage Management](#) > [System Drives](#) > System Drive Details

System Drive Details

Information

Comment:

System Drive ID: 0 Rack : SD: 0 : 0
 Rack Name: Rack 0 Serial: MYLEX 00:00:A8:92:20:00:00:80:E5:12:A8:92:00:00:00:00:00:00:00
 Manufacturer (Model): MYLEX (FFx2) Version: 7850

Capacity: 393.39 GB

Status: ● OK apply

Performance Settings

☐ Superflush Stripe Size: 32 KB
Width: 3

Low Level Initialization Status

System Drive is low level initialized
[Start foreground initialization](#) [Start background initialization](#)

FC Path

Current Host Port 1	Preferred Host Port None
Current RAID Controller 0 :: A8:B2:12:E5:80:00:00:20	Preferred RAID Controller None
Current Port Name 23000080E512B2A8	Preferred Port Name None

Storage Pool Configuration

Storage Pool Label: [pool0](#)
 Storage Pool Status: ● Healthy

Actions: allow access deny access forget delete | [Start Consistency Check](#)

Shortcuts: [Physical Disk Status](#) [Active Tasks](#)

Item / Field	Description
Information	• Label (FC-14 and SA-14 only): The label assigned to the System Drive when it was created. • Comment: Enter additional information regarding the System Drive. • System Drive ID: A unique identification number assigned to the System Drive when it was first seen by the server. • Rack: SD (FC-16 only): Identifies the location of the System Drive. • Rack name: The name of the RAID rack hosting the System Drive. • Serial: The serial number of the System Drive. • Manufacturer, Model: The manufacturer and model of the RAID rack hosting the System Drive. • Version: The version of firmware running on the RAID rack hosting the SD. • Media Scan (FC-14 and SA-14 only): Enable or disable the RAID controller's media scan to check for bad blocks in both data and parity sections of the System Drive. • RAID Level (FC-14 and SA-14 only): Indicates whether the System Drive is a RAID 0 or RAID 5 array. • Capacity: The size of the System Drive. • Status: The current health of the System Drive. To save any changes made to the System Drive, click apply.
Performance Settings	• Superflush: Displays the Stripe Size and Width settings applied to the System Drive when it was created. Super Flush parameters are automatically configured by Titan for optimal performance. For more information, refer to the section on Super Flush. • Cache (FC-14 and SA-14 only): • Write-Back Cache: Enable or disable write-back caching for the System Drive. • Read-Ahead Cache Multiplier (SA-14 only): Enable or disable read-ahead by the RAID controller for this System Drive.
Low Level Initialization Status	For System Drives in FC-14, FC-16, or SA-14 enclosures, this will indicate whether the parity information in the System Drives has been fully initialized. To check the System Drive initialization state on AT-14 or AT-42 enclosures, access the controller's UI through the system monitor. If the System Drive is in a FC-16 enclosure, initialization options are presented. • Start foreground initialization: click to start a foreground initialization of the System Drive. A foreground initialization will destroy all data on the System Drive. As a result, this option cannot be selected if a Storage Pool exists. • Start background initialization: click to start a background initialization of the System Drive.

FC Path	Identifies the Current and Preferred paths through which a System Drive is accessed.
Storage Pool Configuration	Information about the Storage Pool residing on the System Drive: - Storage Pool Label: The label of the Storage Pool hosted by this System Drive. - Storage Pool Status: The current health of the Storage Pool.
Mirror Configuration	Provides the following information on the primary and secondary System Drives: - The label assigned to the System Drives when created. - The number identifying each System Drive. - The name of the rack to which each System Drive belongs. - Role classifying whether the System Drive is primary or secondary. - Status indicating each System Drive's functional state.

The **Allow/Deny Access** button will set the access to the System Drive: Allowed or Denied.

The **Forget** button will remove a System Drive from the Titan SiliconServer's configuration. The System Drive must be *Not Present* for it to be deleted.

The **Delete** button will delete the System Drive on a FC-14 or FC-16 storage enclosure.

Super Flush

Super Flush is a performance optimizing technique Titan uses to maximize the efficiency with which write requests are sent to System Drives. Super Flush only applies to RAID 5 arrays and is configured by setting the following parameters:

- **Stripe size:** Also referred to as the segment size, this setting defines the size of the data patterns written to individual disks in a System Drive. The value specified for the stripe size should always match the value configured at the RAID controller. In most cases, the stripe size should be set to 32 KB.
- **Width:** This is the number of disks that can be written to in a single write request. A typical system drive will contain n data disks and one parity disk. This type of array is often referred to as $n+1$. In such an array, a single write request can be made to n number of disks. In other words, the width will typically be set to the number of disks in the system drive, minus one.

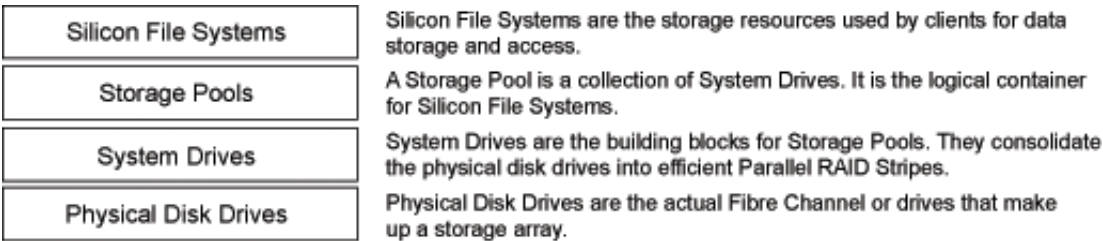
Super Flush parameters are automatically configured for optimal performance on all System Drives in all storage enclosures.

5 Storage Management

Introduction

The Titan SiliconServer has an architecture involving several storage components including [Storage Pools](#), [Silicon File Systems](#), and [Virtual Volumes](#). These storage resources are supplemented by a flexible [quota management](#) system for managing the utilization of these storage resources and a [data migration service](#), which optimizes the available storage resources. This chapter describes each of these storage components and functions in detail.

The following diagram illustrates a simplified view of the architecture:



System Drives

System Drives (SDs) are the basic storage element used by the Titan SiliconServer. Storage subsystems use RAID technology to aggregate multiple disk storage devices into System Drives. For more information refer to "[System Drives](#)."

About Storage Pools

A Storage Pool is the logical container for Silicon File Systems. Storage Pools are created on a collection of one or more System Drives. Storage Pools can be expanded as additional System Drives are created in the storage subsystems and can grow to a maximum capacity of 256 TB. Expanding a Storage Pool will not interrupt access to the storage resources by network clients.

A Storage Pool can hold up to 120 Silicon File Systems and it helps to centralize and simplify the management of the file systems it contains. For example, the settings applied to a Storage Pool can either allow or restrict the expansion of every file system in the Storage Pool.



Note: A Storage Pool license is required to add more than one Silicon File System to a Storage Pool. Without this license, only a single file system is permitted. However, even without the license, Storage Pools and Silicon File Systems can be expanded as long as the Storage Pool contains a single file system.

About Chunks

Storage Pools are composed of a number of small allocations of storage called "chunks." The size of the chunks in a Storage Pool is defined when the Storage Pool is created. A Storage Pool can contain up to a maximum of 16,384 chunks. Likewise, an individual file system can contain up to a maximum of 1024 chunks. When file systems in a Storage Pool expand, they grow in size in full chunk size increments.

Planning the chunk size is an important consideration when creating Storage Pools for two reasons.

- Chunks define the size increment with which file systems will grow when they are expanded.
- As a file system can only contain 1024 chunks, the chunk size may limit the future growth of file systems in a Storage Pool.

About Silicon File Systems

The Silicon File System is the main storage component of the Titan Storage System. All other features on the server either directly or indirectly support it. The first generation Titan blades supported up to 60 mounted file systems. The Titan 2000 Series supports up to 120 mounted file systems. The maximum size of the file system depends on three factors.

- The model of the Titan SiliconServer.
- The file system block size.
- Available chunks.

The following table shows the maximum size of the file system, assuming that there are sufficient chunks available to support the maximum size.

	Model 2100	Model 2200
4 KB Blocks	16 TB	128 TB
32 KB Blocks	32 TB	256 TB

Silicon File Systems have many features that provide control and monitoring of their capacity, allocation, and performance. Quotas can be used to control the amount of storage given to clients. Graphs can be used to view traffic and usage activity. Virtual Volumes can be used to divide a Silicon File System into discrete storage areas that appear to clients as independent file

systems. And finally, free space triggers can be used to initiate storage reallocation routines through [BlueArc Data Migrator](#), keeping the most frequently used data on high-performance storage devices while migrating less frequently used data onto low-performance, lower cost, storage devices.



Note: Only Silicon File Systems that reside on FC-14 and SA-14 storage arrays may be part of the same Storage Pool and be assigned to different EVS. On other storage arrays, all file systems in a Storage Pool must be assigned to the same EVS.

About Virtual Volumes

A Silicon File System can be divided into discrete areas of storage called Virtual Volumes. From a client's perspective, a Virtual Volume will appear to be a normal file system. Virtual Volumes provide a simple method for allocating directories to users and groups and controlling them with quotas. For more information, see "[Understanding Virtual Volumes](#)."

Using Storage Pools

Storage Pools are primarily used as a container in which Silicon File Systems are created. They can also be used to define the auto-expansion policy for all of the Silicon File Systems created in the Storage Pool.

Storage Pools can be created, deleted, expanded, removed from service, or renamed. The following procedures describe how to perform those tasks.

To Create a Storage Pool

As long as there are available System Drives, a Storage Pool can be created at any time. Creating a new Storage Pool involves deciding on a pool size, giving it a name, selecting one or more System Drives, and setting the chunk size.

A Storage Pool can be created with up to 32 System Drives. However, it can later be extended by adding more System Drives until the total size of the pool has reached 256 TB. For instructions, see "[To Expand a Storage Pool](#)."

When creating a new Storage Pool, to attain optimal performance, it is recommended that the Storage Pool being created should utilize as many System Drives as possible. After the Storage Pool has been created, smaller file systems can be created in the pool for granular storage provisioning. This methodology should also be applied when expanding a Storage Pool.

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Storage Pools** to view a list of all Storage Pools.

3. From the box at the bottom of the page, click **create** to view the Storage Pool Wizard page.

BLUEARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Storage Management | Home > Storage Management > Storage Pools > Storage Pool Wizard

Storage Pool Wizard Page 1 of 2

Raw Capacity: 0.00 Bytes
Usable Capacity: 0.00 Bytes

Available System Drives

ID	Capacity	Manufacturer	Comment / Rack Name	RAID Level	Disk Type	Disk Size	Width	Stripe Size
☐ 6	393.39 GB	MYLEX	Rack 0	5	FIBRE	131.13 GB	3	32 KB
☐ 7	393.39 GB	MYLEX	Rack 0	5	FIBRE	131.13 GB	3	32 KB

[Check All](#) | [Clear All](#)

Storage Pool Label:

Guideline Chunk Size: ☒ Default: 5.00 GB
☐ Custom: GB

[What chunk size should I choose?](#)

[back](#) [next](#) [cancel](#)

Item / Field	Description
Raw Capacity of Selected System Drives	Shows a running total of selected System Drive sizes.
Usable Capacity of Selected System Drives	Shows the capacity of the Storage Pool that will be created based on the selected System Drives. Ideally, this and the Raw Capacity numbers should be equal.
ID	Shows the System Drive number assigned by Titan. Appears in the Event Log.
Capacity	Shows the System Drive's size.
Manufacturer	Shows the manufacturer of the System Drive.
Comment / Rack Name	Shows the Rack's name and any additional information.
RAID Level	Shows the RAID Level for the System Drive.
Disk Type	Shows type of System Drive; for example, Fibre, SATA, and PATA.

Disk Size	Show the capacity of each physical disk in the System Drive
Width	Shows the number of physical disks in a System Drive.
Stripe Size	Shows the data format size used for writing to a System Drive.

4. From the **ID** column, select one or more system drives that must be used to build the new Storage Pool.

A Storage Pool cannot consist of System Drives with different manufacturers, disk types, or RAID levels. Any attempt to create a Storage Pool from such dissimilar System Drives will be refused.

For the highest level of performance and resiliency, BlueArc strongly recommends that all System Drives be of the same capacity, width, stripe size, and consist of disks of equal size. However, creating a Storage Pool with such System Drives is allowed after first acknowledging a warning prompt.

5. Set the chunk size for the new Storage Pool:
 - If the default chunk size is desired, then click **Default**. The default chunk size will be shown in the adjacent text box. The default size will automatically be calculated as (Storage Pool size)/256.
 - If a specific chunk size is desired, click **Custom** and enter the desired chunk size. The size can range from 512 MB to 1 TB. However, a chunk size of less than 5 GB is not recommended.

For more information on chunks, see "[About Chunks](#)" or click **What chunk size should I choose?**

6. In the **Storage Pool Label** text box, type a name for the Storage Pool.
7. From the bottom of the page, click on **Next** to go to a Confirmation page.
8. Click on the **create** button to create the Storage Pool.

After the Storage Pool has been created, it can be filled with Silicon File Systems. For instructions, see "[To Create a Silicon File System](#)."

To Delete a Storage Pool

A Storage Pool that does not contain any Silicon File Systems can be deleted at any time. If it does contain file systems, those file systems must be deleted first. After the pool has been deleted, the system drives used by it will become free and available for use by new or existing Storage Pools. For instructions about deleting a file system, see "[To Delete a Silicon File System](#)."

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Storage Pools** to view a list of all pools.

3. From the right-hand column, click on the **details** button for the Storage Pool that must be deleted.
4. From the list of **Actions** located on the bottom of the page, click **delete** to open a Confirmation dialog box.
5. Click **OK** to delete the Storage Pool.

To Expand a Storage Pool

Expand a Storage Pool when more storage is needed. A pool can be expanded at any time and without interrupting service to clients. It only involves adding more System Drives to the pool. A Storage Pool can be extended until its total size has reached 256 TB.

When expanding a new Storage Pool, to attain optimal performance of the new storage, it is recommended that the Storage Pool being expanded should utilize as many System Drives as possible.

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Storage Pools** to view a list of all pools.
3. From the **Label** column, select the Storage Pool that must be expanded.
4. From the list of **Actions** located on the bottom of the page, click **expand** to view a list of available System Drives.
5. From the **ID** column, select the drives that will be used to expand the pool.
6. From the bottom of the page, click **next** to view a confirmation page.
7. From the bottom of the page, click on **expand** to add the drive(s) to the pool.

To Reduce the Size of a Storage Pool

The size of a Storage Pool cannot be reduced.

To Deny Access to a Storage Pool

Denying access to a Storage Pool will make all its file systems inaccessible from a client's point of view. It can be used to prepare the storage array for physical relocation. The pool and its contents are not lost, nor deleted, and access to it can be returned when needed.



Note: Denying access to a Storage Pool also removes the association between the file systems hosted by the pool and their EVS. Once access to the Storage Pool is allowed, the file systems must be reassociated with an EVS. Denying access to a Storage Pool should only be performed during a planned maintenance window and only at the direction of BlueArc Global Services.

The procedure for denying access to a Storage Pool involves unmounting each Silicon File System in the pool, and then changing the pool's access mode. For instructions on unmounting Silicon File Systems, see ["To Unmount a Silicon File System."](#)

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Silicon File Systems** to view a list of all file systems.
3. From the **Label** column, select every Silicon File System in the pool.
4. From the list of **Actions** located on the bottom of the page, click on **unmount** to open a confirmation dialog box.
5. Click the **OK** button to unmount the file systems.
6. From the list of **Actions** located on the bottom of the page, click on **Storage Pools** to view a list of all pools.
7. From the **Label** column, select the Storage Pool that will have its access mode changed.
8. From the list of **Actions** located on the bottom of the page, click **deny access** to open a confirmation dialog box.
9. Click **OK** to restrict access to the Storage Pool. This will also remove the pool from the Storage Pools list, but it will not be deleted.

To Allow Access to a Storage Pool

A Storage Pool can be set so that clients cannot access any of its Silicon File Systems. This procedure will return access to a Storage Pool, but it can also be used when a storage array that has been previously owned by another Titan SiliconServer has been physically relocated to be served by this server. The process involves restoring access to one of the System Drives that belong to the pool, and then restoring access to the pool itself.

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **System Drives** to view a list of all System Drives.
3. From the **ID** column, select one of the System Drives that belong to the pool that needs its access restored.
4. From the list of **Actions** located on the bottom of the page, click on **allow access** to restore access to the System Drives.
5. From the **Storage Pool** column, click on the name of the pool to view its Storage Pool Details page.
6. From the list of **Actions** located on the bottom of the page, click on **allow access** to open a confirmation dialog box.
7. Click the **OK** button to restore access to the Storage Pool.

If the Storage Pool contains any file systems, each file system will need to be associated with an EVS before it can be made accessible. To do this, navigate to the details page for each Silicon File System in the Storage Pool and assign it to the desired EVS.

To Rename a Storage Pool

The name for a Storage Pool can be changed at any time, and without affecting any clients.

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Storage Pools** to view a list of all pools.
3. From the right-hand column, click on **details** of the pool that needs to be renamed to view its Storage Pool Details page.
4. In the **Label** text box, type in a new name for the pool.
5. Click on **rename** to change the pool's name.

To Stop File System Expansion for an Entire Storage Pool

Use this procedure to prohibit the automatic expansion of all Silicon File Systems in the specified Storage Pool. This setting will override any auto-expansion setting on the individual file systems in the Storage Pool.

This setting only affects auto-expansion. Manual expansion of the file systems in the pool will continue to be allowed.

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Storage Pools** to view a list of all pools.
3. From the right-hand column, click on **details** to view the Storage Pool Details Page for the pool.
4. From the **FS Auto-Expansion** option box, click the **disable auto-expansion** button to open a confirmation dialog box.
5. Click **OK** to stop file system expansion for the entire Storage Pool.

To Allow File System Expansion for an Entire Storage Pool

Use this procedure to allow file systems in a Storage Pool to automatically expand. When expanding, the file system will grow in increments defined by the Storage Pool chunk size. Be aware that after a file system has expanded, its size cannot be reduced.

Even if the Storage Pool is configured to allow its file systems to automatically expand, the file systems must also be configured to support automatic expansion. For more information, see "[To Automatically Expand A Silicon File System](#)".

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Storage Pools** to view a list of all pools.
3. From the right-hand column, click on **details** to view the Storage Pool Details page for the pool.

4. From the **FS Auto-Expansion** option box, click the **enable auto-expansion** button to open a confirmation dialog box.
5. Click **OK** to allow automatic expansion for every file system in the Storage Pool.

Using Silicon File Systems

Use a Silicon File System for storing an organization's files and directories in a hierarchical tree structure. Titan provides extensive facilities to monitor and manage file systems, and different techniques can be used to protect the data located in them. The amount of storage space used can be monitored and restricted. Should a file system become full, it can be extended.

To Create a Silicon File System

Use this procedure to create a new Silicon File System in an existing Storage Pool. If a Storage Pool will be used to contain more than one Silicon File System, a Storage Pools license must be installed. A Storage Pool is required before a file system can be created. For instructions, see "[To Create a Storage Pool](#)."

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Silicon File Systems** to view the Silicon File System page.
3. From the box at the bottom of the page, click the **create** button to view the Create File System page.
4. Click on **An Existing Storage Pool** link to view a list of available Storage Pools.
5. From the **Label** column, select a Storage Pool.

6. At the bottom of the page, click on **next** to view the Configuration page for the new file system.

The following page will be displayed:

The screenshot shows the BlueArc Storage Management web interface. The header includes the BlueArc logo, navigation links (Help, About, Sign Out), and system information (Titan - 192.0.2.2, Advanced Mode: ON). The breadcrumb trail is: Storage Management > Home > Storage Management > Create File System.

Create File System on pool0

Storage Pool: pool0
Free Capacity: 616.03 GB
Guideline Chunk Size: 5.00 GB

Size Limit: GB

Rounded Size Limit: [Rounded to nearest chunk](#)

Auto-Expansion:

- ☒ **Enabled** Create a small file system and allow it to automatically expand to the *Size Limit*.
- ☐ **Disabled** Create the file system to the full size specified by the *Size Limit*. The file system will not grow automatically.

Label:

Assign to EVS: (EVS selection limited by file system dependencies)

WORM:

Block Size:

- ☒ **32 KB** Provides higher throughput when transferring large files
- ☐ **4 KB** More efficient space utilization with lots of relatively smaller files

Item / Field	Description
Storage Pool	The name of the Storage Pool in which the file system is being created.
Free Capacity	The amount of available space available in the Storage Pool that can be used by file systems.
Guideline Chunk Size	The approximate size of the chunks used in the selected Storage Pool.
Size Limit	If Auto-Expansion is enabled, this will be the maximum size a file system will be allowed to expand automatically. If Auto-Expansion is disabled, this specifies the capacity with which the new file system should be created.

Rounded Size Limit	This shows the approximate size limit, based on the defined Size Limit and the chunk size defined for the Storage Pool. For more information, click Rounded to nearest chunk .
Auto-Expansion	Enable or Disable Auto-Expansion. Use this to allow or constrain growth of this file system.
Label	Enter the label by which the file system should be referenced.
Assign to EVS	Select the EVS to which the file system should be assigned.
WORM	Use to enable retention control. For more information, see " WORM File Systems ."
Block Size	Use to configure optimal block size for the file system. For more information, see " Choosing a File System Block Size ."

7. Enter a **Size Limit** for the file system. This defines the maximum size the file system will grow through Auto-Expansion. This value can be changed on the **File System Details** page once it has been created. This limit is not enforced for manual file system expansions performed through the CLI.
8. Set the Auto-expansion Mode:
Be aware that Storage Pools can be configured to prevent the growth of file systems. A file system can never shrink, no be reduced in size. When expanding, it will use the Storage Pool's chunk size as the growth increment. File systems configured to automatically expand will do so when they approach about 80% of capacity. File systems can be expanded manually through the CLI. File system expansion does not interrupt file services or require the file system to be unmounted.
9. In the **Label** text box, type in a name for the new file system.
10. From the **EVS** drop-down list, select the [EVS](#) to which the file system should be assigned.
11. Select whether the file system should be a normal or WORM file system. Unless the file system is to be used for regulatory compliance purposes, select **Not WORM**. To learn more, see "[WORM File Systems](#)."
12. Select the desired file system block size. For more information, see "[Choosing a File System Block Size](#)."
13. Click **OK** to create the new Silicon File System and view its details.

To Delete a Silicon File System

A Silicon File System can be deleted at any time, unless it is a Strict WORM file system. After a file system has been deleted, the free space is restored to its Storage Pool. After a file system has been deleted, it cannot be recovered.

A user must be either a Global Admin or Storage Admin, and must have Advanced Mode enabled to delete a file system. For more information, see "[User Management](#)".

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Silicon File Systems** to view a list of all file systems.
3. From the right-hand column, click on **details** to view the Silicon File System Details page for the file system to be deleted.
4. If the file system is mounted, do the following.
 - ❑ From the box at the bottom of the page, click on the **unmount** button to open a confirmation box.
 - ❑ Click the **OK** button to unmount the File System.
5. From the list of **Actions** located on the bottom of the page, click on the **delete** button to open a confirmation box.
6. Click the **OK** button to delete the file system.

To Format a Silicon File System

Formatting a file system prepares it for use by clients for data storage. File systems created through the Web UI will be formatted and mounted automatically. As a result, this procedure should rarely, if ever, be used.

This procedure describes the steps to format an existing Silicon File System. Any existing data in the file system will be lost.

A user must be either a Global Admin or Storage Admin, and must have Advanced Mode enabled to format a file system. For more information, see "[User Management](#)".

1. Move to the SMU **Home** Page.
2. From the **Storage Management** heading, click on **Silicon File Systems** to view a list of all file systems.
3. If the file system is mounted, do the following to unmount it.
 - ❑ From the **Label** column, select the file System that needs to be unmounted and formatted.
 - ❑ From the list of **Actions** located on the bottom of the page, click on **unmount** to open a confirmation dialog box.
 - ❑ Click the **OK** button to unmount the file system.
4. Do the following to format the file system.
 - ❑ From the right-hand column, click on **details** to view the Silicon File System Details page for the file system to be formatted.
 - ❑ From the list of **Actions** located on the bottom of the page, click on the **format** button to open a Warning Message box.
 - ❑ Click **OK** to format the file system.

To Mount a Silicon File System

Use this procedure to manually mount a file system. Mounting a formatted file system makes it available to be shared or exported, and thus accessible for use by network clients. This procedure may also be used when an auto-mount of a file system has failed, which may occur in the following situations:

- ☐ The file system was not mounted when Titan was shutdown.
 - ☐ The command line interface was used to disable auto-mounting.
 - ☐ A storage system failure caused Titan to restart.
 - ☐ A storage subsystem failure caused Titan to restart three times within a 30 minute period.
1. Move to the SMU **Home** page.
 2. From the **Storage Management** heading, click on **Silicon File Systems** to view a list of all file systems.
 3. From the **Label** column, select one or more Silicon File Systems that need to be mounted.
 4. From the list of **Actions** located on the bottom of the page, click on **mount** to open a confirmation dialog box.
 5. Click the **OK** button to mount the file system(s).

To Unmount a Silicon File System

Unmount a Silicon File System when it needs to be removed from service. From a client's point of view, the file system simply disappears. This will not harm the file system, nor affect any of the data in it.

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Silicon File Systems** to view a list of all file systems.
3. From the **Label** column, select one or more Silicon File Systems that need to be unmounted.
4. From the list of **Actions** located on the bottom of the page, click on **unmount** to open a confirmation dialog box.
5. Click the **OK** button to unmount the file system(s).

Expanding a Silicon File System

A Silicon File System can be expanded at any time and without interruption of service if the following conditions exist:

- ☐ There is sufficient available free space in its Storage Pool.
- ☐ The file system expansion will not cause the file system to exceed the maximum allowable number of **chunks** in a file system.
- ☐ There are sufficient **chunks** available in the Storage Pool to support the desired expansion.

There are two ways a Silicon File System can be expanded. One is manually, and the other is automatically. File systems cannot be reduced in size.

To Manually Expand a Silicon File System

Manual expansion of Silicon File Systems is an operation supported through the Command Line Interface. For detailed information on this process, run `man filesystem-expand` at the CLI.

To Automatically Expand A Silicon File System

The amount of space a file system occupies in a Storage Pool can be automatically increased when needed. An overall size limit can also be set to control the amount of space it takes in a pool. The change can be applied without removing the file system from service.

1. Move to the SMU **Home** page.
2. From the **Storage Management** heading, click on **Silicon File Systems** to view a list of all file systems.
3. From the right-hand column, click on **details** to view the Silicon File System Details page for the file system to be expanded.
4. From the **Auto-Expansion** options box, select the **enabled** radio button.
5. If the file system must not expand beyond a specific size, do the following.
 - ☐ Select the checkbox.
 - ☐ Use the **Prevent Auto-expansion Beyond** text box and drop-down list to set the size limit.
6. Click the **Apply** button to make the change.

Reducing the Size of a Silicon File System

The size of a Silicon File System cannot be reduced. This is also the case with a Storage Pool.

Relocating a Silicon File System

Every Silicon File System must be associated with an EVS for it to be shared or exported, making it available to network clients. The association between a file system and a particular EVS is established when the file system is created. Over time, requirements for storage

resources may change and it may be desirable to reassociate a file system with a different EVS. File System Relocation will perform the following operations:

- ❑ Re-associate the file system with the selected EVS.
- ❑ Transfer explicit CIFS shares of the file system to the new EVS.
- ❑ Transfer explicit NFS exports of the file system to the new EVS.
- ❑ Migrate configured FTP mounts and FTP users to the new EVS.
- ❑ Migrate the snapshot rules associated with the file system to the new EVS.

If the file system that is to be relocated resides in a Cluster Name Space (CNS), the relocation can be performed with no change to the configuration of network clients. This is true if the file system is shared to Windows clients or exported to Unix clients through file system links within the name space. In this case, clients will be able to access the file system through the same IP address and share/export name after the relocation as they did before the relocation was initiated. For more information on CNS, see "[Cluster Name Space](#)."



Caution: Whether the file system resides in a CNS or not, relocating a file system will disrupt CIFS communication with the server. If Windows clients require access to the file system, the file system relocation should be scheduled for a time when CIFS access can be interrupted.

File System Relocation will affect the way in which network clients access the file system in any of the following situations:

- ❑ The file system resides in a Cluster Name Space, but is shared or exported outside of the context of the name space.
- ❑ The server does not use a Cluster Name Space.
- ❑ The file system contains FTP mount points.

In each of the above cases, access to the shares, exports, and FTP mounts will be changed. In order to access the shares, exports, and/or FTP mount points after the relocation, use an IP address of the new EVS to access the file service.

Relocating file systems that contain iSCSI Logical Units is not recommended. In doing so, not only will the relocation interrupt service to attached Initiators, but also manual reconfiguration of the Logical Units and Targets will be required once the relocation is complete. If relocating a

file system with Logical Units is required, the following steps must be performed:

- ❑ Disconnect any iSCSI Initiators with connections to Logical Units on the file system to be relocated.
- ❑ Unmount the iSCSI Logical Unit.
- ❑ Relocate the file system as normal. This procedure is described in detail below.
- ❑ Recreate the Logical Units on the EVS to which the file system has been relocated. During this process, the .iscsi file on the file system must be referenced as a Logical Unit that already exists.
- ❑ Recreate the iSCSI Targets.
- ❑ Delete the original iSCSI Logical Unit and iSCSI Target references on the original EVS.
- ❑ Re-connect with the new Targets with the iSCSI Initiators. Be aware that the Targets will be reference by a new name corresponding to the new EVS.

File System Relocation may require relocating more than just the specified file system. This will occur in the following two cases:

- ❑ The file system is a member of a [Data Migration Path](#). In this case, both the data migration source and target file systems will be relocated. It is possible for the target of a Data Migration Path to be the target for more than one source file system. If a data migration target is relocated, all associated source file systems will be relocated as well.
- ❑ The file system is a member of a Storage Pool with more than one file system and the Storage Pool is hosted by a storage array that is not FC-14 or SA-14. Only FC-14 and SA-14 storage arrays support Storage Pools with file systems associated with different EVS.

If more than one file system must be relocated, a confirmation dialog will appear indicating the additional file systems that must be moved. Explicit confirmation must be acknowledged before the relocation will be performed.

To Relocate a Silicon File System

1. Move to the SMU **Home** page.
2. Click on the **Storage Management** heading to view the Storage Management page.
3. From the **SiliconFS Management** list, click on **File System Relocation** to view the File System Relocation page.
4. Click on the **change** button to view the Select a File System page.
5. From the **EVS/File System Label** list, click on the file system that needs to be relocated. This will also return you to the File System Relocation page.
6. From the **Relocate to EVS** drop-down list, select the new EVS for the file system.
7. Click **next**. If a message box appears, acknowledge the request by clicking **OK**, or cancel the relocation by clicking **cancel**.

- 8. From the Relocating File Systems page, click **OK** to begin the relocation process. This page will show the progress of the relocation by checking-off each item in the relocation list.

Choosing a File System Block Size

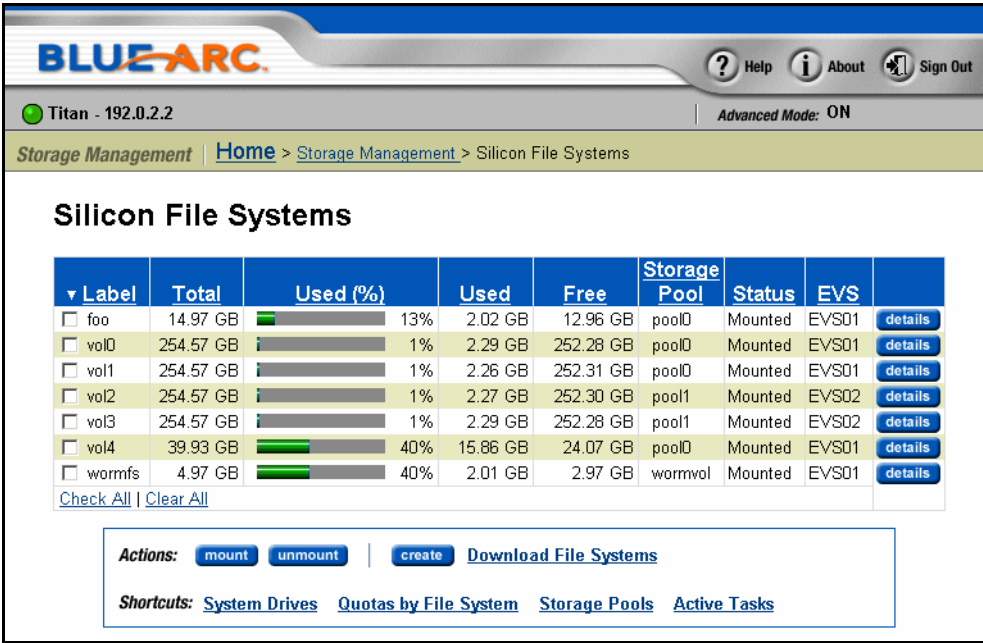
Choosing a File System block size is an important decision, as it affects performance, storage size, and efficiency of storage utilizations:

- A 32 KB File System provides higher throughput when transferring large files. However, 4 KB File Systems will perform better than 32 KB File Systems when subjected to a large number of smaller I/O operations.
- If the File System contains lots of relatively small files, a 4 KB File System will be much more efficient in terms of space utilization.
- For instance, with a 32 KB file system block size, a 42 KB file would take up two 32 KB blocks ($2 \times 32 \text{ KB} = 64 \text{ KB}$). This wastes 22 KB of space. To avoid this scenario, eleven 4 KB file system blocks (i.e. $11 \times 4 \text{ KB} = 44 \text{ KB}$) can be used to accommodate the 42 KB file. With a 4 KB file system block size, only 2 KB of space is unused.
- The maximum size for a Silicon File System depends on the relationship between the file system Block Size and Titan memory size. Blocks sizes can be either 4 KB or 32 KB, and Titan memory sizes can be either 2 GB or 4 GB. The table shown below shows the maximum file system size for different combinations of block and memory sizes.

	Titan Model 2100	Titan Model 2200
4 KB Blocks	16 TB	128 TB
32 KB Blocks	32 TB	256 TB

To View Available File Systems

From the **Storage Management** page, click **Silicon File Systems**.



BLUEARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Storage Management | [Home](#) > [Storage Management](#) > Silicon File Systems

Silicon File Systems

Label	Total	Used (%)	Used	Free	Storage Pool	Status	EVS	
☐ foo	14.97 GB	13%	2.02 GB	12.96 GB	pool0	Mounted	EVS01	details
☐ vol0	254.57 GB	1%	2.29 GB	252.28 GB	pool0	Mounted	EVS01	details
☐ vol1	254.57 GB	1%	2.26 GB	252.31 GB	pool0	Mounted	EVS01	details
☐ vol2	254.57 GB	1%	2.27 GB	252.30 GB	pool1	Mounted	EVS02	details
☐ vol3	254.57 GB	1%	2.29 GB	252.28 GB	pool1	Mounted	EVS02	details
☐ vol4	39.93 GB	40%	15.86 GB	24.07 GB	pool0	Mounted	EVS01	details
☐ wormfs	4.97 GB	40%	2.01 GB	2.97 GB	wormvol	Mounted	EVS01	details

[Check All](#) | [Clear All](#)

Actions: [mount](#) [unmount](#) | [create](#) [Download File Systems](#)

Shortcuts: [System Drives](#) [Quotas by File System](#) [Storage Pools](#) [Active Tasks](#)

Item/Field	Description
Label	The name of the File System. This is assigned when the File System is created, and used to identify the File System when performing certain operations, like creating an export or taking a snapshot.
Total	The size of the File System (GB).
Used	The amount of space used (GB).
Free	The amount of free space available (GB).
Storage Pool	The name of the Storage Pool of which the file system is a member.

Status (Normal)	• Mounted: The file system is mounted and available for service. • Formatted (Ready To Mount): The file system is fully initialized and ready to be mounted. • Formatted (Initializing system drive): The file system has been formatted, but its System Drives are in the progress of initializing. Until the initialization is complete, the storage arrays are not fully protected from fault. • Formatted (System drive is not initialized): The file system has been formatted, but its System Drives have not initialized any RAID parity information. Initialize the System Drives before using the file system. Until the initialization is complete, the storage arrays are not fully protected from fault. • Formatted (SD initialization status unknown): The file system has been formatted, but the initialization status of the System Drives is unknown. This is normal for System Drives on AT-14 and AT-42 storage arrays. View the embedded UI of the AT-14 or AT-42 to view the initialization status. • Checking: The file system is being checked. When checking, an approximate percentage complete is displayed. • Fixing: The file system is being repaired. When fixing, an approximate percentage complete is displayed.
Status (Errored)	• Failed: The file system has failed and cannot be mounted. The storage arrays may be offline. Contact BlueArc support. • RequiresRecovery: The file system needs to be recovered. This may be expected if the file system is mounted on a cluster node that does not contain a valid copy of its NVRAM. • RequiresCheck: The file system is in an errored state. Run checkfs to determine the status of the file system. • RequiresFix: The file system is in an errored state. Contact BlueArc support or run fixfs to restore the file system to normal operation. • RequiresExpansion: The server unexpectedly reset during a file system expansion operation. Contact BlueArc support or run expandfs from the CLI to complete the expansion and restore the file system to normal operation. • Unformatted: No valid file system information was identified. The storage arrays may be offline. Format the file system to destroy any existing content or contact BlueArc support.

Status (Other)	- Recovering: The file system is in the process of rolling back to its last good checkpoint. If the server was reset uncleanly, the contents of NVRAM may be being replayed. - Failing: Rarely seen - the file system has failed but is being recovered or is in use by checkfs or fixfs. - RequiresDetermining: Rarely seen - this is a transitional state between when a file system has been noticed by the server and when its state has been determined. This state will typically be followed by the status "Formatted (Ready To Mount)" or Failed. - Determining: Rarely seen - this is a transitional state which indicates that the server is determining whether or not the file system is formatted. - Removing: Rarely seen - this is a transitional state indicating that the file system is being removed from service because the EVS to which it is assigned is being taken offline.
EVS	The EVS to which the File System is assigned.
Mount	Mount an unmounted file system.
Unmount	Unmount a mounted file system.

If Usage Alerts are enabled on the Entire File System, then the sliding bar turns **yellow** when the **warning** limit is exceeded and **amber** when the **severe** limit is exceeded.

If Usage Alerts are not enabled then the sliding bar turns **yellow** when 85% capacity is reached and **amber** when the File System is full.

To download a spreadsheet containing information about all of the listed Silicon File Systems, click **Download File Systems**.

The **System Drives** link will bring up the **Systems Drives** page.

The **Quotas by File System** link will bring up the **Quotas by File Systems** page described in the [Managing Usage Quotas](#) section.

Click **Storage Pools** to view the list of Storage Pools on the server.

Clicking on the **create** button will display the **File System Wizard** page, used to create a new File System.

Clicking on the **expand** button will display the **File System Wizard** page, used to expand a new File System.



Note: Titan remembers which file systems were mounted when it shuts down, and mounts them automatically during system startup.

To View the Details of a File System

From the **Silicon File Systems** page, click the **details** button next to the desired File System.

Silicon File System Details

Settings/Status

Label: [rename](#)

1% Total Used Space

Legend: ■ Live File System ■ Snapshots

Status: Mounted
EVS: EVS01 (online)

Security: [Mixed \(Windows and UNIX\) \(Inherited\)](#)
WORM: Not WORM
Block Size : 4 KB

Capacity

Capacity: 254.57 GB
Free: 252.28 GB (99%)
Total Used: 2.29 GB (1%)

Live File System: 2.29 GB (1%)
Snapshots: 0.00 Bytes (0%)

Auto-Expansion

Manual Expansion limit: 870.60 GB

☐ Enabled
☐ Prevent auto-expansion beyond GB

☒ Disabled

[apply](#)

Usage Thresholds

File System Usage

	Live File System	Snapshots	Entire File System
Current:	1 %	0 %	1 %
Warning:	75 %	75 %	75 %
Severe:	95 %	95 %	95 %

☒ Do not allow the [live](#) file system to expand above it's **Severe** limit

[apply](#)

Check/Fix

Status: File System has not been checked since reboot.
Scope: ☐ Entire File System
☒ Directory Tree [browse...](#)
[check](#) [fix](#) [cancel](#) [Active Tasks...](#)

Storage Pool: [pool0](#)
Capacity: 1.15 TB
Free: 616.03 GB (52 %)
Used: 564.12 GB (48 %)

Actions: [mount](#) [unmount](#) [format](#) [delete](#)

Shortcuts: [Data Migration Paths](#) [Data Migration Target File System](#)

Item /Field	Description
Label	The name of the File System. The label is automatically assigned when the File System is created, and used to identify the File System when performed certain operations (e.g. creating an export or taking a snapshot).
Status	The current status of the file system, showing the amount of total used space and if the File System is mounted or unmounted.

Current EVS	The EVS to which the File System is assigned. If the file system is not currently assigned to an EVS, a list of EVS will appear to which the file system can be assigned.
Status	Indicates whether the EVS is online or offline.
Security	Displays the file system security policy defined for the file system.
Formatted Capacity	The total amount of formatted space (free + used space)
Free Space	The total amount of free space (GB)
Total Used Space	The total amount of used space: GB (%): live File System and snapshots .
Block Size	The file system block size. 32 KB or 4 KB, as defined when the file system was formatted.
Auto-Expansion	Enable or Disable Auto-Expansion. If Auto-Expansion is enabled, a limit can be defined to constrain the growth allowed by Auto-Expansion.
Usage Alerts	Refer to Controlling File System Usage .
Current	Displays the currently used capacity as a percentage of the total capacity.
Warning	Specifies the warning threshold as a percentage of the total capacity. When the file system utilization crosses this threshold, Titan records an Information event in the event log. For example, if the capacity is set to 4 TB and the warning threshold to 75%, the system records a Warning alert in the event log when 3 TB of the file system has been used.
Severe	Specifies the severe threshold as a percentage of the total capacity. When the file system utilization crosses this threshold, Titan records a Warning event in the event log.
Do not expand above Severe limit	When selected, it prevents the live File System from growing beyond the severe threshold. This effectively reserves the remaining space for use by snapshots .

Check/Fix - Status Since Reboot	Displays whether the file system has been checked and displays its status since its last reboot: • File System fixed. • File System checked. • File System fix was aborted by the user. • File System check was aborted by the user. • Could not find the directory tree to fix. • Could not find the directory tree to check. • File System is being fixed. • File System is being checked. • File System has not been fixed since reboot. • File System has not been checked since reboot. • File System fix failed. • File System check failed. • File System checking does not cease after failing initially.

Recovering Silicon File Systems

Some system failures may result in a file system requiring manual recovery before it can be mounted. Performing **recovery** will roll the file system back to its last **checkpoint** and **replay** any data in NVRAM. In extreme cases, it may be necessary to perform a **forced recovery**, which will discard the contents of NVRAM before mounting the file system.

If a File System displays "Requires Recovery" in the status field:

BLUE ARC

?

 Help

i

 About

Logout

 Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > Silicon File Systems

Silicon File Systems

Label	Total	Used (%)	Used	Free	Ops / sec (average)	Status	EVS	
☐ vol0	393.34 GB	1%	2.92 GB	390.41 GB	0	Mounted	EVS01	details
☐ vol1	393.34 GB					RequiresRecovery	EVS02	details
☐ vol2	393.34 GB	1%	2.40 GB	390.94 GB	0	Mounted	EVS03	details
☐ vol3	393.34 GB					RequiresRecovery	EVS04	details
☐ vol4	393.34 GB	1%	2.40 GB	390.94 GB	0	Mounted	EVS05	details
☐ vol5	393.34 GB	1%	2.44 GB	390.89 GB	0	Mounted	EVS06	details
☐ vol6	393.34 GB	1%	2.40 GB	390.94 GB	0	Mounted	EVS07	details
☐ vol7	393.34 GB	1%	2.44 GB	390.89 GB	0	Mounted	EVS07	details

[Check All](#) | [Clear All](#)

Actions:

mount

unmount

format

create

expand

delete

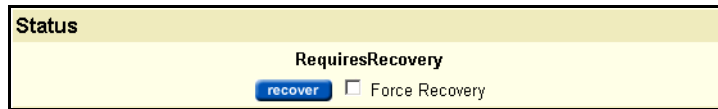
[Reset the Ops / Sec on All File Systems](#)

Shortcuts:

[System Drives](#)

[Quotas by File System](#)

1. Click **details** to access the details page for the relevant file system.



2. Click **recover**. This will initiate the file system recovery. Refresh the page and refer to the file system Status to check the progress of the recovery operation.
3. If this does not recover the file system, choose from the following options:
 - If the file system is part of a cluster, migrate the EVS to which the file system is bound to the other Cluster Node. Then, re-issue the recover request. This is sometimes necessary if only the partner node in the cluster has the current available data in NVRAM necessary to replay write transactions to the file system following the last checkpoint. For more details on migrating EVS, refer to [Migrating an EVS between Cluster Nodes](#).
 - If the first option fails, or if the contents of NVRAM are not required, then check **Force Recovery**, and then click **recover** to execute a file system recovery without replaying the contents of NVRAM.



Caution: Issuing a forced file system recovery will discard the contents of NVRAM, data which may have already been acknowledged to the client. Forced Recovery should only be done at the recommendation of BlueArc Global Services.

WORM File Systems

Titan supports Write Once Read Many (WORM) file systems. WORM file systems are widely used to store crucial company data in an unalterable state for a specific duration. WORM file systems can be used to ensure that a company's data retention policies comply with government regulations.



Note: A license is required to use WORM file systems. Contact BlueArc to purchase a WORM license.

WORM Characteristics

Network clients can access files on a WORM file system in the same way they access other files. But once marked as WORM, that particular file is "locked down". WORM files cannot be modified, renamed, deleted, or have their permissions or ownership changed. These restrictions apply to all users including the owner, Domain Administrators, and 'root'. Once marked, a file remains a WORM file until its retention date has elapsed. Files not marked as WORM can be accessed and used just as any normal file.

Titan supports two types of WORM file systems: lax and strict.

- Lax WORM file systems can be reformatted and so should only be used for testing purposes. Should a lax WORM file system need to be deleted, it must first be reformatted as a non-WORM file system.
- Strict WORM file systems cannot be deleted or reformatted and should be used once strict compliance measures are ready to be deployed.

Creating a WORM file system

Designating a file system as WORM is done when a file system is created. For more information, see ["To Create a Silicon File System"](#).

Any existing non-WORM file system can be reformatted as a WORM file system. Reformatting a file system to use a different file system type, must be done at the CLI. For detailed information on this process, run `man format` at the CLI.

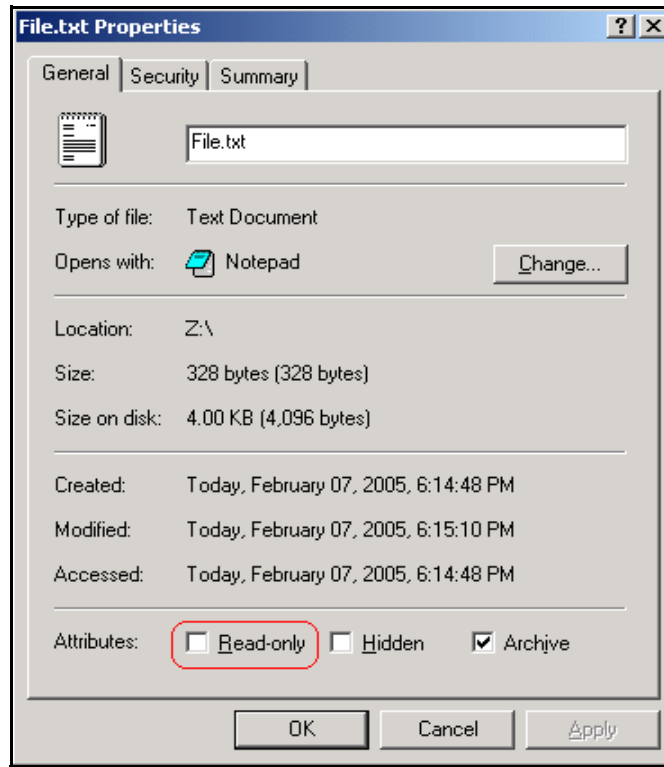
Retention Date

Before marking a file as WORM, designate its retention date. To configure the retention date, set the file's "last access time" to a specific time in the future. The "last access time" can be set using the Unix command 'touch', e.g. `touch -a MMDDhhmm[YY] ./filename`. Should the retention date be less than or equal to the current time, the retention date will never expire.

After a file is marked as WORM, file permissions cannot be altered until the file reaches its retention date. Once a WORM file reaches its retention date, its permissions can be changed to allow read-write access. When write access is granted, the file can be deleted. However, the contents of the file will still remain unavailable for modification.

Marking a file as WORM

Once the retention date has been set, a file can be marked as WORM. To mark a file as WORM, configure the permissions of the file as read-only. To do this from a Unix client, remove the write attribute permissions. From a Windows client, mark the file as read-only through the file's properties.



Controlling File System Usage

Titan can monitor space allocation on a File System and trigger alerts when certain pre-set thresholds are reached. It is also possible to prevent users from creating more files when one of these thresholds has been reached. Alternatively, the File System can be expanded online. File system space is consumed for two different reasons:

- Network users are adding files or increasing the size of existing files. The space taken up by user files is referred to as the *live File System*.
- [Snapshots](#), which provide consistent File System images at specific points in time, are growing in space. Snapshots are not full copies of the live File System, but rather track changes in the File System. As a result, they grow in size whenever files that existed when the snapshot was taken are modified or deleted.



Note: Deleting files from the live File System may increase the space taken up by snapshots, so that no disk space is actually reclaimed as a result of the delete operation. The only sure way to reclaim space taken up by snapshots is to delete the oldest snapshot.

Titan tracks space taken up by:

- The live File System
- Snapshots

- Both of the above

For all of these, it is possible to configure both a warning and a severe threshold. Although settings will be different from system to system, the following should work in most cases:

	Warning	Severe
Live File System	70%	90%
Snapshots	20%	25%
Entire File System	90%	95%

When the storage space occupied by the volume crosses the warning threshold, a **Warning** event is recorded in the [event log](#). If the Entire File System Warning threshold has been exceeded, the space bar used to indicate disk usage turns yellow. When the space reaches or crosses the severe threshold, a **Severe** event is recorded and alerts are generated. If the Entire File System Severe threshold has been exceeded, the space bar used to indicate disk usage turns amber.



In the absence of auto-expansion, the growth of the live file system can be contained to prevent it from crossing the severe threshold. This effectively reserves the remaining space for use by snapshots.



Note: To track and control space the number of files in the live file system, configure quotas for users and groups or create Virtual Volumes.

Monitoring File System Load

Titan’s performance can be measured by how many operations per second (ops/sec) it is performing. Through the Web UI, a graphic representation of the number of ops/sec it is performing can be viewed. For details on displaying or downloading these statistics, see [Server and File System Load \(Ops per second\)](#).

Setting Usage Quotas

Disk usage can be controlled and monitored by applying quotas, which can prevent network users from consuming more disk space (or creating more files) than allowed. Titan supports the following types of quotas:

- **User and group quotas.** Creating user and group quotas can help monitor and control disk usage for individual users or groups of users.
- **Virtual Volume quotas.** Creating [Virtual Volumes](#) can be useful to monitor and control disk usage on a per-directory basis. With Virtual Volumes, directory tree usage can be managed independently of users or groups. In addition, user and group quotas can be created within the Virtual Volume.



Note: In this section, the terms ‘user’ and ‘group’ are used to indicate NFS or CIFS users and groups.

Understanding Quotas

Quotas track the number and total size of all files. When these reach specified thresholds, emails are sent to alert the list of contacts associated with the File System and, optionally, Quota Threshold Exceeded [events](#) are logged. Operations that would take the user or group beyond the configured limit can be disallowed by setting *hard limits*.



Note: When both Usage and File Count limits are defined, Titan will enforce whichever is the first quota to be reached.

Quota Thresholds

The configuration settings defining the restrictions a Quota places on the disk usage are called thresholds, and are described in the following table:

	Space Usage	Number of Files
Limit	The total size of all the files should not exceed this value.	The total number of files should not exceed this value.
Hard Limit	Titan will block any operation which may cause a Hard Limit to be exceeded. If a ‘soft’ limit is exceeded, an alert will be issued, but the operation will be allowed.	
Warning	When the total size of all the files reaches this value, a Warning alert is issued.	When the total number of files reaches this value, a Warning alert is issued.

Severe	When the total size of all the files reaches this value, a Severe alert is issued.	When the total number of files reaches this value, a Severe alert is issued.
Reset	Alerts for Quotas are <i>hysteresis</i> based, so that alerts are <i>disabled</i> once a certain threshold is crossed and an alert is issued. No other alerts are issued until a <i>reset</i> level (threshold) is crossed, after space (or a number of files) is recovered on disk. This means that the server does not continually issue alerts stating that a threshold has been crossed. Quota alerting is <i>re-enabled</i> once the used space (or number of files) drops a certain amount below the threshold. The default value for this reset is 5% of the limit.	

Important information about Quota Thresholds:

- While quotas keep track of used disk space and number of files, neither file system metadata nor snapshot files count towards the quota limits.
- File sizes are computed based on the number of File System blocks used up. For example, with a 32 KB File System block size, a 55 KB file will get reported as 64 KB.
- Files with multiple hard links are included once only. A symbolic link adds the size of the symbolic link file to a quota and not the size of the file to which it links.

Explicit, Default and File Systems Quotas

There are two types of File System Quotas:

1. Explicit User/Group Quotas

A quota can be explicitly created to impose restrictions on an individual user or group, defining a unique set of thresholds.

2. Default User/Group Quotas

Quotas can be set automatically for all users and groups that do not have explicit quotas. This is done by defining a set of thresholds ('Quota Defaults'), which will be used to create a quota automatically when a file is created or modified.

User Quota Defaults are a set of thresholds used to create a quota for a user the first time that user saves a file in the File System.

Group Quota Defaults are a set of thresholds used to create a quota for a group the first time a user in that group saves a file in the File System.

Initially, these Quota Defaults are set to zero (i.e. 'not set'). When activity occurs in the File System, although it is tracked, no quotas are created. Quota Defaults are defined by setting at least one threshold to a non-zero value. Default Quotas will then be automatically created. As soon as a set of Quota Defaults is defined in this way, a User or Group Quota (as appropriate) will be created for the owner of the directory at the root of the file system.

Managing Usage Quotas

From the **Storage Management** page, click **Quotas by File System**.

BLUE ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management | Home > Storage Management > Silicon File Systems > Quotas by File System

Quotas by File System

EVS / File System: EVS02 / All File Systems [change...](#)

Filter

Filter Quota Type: All Types

where User/Group Account matches:

and space used: more than 0 MB [filter](#)

quotas 1-3 of 3 : Page: 1

▲ User/Group Account	File System	Quota Type	Created By	Usage Limit	Space Used	Space Used (%)	File Count Limit	File Count	File Count (%)	
☐ root	vol1	User	Automatically Created	500.00 MB	130.46 MB	26	0	53	n/a	details
☐ SHIRE\Administrator	vol1	User	Automatically Created	500.00 MB	362.22 MB	72	0	5,239	n/a	details
☐ 10001	vol1	User	User Defined	50.00 MB	0.00 Bytes	0	0	0	n/a	details

[Check all](#) | [Clear all](#) quotas 1-3 of 3 : Page: 1

Actions: [add](#) [delete](#) [Delete All Quotas](#) | [User Defaults](#) [Group Defaults](#) [Modify Email Contacts](#)

Section	Description	
EVS/File System	The EVS and the File System to which these quotas apply. To select a different EVS/File System, click change...	
Filter	Since many quotas can exist on a single File System, it may be easier to find the quota information required by filtering the list. This can be done by specifying certain parameters in the Filter section (as follows) and clicking filter :	
	Filter Types	Select from All Types (default), Users or Groups
	where name matches	Enter a name to be matched. The wildcard character * may be used.
	and space used	Select from more than or less than . Enter an amount of space used: zero will include all quotas. Select units of space used from MB, GB, or %.

Page Description	Only 20 quotas are displayed on a page. The pages of quotas can be navigated by using the links at the top and bottom of the list. Hovering a mouse over the links will display 'screen tips' describing their use (e.g. Go to first page , Jump back , etc.).
Actions	Delete a quota (or selection of quotas) by ticking the checkboxes next to the quotas' names, and clicking delete . Add a quota or view the details of a quota.

The Quota list itself shows the following characteristics of each quota:

Column	Description
User/Group Account	A quota name may consist of a CIFS domain and user or group name, such as 'bb\Smith' or 'bb\my_group' (where 'bb' is a domain, 'Smith' is a user and 'my_group' is a group). An NFS user or group such as 'richardb' or 'finance' (where <i>richardb</i> is an NFS user and <i>finance</i> is an NFS group).
File systems	The File System on which the quota applies
Quota Type	The type of source of File System activity. Possible values are User or Group .
Created By	The way in which the quota was created. Possible values are Automatically Created (created using a Quota Default) or User Defined (in which the thresholds were set uniquely for that one quota).
Usage Limit	The overall limit set for the total size of all files in the File System owned by the target of the quota.
Space Used	The total space in the File System used by all the files owned by the quota target.
Space Used (%)	The space used as a percentage of the Usage Limit
File Count Limit	The overall limit set for the total number of files in the File System owned by the target of the quota.
File Count	The total number of files (in the File System) owned by the target of the quota.
File Count (%)	The file count as a percentage of the File Count Limit.

To Set User Defaults

From the **Quotas by File System** page, click **User Defaults**.

BLUE-ARC TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > [Silicon File Systems](#) > [Quotas by File System](#) > File System Quota Defaults

User File System Quota Defaults

EVS / File System: EVS01 / vol0 [change...](#)

Usage	File Count
Limit: GB	Limit:
Hard Limit: ☒	Hard Limit: ☒
Warning: 75 %	Warning: %
Severe: 95 %	Severe: %

[OK](#) [clear defaults](#) [cancel](#)

Item/Field	Description
EVS/File System	The EVS and File System on which the User File System Quota applies.
Usage	
Limit	The amount of space to enable in Bytes, KB, MB, GB or TB.
Hard Limit	If this box is ticked, the amount of space specified in the <i>Limit</i> field may not be exceeded.
Warning	Enter the percentage of the Limit at which a Warning alert will be sent.
Severe	Enter the percentage of the Limit at which a Severe alert will be sent.
File Count	
Limit	Enter a maximum number of files to enable for this quota.
Hard Limit	If this box is ticked, the number of files specified in the Limit field may not be exceeded.
Warning	Enter the percentage of the Limit at which a Warning alert will be sent.
Severe	Enter the percentage of the Limit at which a Severe alert will be sent.

If a zero (or nothing) is left in a field, that entry will be regarded as being ‘not set’. For example, a File Count Limit of zero means that a quota created will not have a limit on the number of files it may contain, and the Warning and Severe thresholds will also be ‘not set’.

When all necessary fields have been completed, click **OK**.

If the User Defaults are to be cleared, so that no further Default Quotas will be created in the File System, click **clear defaults**. This will convert any existing "Automatically Created" User Quotas into "User Defined" User Quotas.

To Set Group Defaults

From the **Quotas by File System** page, click **Group Defaults**.

The details of this screen are the same as those detailed in the previous table for users, except for the checkbox labeled *Automatically create quotas for Domain Users*. The purpose of this option is to allow the creation of default quotas for the group "Domain Users". By default every NT user belongs to the group "Domain Users", so enabling this option effectively includes every NT user in the quota, (unless each user's primary group has been explicitly set).

To Add a File System Quota

From the **Quotas by File Systems** page, click **add**.

BLUE ARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Storage Management | Home > Storage Management > Silicon File Systems > Quotas by File System > Add File System Quota

Add File System Quota

EVS / File System: EVS01 / vol0 [change...](#)

Quota Type: ☒ User User Account i.e. domain\user (CIFS) or user (NFS)
☐ Group Group Account i.e. domain\group (CIFS) or group (NFS)

Usage	File Count
Limit: Bytes	Limit:
Hard Limit: ☒	Hard Limit: ☒
Warning: 75 %	Warning: 75 %
Severe: 85 %	Severe: 85 %

[OK](#) [cancel](#)

The table below describes the fields on this screen:

Item/Field	Description

EVS/File System	The EVS and the File System on which to add this quota. To select a different EVS/File System, click change...
Quota Type	The type of source of File System activity. Possible values are User or Group.
User/Group Account	A User/Group Account name may consist of: A CIFS domain and user or group name, such as 'bb\Smith' or 'bb\my_group' (where 'bb' is a domain, 'Smith' is a user and 'my_group' is a group). An NFS user or group such as 'richardb' or 'finance' (where richardb is an NFS user and finance is an NFS group).
Usage	
Limit	The amount of space to enable in Bytes, KB, MB, GB or TB.
Hard Limit	If this box is ticked, the amount of space specified in the Limit field may not be exceeded.
Warning	Enter the percentage of the Limit at which a Warning alert will be sent.
Severe	Enter the percentage of the Limit at which a Severe alert will be sent.
File Count	
Limit	Enter a maximum number of files to enable for this quota.
Hard Limit	If this box is ticked, the number of files specified in the Limit field may not be exceeded.
Warning	Enter the percentage of the Limit at which a Warning alert will be sent.
Severe	Enter the percentage of the Limit at which a Severe alert will be sent.

If a zero (or nothing) is left in a field, that entry will be regarded as being 'not set'. For example, a File Count Limit of zero means that a quota created will not have a limit on the number of files it may contain, and the Warning and Severe thresholds will also be 'not set'.

When all necessary fields have been completed, click **OK**.

To Modify a File System Quota

From the **Quotas by File Systems** page, click **details** at the end of the row of the quota to be modified.

The limits and thresholds are defined in the previous section, [To Add a File System Quota](#).

When all necessary fields have been completed, click **OK**.

To Delete a File System Quota

On the **Quotas by File Systems** page, select the quota or quotas to be deleted by using the checkboxes to the left of the quotas' names. Then, click **delete**.

Using Virtual Volumes

Virtual Volumes are a simple way to manage directory trees in a File System. Titan treats the directory that is at the 'root' of the Virtual Volume, together with all its sub-directories, as a self-contained File System. The Virtual Volume will keep track of its usage of space and number of files, to provide a way of monitoring File System usage. This tracking allows restrictions, called quotas, to be imposed on the levels of disk space usage as well as the total number of files. Quotas can be imposed for the entire Virtual Volume, including individual users, and groups of users. Where many users or groups will have access to a Virtual Volume, a set of Quota Defaults can be defined. In the absence of *explicit* user or group quotas, *default* quotas apply.



Note: In this section, the terms 'user' and 'group' are used to indicate NFS or CIFS users and groups.

Understanding Virtual Volumes

Virtual Volumes are directory trees that are treated as self-contained file systems and used to monitor and control File System usage.



Note: When it comes to 'moving' or 'hard linking' files, Virtual Volumes behave the same as real File System volumes. Moving or linking files across different Virtual Volumes returns a 'cross volume link' error. For a move operation, most CIFS or NFS clients will suppress this error and, instead, will copy the files to the target location and delete the original ones.

Virtual Volumes have the following characteristics:

- **Name:** a name or 'label' by which the Virtual Volume is identified. This will often be the same as a CIFS share or NFS export rooted at the Virtual Volume's root directory.
- **File System:** the File System in which the Virtual Volume is created
- **Path:** the directory at the 'root' of the Virtual Volume
- **Email Contacts:** a list of Email addresses, to which information and alerts about Virtual Volume activity are sent. The list can also be used to send emails to individual users.

Important information about Virtual Volumes:

- While quotas keep track of used disk space and number of files, neither File System metadata nor snapshot files count towards the quota limits.
- Files with multiple hard links are included only once. A symbolic link adds the size of the symbolic link file to a quota and not the size of the file to which it links.

Managing Virtual Volumes

From the **Storage Management** page, click **Virtual Volumes & Quotas**.

BLUE-ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > Virtual Volumes

Virtual Volumes

EVS / File System
EVS01 / All File Systems [change...](#)

Filter
Name:
Path: [filter](#)

vivols 1-2 of 2 : Page: 1

▼ Name	File System	Contact	Path	
☐ EngVIVol	vol0	administrator@bluearc.com	/engineering	details
☐ SalesVIVol	vol0	salesadmin@bluearc.com	/sales	details

[Check All](#) | [Clear All](#)

vivols 1-2 of 2 : Page: 1

Actions: [delete](#) [add](#) | [View Quotas](#) | [Download All Quotas](#)

Item / Field	Description
Filter	Filters can be defined to reduce the number of Virtual Volumes displayed on the page. Filters can be configured based on the name or the path.
EVS/File System	The name of the selected EVS and File System.
Name	The name of the Virtual Volume .
File System	The name of the file system.
Contact	The contact email address to which information and alerts about Virtual Volume activity are sent.
Path	The directory on which the Virtual Volume has been created.

The Virtual Volumes for the selected file system are listed. These Virtual Volumes may be sorted in *ascending* or *descending* order in any column, or a different set of Virtual Volumes may be viewed by clicking **change...** and selecting a different file system.

Only the first contact email address is shown: to view the full set of contacts, or otherwise modify the Virtual Volume, click **details**. Other actions available from this page are **add**, **view quotas**, **delete** and **Download All Quotas**. These are described in the following sections.

To Add a Virtual Volume

From the **Storage Management** page, click **Virtual Volumes & Quotas**. Then, click **add**.

BLUE ARC

?

 Help

i

 About

Sign Out

Titan - 192.0.2.2

Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > [Virtual Volumes](#) > Add Virtual Volume

Add Virtual Volume

EVS / File System: EVS01 / lab01

change...

Virtual Volume Name:

☐ Create a CIFS Share with the same name as the Virtual Volume

☐ Create a NFS Export with the same name as the Virtual Volume

☐ Allow exports to overlap

Path: /

browse...

☒ Create path if it does not exist

Email Contacts:

Add

X

OK

cancel

The following table describes the fields on this screen:

Item/Fields	Description
EVS/File System	The EVS and the file system to which to add this Virtual Volume. If the Virtual Volume is to be added to a different EVS/File System, click change... and select the EVS/File System required.
Virtual Volume Name	The name may consist of up to 128 characters. The following characters are not supported: ?*=[] ; : / , < > \
Create a CIFS Share or NFS Export with the same name as the Virtual Volume	To access the Virtual Volume through CIFS or NFS, it may be convenient to have a share or export with the same name as the Virtual Volume. Ticking this checkbox will ensure such a share or export, if it does not exist, is created.  Note: The CIFS Share or NFS Export name may not exceed 80 characters.

Allow exports to overlap	As overlapping exports can potentially expose security loopholes, the condition can be tested for and, if found, the export creation can be denied. To prevent this check and allow overlapping NFS exports to be created, check the box labeled ' Allow exports to overlap '.
Path	A directory in the file system that will be the 'root' of the Virtual Volume. Example: /company/sales. All sub-directories of this path will be a part of this Virtual Volume. Once created, the path may not be changed. Virtual Volumes cannot be created at the root of the file system ("/"). They must be applied to the directories in the file system. Virtual Volumes can only be created and assigned to empty directories. To create a Virtual Volume on a directory that contains data, first move the data out of the directory. Once empty, the Virtual Volume can be created and assigned to that directory. Then, the data can be moved back in.

Email Contacts	It may be important for Email alerts, about Virtual Volume usage, to be sent to a number of contacts in the enterprise. Enter each Email address in the box, and click the add arrow to append it to the list below. If an address is entered in error, select it in the list, and click the X button to delete it. Email recipients can be configured to receive email notification when usage thresholds have been reached. Explicitly defined email recipients (e.g. admin@company.com) will receive email notification any time a defined threshold has been reached. Titan can also send emails to all user accounts when their corresponding user quota has been reached. This is done by adding an email address beginning with * to the Email Contacts list (e.g. *@company.com). For instance, if *@company.com has been added to the Email Contacts list and a user quota for 'ntdomain\user' has been created, then if 'ntdomain\user' has reached the defined usage threshold, an email alert will be sent to user@company.com. The same applies to N FS users that have been defined in Titan's NFS User list. The Email list is limited to a maximum of 512 characters total.  Note: If no email contacts are specified for the Virtual Volume, Titan generates events for quota warnings. To generate events in addition to Email alerts, issue the 'quota-event--on' command from Titan's command line interface.

Click **OK** to create the Virtual Volume. The Virtual Volume may be subsequently modified by clicking **details** in the Virtual Volume list page.

To Modify a Virtual Volume

1. From the **Storage Management** page, click **Virtual Volumes**. Then, click **details** next to the Virtual Volume to be modified.
2. Edit the values as required, and click **OK** to submit the changes.

To Delete a Virtual Volume

1. From the **Storage Management** page, click **Virtual Volumes**.
2. Select the Virtual Volume(s) to be deleted. If all Virtual Volumes are to be deleted, click **Check All**.

3. On clicking **delete**, a warning will displayed asking for confirmation that this action is definitely required. Click **OK** to continue deleting the Virtual Volumes.



Note: A Virtual Volume can only be removed from a directory when the directory is empty. To delete a Virtual Volume which is assigned to a directory that contains data, first remove the data, then delete the Virtual Volume.

Managing Quotas on Virtual Volumes

There are three types of quotas that are maintained for each Virtual Volume:

1. Explicit User/Group Quotas

A quota can be explicitly created to impose restrictions on an individual user or group, defining a unique set of thresholds.

2. Default User/Group Quotas

Quotas can be set automatically for all users and groups that do not have explicit quotas. This is done by defining a set of thresholds ('Quota Defaults'), which will be used to create a quota automatically when a file is created or modified in the Virtual Volume.

Default quotas for Virtual Volumes operate in the same manner as those defined for File Systems. User (Group) Quota Defaults are a set of thresholds used to create a quota for a user (group) the first time that user (group) saves a file in the file system.

Initially, these Quota Defaults are set to zero (i.e. 'not set'). When activity occurs in the Virtual Volume, although it is tracked, no quotas are created. Quota Defaults are defined by setting at least one threshold to a non-zero value. Default Quotas will then be automatically created. As soon as a set of Quota Defaults is defined in this way, a User or Group Quota (as appropriate) will be created for the owner of the directory at the root of the Virtual Volume.

3. Virtual Volume Quotas

A Virtual Volume Quota tracks the space used within a specific directory on the file system. A quota can be explicitly created to define a set of thresholds restricting all operations in the Virtual Volume, irrespective of which user or group initiated them.

Quotas track the number and total size of all files. When these reach specified thresholds, emails are sent to alert the list of contacts associated with the File System and, optionally, Quota Threshold Exceeded [events](#) are logged. Operations that would take the user or group beyond the configured limit can be disallowed by setting *hard limits*.



Note: When both Usage and File Count limits are defined, Titan will enforce whichever is the first quota to be reached.

To View / Modify Virtual Volume Quotas

- 1. From the **Storage Management** page, click **Virtual Volumes & Quotas**.
- 2. From the **Virtual Volumes** page, select the Virtual Volume for which the Quotas are to be viewed.
- 3. Click **View Quotas**.

BLUE ARC

?

Help

i

About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: ON

Storage Management

 | [Home](#) > [Storage Management](#) > [Virtual Volumes](#) > Quotas

Quotas

Virtual Volume

EVS / File System: EVS01 / vol0

Virtual Volume Name: EngVIVol

Path: /engineering

Filter

Filter Quota Type: All Types

where User/Group Account matches:

and space used: more than MB

filter

quotas 1-1 of 1 : Page: 1

User/Group Account	Quota Type	Created By	Usage Limit	Space Used	Space Used (%)	File Count Limit	File Count	File Count (%)	
☐	Virtual Volume User Defined		250.00 GB	0.00 Bytes	0	0	1	n/a	details

Check all

 |

Clear all

quotas 1-1 of 1 : Page: 1

Actions:

delete

add

User Defaults

Group Defaults

Download Quotas for this Virtual Volume

The table below describes the sections of this screen:

Section	Description
Virtual Volume	Identifies the Virtual Volume to which these quotas apply: EVS/File System: the EVS and File System on which the Virtual Volume resides. Virtual Volume Name: the name of the Virtual Volume. Path: the directory on which the Virtual Volume has been created.
Filter	Since many user/group quotas can exist on a Virtual Volume, Titan provides a way to filter the list.
	Filter Types Select from All Types (default), Users or Groups
	where name matches Enter a name to be matched. The wildcard character * may be used.
	and space used Select from more than or less than . Enter an amount of space used: zero will include all quotas. Select units of space used: MB, GB, or %.

Only 20 quotas are displayed on a page. The pages of quotas can be navigated by using the links at the top and bottom of the list. Hovering a mouse over the links will display 'screen tips' describing their use (e.g. **Go to first page**, **Jump back**, etc.).

The Quota list itself shows the following characteristics of each quota:

Column	Description
User/Group Account (also known as the target)	A quota name may consist of: A CIFS domain and user or group name, such as 'bb\Smith' or 'bb\my_group' (where 'bb' is a domain, 'Smith' is a user and 'my_group' is a group). An NFS user or group such as 'richardb' or 'finance' (where richardb is an NFS user and finance is an NFS group). A name may be empty (if the quota is a Virtual Volume Quota - see below) or '0' (if the quota was created for the owner of the directory at the root of the Virtual Volume).
Quota Type	The type of source of Virtual Volume activity. Possible values are User , Group , or Virtual Volume . The last target type is anyone initiating activity in the entire Virtual Volume, and only one quota with this target type may exist on each Virtual Volume.
Created By	The way in which the quota was created. Possible values are Automatically Created (created using a Quota Default) or User Defined (in which the quota was set uniquely for that one quota).

Usage Limit	The overall limit set for the total size of all files in the Virtual Volume owned by the target of the quota.
Space Used	The total space in the Virtual Volume being used by all the files owned by the target of the quota.
Space Used (%)	The Space Used as a percentage of the Usage Limit
File Count Limit	The overall limit set for the total number of files in the Virtual Volume owned by the target of the quota.
File Count	The total number of files (in the Virtual Volume) owned by the target of the quota.
File Count (%)	The File Count as a percentage of File Count Limit.

To Set User Defaults

On the **Quotas** page, click **User Quota Defaults**.

BLUE ARC

?

Help

i

About

Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

Storage Management | [Home](#) > [Storage Management](#) > [Virtual Volumes](#) > [Quotas](#) > Quota Defaults

User Quota Defaults

EVS / File System: EVS01 /
Virtual Volume Name: wvol0

Usage

Limit: Bytes

Hard Limit: ☒

Warning: %

Severe: %

File Count

Limit:

Hard Limit: ☒

Warning: %

Severe: %

OK

clear defaults

cancel

Item/Field	Description
EVS/File System	The EVS and File System on which the User Quota applies.

Virtual Volume Name	The name of the Virtual Volume on which the User Quota is assigned.
Usage	
Limit	The amount of space to enable in Bytes, KB, MB, GB or TB.
Hard Limit	If this box is ticked, the amount of space specified in the <i>Limit</i> field may not be exceeded.
Warning	Enter the percentage of the Limit at which a Warning alert will be sent.
Critical	Enter the percentage of the Limit at which a Critical alert will be sent.
File Count	
Limit	Enter a maximum number of files to enable for this quota.
Hard Limit	If this box is ticked, the number of files specified in the Limit field may not be exceeded.
Warning	Enter the percentage of the Limit at which a Warning alert will be sent.
Severe	Enter the percentage of the Limit at which a Critical alert will be sent.

On the **User Quota Defaults** page, an EVS/File System and a Virtual Volume Name will be displayed for each User Quota.

If a zero (or nothing) is left in a field, that entry will be considered **not set**. For example, a File Count Limit of zero means that a quota created will not have a limit on the number of files it may contain. The Warning and Severe thresholds will also be considered **not set**.

After defining the User Default Quota, click **OK**.

To clear User Quota defaults, click **clear defaults**. The **clear defaults** button prevents additional User Quota defaults from being created in the Virtual Volume. It also converts any existing "Automatically Created" User Quotas into "User Defined" User Quotas.

To Set Group Defaults

On the **Quotas** page, click **Group Quota Defaults**.

The details of this screen are the same as in the previous table for users, except for the **Automatically create quotas for Domain Users** checkbox. This option allows default quotas for the group "Domain Users" to be created. By default, every NT user belongs to the group "Domain Users" which includes every NT user in the quota unless each user's primary group has been explicitly set.

To Add, View, and Modify a Quota

From the **Quotas** page, click **add**.

BLUE ARC

?

 Help

i

 About

Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

Storage Management | [Home](#) > [Storage Management](#) > [Virtual Volumes](#) > [Quotas](#) > Add Quota

Add Quota

EVS / File System: EVS01 / vol0

Virtual Volume Name: vol0

Quota Type: ☒ User User Account i.e. domain\user (CIFS) or user (NFS)
☐ Group Group Account i.e. domain\group (CIFS) or group (NFS)
☐ Virtual Volume

Usage

Limit: Bytes

Hard Limit: ☒

Warning: 75 %

Severe: 85 %

File Count

Limit:

Hard Limit: ☒

Warning: 75 %

Severe: 85 %

OK

cancel

Item /Field	Description
EVS/File System	The Name of the EVS and the File System on which the quota has been added.
Virtual Volume Name	The Name of the Virtual Volume on which the quota has been added.
Quota Type	The type of source of Virtual Volume activity. Possible values are User , Group , or Virtual Volume .
User/Group Account	A User/Group Account name may consist of: A CIFS domain and user or group name, such as 'bb\Smith' or 'bb\my_group' (where 'bb' is a domain, 'Smith' is a user and 'my_group' is a group). An NFS user or group such as 'richardb' or 'finance' (where richardb is an NFS user and finance is an NFS group). If Virtual Volume has been selected as the Quota Target Type, it will not be possible to specify a Quota Name.

Usage	
Limit	The amount of space to enable in Bytes, KB, MB, GB or TB.
Hard Limit	If this box is ticked, the amount of space specified in the Limit field may not be exceeded.
Warning	Enter the percentage of the Limit at which a Warning alert will be sent.
Severe	Enter the percentage of the Limit at which a Severe alert will be sent.
File Count	
Limit	Enter a maximum number of files to enable for this quota.
Hard Limit	If this box is ticked, the number of files specified in the Limit field may not be exceeded.
Warning	Enter the percentage of the Limit at which a Warning alert will be sent.
Severe	Enter the percentage of the Limit at which a Severe alert will be sent.

If a zero (or nothing) is left in a field, that Item/Field will be regarded as being 'not set'. For example, a File Count Limit of zero means that a Quota created will not have a limit on the number of files it may contain, and the Warning and Severe thresholds will also be 'not set'. When all necessary fields have been completed, click **OK**.

To Delete a Quota

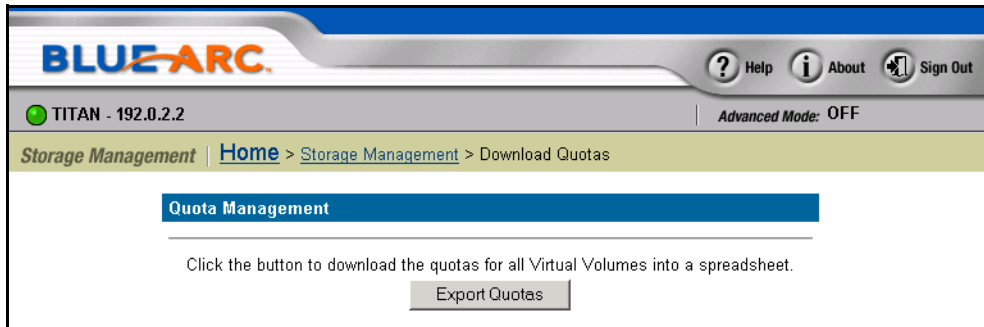
On the **Quotas** page, select the quota or quotas to be deleted using the checkboxes to the left of the quotas' names. Then, click **delete**.



Note: Certain quotas (e.g. Default Quotas for the owner of the Virtual Volume's root directory) will automatically reappear in the quota list after they are deleted.

To Export Quotas for all Virtual Volumes

1. From the **Storage Management** page, select **Virtual Volumes** and from the page displayed, click **Download All Quotas**.



2. Click **Export Quotas**, and a *File* dialog box will be displayed; so that a comma separated value (.csv) file can be specified and saved.

To Export Quotas for a Specific Virtual Volume

In the Quota list page for the chosen Virtual Volume, click **Download Quotas for this Virtual Volume**.

Retrieving Quota Usage through rquotad

This section details how **rquotad** can be used with Titan.

The Quota Command

The *quota* command can be issued on a Unix workstation to retrieve information on the disk quota usage of the user or group based on their ID. The retrieved report contains the block count, file count, quota limits on both, and information based on other options chosen with the command. Refer to the client's "man" pages for accurate command syntax since implementation varies with each client OS.

Implementing rquota on Titan

The rquota protocol runs on Open-Network Remote Procedure Calls (ONC RPC) and retrieves quota information from the rquotad service on an NFS server such as Titan. It is used in conjunction with NFS, since NFS does not implement quotas.

The rquotad service has been implemented for use on Titan. It functions as a read-only protocol and is only responsible for procuring information about user and group quotas. Quotas can be created, deleted, or modified through the Storage Management section of the UI.

Titan reports only the Hard Limit quota information through rquotad. As mentioned in the previous sections, there can be three different quota limitations defined:

1. User and group quotas limiting the individual user or group's space and file count usage within a Virtual Volume.
2. User and group quotas limiting the individual user or group's space and file count usage in the entire file system.
3. Virtual Volume quotas limiting the space and file count used by a Virtual Volume as a whole.

rquotad can be configured to report quota information based on two criteria:

1. Matching—Searching for a quota in a defined order.
2. Restrictive—Choosing the quota with the most constraints on the user or group.

Matching Configuration

Using the Matching option, **rquotad** follows a specific order to find a match for relevant quota information:

- ❑ First, if **rquotad** is returning quota information about a user, it will return the user's individual quota within the Virtual Volume if it exists,
- ❑ Otherwise, it will move to the user's file system quota if that exists.
- ❑ If no file system quota exists for the user, then it will move to the Virtual Volume quota.

In this manner, **rquotad** keeps checking until a quota is found for the specified user or group. Once the quota is found, **rquotad** returns the quota information.



Note: rquotad can report quota usage information on explicitly defined user, group, and Virtual Volume quotas, as well as automatically created quotas based on the defined default quota. The automatically created quota will be used if an explicit quota has not been defined.

Restrictive Configuration

If this option is chosen, rquotad picks the first quota among the applicable quotas that the user risks exceeding. This enables the user to determine the amount of data that can be safely recorded against this quota before reaching its Hard Limit. This is the default configuration option for rquotad on Titan.



Note: The restrictive configuration option returns quota information combined from the quota that most restricts usage and the quota that most restricts file count.

For example:

If the user quota allowed 10K of data and 100 files to be added, and the Virtual Volume quota allowed 100K of data and 10 files to be added, rquotad would return information stating that 10K of data and 10 files could be added. Similarly, if the user quota is 10K of data of which 5K is used, and the Virtual Volume quota is 100K of data of which 99K is used, rquotad would return information stating that 1K of data could be added.

The console command "rquotad" is provided to change between the two options, and also to disable access to quota information. For information on how to configure rquotad, please refer to the Command Line Reference.



Note: If access is disabled, all requests to rquotad will be rejected with an error code of "EPERM".

BlueArc Data Migrator

Titan supports multiple storage technologies, with different performance and cost characteristics. In order to take full advantage of [Multi-Tiered Storage \(MTS\)](#), data should be organized using a tiered hierarchy of importance and need. BlueArc Data Migrator makes this possible.

There are five key reasons to use Data Migrator with Titan:

- **Cost-Efficient Storage Utilization** - Titan's Data Migrator best utilizes the MTS architecture by maximizing space utilization on higher performing and higher cost fibre channel based primary storage. Using Data Migrator, newer or routinely accessed data can be retained on primary storage, while older, less-accessed, or less performance critical data can be migrated to cost-efficient, but slower ATA based secondary storage.
- **Easy Configuration** - Titan deploys Data Migrator using logical policies that use simple building blocks of rules to classify files as available for migration. Titan has provisions for establishing rules and pre-conditions where a file's size, type (for example, all .mp3 files), access history, etc. can be used as criteria for migrating files.
- **Discreet Migration** - Migrations from primary to secondary storage are handled as automated background tasks with minimal impact on server performance. While migrations are in progress, all data can continue to be accessed as normal.
- **Client Transparency** - Files migrated off of primary storage are replaced by a link. While using only 1 KB of space, the link otherwise looks and functions identically to the original file. When the link is accessed, the file contents are transparently retrieved from its location on secondary storage. To the client workstation, it is indistinguishable whether the file's contents have been migrated or still remain on primary storage.
- **Maximizing Storage Efficiency through Migration Reports** - Migration reports are created at the end of each migration cycle. Studying these reports, file usage and space consumption patterns become more apparent. Furthermore, migration possibilities can be gauged by scheduling Data Migrator [test runs](#) where reports can be produced without an actual migration taking place. Armed with this knowledge, more aggressive migration policies can be created to free up more primary space, maximizing the efficiency and functionality of BlueArc's Multi-Tiered Storage system.



Note: A license is required to use Data Migrator. Contact BlueArc to purchase a Data Migrator license.

Configuring Data Migrator

In order to use Data Migrator on Titan, the following need to be defined:

- ❑ Data migration paths from primary to secondary storage.
- ❑ Data migration rules, which determine the properties of files that will be migrated.
- ❑ Data migration policies, which define rules to apply to specific data migration paths based on the available free space on the source file system or Virtual Volume.
- ❑ Schedules in which the frequency with which the data migration policies will be run.

Data Migration Paths

Before Data Migrator can be used, the primary and secondary storage must first be identified. Primary storage, typically fibre channel disk arrays, will be the *source* for data migrations. Secondary storage, typically ATA disk arrays, will be the *target* for data migrations. Once Data Migrator has been configured, data will be migrated from primary to secondary storage based on the rules defined, freeing up space and extending the capacity of the primary storage.



Note: No attempt should be made to directly access data migrated to Secondary Storage. The organizational structure of migrated data on Secondary Storage does not mirror that of Primary Storage. Furthermore, accessing files directly on Secondary Storage may alter access and modification times of the files, resulting in unexpected results when performing backups.

Data Migration Paths are used to define the relationship between primary and secondary storage. The primary and secondary storage defined in the Data Migration Paths must be owned by the same [EVS](#).



Caution: If either the primary or the secondary File System is moved to a different EVS, access to migrated files will be lost.

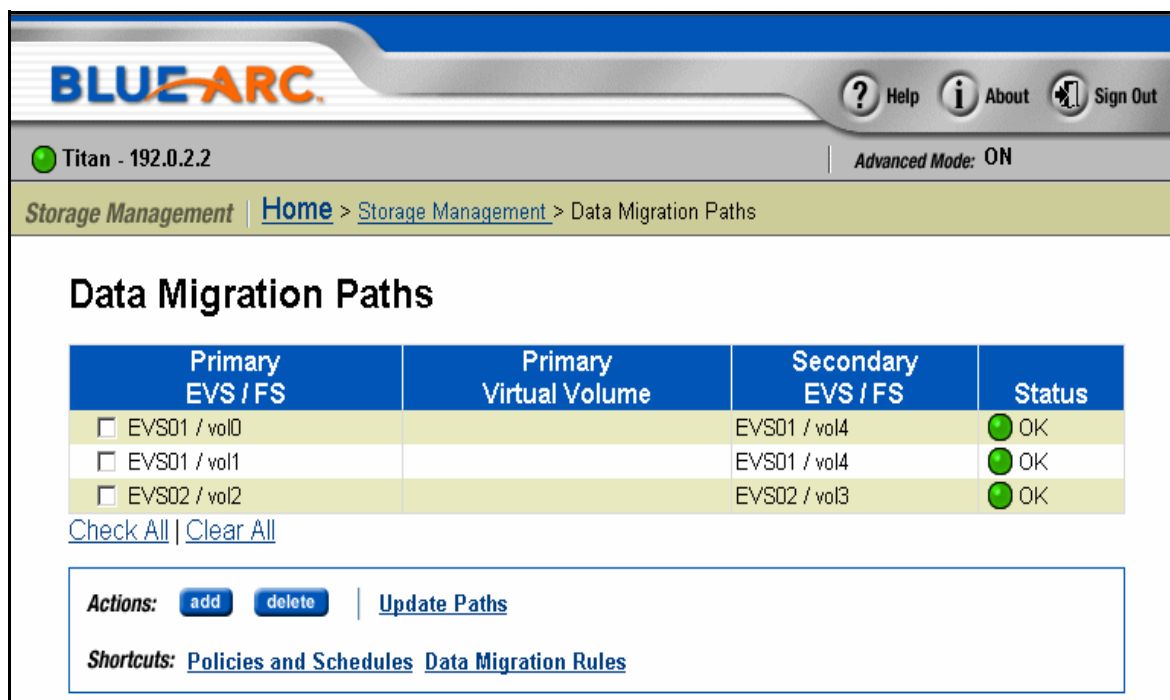
When defining Data Migration Paths, a file system or Virtual Volume can be specified as the primary storage. If a file system is selected as primary storage, then the entire file system, including all Virtual Volumes, are included as a part of the Data Migration Policy. To create individual policies per Virtual Volume, each Virtual Volume should be assigned a specific Migration Path.



Note: Once a Migration Path has been assigned to a Virtual Volume, a subsequent Migration Path cannot be created to its hosting file system. Also, once a Migration Path has been assigned to a file system, subsequent Migration Paths cannot be created from Virtual Volumes hosted by that file system.

To configure Data Migration Paths

1. From the **Home** page, click **Storage Management**. Then, click **Data Migration Paths**.



BLUEARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Storage Management | [Home](#) > [Storage Management](#) > Data Migration Paths

Data Migration Paths

Primary EVS / FS	Primary Virtual Volume	Secondary EVS / FS	Status
☐ EVS01 / vol0		EVS01 / vol4	OK
☐ EVS01 / vol1		EVS01 / vol4	OK
☐ EVS02 / vol2		EVS02 / vol3	OK

[Check All](#) | [Clear All](#)

Actions: [add](#) [delete](#) | [Update Paths](#)

Shortcuts: [Policies and Schedules](#) [Data Migration Rules](#)

The fields on this screen are described in the table below:

Item / Field	Description
Primary EVS/File System	Displays the EVS and file system from which data will be migrated.
Primary Virtual Volume	If a Virtual Volume has been selected as primary storage, this will display the name of the Virtual Volume from which data will be migrated.
Secondary EVS/File System	Displays the EVS and file system on secondary storage to which the data will be migrated.
Status	The status of the Data Migration Path. The status should always be OK. If it displays something else, migrated files may be inaccessible.

Update Paths	Use this to refresh the status of the Data Migration Path. This may be necessary after a reverse migration is completed to indicate that the Migration Path has no dependencies on secondary storage and can be deleted.

2. Click **add**.
The **Add Data Migration Path** page appears.



?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > [Data Migration Paths](#) > Add Data Migration Path

Add Data Migration Path

Primary EVS / File System: EVS05 / vol3

change...

File Accessed Time Update Interval 4 hours

☒ Virtual Volume: engVVol

Destination File System: vol4

OK

cancel

Item/Field	Description
Primary EVS/File System	Select the EVS and file system on primary storage. This defines the source for the Data Migration Path. To change the currently selected EVS and file system, click change...
File Accessed Time Update Interval	Displays the currently configured Accessed Time Update Interval. This defines the maximum time that will elapse between when a file is accessed and when the “last accessed time” field on the file will be updated. This value is important to note if migrations based on an aggressive file access policy will be defined. Refer to the <i>Titan Command Line Reference</i> for details on configuring this value.
Virtual Volume	By default, the entire file system is included in the data migration policies. To configure migrations on a Virtual Volume basis, check the box and select the Virtual Volume to be used as the primary storage for this Data Migration Path.

Destination File System	Select the destination file system from the drop-down menu. The file system selected should be on secondary storage.

Click **OK** to create the Data Migration Path as configured.

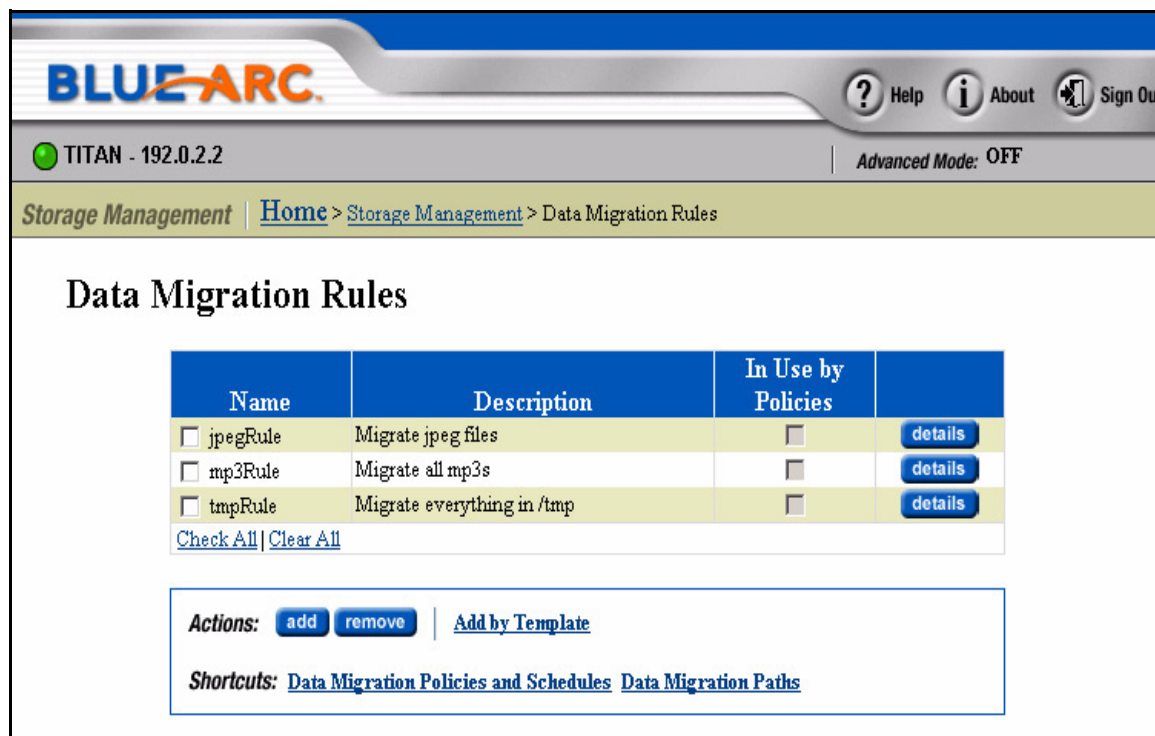
Click **cancel** to discard the current selection and return to the **Data Migration Paths** page.

Data Migration Rules

The **Data Migration Rules** page lists all existing rules, and allows new rules to be created. Data migration rules are used in conjunction with Data Migration Paths to set up Data Migration Policies.

To view the Data Migration Rules

From the **Home** page, click **Storage Management**. Then, click **Data Migration Rules**.



BLUE ARC ? Help i About Sign Out

TITAN - 192.0.2.2 | Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > Data Migration Rules

Data Migration Rules

Name	Description	In Use by Policies	
☐ jpegRule	Migrate jpeg files	☐	details
☐ mp3Rule	Migrate all mp3s	☐	details
☐ tmpRule	Migrate everything in /tmp	☐	details

[Check All](#) | [Clear All](#)

Actions: [add](#) [remove](#) | [Add by Template](#)

Shortcuts: [Data Migration Policies and Schedules](#) [Data Migration Paths](#)

The fields on this screen are described in the table below:

Item / Field	Description
Name	Displays the name given to the Rule. This is assigned when the Rule is created, and is used to identify the Rule when creating or configuring policies.

Description	A description given to the rule to help in identifying the criteria to be applied.
In Use by Policies	A check in the box indicates that the rule is being used by one or more policies.

Click the **details** button next to the rule to view the complete details regarding it.
Select a Rule and click **remove** to delete it.



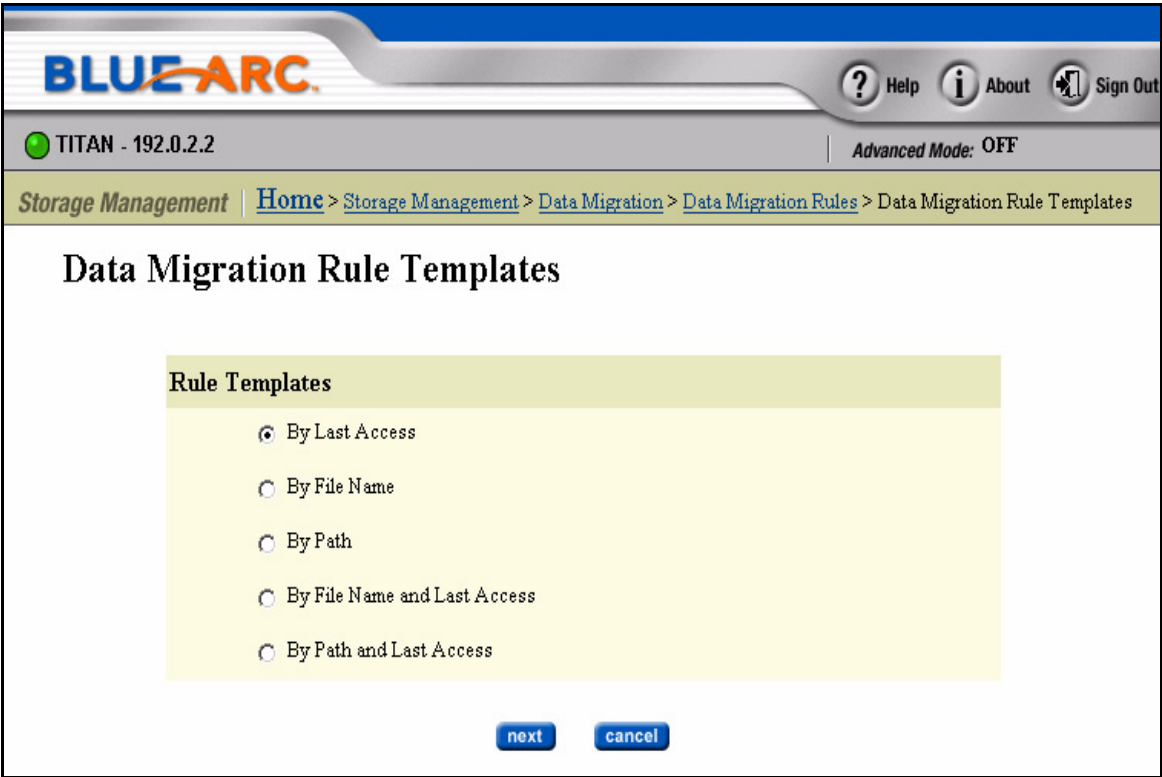
Caution: Care should be used when modifying rules in use by existing policies as it may result in unintentional changes to existing policies.

Two methods exist to create Data Migration Rules. The first is to use predefined templates to create simple rules. The second is to create custom rules that will exactly define the criteria by which files will be migrated.

To add a Data Migration Rule by Template

- 1. From the **Home** page, click **Storage Management**. Then, click **Data Migration Rules**.
- 2. Click **Add by Template**.

The **Data Migration Rule Templates** page appears with the choice of a number of **Rule Templates**.



3. Select one of the **Rules Templates** and click **Next**, to further define it.

Rule Template	Description
By Last Access	This template can be used to migrate all files that have remained inactive for a certain period of time.
By File Name	This template can be used to migrate all files with the same extension, i.e. .mp3, .html, or .doc.
By Path	This template can be used to map a path to a certain directory and migrate all files under it.
By File Name and Last Access	This template can be used to migrate files of a certain type (file extension) that have remained inactive for a certain period of time.
By Path and Last Access	This template can be used to migrate all files under a certain directory that have remained inactive for a certain period of time.

Rules Template: By Last Access

Item /Field	Description
Name	Enter a name for the new rule.
Description	Enter a description of what the rule does.
Include Criteria	To specify the maximum number of days a file can be inactive before being migrated to a secondary file system, do the following: 1. Select inactive over from the drop-down menu. 2. Enter numerically the threshold number in the days field. The drop-down menu also has an option for selecting the opposite of the above scenario, i.e. choose active within to only select files that have been active within the specified number of days. Refer to Rule Syntax for important information about rule criteria.

Rules Template: By File Name

Item /Field	Description
Name	Enter a name for the new rule.
Description	Enter a description of what the rule does.
Case sensitive pattern checks	Select the checkbox if the rule checking must be case sensitive.
Include Criteria	To specify the type of files (based on their file extension) to be migrated to a secondary file system, do the following: 1. Select include from the drop-down menu. 2. Enter the file extension in the all files named field. More than one file type can be named in this field separated by commas. For instance, *.jpg, *.bmp, *.zip. The drop-down menu also has an option for selecting the opposite of the above scenario, i.e. choose exclude to select all files that are not mp3. Refer to Rule Syntax for important information about rule criteria.

Rules Template: By Path

Item /Field	Description
Name	Enter a name for the new rule.
Description	Enter a description of what the rule does.
Case sensitive pattern checks	Select the checkbox if the rule checking must be case sensitive.
Include Criteria	To specify the path to the files under a certain directory so that they can be migrated to a secondary file system, do the following: 1. Select include from the drop-down menu. 2. Enter the directory file path in the all files in the path field. The drop-down menu also has an option for selecting the opposite of the above scenario, i.e. choose exclude to select all files that are not in the path. Refer to Rule Syntax for important information about rule criteria.

Rules Template: By Last Access Time and File Name

Item/Field	Description
Name	Enter a name for the new rule.
Description	Enter a description of what the rule does.
Case sensitive pattern checks	Select the checkbox if the rule checking must be case sensitive.
Include Criteria	To specify the type of inactive files to be migrated to a secondary file system, do the following: 1. Enter the file extension in the All files named field. 2. Enter numerically the threshold number in the All files not accessed within____days field. Refer to Rule Syntax for important information about rule criteria.

Rules Template: By Path and Last Access

Item/Field	Description
Name	Enter a name for the new rule.
Description	Enter a description of what the rule does.
Case sensitive pattern checks	Select the checkbox if the rule checking must be case sensitive.
Include Criteria	To migrate inactive files from a certain directory to a secondary file system, do the following: 1. Enter the directory file path in the All files in the path field. 2. Enter numerically the threshold number in the All files not accessed within____days field. Refer to Rule Syntax for important information about rule criteria.

Click **OK** to add the rule template and return to the **Data Migration Rules** page.

Click **cancel** to clear the screen and return to the **Data Migration Rules** page.

To add a Custom Data Migration Rule

From the **Data Migration Rules** page, click **add**. The **Add Data Migration Rule** page appears.

BLUEARC

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management

 | [Home](#) > [Storage Management](#) > [Data Migration Rules](#) > Add Data Migration Rule

Add Data Migration Rule

Rule

Name:

Description:

☒ Case-sensitive pattern checks

Rule Definition

OK

cancel

Item / Field	Description
Name	Enter a name for the new rule.
Description	Enter a description of what the rule does.
Case sensitive pattern checks	Select the checkbox if the rule checking must be case sensitive.
Rule Definition	Insert the syntax for the Data Migration Rule. Refer to Rule Syntax for important information about rule criteria.

Click **OK** to create the rule as configured and return to the **Data Migration Rules** page.

Click **cancel** to discard the configuration and return to the **Data Migration Rules** page.

Rule Syntax

Data migration rules can be built with a series of INCLUDE and EXCLUDE statements, each containing a number of expressions identifying the criteria for data migration.

Remember the following guidelines when building rules:

- ❑ Each rule must have at least one INCLUDE or EXCLUDE statement. If a rule consists only of EXCLUDE statements, it is implied that everything on primary storage should be migrated except what has been specifically excluded.
- ❑ The asterisk "*" can be used as a wildcard character to qualify PATH and FILENAME values. When used in a PATH value, "*" is only treated as a wildcard if it appears at the end of a value, e.g. <PATH /tmp*>. In a FILENAME value, **a single** "*" can appear either at the beginning or the end of the value. Multiple instances of the wildcard character are not supported and additional instances in a value definition will be treated as literal characters.
- ❑ Expressions identifying the migration criteria should be enclosed in brackets. All criteria contain a **keyword**, defining the condition for data migration, followed by a single value or a list of values. e.g. <FILENAME *.doc>
- ❑ When using several INCLUDE or EXCLUDE statements they are evaluated using top-down ordering. For more information on ordering, refer to the [Statement Order](#) section below.
- ❑ Parentheses are used to group the criteria in INCLUDE and EXCLUDE statements, e.g. INCLUDE (<PATH /Temp/*>).
- ❑ When defining multiple values in a FILENAME list, use a comma to separate values, e.g. INCLUDE (<FILENAME *.mp3, *.wav, *.wmv>)
- ❑ The following characters need to be *escaped* with a backslash (\) when used as a part of PATH or FILENAME values: \ (backslash), > (greater than), and , (comma).

For example:

```
INCLUDE (<FILENAME *a\, b> OR <PATH /tmp/\>ab>)
```

- ❑ The forward slash (/) is used as a path separator. As such, it must not be used in a FILENAME list.
- ❑ If a PATH element is not specified in a statement, the statement will apply to the entire file system or Virtual Volume defined in the Data Migration Path.
- ❑ Quotation marks (") are not allowed around a FILENAME or PATH list.

Keywords

The following table describes the keywords and their related values that can be used to build rule statements. Each keyword can be defined in the rule with an INCLUDE or EXCLUDE statement to indicate how the keyword values are to be applied.

Keyword	Value(s)
FILENAME	The names and types of files that will be a part of the rule. If multiple names are being specified, they should be separated by commas. FILENAME values may start or end with a "*" wildcard character to indicate all files starting/finishing with specific characters. Usage: FILENAME will often be used with an INCLUDE statement to ensure that non-essential files are migrated to secondary storage. It can also be used with an EXCLUDE statement to prevent specific important data sets from being migrated. For example: (<FILENAME *.mp3, *.txt, filename*>)
PATH	Specifies literal paths in which the rule should apply. Values must be full paths, starting with "/". If multiple paths are to be specified, they should be separated by commas. PATH values may end with a "*" wildcard character to indicate all subdirectories under the specified path. Usage: When used in an INCLUDE statement, PATH allows specific directories to be included for migration. This is useful when migrating less-critical directories such as temp or home directories. When used in an EXCLUDE statement, directories can be excluded from migration, leaving all the files within on primary storage. For example: (<PATH /temp/*, /home*, /other/dir*>)
FILE_SIZE_OVER	Identifies file in the rule whose sizes fall <i>above</i> a specific size threshold. The value is appended to the keyword and is defined by the threshold size in B, KB, MB, or GB. Usage: This will likely be used with INCLUDE statements to ensure files of very large sizes are migrated to secondary storage. For example: <FILE_SIZE_OVER 4GB>

FILE_SIZE_UNDER	Identifies file in the rule whose sizes fall <i>below</i> a specific size threshold. The value is appended to the keyword and is defined by the threshold size in B, KB, MB, or GB. Usage: This will usually be used in an EXCLUDE statement to ensure that very small files are not migrated en masse. Migrating small files which take up little space provide minimal value in extending the efficiency of primary storage. For example: <FILE_SIZE_UNDER 10KB>
INACTIVE_OVER	Identifies files that <i>have not</i> been <i>accessed</i> within a specific number of days. A file's last access time is updated whenever the file is read or modified. The value is appended to the keyword and is defined by the number of days of inactivity. Usage: Used primarily in INCLUDE statements to ensure that older, less frequently used files are migrated. For example: <INACTIVE_OVER 21>
ACTIVE_WITHIN	Identifies files that <i>have</i> been <i>accessed</i> within a specific number of days. A file's last access time is updated whenever the file is read or modified. The value is appended to the keyword and is defined by the number of days in which the activity has occurred. Usage: Used primarily in EXCLUDE statements to prevent actively used files from being migrated. For example: <ACTIVE_WITHIN 30>

UNCHANGED_OVER	Identifies files that <i>have not</i> been <i>modified</i> within a specific number of days. A file's modification time is updated whenever the file's contents have been changed. The value is appended to the keyword and is defined by the number of days of inactivity. Usage: Used primarily in INCLUDE statements to ensure that older, less frequently used files are migrated. For example: <UNCHANGED_OVER 14>
CHANGED_SINCE	Identifies files that <i>have been modified</i> within a specific number of days. A file's last access time is updated whenever the file's contents have been changed. The value is appended to the keyword and is defined by the number of days of inactivity. Usage: Used primarily in EXCLUDE statements to prevent actively used files from being migrated. For example: <CHANGED_SINCE 7>

Understanding AND & OR Usage in Rules

When **AND** is used in the middle of two rule statements, the rule expects both statements to be satisfied.

For example:

```
INCLUDE (<FILENAME *.mp3> AND <FILE_SIZE_OVER 5GB>)
```

In the above rule there are two conditions:

1. All files with the .mp3 name may be included.
2. All files that are 5 GB or bigger in size may be included.

The importance of the AND here is that a 5 GB .pdf file cannot be included because it does not satisfy the first condition. A 4 GB .mp3 file cannot be included because it does not satisfy the second condition. So, only .mp3 files that are 5 GB or more in size satisfy both conditions of the rule and will be included for migration.

If **OR** was used instead of AND in the above example:

```
INCLUDE (<FILENAME *.mp3> OR <FILE_SIZE_OVER 5GB>)
```

The same two conditions apply:

1. All files with the .mp3 name must be included.
2. All files that are 5 GB or bigger in size must be included.

But the rule is specifying entirely different criteria. Where AND is used to satisfy two different conditions, OR is used to include *either* of the two conditions. Therefore, any .mp3 file, or any file that is over 5 GB in size will be included under this rule. A 4 GB .mp3 file will be included since it at least satisfies the first condition. A 5 GB .pdf file will be included because it at least satisfies the second condition.

The best way to remember AND & OR usage in building rules is that AND stands for *satisfying both conditions in a rule*, and OR stands for *satisfying either condition in a rule*.

Interpreting Rules

The following table shows a set of rules with explanations. If the syntax looks complicated, break it down to cause and effect statements of **IF** and **THEN** to understand it.

Rule	Description
INCLUDE (<FILENAME *.doc>)	IF the file is a .doc file, THEN include it for migration.
EXCLUDE (<PATH /mydir/*>)	IF the path is the /mydir directory THEN exclude it from migration.
INCLUDE (<FILENAME *.prj> AND <FILE_SIZE_OVER 4GB>)	IF the file is a .prj file AND the .prj file is over 4 GB in size, THEN include it for migration.
INCLUDE (<PATH /unimportant>)	IF the path is the /unimportant directory THEN include it for migration.
EXCLUDE (<FILE_SIZE_OVER 100GB>) INCLUDE (<FILE_SIZE_OVER 12GB>)	IF files are larger than 12 GB but smaller than 100GB in size, THEN include them for migration.

Statement Order

When defining statements within a rule, the order in which the statements appear define the way in which the rule will be carried out. Statements are evaluated top-down, starting with the first statement defined. As a result, it is usually best practice to specify EXCLUDE statements at the top of the rule. The following example will illustrate this:

Rule Scenario A

```
INCLUDE (<PATH /Temp> AND <FILENAME *.mp3>)  
EXCLUDE (<ACTIVE_WITHIN 14>)  
EXCLUDE (<FILE_SIZE_UNDER 2MB>)
```

The above rule is interpreted as:

IF path name includes /Temp AND filename is *.mp3 THEN MIGRATE.

IF file is active less than 14 days AND less than 2MB in size THEN EXCLUDE.

In scenario A, all the .mp3 files under Temp will be migrated based on the first INCLUDE statement. Statements 2 and 3 are disregarded since they follow the more inclusive INCLUDE statement that has already added what rules 2 and 3 are trying to exclude.

Rule Scenario B

If the same rules were ordered differently:

```
EXCLUDE (<FILE_SIZE_UNDER 2MB>)  
EXCLUDE (<ACTIVE_WITHIN 14>)  
INCLUDE (<PATH /Temp> AND <FILENAME *.mp3>)
```

The above rule is interpreted as:

IF file is under 2 MB in size AND active less than 14 days THEN EXCLUDE.

IF path name includes /Temp AND filename is *.mp3 THEN MIGRATE.

While Scenario A includes all .mp3 files from the folder /Temp, in Scenario B, only the .mp3 files greater than 2 MB in size that have been inactive for over 14 days will be migrated. Looking at the different migration results of scenarios A and B, the importance in statement ordering should be evident.



Tip: To create rules that are specific and detailed:

1. Start with a simple INCLUDE statement that is specific about what should be migrated, such as:

```
INCLUDE (<PATH /Temp> AND <FILENAME *.mp3>)
```

2. Refine the INCLUDE statement by adding exceptions to the rule with restrictive EXCLUDE statements. But add these EXCLUDE statements **above** the INCLUDE, such as:

```
EXCLUDE (<FILE_SIZE_UNDER 2MB>)
```

```
EXCLUDE (<ACTIVE_WITHIN 14>)
```

3. The rule should finally appear this way:

```
EXCLUDE (<FILE_SIZE_UNDER 2MB>)
```

```
EXCLUDE (<ACTIVE_WITHIN 14>)
```

```
INCLUDE (<PATH /Temp> AND <FILENAME *.mp3>)
```

Given the guidelines for creating rules and the assortment of keywords and building blocks for rules shown in the samples above, creating rules for Data Migration should be easier.

Data Migration Policies

Having created both Data Migration Paths and Rules, Data Migration Policies can now be created. Policies assign a rule or set of rules to a specific Data Migration Path. They also define the conditions that initiate data migrations.

To view Data Migration Policies

From the **Home** page, click **Storage Management**. Then, click **Data Migration**.

BLUEARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management Home > Storage Management > Data Migration

Data Migration

Migration Policies

Name	Server / EVS	Primary File System	Secondary File System	Rule	
☐ policy_mp3c	TITAN / EVS01	vol2 / fs2vivoll	vol3	rule_mp3	details
☐ policy_mp3	TITAN / EVS01	vol1 / fs1vivoll	vol3	rule_mp3	details
☐ policy_path1	TITAN / EVS01	vol1 / fs1vivoll	vol3	rule_path1	details

[Check All](#) | [Clear All](#)

Actions: [add](#) [remove](#)

Shortcuts: [Data Migration Rules](#) [Data Migration Paths](#) [NDMP Configuration](#)

Scheduled Migrations

Policy Name / Schedule ID	Server / EVS	Next Run	Interval	
☐ policy_mp3 / 54	TITAN / EVS01	None.	ONCE	details
☐ policy_mp3 / 55	TITAN / EVS01	None.	ONCE	details
☐ policy_mp3c / 56	TITAN / EVS01	None.	ONCE	details
☐ policy_path1 / 57	TITAN / EVS01	None.	ONCE	details

[Check All](#) | [Clear All](#)

Actions: [add](#) [remove](#) | [Abort Migration\(s\)](#)

Shortcuts: [View Completed Migrations](#)

The fields on this screen are described in the table below:

Item / Field	Description
Name	Displays the name given to the Data Migration Policy.

Server/EVS	Displays the primary EVS from which the migration originates.
Primary File System	Displays the primary file system or Virtual Volume that will be migrated.
Secondary File System	Displays the secondary file system, to which all data will be migrated.
Rule	Displays the rules which may be triggered in this migration policy.

Click the **details** button next to the policy to view the complete details regarding it.

To add a Data Migration Policy

- From the **Data Migration Policies** page, click **add**. The **Add Data Migration Policy** screen appears.

BLUE ARC

?

Help

i

About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > [Data Migration](#) > Add Data Migration Policy

Add Data Migration Policy

Policy Identification

Name:

Migration Path

Primary EVS / File System:

EVS05 / vol3

Virtual Volume:

engVIVol

Secondary File System:

vol4

change...

(For more Primary/Secondary options,
see [Data Migration Paths](#))

Pre-Conditions

x

remove

Apply

Old_files

if source's free space falls below < % add

if other conditions are not met

apply

cancel

Item	Description
Name	Give the new policy a name.

Primary EVS/File System	The EVS and file system name on primary storage; the migration source.
Virtual Volume	If a Virtual Volume has been selected as primary storage, then the Virtual Volume name will be displayed.
Secondary File System	The file system on secondary storage that will host the migrated data; the migration target. To change the selected Migration Path, click change...: ☐ A list of paths will appear in the Select a Path screen. ☐ Select a path for the migration. Then, click OK.
Pre-Conditions	Rules that have been defined with specific threshold limits are displayed here. This list of rules define the set of conditions by which file migrations are triggered. To remove a Pre-Condition, select it and click remove .
Apply	Select a rule from the drop-down menu to be applied if either of the following conditions are met: ☐ If primary's Free Space falls below ____% (set the percentage level for the condition) ☐ If other conditions are not met Once defined, add the rule and threshold to the list of Pre-Conditions by clicking add.

2. Define the desired Data Migration Policy.

3. When finished, click **apply**.

Click **cancel** to clear the screen and return to the **Data Migration** screen.

Using Pre-Conditions

When a Migration Policy is **scheduled** to run, the percentage of available free space in the Policy's Primary Storage will be evaluated. Based on this free space, a single rule may be triggered and used to define the data set subject to migration. Migrations of data from Primary Storage will then be applied based on the statements in the rule that was triggered. Only migrations based on a single rule will be engaged during any particular migration.

When defining these pre-conditions, it is recommended to tier them with exceeding aggressiveness. In other words, it may be desirable to migrate .mp3 files and the contents of the directory /tmp regardless of the available free space. Then, if free space on Primary Storage is reduced to less than 50%, then also migrate all files not accessed within the last sixty days. Finally, if the available free space is reduced to less than 15%, then also migrate the contents of users home directories.

The following will illustrate this scenario:

Rules

Rule 1	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>)
Rule 2	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>)
	INCLUDE (<INACTIVE_OVER 60>)
Rule 3	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>)
	INCLUDE (<INACTIVE_OVER 60>)
	INCLUDE (<PATH /home/*>)

Pre-conditions

- Rule 3 if free space is less than 15%.
- Rule 2 if free space is less than 50%.
- Rule 1 if no other condition applies.

When the Migration Policy is scheduled to run, different rules may be triggered based on the available free space on Primary Storage. Remember, that when a Migration Policy has been engaged, only a single rule will be triggered to run.

- For example:
- If free space is at 80%, then Rule 1 will be used.
 - If free space is at 40%, then Rule 2 will be used.
 - If free space is at 10%, then Rule 3 will be used.

When percentage thresholds are specified, they are evaluated based on whole number percentages. This means that if two rules are specified, one that will take effect at 8% of free space and one at 9% of free space, if the file system has 8.5% free space available, then the rule with the 8% pre-condition will apply.



Note: If the Primary Storage defined in the Migration Path is a Virtual Volume, free space will be based on the limit defined by the [Virtual Volume Quota](#). If a Virtual Volume quota has not been defined, then the free space available will be based on the free space of the file system hosting the Virtual Volume.

Data Migration Schedules

Once a Data Migration Policy has been defined, it must then be scheduled to run. How often to run the Policy will be entirely dependent on the Rules defined. For example:

- ❑ A policy with a single Rule to migrate all .mp3 files may be scheduled to run once every month.
- ❑ Another policy, used to archive a working project directory once the project is complete, may be scheduled as a Once Only Schedule.
- ❑ Other policies which migrate based on various Pre-conditions, which are triggered on available free space, may be scheduled to run every week.

When planning Migration Schedules, it is recommended to schedule them to run during off-peak times such as in the evenings or over the weekends.

Once a data migration has begun, additional data migrations for the same policy cannot be started until the current one has completed. However, it is possible to start multiple concurrent data migrations, each for its own policy.

To view Scheduled Migrations

From the **Home** page, click **Storage Management**. Then, click **Data Migration**.

BLUEARC

?

Help

i

About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > Data Migration

Data Migration

Migration Policies

Name	Server / EVS	Primary File System	Secondary File System	Rule	
☐ policy_mp3c	TITAN / EVS01	vol2 / fs2vivoll	vol3	rule_mp3	details
☐ policy_mp3	TITAN / EVS01	vol1 / fs1vivoll	vol3	rule_mp3	details
☐ policy_path1	TITAN / EVS01	vol1 / fs1vivoll	vol3	rule_path1	details

[Check All](#) | [Clear All](#)

Actions:

[add](#) [remove](#)

Shortcuts:

[Data Migration Rules](#) [Data Migration Paths](#) [NDMP Configuration](#)

Scheduled Migrations

Policy Name / Schedule ID	Server / EVS	Next Run	Interval	
☐ policy_mp3 / 54	TITAN / EVS01	None.	ONCE	details
☐ policy_mp3 / 55	TITAN / EVS01	None.	ONCE	details
☐ policy_mp3c / 56	TITAN / EVS01	None.	ONCE	details
☐ policy_path1 / 57	TITAN / EVS01	None.	ONCE	details

[Check All](#) | [Clear All](#)

Actions:

[add](#) [remove](#) | [Abort Migration\(s\)](#)

Shortcuts:

[View Completed Migrations](#)

The fields on this screen are described in the table below:

Item /Field	Description
Policy Name/ Schedule Id	Displays the name given to the Data Migration Policy.
Server/EVS	Displays the primary server and EVS from where the migration is scheduled to originate.
Next Run	Displays the month, date, year and time for the next scheduled data migration run for this policy.
Interval	Displays the frequency at which the data migration has been scheduled to run.

Select a Migration Schedule and click **Abort Migrations** to abort the selected migration. Only in-progress migrations can be aborted.

Click **Add** to add a new schedule from the **Add Data Migration Schedule** page.

Click **Remove** to clear a selected schedule from the list.

To add a Data Migration Schedule

1. From the **Home** page, click **Storage Management**. Then, click **Data Migration**
2. Under **Scheduled Migrations**, click **add** to schedule a new data migration. The **Add Data Migration Schedule** page appears.

BLUE-ARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Storage Management Home > Storage Management > Data Migration > Add Data Migration Schedule

Add Data Migration Schedule

Policy

Migration Policy:

Timing

Time of Initial Run: (24 hour time)

Date of Initial Run:

Current SMU Date and Time: 02/08/2006 18:16

Run Options

Schedule Options

☒ - with respect to the scheduled date and time.

☐ Once Only - at the scheduled date and time.

Report Options

☐ List Migrated Files - once only at the scheduled date and time.

☐ Test Only - once only at the scheduled date and time.

These options only generate reports: no files will be migrated.

The data migration policy needs to be set up before it can be scheduled.

Item	Description
Migration Policy	Select a migration policy from the drop-down menu.
Time of Initial Run	Enter the scheduled run time in a 24 hour setting (i.e. 11:59 PM will be entered as 23:59). The current SMU date and time are provided below for reference.
Date of Initial Run	From the calendar next to the field, select the start date for the policy's initial run. The selected date appears on the field.

Schedule	• When selecting the first option, pick a pre-set rule of: daily, weekly, or monthly from the drop-down menu to be applied at the same time of day as the Initial Run • Selecting Once Only indicates that the policy is scheduled to run only once, the initial run.
Report Options	• Select List Migrated Files to generate a report of all migrated files in the selected Data Migration Path. • Select Test Run to initiate a one-time test run. The files are not migrated under this option, but reports can be generated on these nonetheless, which can provide valuable insights about the validity of using a certain policy and its rules.

3. Click **OK** to add the schedule and return to the **Data Migration** page.
Click **cancel** to clear the screen and return to the **Data Migration** page.

To modify a Data Migration Schedule

Once defined, schedules can be easily modified to meet the changing requirements of the Data Migration Policies. When modifying a schedule, the scheduled date and time, as well as the interval in which the schedule will run can be changed.

1. From the **Data Migration** page, select a schedule to modify.
2. Click **details**.

The screenshot shows the 'Modify Data Migration Schedule' page in the BlueArc Data Migrator web interface. The page has a blue header with the BlueArc logo and navigation links (Help, About, Sign Out). Below the header, a breadcrumb trail shows 'Storage Management > Home > Storage Management > Data Migration > Modify Data Migration Schedule'. The main content area is titled 'Modify Data Migration Schedule' and contains several sections:

- Policy**: A section with a label 'Migration Policy:' and a value 'Unused_Files'.
- Timing**: A section containing:
 - 'Next Run: 02/08/2006 23:59' and 'Current Schedule: 02/08/2006 23:59'.
 - A 'Reschedule' checkbox, which is currently unchecked.
 - Input fields for '(24 hour time)' and '(date)'.
 - 'Current SMU Date and Time: 02/08/2006 18:25'.
- Run Options**: A section containing:
 - Schedule Options**: Two radio buttons. The first is selected and labeled 'weekly' with a dropdown arrow, followed by '- with respect to the scheduled date and time.' The second is labeled 'Once Only - at the scheduled date and time.'
 - Report Options**: Two radio buttons. The first is labeled 'List Migrated Files - once only at the scheduled date and time.' The second is labeled 'Test Only - once only at the scheduled date and time.'
 - A note: 'These options only generate reports: no files will be migrated.'

At the bottom of the form, there is an 'Actions:' section with three buttons: 'OK', 'cancel', and 'run now'.

3. To define a new starting date and time for the selected schedule, click **re-schedule** and enter the new values in the appropriate fields.
4. To change the schedule's interval, configure the schedule to repeat either daily, weekly, or monthly, or configure the schedule to run **Once Only**.
5. To change the Schedule to run a report, click **List Migrated Files** to list all migrated files in the selected Data Migration Path or **Test Only** to generate a report of what files would be migrated if the specified Migration Policy were run.
6. Click **run now** to run the selected Schedule immediately. Or, click **OK** to apply the changes or **cancel** to discard them, and return to the **Data Migration** page.

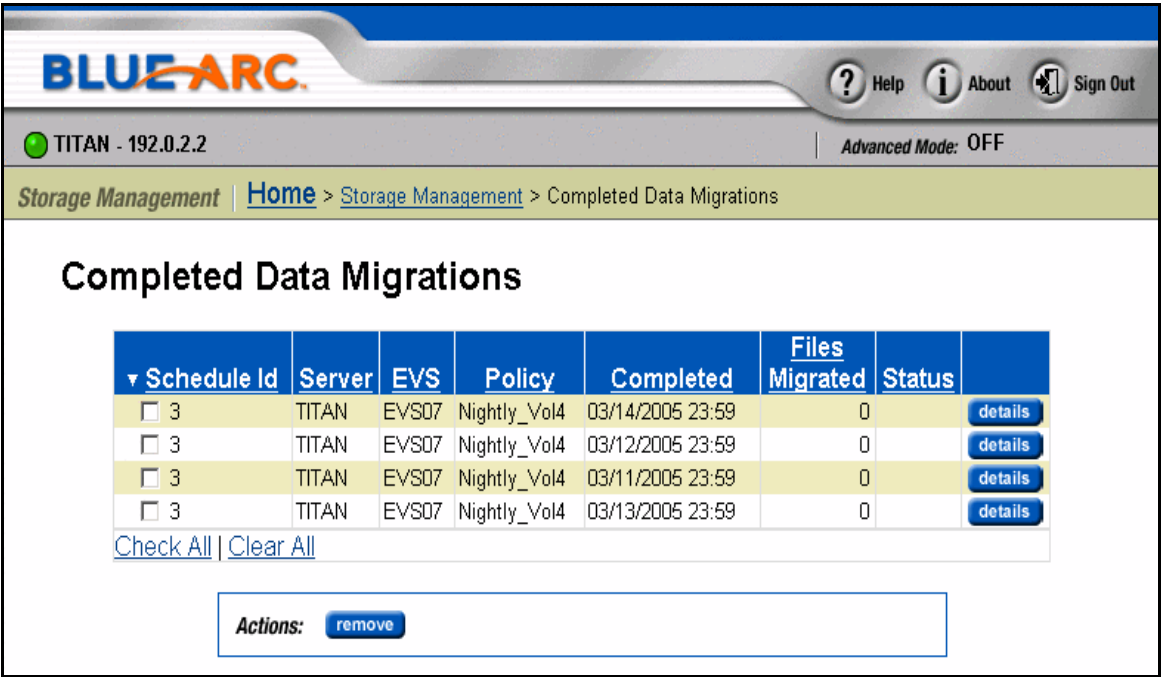
Data Migration Reports

Once a Data Migration Policy has completed, a Data Migration Report is generated that includes a number of reporting details on files migrated, available free space before and after the migration, etc. Reports of the last five scheduled migrations are routinely saved, while the rest are purged. If a schedule is deleted, so are its reports.

These Migration Reports can be saved and printed, and used to study the system's access patterns, file storage tendencies, the efficiency of rules, paths, policies and schedules. By gauging file and space usage statistics of Primary and Secondary Storage, Data Migrator reports can be used to refine a rule or pre-condition. The more precise and aggressive the rule, the better Data Migrator serves the storage system.

To view Completed Migrations

From the **Home** page, click **Storage Management**. Then, click **Completed Data Migrations**.



The following will be displayed:

Item	Description
Schedule ID	Displays the ID number for the completed migration.
Server	Displays the primary file system's server.
EVS	Displays the primary file system's EVS.
Policy	Displays the policy's name.

Completed	Displays the month, date, year and time when the migration was completed.
Files Migrated	Displays the number of files that were migrated.
Status	Displays the status on whether the migration was successfully completed.

Click **details** to view the completed migration report.

Click **remove** to delete one or more completed migrations listed on the page.

To view Data Migration Reports

- 1. From the **Home** page, click **Storage Management**. Then, **Completed Migrations**.
- 2. Select the completed migration of interest and click **details** next to it.

The following page appears:

BLUE ARC

?

Help

i

About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management

Home

Storage Management

Completed Data Migrations

Completed Data Migration Details

Completed Data Migration Details

Report Summary

Migration Policy:

policy_mp3

Schedule ID:

13

Status:

Ok [View Log](#)

Frequency:

ONCE

Start Time:

02/24/2005 15:26

End Time:

02/24/2005 15:26

Duration:

00:00:51

Server / EVS:

TITAN / EVS01

Rule Used:

rule_mp3

Amount Migrated:

102.38 MB

Files Migrated:

[37](#)

Files Excluded:

0

vol1 - Primary File System Statistics

Pre-Migration			Post-Migration			File System	Live File System	Total File System
File System Space Used			File System Space Used			Capacity	Reclaimed	Reclaimed
Live FS	SnapShots	Total Usage	Live FS	SnapShots	Total Usage			
20.11 GB	0.00 Bytes	20.11 GB	20.05 GB	0.00 Bytes	20.05 GB	338.94 GB	65.28 MB (0.02 %)	65.28 MB (0.02 %)
(5.93%)	(0.00%)	(5.93%)	(5.92%)	(0.00%)	(5.92%)			

fs1vivol1 (fs1vivol1) - Primary Virtual Volume Statistics

Pre-Migration	Post-Migration	Virtual Volume
Virtual Volume Space Used	Virtual Volume Space Used	Reclaimed
14.25 GB (4.20 %)	14.15 GB (4.17 %)	102.91 MB (0.03 %)

vol6 - Secondary File System Statistics

Pre-Migration			Post-Migration			File System	Live File System	Total File System
File System Space Used			File System Space Used			Capacity	Consumed	Consumed
Live FS	SnapShots	Total Usage	Live FS	SnapShots	Total Usage			
684.08 GB	0.00 Bytes	684.08 GB	684.21 GB	0.00 Bytes	684.21 GB	689.77 GB	127.47 MB (0.02 %)	127.47 MB (0.02 %)
(99.18%)	(0.00%)	(99.18%)	(99.19%)	(0.00%)	(99.19%)			

- Secondary Virtual Volume Statistics

Pre-Migration	Post-Migration	Virtual Volume
Virtual Volume Space Used	Virtual Volume Space Used	Consumed
0.00 Bytes (0.00 %)	0.00 Bytes (0.00 %)	0.00 Bytes (0.00 %)

Actions:

back

delete

[View Log](#)

[View Files Migrated](#)

[Download Migration Report](#)

The following will be displayed:

Item	Description
Report Summary	
Migration Policy	Displays the completed migration policy's name.
Schedule ID	Displays the migration schedule ID.
Status	Indicates whether the migration was successfully completed.
Frequency	Displays how often the Policy is scheduled to run.
Start Time	Displays the date and time when the migration began.
End Time	Displays the date and time when the migration ended.
Duration	Displays the time taken to complete the migration.
Server/EVS	Displays the EVS on which the Primary and Secondary Storage reside.
Rule	Displays the rule used by the policy.
Amount Migrated	Displays the migrated data amount in GB.
Files Migrated	Displays the number of files that were migrated. If files have been migrated, click this to view a list of the files that were migrated. The list provides details on their path, size, and their start and end times.
Files Excluded	Displays the number of files that should have been migrated but could not. For example, files in use at the time of the migration may not be migrated.
Primary File System Statistics	
Pre-Migration File System Space Used	Details the file system size, space used by snapshots and the total space used before the migration.
Post-Migration File System Space Used	Details the file system size, space used by snapshots and the total space used after the migration.
File System Capacity	Displays the file system's total capacity.
Live File System Reclaimed	The reclaimed space in the live file system. The live file system is the usable space on the file system, i.e. the part of the file system not reserved or in use by snapshots.

Total File System Reclaimed	The reclaimed space in the total file system. The total file system space is the entire capacity of the file system and includes usable space and space that is reserved or in use by snapshots.
Primary Virtual Volume Statistics	
Pre-Migration Virtual Volume Space Used	Details the Virtual Volume's size and the total space used before the migration.
Post-Migration Virtual Volume Space Used	Details the Virtual Volume's size and the total space used after the migration.
Virtual Volume Reclaimed	Displays the Virtual Volume space gained due to the migration.
Secondary File System Statistics	
Pre-Migration File System Space Used	Details the file system size, space used by snapshots and the total space used before the migration.
Post-Migration File System Space Used	Details the file system size, space used by snapshots and the total space used after the migration.
File System Capacity	Displays the file system's total capacity.
Live File System Consumed	Displays the space taken up due to the migration.
Total File System Consumed	Displays the total space used in the file system due to the migration.
Secondary Virtual Volume Statistics	
Pre-Migration Virtual Volume Space Used	Details the Virtual Volume's size and the total space used before the migration.
Post-Migration Virtual Volume Space Used	Details the Virtual Volume's size and the total space used after the migration.
Virtual Volume Consumed	Displays the Virtual Volume space taken up due to the migration.

Click **delete** to delete a completed migration.

Click **View Log** to view a log file consisting time, duration and status details of the migration. A View Log link is available at both the top and bottom of the page.

Click **Download Migration Report** to view a report on the completed data migrations with details on the primary and secondary file systems and Virtual Volumes: their status, space utilization before and after the migration, the duration, start, and end time for the migrations, etc.

Reclaimed space

Reclaimed space is the difference in space between the start of the migration and when the migration completed. It is not a report of the amount of data migrated from the source file system to the target. For this detail, refer to Amount Migrated.

It is likely that the file system will be in use by network clients while the migration is in progress. As a result, the reclaimed space can be substantially different than the amount migrated. The value can even be negative if files were added to the source.

Once a data migration has completed, copies of the files may be preserved on the source file system in snapshots. For the space to be fully reclaimed, all snapshots on the source file system that reference the migrated files must be deleted.

Reverse Migration

Though Titan does not support automatic reverse migration of files, it is possible to restore a migrated file in two different ways:

Reverse Migration through the Titan CLI

Individual files or whole directory trees can be reverse-migrated through the CLI. The files which are included in the reverse migration can be identified by pattern or by last access time. For detailed information on this process, run `man reverse-migrate` at the CLI.

Reverse Migration from a network client

A file can be restored from a network client by performing the following sequence of operations:

1. From a Windows or Unix client, make a copy of the file (using a temporary file name) on the Primary Storage. This copy of the file will reside fully on Primary Storage.
2. Delete the original file. This will delete the link on Primary Storage, and the migrated data from Secondary Storage.
3. Rename the copied file to its original name.

Considerations when using Data Migrator

Titan uses Data Migrator with the following considerations:

Snapshots

To preserve snapshot protection on migrated files, when snapshots are created on the primary file system, corresponding snapshots are automatically created on the secondary file system. Likewise, when a snapshot is deleted on the primary file system, the corresponding snapshot on the secondary file system will also be automatically deleted.

When attempting to access a migrated file through a snapshot on Primary Storage, Titan will look for the corresponding snapshot on Secondary Storage and retrieve the migrated data from that snapshot. If the secondary file system does not contain any snapshots, then the file contents will be retrieved from the live file system.

Virtual Volumes

If Virtual Volumes are present on Primary Storage they will be automatically created during the first scheduled run of the Data Migration Policy.

Quota space tracking

Quotas are enforced only on the file system or Virtual Volume on which they were created. When a file is migrated through Data Migrator, the contents are moved from one file system or Virtual Volume to another. The result is that quotas on Primary Storage are only effective on files that have not been migrated. To track space utilization of migrated data, quotas will need to be manually defined on Secondary Storage. Quota restrictions on Virtual Volumes cannot be set until after the policy has been completed.

Backup, Restore, and Replication of Migrated Files

While backing up a migrated file, NDMP will backup the entire contents of the file by retrieving it from Secondary Storage. Additionally, the backed up file will be identified as having been a migrated file. In this way, if the file is restored to a file system or Virtual Volume that has been configured as Primary storage in a [Data Migration Path](#), the contents of the file will automatically be restored to Secondary Storage, leaving a cross-file system link on the Primary Storage. If the restore target is not part of a Data Migration Path, the file will be restored in its entirety.

Backups and replications typically copy data from Snapshots that are created when the operation begins. These Snapshots, however, are only taken on the Primary Storage. As a result, the backup or replication will retrieve the copy of the migrated file from the live file system on Secondary Storage. To avoid inconsistencies in the archived data set, migrated files should not be modified while backups or replications are in progress.

Alternatively, the NDMP environment variable [NDMP_BLUEARC_EXCLUDE_MIGRATED](#) can be used to prevent migrated data from being backed up. This can also be useful if the effective [Data Migration Policies](#) are configured to migrate non-critical files such as music and video files from home directories or aged data. It can also improve backup and replication time, and isolate the backup data set to include only the critical information on Primary Storage.

It is important to remember that Data Migrator extends the maximum available capacity of Primary Storage by migrating data to Secondary Storage. This means that the capacity of the backup solution, whether tape libraries or a replication target, must also support the new maximum available capacity. To maintain a reliable backup and recovery system, ensure that the capacity of the deployed backup solution is at least equal to the combined capacity of Primary and Secondary Storage. Alternatively, use [NDMP_BLUEARC_EXCLUDE_MIGRATED](#) to isolate the backup dataset to only those files that are hosted natively on Primary Storage.

iSCSI Logical Units

Mounted iSCSI Logical Units cannot be migrated, regardless what has been defined in the Data Migration Policy. Due to the types of applications typically hosted on iSCSI storage, BlueArc does not recommend migrating iSCSI Logical Units to secondary storage. However, if this is desired, it can be accomplished by performing the following:

- ❑ Disconnect any iSCSI Initiators with connections to Logical Unit.
- ❑ Unmount the iSCSI Logical Unit. This can be done through the iSCSI Logical Unit Properties page.
- ❑ Run the Data Migration Policy to migrate the Logical Unit.
- ❑ Re-mount the iSCSI Logical Unit.
- ❑ Reconnect the Initiator to the iSCSI Target.

6 File Services

File Service Protocols

Titan is a file-serving product, and its principal use is to satisfy incoming file access requests issued from network clients. The Titan SiliconServer supports the CIFS, NFS (TCP and UDP, version 2 and 3), and FTP protocols for client file access. In addition, Titan supports iSCSI for block-level access to storage. All supported protocols can be enabled or disabled.

Titan allows NFS, CIFS, and FTP users to access the same file space. See [Mixed Mode Operation](#) for more information about how Titan resolves differences between these file access protocols. However, although iSCSI Logical Units reside on file systems, it is not possible to access folders and files located on an iSCSI target through Titan's file services (like CIFS or NFS).



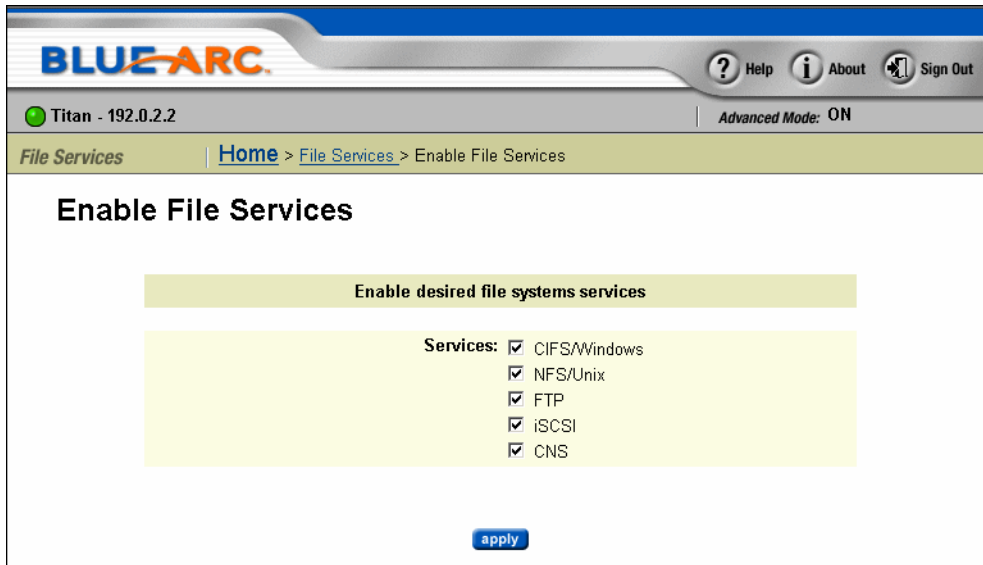
Note: These protocols, with the exception of FTP, require a [license key](#) for activation.

Enabling File Services

Use the **Enable File Services** page to enable or disable the desired file services for the system.

To enable file services

1. From the **Home** page, click **File Services**. Then, click **Enable File Services**.



The table below describes the fields on this screen:

Item / Field	Description
Services	Select the Services checkbox(es) that are required for the system: • CIFS/Windows • NFS/Unix • FTP • iSCSI • CNS

2. Click **apply**.
3. Depending on what services have been changed, a reboot may be required. If so, then follow the on-screen instructions to restart the server.

File System Security

File system security is designed for concurrent access from multiple protocols. The file system supports both UNIX-like security (user ID, group ID) and CIFS-like security (access control lists).

The following security modes are supported:

Mode	Clients	Notes
Mixed	CIFS	The server authenticates CIFS sessions by communicating with a domain controller, which returns user security information. Accesses to files that have NT permissions are checked against this security information. If a file has UNIX permissions, the security information is mapped to an equivalent UNIX identity and checked against the file permissions.
	NFS	A client user's unauthenticated UNIX identity (a user ID and one or more group IDs) accompanies each NFS request. Accesses to files that have UNIX-only permissions are checked against this. If a file has NT permissions, the identity is mapped to an equivalent NT identity and checked against the file permissions.
UNIX	CIFS	The server authenticates CIFS sessions by communicating with a domain controller, which returns user security information. All files have UNIX permissions, so the security information is mapped to an equivalent UNIX identity and checked against the file permissions.
	NFS	NFS clients are trusted to supply the requesting user's UNIX identity with every request. This identity is checked against UNIX per-file permissions to determine whether or not an operation is permissible.



Note: FTP clients follow either the Windows or the UNIX security model depending on how they were authenticated. FTP clients authenticated by an NT domain appear as CIFS clients for the purpose of security. Similarly, FTP clients authenticated though NIS appear as NFS clients.

With both Mixed and UNIX security mode it is necessary to [configure user and group mappings](#) between UNIX and Windows. However, NFS users do not require security mappings when in UNIX mode.

Mixed Security Mode

Titan’s mixed security mode supports both Windows and UNIX security definitions. Security is set up uniquely on each file (or directory), depending on which user created the file (or directory), or last took ownership of the file (or directory). If a Windows user owned the file (or directory), the security definition will be CIFS native and subject to Windows security rules. If, on the other hand, the file belongs to a UNIX user, the security definition will be NFS native and subject to UNIX security rules.

CIFS Access to Native CIFS Files

When a CIFS client tries to access a *native* file, one with Windows security information, the server checks the user information against the file’s security information to determine whether or not an operation is permissible.

Security information on a user is contained in an *access token*, which comprises the user security identifier (SID), primary group SID, and other SIDs. The server gets the token from the domain controller and caches it for use throughout the user's session.

Security information on a file is contained in its *security descriptor*, which comprises the owner SID, group SID, and access control list (ACL). The ACL can contain several access control entries (ACEs), which specify whether or not to allow access.

NFS Access to Native NFS Files

When an NFS client tries to access a *native* file, one with UNIX security information, the server checks the user's UNIX credentials against the file's security information to determine whether or not an operation is permissible. The file security information comprises a user ID, group ID, and read, write, and execute permissions.

Client Access to Non-Native Files

CIFS users may access files which have UNIX security information, and NFS users may access files which have Windows security information. The server provides the following features to make this possible:

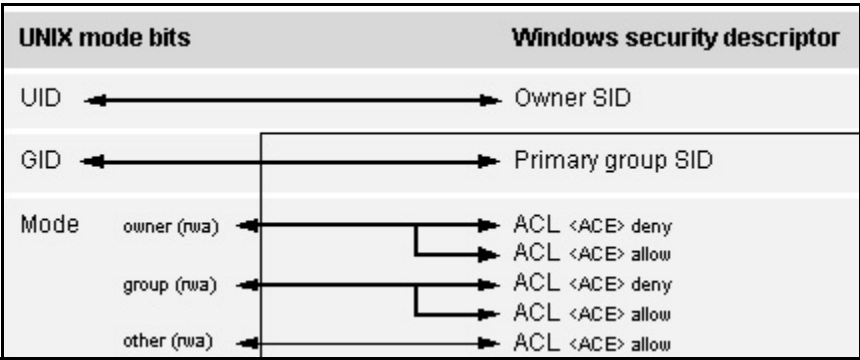
- Using the Web Manager, you set up mapping tables that associate the names of NFS users and groups with their Windows equivalents.

For example, when a CIFS user tries to access a file that has UNIX-only security information, the server automatically maps the user name to the corresponding NFS name in the mapping table.

- Titan automatically translates user security information from UNIX to Windows format, or vice-versa, and caches it for the duration of the session.

UNIX credential		NT access token
UID	User mapping table	User SID
GID	Group mapping table	Primary group SID
Other groups	Group mapping table	Other groups

- The system automatically converts file security attributes from Windows to UNIX format and stores the result in file metadata. This means that the files are henceforth native to both CIFS and NFS clients. Although UNIX files are also converted to Windows format, the results are not stored in file metadata.



- Any changes that a user makes to a file’s security attributes are applied equally to the Windows and UNIX attributes.

In summary, when a CIFS user tries to access a file that has UNIX-only security information, the server maps the user to an NFS name and converts the user’s access token to UNIX credentials. It then checks these credentials against the file’s security attributes to determine whether or not the operation is permissible.

Similarly, when an NFS user tries to access a file that has Windows-only security information, the server maps the user to a Windows name and converts the user’s UNIX credentials to a Windows access token. It then checks the token against the file’s security attributes.

UNIX Security Mode

When Titan is configured in UNIX security mode, it supports UNIX security for CIFS and NFS clients. However, all security settings applied are saved with Unix file attributes. As a result, NFS clients are always accessing files in native mode, while CIFS clients are always accessing file non-native mode (see the [Mixed Security Mode](#) section for more information on both these modes of operation).



Note: With UNIX security mode, NFS users do not need to rely on the presence of a Windows Domain Controller (DC) in order to access files. As a result, they are fully isolated from potential DC failures.

Security Mode Configuration

Security modes can be configured per-EVS, per-file system, or per-Virtual Volume. Selecting security modes on such a tiered basis, rather than a system-wide selection, enhances the granularity and convenience of managing system security.

To view the server's Security Configuration

From the **Home** page, click **File Services**. Then, click **File System Security**.

BLUE ARC

TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management [Home](#) > [File Services](#) > File System Security

File System Security

Filter:

EVS: ☐ Show File Systems

EVS	File System	Mode
☐ EVS01		Unix (also supports Windows clients) details
☐ EVS02		Unix (also supports Windows clients) details
☐ EVS03		Unix (also supports Windows clients) details
☐ EVS04		Unix (also supports Windows clients) details
☐ EVS05		Unix (also supports Windows clients) details
☐ EVS06		Unix (also supports Windows clients) details
☐ EVS07		Unix (also supports Windows clients) details
☐ EVS08		Unix (also supports Windows clients) details

Actions: [View Virtual Volume Security](#)

Shortcuts: [CIFS Setup](#)

Item / Field	Description
EVS	The list of all EVS defined by the filter.
File System	If this column is blank, the security mode displayed is associated with the EVS. If this column displays a file system label, then the security mode displayed is associated with this specific file system.
Mode	The security mode defined on the EVS or file system. On file systems without an explicit security mode configuration, the mode will be inherited from the EVS.

Filtering EVS/File System

The **File System Security** page displays all EVS and the configured security mode. To display the security configuration for a single EVS, select the **EVS** from the drop-down menu. To view or configure security modes on individual file systems, check **Show File Systems**. Click **filter** to display the list of EVS and file systems as specified.

To change the security mode for an EVS

1. From the **File System Security** page, click the **details** button next to the EVS on which the security mode is to be changed.



The **Security Configuration** page for the selected EVS displays the EVS name and a drop-down menu in which to specify the security **Mode**.

2. Select the desired security mode for the EVS from the drop-down menu.
3. Click **OK**.
Click **cancel** to return to the **File System Security** page.

To change the security mode for a file system

By default, the file system inherits the parent EVS security mode. In other words, when the parent EVS has a Unix security mode, the file system associated with the EVS will inherit the Unix security mode. To change the file system to use a different security mode, do the following:

1. From the **File System Security** page, select the parent EVS of the desired file system from the EVS drop-down menu.
2. Select the **Show File Systems** checkbox.
3. Click **filter**.

All the file systems associated with the EVS defined by the filter will appear in the list. File systems can be identified by their labels which will be displayed under the **File System** column.

BLUEARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management | [Home](#) > [File Services](#) > File System Security

File System Security

Filter: EVS: All EVS

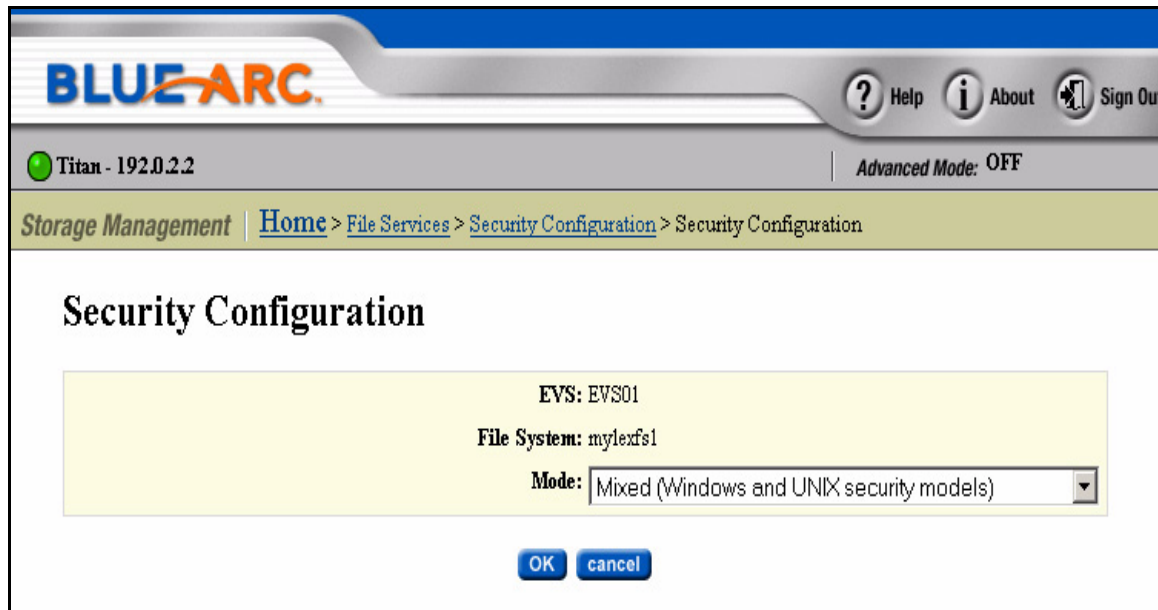
☒ Show File Systems [filter](#)

EVS	File System	Mode	
☐ EVS01		Unix (also supports Windows clients)	details
☐ EVS02		Unix (also supports Windows clients)	details
☐ EVS03		Unix (also supports Windows clients)	details
☐ EVS04		Unix (also supports Windows clients)	details
☐ EVS05		Unix (also supports Windows clients)	details
☐ EVS06		Unix (also supports Windows clients)	details
☐ EVS07		Unix (also supports Windows clients)	details
☐ EVS08		Unix (also supports Windows clients)	details

Actions: [View Virtual Volume Security](#)

Shortcuts: [CIFS Setup](#)

- Click the **details** button next to the file system on which the security mode is to be changed.



The **Security Configuration** page for the file system displays the names of the parent EVS and the file system, and a drop-down menu in which to specify the security **Mode**.

- Select the desired security mode for the file system from the drop-down menu.
- Click **OK**.
Click **cancel** to return to the **File System Security** page.

To change the security mode for a Virtual Volume

By default, the Virtual Volume inherits the parent file system's security mode. In other words, if the parent file system has a Unix security mode, the Virtual Volume associated with that file system will inherit the Unix security mode. To apply a different security mode to a Virtual Volume, do the following:

- In the **File System Security** page, put a check in the box next to the EVS on which to view the Virtual Volumes.

2. Click **View Virtual Volume Security**.

The **Virtual Volume Security Configuration** page displays a list of all Virtual Volumes corresponding to the defined filter.

BLUEARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Storage Management | [Home](#) > [File Services](#) > [Security Configuration](#) > Virtual Volume Security Configuration

Virtual Volume Security Configuration

Filter:

EVS:

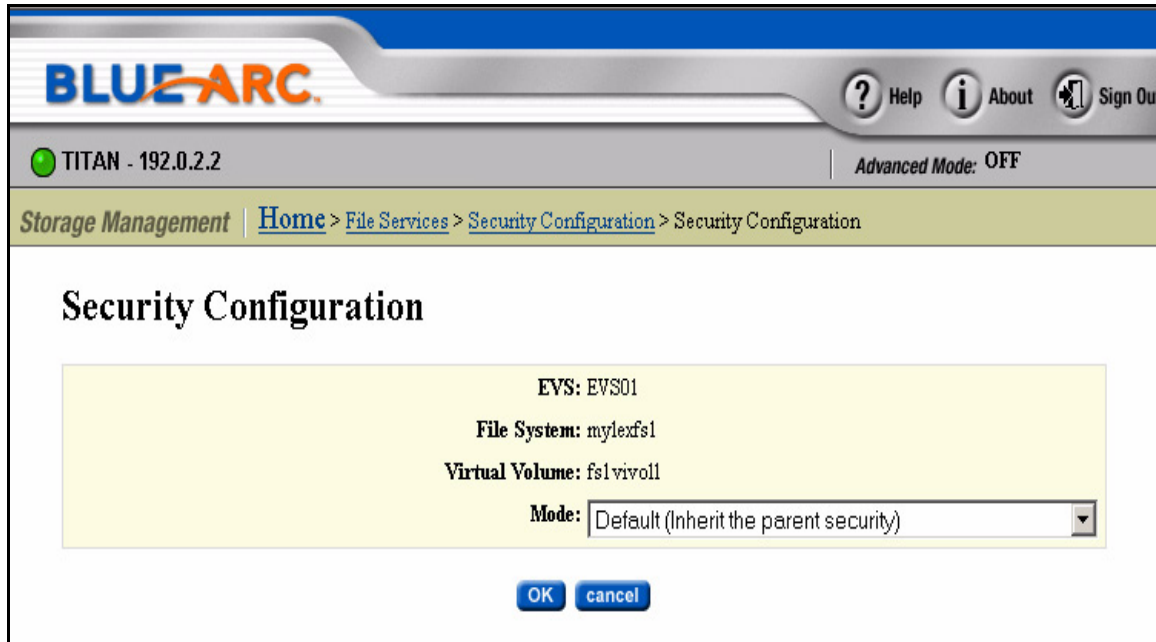
File System:

EVS	File System	Virtual Volume	Mode	
☒ EVS01	mylexfs1	fslvivoll	Mixed (Windows and UNIX security models) (Inherited)	details
☐ EVS01	mylexfs2	mylexfs1_fslvivoll	Mixed (Windows and UNIX security models) (Inherited)	details

Shortcuts: [CIFS Names](#)

Item /Field	Description
EVS	The list of EVS defined by the filter.
File System	The list of file systems defined by the filter.
Virtual Volume	The names of all Virtual Volumes found on the file systems defined by the filter.
Mode	The security mode defined on the EVS or file system. On file systems without an explicit security mode configuration, the mode will be inherited from the EVS.

- Click the **details** button next to the Virtual Volume on which the security mode is to be changed.



The **Security Configuration** page for the Virtual Volume displays the names of the parent EVS and file system, and a drop-down menu in which to specify the security **Mode**.

- Select the desired security mode for the Virtual Volume from the drop-down menu.
- Click **OK**.
Click **cancel** to return to the **File System Security** page.

Mixed Mode Operation

The Titan SiliconServer allows network clients to share a common pool of storage from both Windows and UNIX clients. This is referred to as mixed mode operation. Although the Titan SiliconServer does this as seamlessly as possible, the protocols are considerably different, so mixed mode operation presents some challenges.

File Name Representation

The maximum length of a file name is 255 characters.

File names may contain any Unicode character. Windows NT 4.0, Windows 2000, Windows 2003, and Windows XP clients can make full use of this, but Windows 9x and NFS clients only support the Latin-1 version of extended ASCII.

Case-sensitivity in file names is significant to NFS and FTP clients but not to CIFS clients.

Symbolic Links

Symbolic links (symlinks) are commonly used in UNIX to aggregate disparate parts of the file system or as a convenience, similar to a shortcut in the Windows environment.

Titan fully supports symlinks when the file system is accessed through NFS. Files marked as symbolic links are assumed, by UNIX clients, to contain a text pathname that can be read and interpreted by the client as an indirect reference to another file or directory. Anyone can follow a symlink, but permission is still needed to access the file (or directory) it points to.

As CIFS and FTP clients are not able to follow these symlinks, Titan supports a server-side symlink following capability. When accessing server-side symlinks, because the storage system is following the symlink on the client's behalf, and presenting the linked-to file rather than the symlink, some symlinks, which are perfectly valid for NFS, cannot be followed. In this case, in line with the behavior of Samba, the server hides the existence of the symlink entirely from the CIFS / FTP client. By default, the following symlinks are not followed by CIFS (and FTP) clients:

- Symlink pointing out of the scope of the share it is in, such as when the link points to a different file system.
- Absolute symlinks. Meaning symlinks starting with '/'.

To enable support for absolute symlinks from CIFS clients, contact BlueArc Support.

File Locks in Mixed Mode

When a CIFS client reads or writes to a file, it respects the locks that both CIFS and NFS clients have taken out. In contrast, an NFS client respects the locks taken out by CIFS clients only. NFS clients must therefore check for existing NFS locks with the Network Lock Manager (NLM) protocol. Titan supports both monitored and non-monitored NFS file locks.

Opportunistic Locks (Oplocks)

An oplock is a performance-enhancing technique used in Microsoft networking (CIFS) environments. It enables applications to speed up file access and minimize network traffic by caching part or all of a file locally. As the data is kept on the client, read and write operations can be performed locally, without involving the server.

Titan supports three categories of oplocks:

- **Exclusive**
An Exclusive oplock enables a single client to cache a file for both read and write purposes. As the client that owns the oplock is the only client accessing the file, it can read and modify part or all of the file locally. The client does not need to post any changes to the server until it closes the file and releases the oplock.
- **Batch**
A Batch oplock enables a single client to cache a file for both read and write purposes, as in the case of an exclusive oplock. In addition, the client can preserve the cached information even after closing the file; file open and close operations are also performed locally. The client does not need to post any changes back to the server until it releases the oplock.
- **Level II**
A Level II oplock enables multiple clients to cache a file for read purposes only. The clients owning the oplock can read file data and attributes from local information, cached or read-ahead. If one client makes any changes to the file, all the oplocks are broken.

When dealing with oplocks, Titan acts in accordance with the CIFS specification. Whether operating in a pure Windows environment or with a mix of CIFS and NFS clients, Titan allows applications to take advantage of local caches while preserving data integrity.

Exclusive and Batch Oplocks

An Exclusive or Batch oplock is an exclusive (read-write/deny-all) file lock that a CIFS client may obtain at the time it opens a file. The server grants the oplock only if no other application is currently accessing the file.

When a client owns an Exclusive or Batch oplock on a file, it can cache part or all of the file locally. Any changes that the client makes to the file are also cached locally. Changes do not need to be written to the server until the client must release the oplock. In the case of an Exclusive oplock, the client releases the oplock when the server requests that it does so, or when it closes the file. In the case of a Batch oplock, the client may keep information (including changes) locally even after closing the file. While the client has an Exclusive or Batch oplock on a file, the server guarantees that no other client may access the file.

If a client requests access to a file that has an Exclusive or Batch oplock, the server asks the client that has the oplock to release it. The client then writes the changes to the server and releases the oplock. Once this operation has finished, the server allows the second client to access the file. This happens regardless of the network protocol that the second client uses. In cases where a CIFS client requests an oplock on a file that has an Exclusive or Batch oplock, the server breaks the existing oplock and grants both clients Level II oplocks instead.

Level II Oplocks

A Level II oplock is a non-exclusive (read-only/deny-write) file lock that a CIFS client may obtain at the time it opens a file. The server grants the oplock only if all other applications currently accessing the file also possess Level II oplocks. If another client owns an Exclusive or Batch oplock, the server breaks it and converts it to a Level II oplock before the new client is granted the oplock.

If a client owns a Level II oplock on a file, it can cache part or all of the file locally. The clients owning the oplock can read file data and attributes from local information without involving the server, which guarantees that no other client may write to the file.

If a client wants to write to a file that has a Level II oplock, the server asks the client that has the oplock to release it, and then allows the second client to perform the write. This happens regardless of the network protocol that the second client uses.

Configuring User and Group Mappings

When Titan is operating in either mixed or UNIX security mode, it is necessary to set up mappings between UNIX and Windows users and groups. For example, user John Doe could have a UNIX user account named `jdoe` and a Windows user account named `johnd`. These two user accounts are made equivalent by setting up a [user mapping](#). By default, the server assumes that equivalent user and group names are the same for both environments. For example, if no explicit mapping is found for user `janed`, the server assumes that the UNIX user account named `janed` is the same as the Windows user account with the same name.

There are two steps to follow when setting up user and group mappings on the server:

1. Specify each NFS user and group's name and ID. Note that this step is not required for Windows users or groups, as the server obtains all of the information it needs from the domain controller (DC).
2. Map the NFS user (group) names to Windows NT user (group) names.

Managing NFS Users and Groups

Windows access to a file created by a UNIX user (or vice-versa) is permitted when the UNIX name and Windows name are recognized as being the same user. However, NFS clients present an NFS operation to an NFS server with numerical UNIX User ID (UID) and UNIX Group ID (GID) as credentials. The server must map the UID and GID to a UNIX user or group name prior to verifying the UNIX to Windows name mapping.

There are three methods by which Titan can map from a numerical UNIX UID or GID to a UNIX user name or group name:

- NFS user and group names can be added manually.
- A UNIX `/etc/passwd` file can be imported, providing the server with a mapping of user name to UID. The `/etc/groups` file should also be imported to provide the server with a mapping of Group name to GID.

- Titan will ignore the other fields from the passwd file, such as the encrypted password and the user's home directory. Users or Groups configured by importing from the /etc/passwd file will appear as 'permanent' in the NFS Users or Groups list.
- You can import the numerical ID to Name mappings directly from a NIS server if one has been configured. Every time a UID is presented to Titan it will issue an NIS request to an NIS server to verify the mapping. This mapping can remain cached in the server for a configurable time. A cached ID to name binding for a User or Group will appear as 'Transient' in the NFS Users or Groups list.

If Titan is configured to use the [Network Information Service](#) (NIS) no special configuration steps are needed; Titan automatically retrieves the user (group) names and IDs from the NIS server.

To specify the NFS user names manually

Each UNIX user name and numerical UID can be manually entered, along with its corresponding Windows user and domain name. Users configured manually will appear as 'permanent' in the NFS users list.

From the **Home** page click **File Services**. Then, click **User Mapping**.

BLUE ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: ON

File Services | Home > File Services > User Mapping

User Mapping

Filter NFS names by
Filter IDs from MIN to MAX Filter

Configured NFS users (Up to 1000 users shown)

User name	User ID	
blasa	924	Permanent
blasha	923	Permanent
test1	50001	Permanent
test10	50010	Permanent
test100	50100	Permanent
test1000	51000	Permanent
test10000	60000	Permanent

Delete User
Delete All Users
Next

NFS User properties

Permanent ☒

User name User ID

NT User name NT domain

Modify User

New NFS User

NFS User name User ID

NT User name NT domain

Add User

Import from file

Filename Browse... Import File

There are two steps to follow when setting up NFS users on the system: First specify each NFS user's name and user ID, and then map the NFS user names to Windows NT user names. If the system has been setup to access the information on an [NIS server](#), it is only necessary to perform the second of these steps; the system automatically retrieves the user names and IDs from the NIS server.

The fields on this screen are described in the table below:

Item /Field	Description	
Filter NFS Names	Enter the user name to use as a filter or enter the user IDs to narrow the search criteria. Note that the display limit is 1000 users.	
Configured NFS Users		
User Name	Displays a list of all defined users and their associated IDs.	
NFS User Properties	Displays the details of the selected user (when selected in the Configured NFS Users box)	
New NFS User		
NFS User name	Type the user details configured in the UNIX environment	Click Add User
User ID		
NT User name	Type the user details configured in the Windows NT environment.	
NT domain		
Import from a file	Enter the filename (or browse to the required file) and click the Import File button. See Importing a Password File for more information.	

To modify NFS users, enter the new **NFS User Name** and **User ID** or the **NT User Name** and **NT Domain** in the specified fields and click the **Modify User** button.



Tip: Where the NT user names match the NFS user names, mappings can be automated by selecting the **Automatic name mapping** checkbox. Even so, NFS user names must be entered.

To delete an individual user, select it in the Configured NFS user box and then click **Delete User**.

To specify NFS group names manually

Each UNIX group name and numerical GID can be manually entered, along with its corresponding Windows group and domain name. Groups configured manually will appear as ‘permanent’ in the NFS group list.

From the **Home** page click **File Services**. Then, click the **Group Mapping** item.

BLUE ARC Titan - 192.0.2.2 Advanced Mode: OFF

File Services | Home > File Services > Group Mapping

Group Mapping

Configured NFS groups (Up to 1000 groups shown)

Group name	Group ID	
group1	1000	Permanent
group2	1001	Permanent
group3	1002	Permanent
group4	1004	Permanent
root	0	Transient

Filter NFS names by: Filter IDs from MIN to MAX

NFS Group properties

Permanent ☒

Group name: Group ID:

NT Group name: NT domain:

New NFS Group

NFS Group name: Group ID:

NT Group name: NT domain:

Import from file

Filename:

There are two steps to follow when setting up NFS groups on the system: First specify each NFS group's name and group ID, and then map the NFS group names to Windows NT group names. If the system has been setup to access the information on an [NIS server](#), it is only necessary to perform the second of these steps; the system automatically retrieves the group names and IDs from the NIS server. The maximum number of groups that can be set up is 1000.

Item / Field	Description	
Filter NFS Names	Enter the group name to use as a filter or enter the group IDs to narrow the search criteria. Note that the display limit is 1000 groups.	
Configured NFS Groups		
Group Name	Displays a list of all defined groups and their associated IDs.	
NFS Group Properties	Displays the details of the selected group (selected in the Configured NFS Groups box)	
New NFS Group		
NFS Group name	Type the group details configured in the UNIX environment.	Click Add Group
Group ID		
NT Group name	Type the group details configured in the Windows NT environment.	
NT domain		
Import from a file	Enter the filename (or browse to the required file) and click the Import File button. See Importing a Password File for more information.	

To modify a group name, ID, or NFS-to-NT mapping, select the group in the Configured NFS groups box and then type the new details in the NFS group properties fields. Click **Modify Group** when this is finished.

To delete an individual group, select it in the Configured NFS groups box and then click **Delete Group**.



Tip: Where the NT group names match the NFS group names, mappings can be automated by selecting the **Automatic name mapping** checkbox. Even so, NFS group names must be entered.

Importing a Password File

A quick way to specify the user or group details is by importing them from a file. There are three possible formats for this file, as described below. Choose one format and use it consistently throughout the file.

1. NFS user/group data only

The source of the user data can be a UNIX password file, such as /etc/passwd. When using the Network Information Service (NIS), typing this command can create the file:

```
ypcat passwd > /tmp/x.pwd
```

The following is an extract from a file in the required format.

```
john:x:544:511:John Brown:/home/john:/bin/bash
keith:x:545:517:Keith Black:/home/keith:/bin/bash
miles:x:546:504:Miles Pink:/home/miles:/bin/bash
carla:x:548:504:Carla Blue:/home/carla:/bin/bash
```

2. NFS-to-NT user/group mappings only

The entries in the file must be in this form:

```
UNIXuser="NT User", "NT Domain"
```

Where the NT domain is optional. The NFS user names cannot contain any spaces, and the NT names must be enclosed in quotation marks. If the domain name is omitted, the server domain is assumed. If the empty domain name is required, it must be specified like this:

```
users="Everyone", ""
```

The Everyone user is the only common account with an empty domain name.

3. Both NFS user/group data and NFS-to-NT user mappings

The entries in the file must be in this form:

```
UNIXuser:UNIXid="NT User", "NT Domain"
```

Where the same rules apply to the NFS and NT names as for the NFS-to-NT user mapping file described above. The following is an extract from a file in the required format.

```
john:544="john", "Domain1"
keith:545="keith", "Domain1"
miles:546="miles", "Domain1"
carla:548="carla", "Domain1"
```

To specify NFS group names by importing a password file

1. In the **Filename** field in the **User Mapping** dialog box, type the full path to the file, or click **Browse** to search for the file.
2. Click **Import File**.
If any names in the file exist in the NFS list, the Web Manager ignores them and displays a warning that it encountered errors or duplicate users.
3. Click **Apply**.

Sharing Resources with NFS Clients

A fundamental part of most UNIX networks, the Network File System (NFS) protocol enables PCs and UNIX workstations to access each other's files transparently. This section describes how to set up NFS exports, users, and groups.

The Titan SiliconServer and NFS

The Titan SiliconServer implements the file-serving functions of an NFS server. The system provides the normal file-serving functions, such as:

- Export manipulation
- File manipulation (read, write, link, create, etc.)
- Directory manipulation (mkdir, readdir, lookup, etc.)
- Byte-range file locking
- File access control (permissions)
- File and directory attributes (sizes, access times, etc.)
- Hard links and symbolic (soft) links

Prerequisites

To enable NFS access to the system:

- ❑ [Enter an NFS license key.](#)
- ❑ [Enable the NFS service.](#)

Supported Clients and Protocols

Platform	Supported versions
Red Hat Linux	7, 8, 9
Fedora Linux	Core 1, Core 2
Solaris (SPARC)	5 through 9
Solaris (Intel)	8, 9
Macintosh OS X	10.3 or later
FreeBSD	4.3, 4.7, 5.0

HP-UX	10, 11
Irix	6.5

The system supports the following UNIX protocols:

NFS	versions 2 and 3
Port Mapper	version 2
Mount	versions 1 and 3
Network Lock Manager (NLM)	versions 1, 3, and 4
Network Status Monitor (NSM)	version 1

NFS Statistics

[Statistics](#) are available to monitor NFS activity since Titan was last started or its statistics were reset. The statistics are updated every ten seconds.

Configuring NFS Exports

NFS exports can be configured on mounted file systems. Titan can support more than 1000 NFS exports. However, the precise limit of any NFS export allocation depends on the overall size of the user's configuration. NFS exports can be configured manually or by importing the details from a file.

To Add an NFS Export

- 1. From the **File Services** page, click **NFS Exports**.
- 2. Click the **add** button.

BLUE ARC

?

Help

i

About

✖

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

File Services | [Home](#) > [File Services](#) > [NFS Exports](#) > Add Export

Add Export

EVS / File System:

EVS01 / vol0

Name:

NFS_Export

Path:

/directory

browse...

☒ Create path if it does not exist

Show snapshots:☒

Ignore Overlap:☒

Access Configuration:

10.1.2.38 (rw)
10.1.*.* (ro)

OK

cancel

The fields on this screen are described in the table below:

Item/Field	Description
EVS/File System	Select an EVS and a File System from the drop down list on which to add the NFS export.
Name	Enter the name of the export.
Path	Type the path to the directory from which to export the files and subdirectories. This path is case-sensitive. Click browse... to find the correct path to the directory.
Create path if it does not exist	Check the box Create path if it does not exist to create the path entered in the Path field.
Show snapshots	Check the box to allow snapshot access from the NFS export.

244

Titan SiliconServer

Ignore Overlap	When checked (default option), this sets up nested NFS exports. For example, export the root directory of a File System and make it available to managerial staff only. This also allows the sub-directories of the root directory to be exported later and each of them can be made available to different groups of users.	
Access Configuration	Enter the IP addresses of the clients who are allowed to access the NFS export. If the system has been set up to work with a name server, enter the client's computer name rather than its IP address. The computer name is not case-sensitive.	
	What to type	Means
	Blank or *	All clients can access the export.
	Specific address or name. Examples: 10.168.20.2 , client.dept.company.com	Only clients with the specified names or addresses can access the export.
	Partial address or name using wildcards. Examples: 10.168.*.* , *.company.com	Clients with matching names or addresses can access the export.
Configuration text	The limit is 7500 characters, this box displays the number of characters used.	

- Click **OK** when all the fields have been completed.

Export qualifiers

The table below describes the qualifiers that can be appended to IP addresses when specifying the clients that can access an NFS export.

Qualifier	Description
read_write, readwrite, rw	Grants read/write access. This is the default setting.
read_only, readonly, ro	Grants read-only access.
root_squash, rootsquash	Maps user and group IDs of 0 (zero) to the anonymous user or group. This is the default setting.
no_root_squash, norootsquash	Turns off root squashing.
all_squash, allsquash	Maps all user IDs and group IDs to the anonymous user or group.
no_all_squash, noallsquash	Turns off all squashing. This is the default setting.

secure	Requires requests to originate from an IP port less than 1024. Access to such ports is normally restricted to administrators of the client machine. To turn it off, use the insecure option.
insecure	Turns off the secure option. This is the default setting.
anon_uid, anonuid	Explicitly sets an anonymous user ID.
anon_gid, anongid	Explicitly sets an anonymous group ID.
noaccess, no_access	Denies the specified clients access to the export.



Note: BlueArc supports the use of NIS netgroups for the NFS export client access qualifiers.

Here are some examples:

❑ **10.1.2.38(ro)**

Grants read-only access to the client whose IP address is 10.1.2.38.

❑ **yourcompanydept(ro)**

Grants read-only access to all members of the NIS group *yourcompanydept*.

❑ ***.mycompany.com(ro, anonuid=20)**

Grants read-only access to all clients whose computer name ends *.mycompany.com*. All squashed requests are to be treated as if they originated from user ID 20.

❑ **10.1.*.* (readonly, allsquash, anonuid=10, anongid=10)**

Grants read-only access to all the matching clients. All requests are squashed to the anonymous user, which is explicitly set as user ID 10 and group ID 10.

The order in which the entries are specified is important. Take the following two lines:

***(ro)**
10.1.2.38(rw)

The first grants read-only access to all clients, whereas the second grants read/write access to the specified client. The second line is redundant, however, as the first line matches all clients. These lines must be transposed to grant write access to 10.1.2.38.

Notes on Specifying Clients by Name rather than IP Address

- Be sure to specify the fully qualified domain name of the client. For example, type *aclient.dept.mycompany.com* rather than simply *aclient*.
- To specify a partial name, a single wildcard, located at the start of the name, may be used.

- The system determines the export options to apply to a specific client when the client mounts the NFS export. Subsequent changes to DNS, WINS, or NIS that would result in the client's IP address resolving to a different computer name are only applied to any mounted exports when the client unmounts the exports and then remounts them.
- The order in which the system uses DNS, WINS, and NIS information to resolve IP addresses may affect the export options that it applies to a client's mount request. If a client name can be resolved through all three services, it is the first service in the name service search order that supplies the name, and this is used in searching the configuration options against the export.

Viewing the Properties of an NFS Export

From the **Home** page, click **File Services**. Then, click **NFS Exports**.

BLUEARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

File Services | [Home](#) > [File Services](#) > NFS Exports

NFS Exports

EVS / File System

EVS01 / vol0 [change...](#)

Filter

Name:

Path: [filter](#)

▼ Name	File System	Path	
☐ /engineering	vol0	/eng_vivol	details
☐ /vol0	vol0	/	details

[Check All](#) | [Clear All](#)

Actions: [add](#) [delete](#) | [Download Exports](#)

Item/Field	Description
Filter	This allows the table to be filtered by name and path. Click filter to display the NFS Export table.
EVS/File System:	The name of the EVS and the File System to which the NFS Export is assigned.
Name	The name of the NFS Export.
File System	The name of the File System to which the NFS Exports is assigned.
Path	The path and directory to which the NFS Export is directed.
Download Exports	Download a comma separated value (.csv) file containing a list of all configured NFS exports on the selected EVS and file system. To download a list of exports from another file system, click change...

1. On the **NFS Exports** page, check the box next to the NFS Export of which to view/modify the properties.
2. Click **details**.

The screenshot shows the BLUE ARC TITAN web interface. The top navigation bar includes the BLUE ARC logo, a status bar showing 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF', and links for Help, About, and Sign Out. The breadcrumb trail is 'File Services > Home > File Services > NFS Exports > NFS Export'. The main heading is 'NFS Export'. Below it, a form contains the following fields: 'File System' (a dropdown menu showing 'vol0'), 'Name' (a text box with '/engineering'), 'Path' (a text box with '/eng_vivol' and a 'browse...' button), 'Show snapshots' (a checked checkbox), 'Ignore Overlap' (an unchecked checkbox), and 'Access Configuration' (a large empty text area). At the bottom of the form are 'OK' and 'cancel' buttons.

3. On the **NFS Export** details page, one or more fields can be modified. Click **OK** if any of the fields are changed.

Deleting an NFS Export

Before an export is deleted, verify that it is not currently being accessed. If an export is deleted while users are accessing it, their NFS sessions will be terminated and any unsaved data may be lost.



Note: When replacing a storage enclosure, delete all the exports associated with it. Then, when the replacement enclosure is available, add new exports on the new System Drives.

Retrieving quota information

Refer to the [Retrieving Quota Usage through rquotad](#) section.

Using CIFS for Windows Access

A file-sharing protocol based on the Server Message Block (SMB) protocol, the Common Internet File System (CIFS) is the protocol used on Windows networks to allow file sharing between workstations and servers.

The Titan SiliconServer and CIFS

The Titan SiliconServer emulates the file-serving functions of a Windows NT 4.0, Windows 2000, or Windows 2003 server. As far as clients are concerned, the Titan is indistinguishable from a Windows file server. It provides all of the normal file-serving functions, such as:

- Share manipulation (add, list, delete, and etc.)
- File manipulation (read, write, create, delete, move, copy, etc.)
- File locking and byte-range locking
- File access control using standard Windows ACLs
- File and directory attributes (read-only, archive, and etc.)

Prerequisites

To enable CIFS access to the server:

- ❑ [Enter a CIFS license key.](#)
- ❑ [Enable the CIFS service.](#)

Depending on the security model used on the CIFS network, configure the SiliconServer using one of the following methods:

Security Model	Client Authentication	Configuration Method
NT Domain security	NT 4 only	Add server to NT domain
Windows 2000 Active Directory	NT 4 only	Add server to NT domain
	Kerberos and NT 4	Join Active Directory
Windows 2003 Active Directory	NT4 only	Add server to NT domain
	Kerberos and NT 4	Join Active Directory

When configured to join an Active Directory, Titan functions the same way as a server added to an NT domain. The only tangible difference is that after joining an Active Directory, Titan can authenticate clients using the Kerberos protocol as well as NT 4 style authentication. Most modern Windows clients support both authentication methods, though a number of older Windows clients only support NT 4 style authentication.

Supported Clients

Platform	Supported versions
Windows 2003	SP1
Windows XP	SP1, SP2
Windows 2000	SP1, SP2, SP3, SP4
Windows NT 4.0	SP4, SP5, SP6a
Windows 98	SE
Macintosh OS X	10.3 or later (native client only)

Domain Controller Interaction

Titan relies on Windows domain controllers to authenticate users and get user information such as group membership. Titan automatically discovers and connects to the fastest and most reliable domain controllers. Since operating conditions may change over time, Titan selects the "best" domain controller every 10 minutes.

By default, when authenticating clients in an Active Directory, Titan uses the time maintained by the domain controller, automatically adjusting for any clock inconsistencies.

Dynamic DNS

On TCP/IP networks, servers communicate with each other through their IP addresses. The Domain Name System (DNS) is the most common method by which clients on a network or on the Internet resolve a host name with an IP address, facilitating IP-based communication between them.

With DNS, records must be created manually for every host name and IP address. Starting with Windows 2000 Microsoft enabled support for Dynamic DNS, a DNS database which allows authenticated hosts to automatically add a record of their host name and IP address, eliminating the need for manual creation of records.

Registering a name

When an EVS goes online, Titan registers each configured ADS CIFS name and IP address associated with the EVS with the [configured DNS servers](#). One entry will be recorded in DDNS for every configured IP address. If a server has more than one configured ADS CIFS name, an entry for each IP address for each configured CIFS name will be registered. Registrations are made to both forward and reverse lookup zones.

Each hostname registered with the DNS server has a Time To Live (TTL) property of 20 minutes, which is the amount of time other DNS servers and applications are allowed to cache it. In other words, the DNS server uses a cache file to retain a copy of the DNS lookup details for 20 minutes. The record's TTL dwindles with passing time and when the TTL finally reaches zero, the record is removed from the cache. After the 20-minute expiration point, the client must execute a fresh name lookup for more information.

The hostname is refreshed every 24 hours. This refresh commences after the first successful registration. For instance, if Titan registers its name at bootup, then every 24 hours after the bootup it *refreshes* its DNS entry. If Titan cannot register or refresh its name, it goes into recovery mode with an attempt to register every 5 minutes. Once it successfully registers, it will resume the 24 hours-per-refresh cycle.

Secure DDNS Updates

Titan supports both secure and insecure DDNS updates. By default, Microsoft Windows 2000 and 2003 DDNS servers only accept “secure”, Kerberos-authenticated registrations. To support both Microsoft and non-Microsoft DDNS servers, Titan will first attempt to register with DDNS insecurely. If the insecure registration fails, Titan will attempt a secure registration.

CIFS Statistics

[Statistics](#) are available to monitor CIFS activity since Titan was last started or its statistics were reset. The statistics are updated every ten seconds.

Configuring CIFS Security

Titan integrates seamlessly into the existing domain and simplifies access control by performing all authentications against the existing domain user accounts. Only accounts that have been created in the domain can access the server. When a user attempts to access a share, the server verifies that he or she has the appropriate permissions to access it. Once access is granted at this level, the standard file and directory access permissions apply.

Titan is configured to operate on a specific domain and can, optionally, join an Active Directory. Titan interacts with a Domain Controller (DC) in its domain to validate user credentials. Titan supports Kerberos based authentication to an Active Directory as well as NTLM authentication (using pre-Windows 2000 protocols). In addition to all users belonging to its domain, Titan allows users who belong to trusted domains to connect through CIFS.

Titan automatically grants administrator privileges to domain administrators who have been authenticated by the DC. In addition, local administration privileges can be assigned including backup operator privileges to selected groups (or users).

Assigning CIFS Names

Windows clients access Titan through configured CIFS names. Traditional Windows servers have a single host name. In environments where multiple Windows servers are being consolidated, Titan can be configured with multiple CIFS names.

In order to appear as a unique server on a Windows network, Titan will do the following for each configured CIFS name:

- ❑ Allows administration through the Microsoft Server Manager (NT 4) or Computer Management (Windows 2000 or 2003) administrative tools.
- ❑ If NetBIOS is enabled, each CIFS name will be registered with the domain Master Browser so each name appears as a unique server in Network Neighborhood.
- ❑ Registers each CIFS name with DDNS or WINS for proper host name resolution.
- ❑ Titan supports up to 256 CIFS names per EVS.

Joining an Active Directory (AD)

To join Active Directory, a CIFS name must be added. For each configured CIFS name, a corresponding computer account must exist in the Active Directory. Computer accounts can be pre-created in the desired folder using the "Active Directory Users and Computers" tool. If no computer account exists, Titan will add a corresponding computer account to the "Computers" folder when the CIFS name is added to Titan's configuration.



Note: For security, the Microsoft AD requires that the time difference between the joining computer and the AD is not more than 5 minutes. Verify that the time on Titan is configured properly and is in sync with the domain before attempting to join the Directory.

1. From the **Home** page, click **File Services**. Then, click **CIFS Setup**.

The screenshot shows the BlueArc CIFS Setup web interface. At the top, there is a header with the BlueArc logo and navigation links: ? Help, i About, and a Sign Out button. Below the header, a status bar shows 'Titan - 192.0.2.2' and 'Advanced Mode: ON'. The main navigation bar includes 'File Services' and a breadcrumb trail: 'Home > File Services > CIFS Setup'. The 'CIFS Setup' section features a dropdown menu for 'EVS' with 'EVS03' selected. Below this are input fields for 'Security Mode' (Mixed), 'Domain Name' (SHIRE), and 'ADS Domain' (shire.bluearc.com). A checkbox for 'Enable NetBIOS (Applies to all EVS)' is present and unchecked. A table titled 'Configured serving names.' displays the following data:

Mode	Serving Name	Disjoint
ADS	SalesSrv	

Below the table, there are radio buttons for 'Select View: Current Names' (selected) and 'Online Names', and a checkbox for 'Show Primary DNS Suffix' which is unchecked. At the bottom, there are 'Add>>' and 'Delete' buttons.

2. From the **EVS** drop-down menu, select the EVS on which to create the CIFS name.
3. Click **Add>>** to add a CIFS name.

4. Select **ADS** as the CIFS name type as shown below:

BLUEARC

?

 Help

i

 About

Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

File Services | [Home](#) > [File Services](#) > Configure CIFS Setup

Configure CIFS Setup

CIFS Serving Names

Add Name

SalesSrv

Delete Name

☒ Replace name(s) if necessary

☐ NT4 Domain Name

☒ ADS DC IP Address

192.168.41.5

DC Admin User

Administrator

DC Admin Password

Apply

Cancel

Enter the information necessary to join the Active Directory:

Item /Field	Description
CIFS Serving Name	The computer name through which CIFS clients will access file services on Titan. The name can be a maximum of 63 characters long.
ADS DC IP Address	The IP address of a Domain Controller in the Active Directory in which the Titan will be configured.
DC Admin User	A user account that is a member of the Domain Administrators group. This privilege is necessary to create a computer account in the Active Directory.  Note: When specifying a user account from a trusted domain, the user account must be entered using the Kerberos format. In other words, use administrator@ADdomain.mycompany.com, not ADdomain\administrator.
DC Admin Password	The correct password for the Domain Administrator user.

5. Click **Apply**.

6. After the CIFS name has been added, the EVS must be restarted. See [EVS Management](#) for more information.

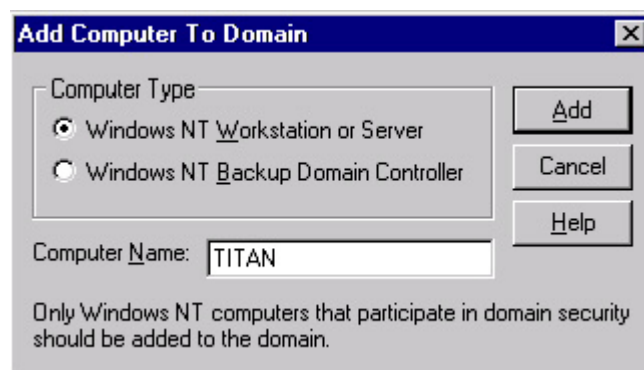
When complete, the Titan should be accessible through its configured CIFS name.

Adding a Server to a NT 4 Domain

To enable access to a Titan in an NT 4 domain, two steps must be performed:

1. A computer account must be created in the NT domain.
2. A corresponding NT 4 CIFS name must be created on the Titan SiliconServer.

To create a computer account in an NT 4 domain, run Server Manager from a Domain Controller in the NT 4 Domain and create a new “Windows NT Workstation or Server” account using the desired host name.



After the computer account has been created, the corresponding CIFS name must be created on Titan. To do so, the following steps must be performed:

1. From the Home page select File Services then click **CIFS Names**.
2. Click **Add>>**.
3. Enter the CIFS Serving name. This name must be identical to the name entered when adding the computer account to the domain.
4. Specify the NT4 domain name where indicated.
5. Click **Apply**.
6. After the CIFS name has been added, the EVS must be restarted. See [EVS Management](#) for more information.

Once complete, the Titan should be accessible through its configured NT 4 CIFS name.

Removing CIFS Names

CIFS names can be removed from Titan's configuration by deleting them from the list of configured CIFS names. When ADS CIFS names are removed, the corresponding computer account in the Active Directory is also removed. Computer accounts in NT 4 Domains must be deleted manually through Server Manager.



Note: At least one CIFS name must be configured on Titan to support connections from Windows clients. As a result, if the last configured CIFS name is removed, Windows clients will no longer be able to access the server over CIFS.

Using NetBIOS

When NetBIOS is enabled, it allows NetBIOS and WINS use on this server. If this server communicates by name with computers that use older Windows versions, this setting is required. By default, Titan is configured to use NetBIOS.

Disabling NetBIOS has a few advantages:

- It simplifies the transport of SMB traffic.
- It removes WINS and NetBIOS broadcast as a means of name resolution.
- It standardizes name resolution on DNS for file and printer sharing.

Disabling NetBIOS

Before choosing to disable NetBIOS, verify that there is no need to use NetBIOS, WINS, or legacy NetBT-type applications for this network connection. In other words, if this server communicates only with computers that run Windows 2000, Windows XP, or Windows 2003, disabling NetBIOS will be transparent and may result in a performance benefit.

NetBIOS should only be disabled if a reliable DNS infrastructure is in place. Once disabled, clients will only be able to communicate with Titan by its name through DNS. [Dynamic DNS](#) registration of CIFS names and IP addresses is an easy way to ensure reliable connectivity.



Caution: Disabling NetBIOS can cause connectivity problems for users of older versions of Windows.

To disable NetBIOS:

1. From the **Home** page, click **File Services**. Then, click **CIFS Setup**.

BLUEARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

File Services | Home > File Services > CIFS Setup

CIFS Setup

EVS EVS03

Security Mode Mixed

Domain Name SHIRE

ADS Domain shire.bluearc.com

☐ Enable NetBIOS
(Applies to all EVS)

Configured serving names.

Mode	Serving Name	Disjoint
ADS	SalesSrv	

Select View: ☒ Current Names ☐ Online Names

☐ Show Primary DNS Suffix

Add>> Delete

2. Uncheck **Enable NetBIOS**.
3. Reboot the server when prompted.

Configuring Local Groups

In a Windows security domain, users and groups exist to identify users (e.g. *jamesg*) and groups of users (e.g. *software*) on the network. Apart from the user-defined network group names (e.g. *software*, *finance*, *test*, etc.), Windows also supports a number of built-in or “local” groups with each providing various privileges and levels of access to the server on which they have been configured.

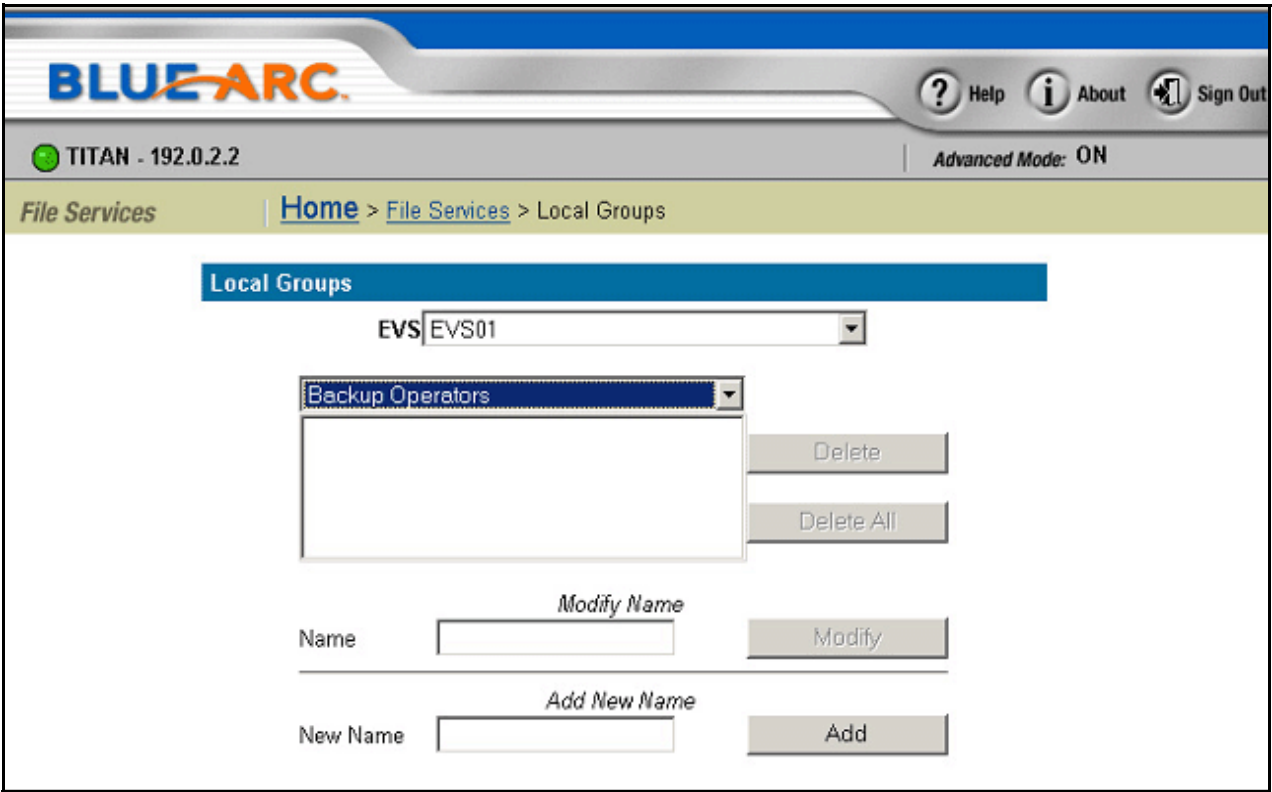
These groups exist on every Windows computer, whatever domain they are in throughout the world. They are not network groups, but are local to each computer. So, the user *jamesg* may be granted Administrator privileges on one computer and not on another.

This is similar in the Titan SiliconServer. The administrator has the ability to add users to any of the local groups named above. Although users can be added to any of these groups, only three of them are currently effective:

- **Administrators** - If a user is a member of the local Administrators group, the user can take ownership of any file in the file system.
- **Backup Operators** - If a user is a member of the local *Backup Operators* group, the user will bypass all security checks in the file system. This is required for accounts that run *Backup Exec* or perform virus scans.
- **Forced Groups** - If a user is a member of the local *Forced Groups* group, on files created by that user, the user's defined primary group will be overridden and the user account will be used instead.

To Add a User or Group to a Local Group

1. From the **Home** page, click **File Services**. Then, click **Local Groups**.



The items on this screen are described in the following table:

Item / Field	Description
Administrators	The local groups currently effective on the Titan SiliconServer.
Backup Operators	
Forced Groups	
EVS	Select the EVS where the local group resides
Name / New Name	The name of the user or group.

2. Select the group from the drop-down list.
3. Select the local group's EVS.
4. Enter the new name in the **Name** field.
5. Click **Add**.

To view / modify a user on a local group

1. Select a local group from the drop down list.
2. Select the local group's EVS.
3. Enter the new name in the **Name** field.
4. Click **Modify**.

To delete a user from a local group

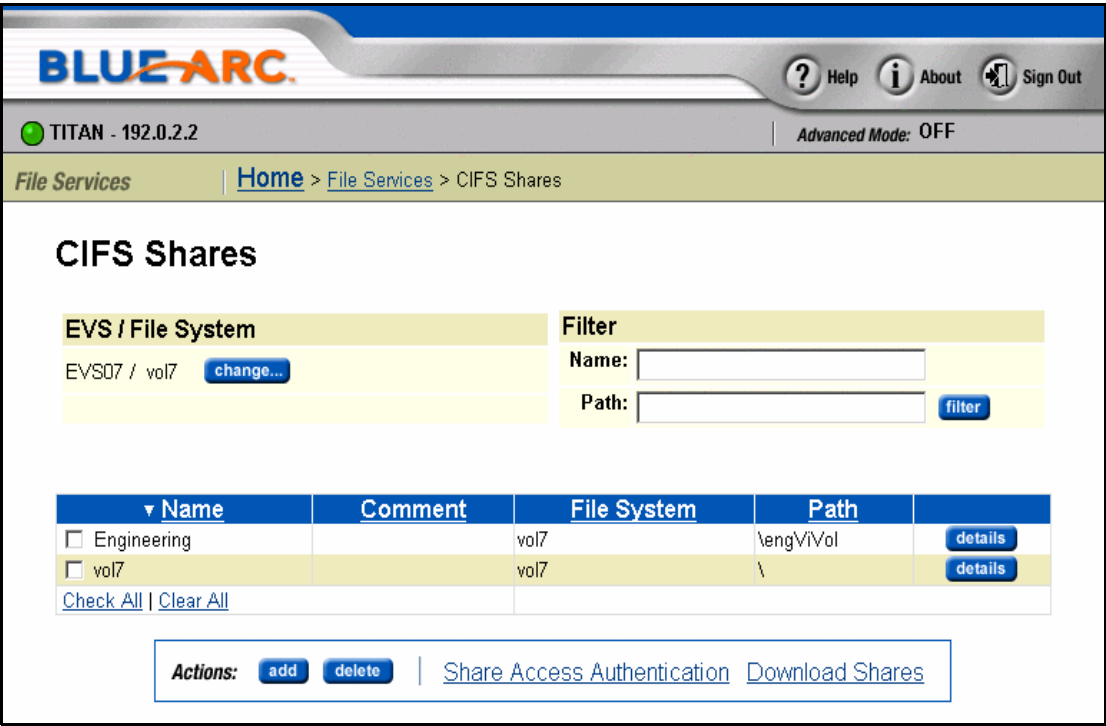
1. Select the user in the box.
2. Click **Delete**.
3. To delete all users, click **Delete All**.

Configuring CIFS Shares

CIFS shares can be set up on mounted volumes. Titan can support well in excess of 1000 shares. However, the exact limit of any share allocation depends on the overall size of the server's configuration.

To Setup a CIFS Share

1. On the **Home** page, click **File Services**. Then, click **CIFS Shares**.



The fields on this screen are described in the table below:

Item /Field	Description
Filter	Filters can be defined to reduce the amount of shares displayed on the page. Filters can be configured based on the share name or the path.
EVS/File System	The name of the EVS and the File System
Name	The name of the CIFS share.
Comment	Additional information associated with the CIFS share.
File System	The name of the File System on which the share is located.
Path	The directory on which the CIFS share is located.
Share Access Authentication	Select a share and click Share Access Authentication to view or configure user and group access permissions on the selected share. Refer to Controlling Access to Shares for more information.

Download Shares	Download a comma separated value (.csv) file containing a list of all configured CIFS shares on the selected EVS and file system. To download a list of shares from another file system, click change...

2. Click **Add**.

The screenshot shows the BlueArc TITAN web interface. The top navigation bar includes the BlueArc logo, a status bar showing 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF', and links for Help, About, and Sign Out. The breadcrumb trail is 'Home > File Services > CIFS Shares > Add Share'. The main heading is 'Add Share'. The configuration form includes the following fields and options:

- EVS / File System:** A dropdown menu currently showing 'EVS01 / vol0'.
- Name:** An empty text input field.
- Comment:** An empty text input field.
- Path:** A text input field with a 'browse...' button to its right.
- Max Users:** A dropdown menu currently showing 'unlimited'.
- Show snapshots:** A checked checkbox.
- Follow symbolic links:** A checked checkbox.
- Force filename to be lowercase:** An unchecked checkbox.
- Enable Virus Scanning:** An unchecked checkbox with the text '(Virus scanning is globally disabled)'.
- Cache Options:** A dropdown menu currently showing 'Manual local caching for documents'.
- Access Configuration:** A large, empty text area.

At the bottom of the form are 'OK' and 'cancel' buttons.

The table below describes the parameters required to configure CIFS shares:

Item /Field	Description	
EVS/File System	Select the EVS and File System on which to assign the CIFS share.	
Name	Enter the name of the CIFS share.	
Comment	Enter additional information regarding the CIFS share. This information is often displayed to clients along with the share name.	
Path	The path to where the CIFS share is located. To find a directory, click Browse... The box is checked to Create path if it does not exist.	
Max Users	The number of users associated with the CIFS share. The default is unlimited.	
Show snapshots	The box is checked to allow snapshot access from this share.	
Follow symbolic links	The box is checked to enable symlink following for this share.	
Force filename to be lowercase	Select this box to force all filenames generated on this share to be lowercase. It is useful for interoperability of UNIX applications.	
Enable Virus Scanning	By default, Virus Scanning is enabled server-wide. To disable Virus Scanning for a specific share, uncheck this box.	
Cache Options	Select the Cache Options for the share: • Manual Local Caching for Documents • Automatic Local Caching for Documents • Automatic Local Caching for Programs • Local Caching Disabled	
Access Configuration	Type the IP addresses of the clients who can access the share.	
	What to type	Means
	Blank or *	All clients can access the share.
	Specific addresses. Example: 10.168.20.2	Only clients with the specified IP address can access the share
	Partial addresses using wildcards. Example: 10.168.*.*	Clients with matching addresses can access the share.

3. Click **OK**.

Share qualifiers

To specify which clients have access to a CIFS share, qualifiers can be appended to the IP address(es):

Qualifier	Description
read_write, readwrite, rw	Grants read/write access. This is the default setting.
read_only, readonly, ro	Grants the specified client read-only access to the CIFS share.
no_access, noaccess	Denies the specified client access to the CIFS share.

Some CIFS share qualifier examples are:

❑ **10.1.2.38(ro)**

Grants read-only access to the client with an IP address of 10.1.2.38.

❑ **10.1.*(readonly)**

Grants read-only access to all clients with an IP address beginning with 10.1.

The order in which the entries are specified is important. For example,

***(ro)**

10.1.2.38(noaccess)

The first grants read-only access to all clients, whereas the second denies access to the specified client. However, the second line is redundant, as the first line matches all clients. These lines must be transposed to ensure access is denied to 10.1.2.38.

Controlling Access to Shares

Access to shares is restricted through a combination of share-level and file-level permissions. These permissions determine the extent to which users can view and modify the contents of the shared directory. When users request access to a share, their share-level permissions are checked first. Then, if the users are authorized to access the share, their file-level permissions are checked.

When the share-level permissions differ from the file-level permissions, the more restrictive permissions take effect (see the table below).

Activity	Read	Change	Full
View the names of files and subdirectories	✓	✓	✓
Change to subdirectories of the shared directory	✓	✓	✓
View data in files	✓	✓	✓
Run applications	✓	✓	✓
Add files and subdirectories	✗	✓	✓
Change data in files	✗	✓	✓
Delete files and subdirectories	✗	✓	✓
Change permissions on files or subdirectories	✗	✗	✓
Take ownership of files or subdirectories	✗	✗	✓



Note: When configuring access to a share, it is only possible to add users or groups known to domain controllers and that the server can see on the network.



Note: If user access is granted to a share, and the user is a member of a group to which a different access level has been granted, the more permissive level applies. For example, if a user has “Read access” to a share but he or she belongs to a group that has Change access, the latter takes effect.

Offline File Access Modes

The server supports Offline Files Access. This allows network clients to cache files that are commonly used from a network/file share. To use Offline Files, the client computer must be a computer running Windows 2000 (or a later version). There are three different share caching modes – the server supports all three modes of caching:

1. **No Caching:** No caching of files or folders occurs.
2. **Manual:** The Manual mode allows the user to specify individual files required for offline access. This operation guarantees a user can obtain access to the specified files whether online or offline.
3. **Automatic:** The Automatic mode is applied to the entire share. When a user uses any file in this share, it is made available to the user for offline access. This operation does not guarantee a user can obtain access to the specified files, because only files that have been used at least once are cached. The Automatic mode can be defined for documents or programs.

Modifying or Deleting a Share

Before modifying or deleting a share, verify that no-one is currently accessing it. Where this is the case, the Shares Configuration dialog box shows the number of Share users to be zero. If a share is modified or deleted while other users are accessing it, their CIFS sessions will be terminated and any unsaved data may be lost.



Note: To replace a storage enclosure, delete all the shares associated with it. When the replacement enclosure is available, add new shares on its System Drives.

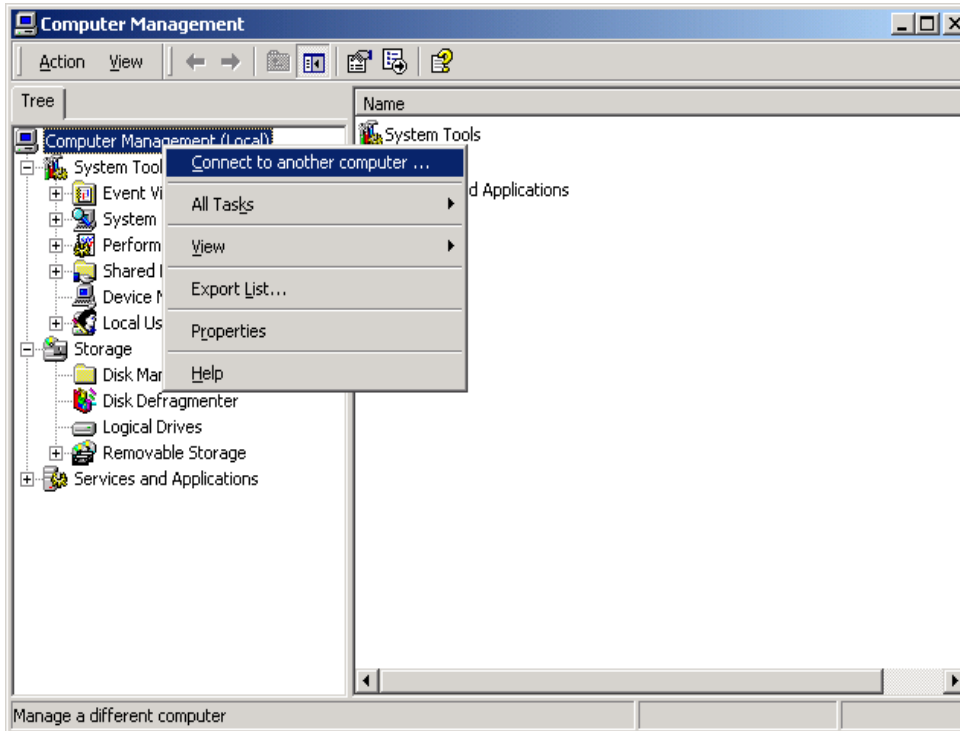
Using Windows Server Management

The Computer Management MMC tool, available for Windows 2000 or later, can be used to perform tasks for managing shares from any remote computer (For older versions of Windows, the equivalent of this tool is provided by Server Manager.) For example, several tasks for managing shares include:

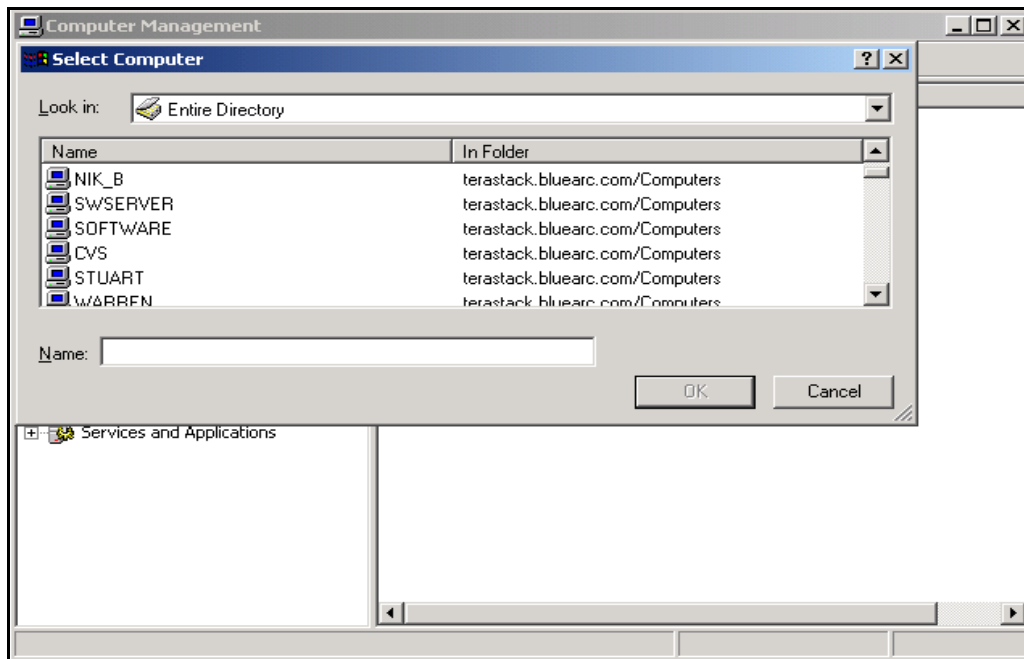
- Viewing a list of all users who are currently connected to the system.
- Creating shares.
- Listing all the shares on the system and the users connected to them.
- Disconnecting one or all of the users connected to the system or to a specific share.
- Closing one or all of the shared resources that are currently open.
- Viewing an event log.

To Use the Computer Management tool

1. Start Computer Management.
2. Select **Connect to another computer.**



3. If necessary, specify the domain in "**look in**".



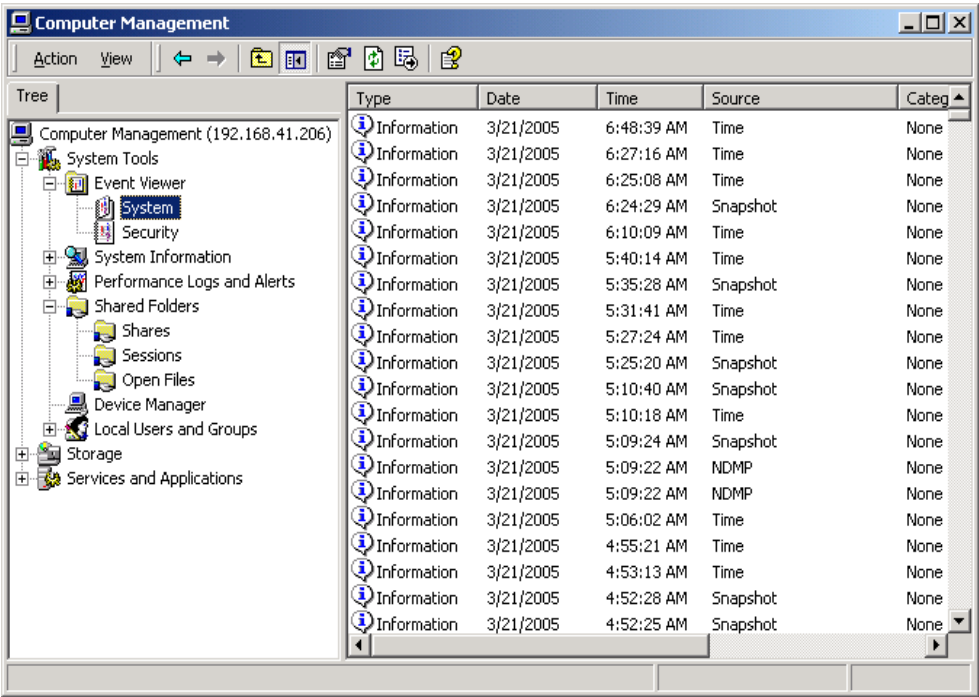
4. Select a name or an IP address that is used for file services on Titan.



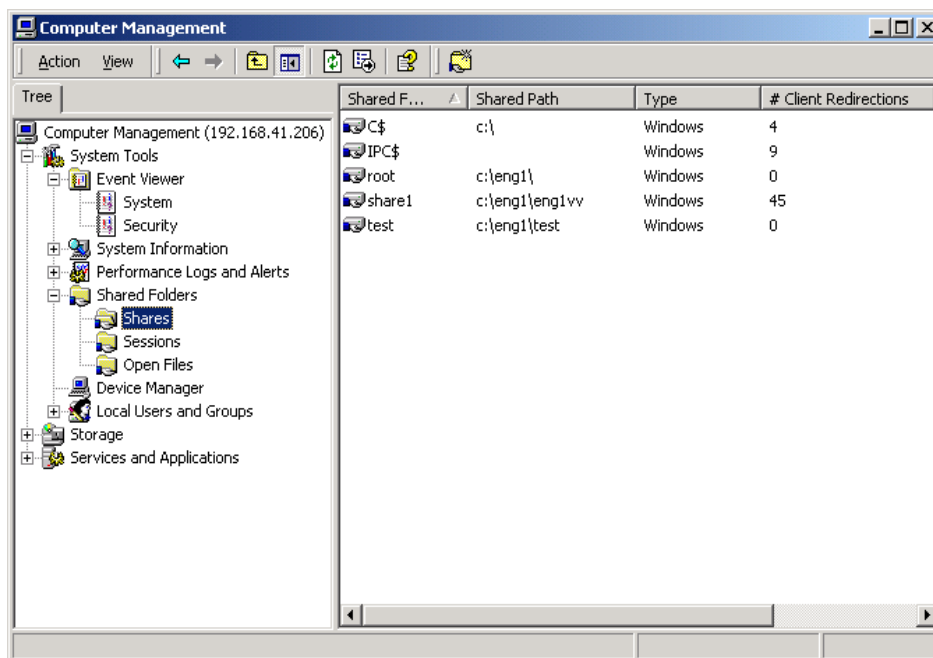
Note: Do not specify a server administration name or [IP address](#) for this purpose.

5. Click **OK**.

- 6. Do one or more of the following:
 - ❑ To view the server's event log, click **Event Viewer**.



- ❑ To list all the shares, click **Shares**. Some or all of the users can be disconnected from specific shares.



- ❑ To list all the open shared resources, click Open Files. Some or all of the shared resources can be closed.
- ❑ To list all users who are currently connected to the system, click Sessions. Some or all of the users can be disconnected.

Creating or Managing Shares

When adding a share, enter the name of the folder to share in the text box provided. The format for this text box is, c:\volname\pathname. volname is the volume on the server and pathname is the path on that volume that is to be shared. For example,

c:\volname
c:\volname\pathname

Paths must exist before they can be shared.



Note: Trailing backslashes are not permitted at the end of the manually entered string.

Transferring files with FTP

This section explains how to set up File Transfer Protocol (FTP) so that users with FTP clients can access files and directories on Titan. As part of the setup process, *mount points* must be created on the File Systems to which to allow FTP access. Then, the login details of FTP users must be specified to associate them with the mount points.

The Titan SiliconServer and FTP

The Titan SiliconServer implements the file-serving functions of an FTP server. Titan provides the file-serving functions required for:

- Mount point manipulation
- File manipulation
- Directory manipulation
- File access control, i.e. permissions

Pre-requisites

Prior to allowing FTP access to the system, FTP [service must be enabled](#). No license key is required for this protocol.

FTP Statistics

[Statistics](#) are available to monitor FTP activity since Titan was last started or its statistics were reset. The statistics are updated every ten seconds.

Configuring FTP Preferences

As part of the process of setting up FTP, choose a service for authenticating the passwords of the FTP users. Also, a timeout must be set with which to end FTP sessions that have been inactive.

To Configure FTP Preferences

1. From the **Home** page, click **File Services**. Then, click **FTP Configuration**.

The screenshot shows the BlueArc Titan web interface for FTP Configuration. The header includes the BlueArc logo, a status bar showing 'Titan - 192.0.2.2' and 'Advanced Mode: OFF', and navigation links for Help, About, and Sign Out. The breadcrumb trail is 'Home > File Services > FTP Configuration'. The main content area is titled 'FTP Configuration' and contains the following settings:

- Password Authentication Services:**
 - NT: ☒
 - NIS: ☐
- Session timeout:**
 - Timeout (mins):

An 'Apply' button is located at the bottom of the configuration area.

2. Select the **Password Authentication Services: NT** or **NIS**. The password authentication services are used to authenticate FTP users. The security mode in which the system is operating determines which of the services is available.

Depending on the service you choose, an FTP user must log in with an NT domain user name and password, which is authenticated through a domain controller, or a UNIX user name and password, which is authenticated through a [NIS server](#).

The configured security mode determines what password authentication service methods can be used. See the section [File System Security](#) for more information about security modes:

If operating in **UNIX** or **Mixed** security mode, both NT and NIS password authentication is supported. If both services are enabled, the FTP user will be authenticated against the configured NT domain first. If authentication fails, Titan will attempt to authenticate the user against the configured NIS domain.

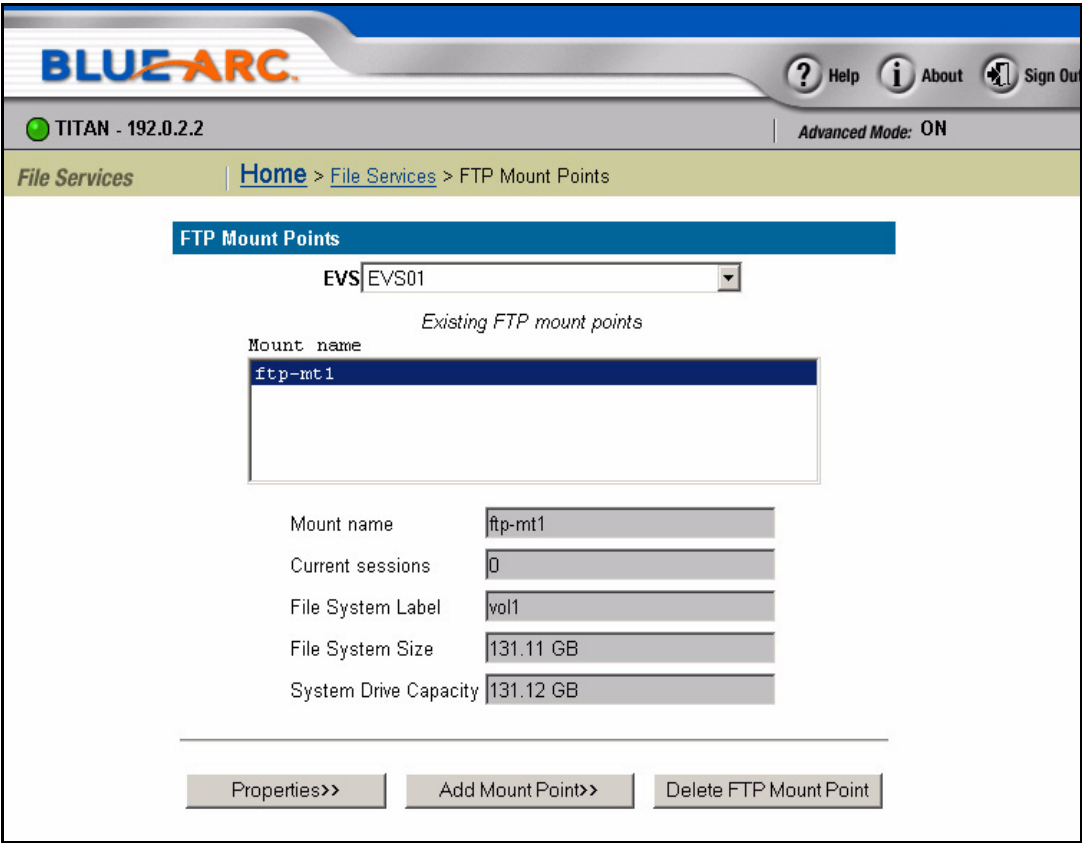
3. In the **Timeout (mins)** field, enter the number of minutes of inactivity after which to end an FTP session automatically. The value must be at least 15 minutes.
4. Click **Apply**.

Setting up FTP Mount Points

One or more mount points can be set up on the file systems to allow FTP access. Each mount point specifies the location within a directory hierarchy that users may access over FTP. Once the mount points have been set up, [FTP users](#) can be assigned to them.

To Set Up FTP Mount Points

1. From the **Home** page, click **File Services**. Then, click **FTP Mount Points**.



Item /Field	Description
EVS	Select the EVS , on which to view the configured Mount Points.
Existing FTP mount points	
Mount name	The box will list any existing mount point names.
Current sessions	The number of active current sessions.

Transferring files with FTP

File System Label	The label for the file system to which the selected mount point is added.
File System Size	The size of the file system to which the selected mount point is added.
System Drive Capacity	The storage capacity of the system drive on which the file system resides.

2. Click **Add Mount Point>>**.

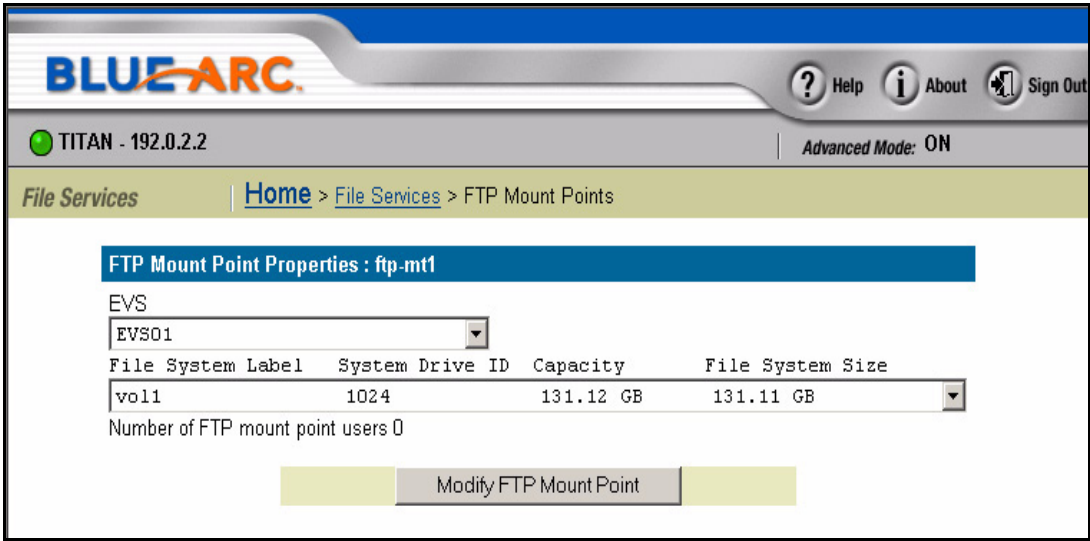
The screenshot shows the BLUE ARC TITAN web interface. At the top, there's a header with the BLUE ARC logo and navigation links: ? Help, i About, and a Sign Out button. Below the header, a status bar shows 'TITAN - 192.0.2.2' and 'Advanced Mode: ON'. The main navigation bar includes 'File Services' and a breadcrumb trail: 'Home > File Services > FTP Mount Points'. The central area is titled 'Add FTP Mount Point' and contains a form. The form has a dropdown menu for 'EVS' with 'EVS01' selected. Below this is a table with columns: 'File System Label', 'System Drive ID', 'Capacity', and 'File System Size'. The table contains one row with values: 'vol1', '1024', '131.12 GB', and '131.11 GB'. Below the table is a text input field for 'FTP mount point name'. At the bottom of the form is a button labeled 'Add FTP Mount Point'.

3. Select the EVS from the drop-down list on which to add a FTP mount point.
4. Using the drop-down list, select the **File System** on which to create the mount point.
5. Enter the **FTP mount point name**.
6. Click **Add FTP Mount Point**.

To View/Modify Mount Point Properties

1. From the **Home** page, click **Files Services**. Then, click **FTP Mount Point**.
2. Select the **EVS** from the drop-down list on which to view the existing mount points.
3. Select the mount point from the list.

4. Click **Properties>>**.



5. To change the EVS to which the mount point is added, select the new **EVS** from the drop-down list.
6. Using the drop-down list, select the new **File System**.



Note: The Number of FTP mount point users is also displayed on the **FTP Mount Point Properties** page. It is recommended not to change the file system assigned to the mount point while FTP users are currently connected.

7. Click **Modify FTP Mount Point**.

Setting Up FTP Users

At least one FTP user for each mount point must be defined. FTP users can be manually setup or their details can be imported from a file.

To Set Up A FTP User

1. From the **Home** page, click **Files Services**. Then, click **FTP Users**.

The screenshot shows the BLUE ARC TITAN web interface. At the top, there's a header with the BLUE ARC logo, navigation links (Help, About, Sign Out), and system information (TITAN - 192.0.2.2, Advanced Mode: ON). Below the header, a breadcrumb trail shows 'Home > File Services > FTP Users'. The main content area is titled 'FTP Users' and features a dropdown menu for selecting an EVS, currently set to 'EVS01'. Below this, a list of existing FTP users is shown, with 'ftp' selected. The user details for 'ftp' are displayed: Mount name (ftp-mt1), Initial directory (/ftp1), File System Label (vol1), and File System Size (131.11 GB). At the bottom, there's a section for 'Import FTP Users' with a filename input field, 'Browse...' and 'Import File' buttons, and three action buttons: 'Properties>>', 'Add User>>', and 'Delete FTP User'.

Item / Field	Description
EVS	Select the EVS on which to view configured FTP users.
Existing FTP Users	
(Up to 500 users shown) User name	The box will display a list of existing FTP users.
Mount name	The mount name to which the selected FTP user is added.
Initial directory	The path of the directory in which the selected FTP user starts when logged in over FTP.
File System Label	The label for the file system that contains the mount point.
File System Size	The size of the file system that contains the mount point.

Import FTP Users	
Filename	The filename to import an FTP User. Use the browse... to find the file name. Then, click Import File .

- 2. Click **Add User>>**.
- 3. Select the **EVS** to which the FTP User is added.
- 4. Using the drop-down list, select the **FTP Mount Point** to which the FTP user will be assigned.
- 5. Enter the **FTP user name**. Enter **anonymous** or **ftp** for anonymous ftp access.
- 6. Enter the **Initial directory for the FTP user**. This is the directory in which the FTP user starts when logging in over FTP.
- 7. To create the path automatically when it does not exist, check the box **Ensure path exists**.
- 8. Click **Add FTP User**.

To Import A FTP User

- 1. From the **Home** page, click **Files Services**. Then, click **FTP Users**.
- 2. Under the **Import FTP User** heading, enter the file name that contains the user details.
- 3. Click **Browse** to search for the filename.
The entries in the filename must follow this pattern:
user_name mount_point initial_directory
For example:
carla Sales /Sales/Documents
miles Sales /Sales
john Marketing /Marketing
- 4. Click **Import File**.

To View / Modify FTP Users

1. From the **Home** page, click **Files Services**. Then, click **FTP Users**.
2. Click **Properties>>**.

BLUEARC

TITAN - 192.0.2.2 | Advanced Mode: OFF

File Services | [Home](#) > [File Services](#) > Modify FTP Mount Points

FTP Mount Point Properties : vol0

EVS

EVS01

File System Label	System Drive ID	Capacity	File System Size
vol0	1024	393.38 GB	393.33 GB

Number of FTP mount point users 0

Modify FTP Mount Point

3. To modify the **EVS** to which the FTP User is added, select the **EVS** from the drop-down list.
4. Using the drop-down list, select a new **FTP Mount Point** to which the FTP User is assigned. An asterisk next to the mount name is noted if the FTP mount point has been selected.
5. To change the **Initial directory for the FTP user**, enter the new path.
6. To locate the path, click **Browse>>**.
7. Uncheck the box **Ensure path exists** if checked.
8. Click **Modify FTP User**.

Setting Up FTP Audit Logging

FTP generates an audit log to keep track of user activity. The system will record the event when each time a user takes any of the following actions:

- Logging in or out
- Renaming or deleting a file
- Retrieving, appending or storing a file
- Creating or removing a directory

The system also records when a session timeout occurs.

Each log file is a tab-delimited text file containing one line per FTP event. Besides logging the date and time at which an event occurs, the system logs the user name and IP address of the client and a description of the executed command. The newest log file is called ftp.log, and the older files are called ftp*n*.log (the larger the value of *n*, the older the file).

To Configure FTP Audit Logging

- 1. From the **Home** page, click **Files Services**. Then, click **FTP Audit Logging**.

BLUE ARC

?

Help

i

About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: ON

File Services | Home > File Services > FTP Audit Logging

FTP Audit Logging

EVS

EVS01

☒ Enable Logging

File System Label	System Drive ID	Capacity	File System Size
vol1	1024	131.12 GB	131.11 GB

*The Logging File System is not currently set.

Logging Directory

☐ Ensure path exists

No. Records per log file

10000

Number of log files

10

Apply

Cancel

Item /Field	Description
EVS	Select the EVS on which the FTP Audit log is located.
Enable Logging	If the box is checked, FTP audit logging is enabled.
File System	Select a File System on which to keep the log files.
Logging Directory	The directory on the specified file system in which to keep the log files.
Ensure path exists	If the box is checked, the Logging Directory is automatically created if it does not exist.
No. Records per log file	The maximum number of records to store in each log file.

Number of log files	The maximum number of log files to keep. Once it has reached this limit, the server deletes the oldest log file each time it creates a new one.

2. Click **Apply** after completing the set up.

Block-Level Access through iSCSI

The Titan SiliconServer supports iSCSI. The Internet Small Computer System Interface (iSCSI) protocol enables block level data transfer between requesting applications and iSCSI Target devices. Using Microsoft's iSCSI Software Initiator (version 1.06 or later), Windows servers can view iSCSI Targets as locally attached hard disks. Windows can create file systems on iSCSI targets, and read and write data as if it was on a "local disk". Window server applications, such as Microsoft Exchange and Microsoft SQL Server can operate using iSCSI Targets as data repositories.



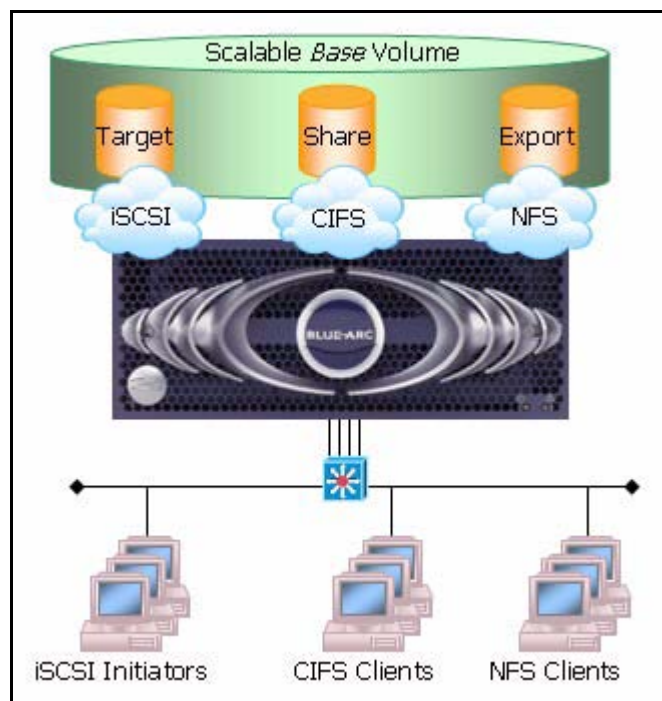
The Titan SiliconServer iSCSI implementation has attained the 'Designed for Windows Server™ 2003' certification from Microsoft. The 'Designed for Windows Server™ 2003' logo helps customers identify products that deliver a high quality computing experience with the Microsoft Windows Server 2003' operating system.

The Titan SiliconServer and iSCSI

To use iSCSI storage on Titan, one or more iSCSI Logical Units (LUs) must be defined. iSCSI Logical Units are blocks of SCSI storage that are accessed through iSCSI Targets. iSCSI Targets can be found through an iSNS database or through a Target Portal. Once an iSCSI Target has been found, an Initiator running on a Windows server can access the Logical Unit as a “local disk” through its Target. Security mechanisms can be used to prevent unauthorized access to iSCSI Targets.

On Titan, iSCSI Logical Units are just regular files residing on a file system. As a result, iSCSI benefits from file system management functions provided by Titan, such as NVRAM logging, snapshots, and quotas.

The contents of the iSCSI Logical Units are managed on the Windows server. Where Titan views the Logical Units as files containing raw data, Windows views each iSCSI Target as a logical disk, and manages it as a file system volume (typically using NTFS). As a result, individual files inside of the iSCSI Logical Units can only be accessed from the Windows server. Titan services, such as snapshots, only operate on entire NTFS volumes and not on individual files.



iSCSI Access Statistics

[Statistics](#) are available to monitor iSCSI activity since Titan was last started or its statistics were reset. The statistics are updated every ten seconds.

Prerequisites

To enable iSCSI capability:

- ❑ [Enter an iSCSI license key.](#)
- ❑ [Enable the iSCSI service.](#)

Offload Engines

Titan currently supports the use of the Alacritech SES1001T and SES1001F offload engines when used with the Microsoft iSCSI initiator version 1.06 or later. Check with BlueArc Support for the latest list of supported offload engines.

Configuring iSCSI

In order to configure iSCSI on Titan, the following needs to be defined:

- ❑ The iSCSI Domain.
- ❑ iSNS Servers.
- ❑ iSCSI Logical Units.
- ❑ iSCSI Targets.
- ❑ iSCSI Initiators (if using mutual authentication).

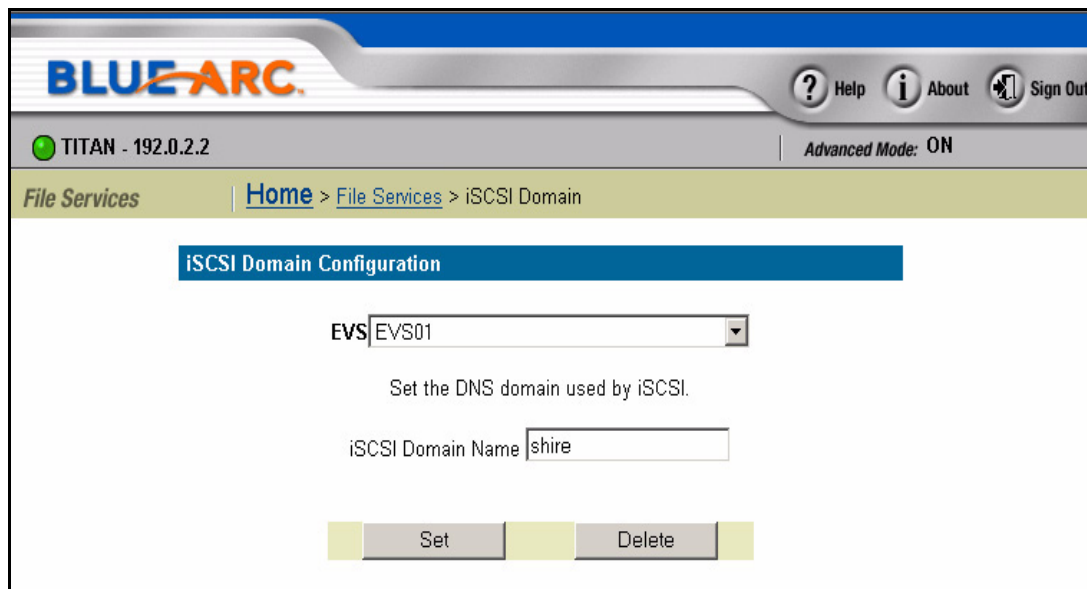
Setting the iSCSI Domain

The iSCSI Domain is the DNS domain used by iSCSI when creating unique qualified names for iSCSI Targets.



Note: The iSCSI domain is maintained independently of the server's DNS configuration.

From the **Home** page, click **File Services**. Then, click **iSCSI Domain**.



The screenshot shows the BlueArc Titan web interface. At the top, the BlueArc logo is on the left, and navigation links for Help, About, and Sign Out are on the right. Below the header, a status bar shows 'TITAN - 192.0.2.2' and 'Advanced Mode: ON'. A breadcrumb trail indicates the path: 'File Services > Home > File Services > iSCSI Domain'. The main content area is titled 'iSCSI Domain Configuration'. It features a dropdown menu labeled 'EVS' with 'EVS01' selected. Below this, a text label reads 'Set the DNS domain used by iSCSI.' followed by a text input field labeled 'iSCSI Domain Name' containing the value 'shire'. At the bottom of the configuration area are two buttons: 'Set' and 'Delete'.

To set the iSCSI Domain name, enter the DNS Domain name used by iSCSI and click **Set**. It is recommended to use the first fully qualified entry in Titan's DNS Search Order configuration.

To delete the currently configured iSCSI Domain name, click **Delete**.

Configuring iSNS

The Internet Storage Name Service (iSNS) is a network database of iSCSI Initiators and Targets. If configured, Titan can add its list of Targets to iSNS, which allows Initiators to easily find them on the network.

The iSNS server list can be managed through the iSNS page. Titan registers its iSCSI Targets with iSNS database when any of the following events occurs:

- A first iSNS server is added.
- An iSCSI Target is added or deleted.
- The iSCSI service is started.
- The iSCSI domain is changed.
- A server IP address is added or removed.

To Add an iSNS Server

1. From the **Home** page, click **File Services**. Then, click **iSNS**.

BLUEARC

TITAN - 192.0.2.2 | Advanced Mode: ON

File Services | Home > File Services > iSNS Servers

iSNS Configuration

EVS EVS01

IP Address	Port
192.168.41.1	3205

Add>> Delete

2. Select the **EVS** on which to add the iSNS server.
3. Click **Add>>**.
4. Enter the IP Address of the iSNS server. The default Port number is 3205.
5. Click **Apply**.

To view or modify the list of the iSNS servers, click the **iSNS** link on the **File Services** page, and then select the EVS from the drop-down list.



Note: To download the latest version of Microsoft iSNS Server, visit:

<http://www.microsoft.com>

Setting up iSCSI Logical Units

An iSCSI Logical Unit (LU) is a block of storage that can be accessed by iSCSI initiators as a locally attached hard disk. A Logical Unit is stored as a file on the Titan file system. Like any other data set on the file system, iSCSI Logical Units can be bound in size using Titan's size management tools, including **Virtual Volumes** and quotas. Logical Units are created with a specific initial size but can be extended over time, as demand requires.

After a Logical Unit has been created and the iSCSI domain name has been set, an iSCSI Target must be created to allow access to the Logical Unit. A maximum of 32 Logical Units can be configured for each iSCSI Target.

Logical Unit Management

An iSCSI Logical Unit is a file within one of Titan's File Systems. Such a file must have a *.iscsi* extension to identify it as an iSCSI Logical Unit. However, apart from this extension there is no other way to determine that a file does indeed represent a Logical Unit.



Note: BlueArc recommends that all iSCSI Logical Units are placed within a well-known directory, for example */.iscsi/*. This provides a single repository for the Logical Units in a known location.

Logical Unit Security

As Logical Units are files, they can be accessed over other protocols, such as CIFS and NFS. This renders the Logical Units vulnerable to malicious users who can modify, rename, delete or otherwise affect them.



Note: BlueArc recommends that sufficient security is set on either the Logical Units' files, the directory in which they reside, or both, to prevent unwanted accesses. If possible, Logical Units should be placed in a directory that isn't accessible via users' CIFS shares or NFS exports.

Concurrent Access to Logical Units

The Titan SiliconServer's iSCSI implementation allows multiple initiators to connect to a single Logical Unit. This is necessary for applications and operating systems that support, or rely upon, concurrent file system access. However, concurrent access can be detrimental to a client machine when the client is oblivious to others accessing the file system.

For example, imagine two independent Microsoft Windows clients who both connect to the same Logical Unit, containing an NTFS file system. If each client modifies data, metadata, and system files without any knowledge of the other, these conflicting disk updates will quickly corrupt the file system. Such a scenario should be strictly avoided.

As another example, imagine a Logical Unit that contains two distinct NTFS partitions. Suppose that one Microsoft Windows client connects to the Logical Unit and accesses only the first partition. Then, a second, independent Microsoft Windows client connects to the Logical Unit and accesses only the second partition. Even though the two clients are accessing separate partitions within the Logical Unit, this scenario should be avoided because a Microsoft iSCSI client will attempt to mount each partition it encounters on the Logical Unit. When a Microsoft Windows client mounts an NTFS partition, it updates system files. Therefore, mounting an NTFS partition concurrently from separate Microsoft Windows clients will cause conflicting system file updates and will cause one or both of the clients to fail.

Taking Snapshots of Logical Units

The contents of an iSCSI Logical Unit are controlled entirely by the client that's using it. Titan cannot interpret the file systems or other data contained within a Logical Unit in any way. Therefore, Titan has no knowledge of whether the data held within an iSCSI Logical Unit is in a consistent state. This introduces a potential problem when taking a snapshot of a Logical Unit. For example, when a client creates a file, it must also add the file's name to the directory in which it's being created. This means that more than one write is required to complete the operation. If Titan takes a snapshot after the file object has been created, but before its name has been inserted into the directory, then the file system contained within the snapshot won't be consistent. If another client were to view the snapshot copy of the file system, it would see a file object without a name in any directory. There are many other ways in which a snapshot copy of a file system can be corrupted.



Caution: BlueArc recommends that prior to taking a snapshot of an iSCSI Logical Unit, all applications should be brought into a known state. A database, for example, should be quiesced. Disconnecting the iSCSI initiators from the Logical Units undergoing snapshot is also recommended. This guarantees that all pending writes are sent to the Logical Unit before the snapshot is taken.

Volume Full Conditions

When a client uses a direct attached disk, it can monitor the amount of free space that's available. If there is no free space within a partition, the client can return a Volume Full condition accordingly. The client can ensure the file system on the partition isn't corrupted due to running out of disk space part way through an operation.

However, if the disk is located on an iSCSI Logical Unit, a Volume Full condition can be hit even if partitions within the Logical Unit contain free space. This is because with snapshots enabled, old data is preserved instead of being overwritten. So, overwriting an area of a Logical Unit will cause extra disk space to be allocated on Titan, even though no extra space will be used up within the client's partition. In this case, the client may receive a Volume Full condition part-way through an operation, causing the file system to be corrupted. Although this corruption should be fixable, this situation should be avoided.



Note: BlueArc recommends that sufficient disk space be allocated on Titan to contain all iSCSI Logical Units and snapshots. Careful monitoring of free disk space is also recommended.

To Add, Delete, or Modify an iSCSI Logical Unit

From the **Home** page, click **File Services**. Then, click **iSCSI Logical Units**.

BLUE-ARC

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

File Services | [Home](#) > [File Services](#) > iSCSI Logical Units

iSCSI Logical Units

EVS

EVS01

Exchange2003

SQL2003

Name

Exchange2003

Path

/exch03.iscsi

Comment

Logical Unit Size

500 MB

File System Label

vol0

File System Mounted

Yes

Logical Unit Mounted

Yes

Properties>>

Add>>

Delete

Delete All

The table below describes the fields on this screen:

Item / Field	Description
EVS	Select the EVS on which to create the Logical Unit.
Name	Identifies the name of the Logical Unit.
Path	The path where the Logical Unit resides. Logical units appear as regular files in Titan File Systems.
Comment	Additional information related to the Logical Unit.
Logical Unit Size	The size of the Logical Unit.  Note: The maximum size of a Logical Unit is 2 TB. This limit is imposed by the SCSI protocol.
File System Label	The name of the file system used to host the Logical Unit.

File System Mounted	Indicates whether the file system is mounted or not.
Logical Unit Mounted	Indicates whether the Logical Unit is mounted or not.

To Add An iSCSI Logical Unit

1. To configure an iSCSI Logical Unit, click **Add>>** on the **iSCSI Logical Units** page.

The screenshot shows the BlueArc TITAN web interface. The top navigation bar includes the BlueArc logo, a status bar for 'TITAN - 192.0.2.2', and links for Help, About, and Sign Out. The breadcrumb trail is 'Home > File Services > Add iSCSI Logical Units'. The main form is titled 'Add iSCSI Logical Unit' and contains the following fields and options:

- EVS**: A dropdown menu with 'EVS01' selected.
- File System Label**: A table with columns 'File System Label', 'System Drive ID', 'Capacity', and 'File System Size'. The row 'vol0' is selected, showing '1024' for System Drive ID, '393.38 GB' for Capacity, and '393.33 GB' for File System Size.
- Name**: A text input field containing 'Exchange2003'.
- Path**: A text input field containing '/vol0/exchange2003', with a 'Browse>>' button to its right.
- Comment**: An empty text input field.
- Size**: A text input field containing '500' and a unit dropdown menu set to 'GB'.
- File Already Exists**: An unchecked checkbox.
- Ensure Path Exists**: A checked checkbox.
- Buttons**: 'Apply' and 'Cancel' buttons at the bottom.

2. Select the **EVS** on which to create the Logical Unit.
3. Select the **File System** on which the Logical Unit will be created.
4. Enter **Name**.
5. Enter **Path**. Click **Browse>>** to find an existing filename or to assist in creating the path. All Logical Unit filenames will have the extension **.iscsi**.
6. Enter additional information about the Logical Unit in **Comment**.
7. Enter the size of the Logical Unit.
8. Select **Bytes, KB, MB, GB, or TB** from the drop-down list.
9. If the file exists, check the box **File Exists**. The Logical Unit will be created on an existing file to restore a back up or a snapshot of a Logical Unit.

To Modify the Properties of an iSCSI Logical Unit

1. Select the Logical Unit from the list.
2. Click **Properties**.
3. Make the necessary changes on the **Logical Units Properties** page.
4. Click **Apply**.

To Delete an iSCSI Logical Unit

1. Select the Logical Unit from the list.
2. Click **Delete**.

Backing Up and Restoring iSCSI Logical Units

When a Logical Unit is backed up, it is backed up as a normal file on a Titan File System. Only a client connected to the Logical Unit through its Target can access and backup the individual files and directories contained in the Logical Unit. If backing up the iSCSI Logical Unit from Titan, either ensure that the iSCSI initiators are disconnected or make the [backup from a snapshot](#).

To Restore An iSCSI Logical Unit

To ensure consistency of data on a Logical Unit, it may be necessary to restore it from a snapshot or a backup. To restore an iSCSI Logical Unit, perform the following steps:

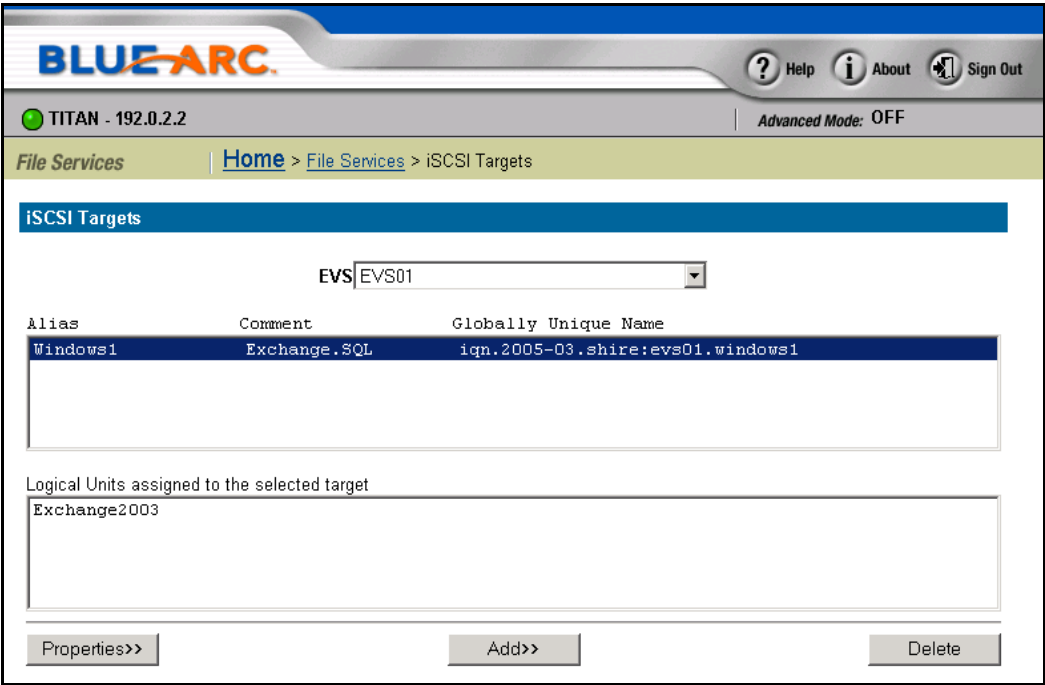
1. Disconnect the iSCSI Initiator from the Target.
2. Unmount the iSCSI Logical Unit by using the following CLI command: `iscsilu unmount <name>`, where name is the name of the Logical Unit.
3. Restore the Logical Unit from a snapshot or backup.
4. Mount the iSCSI Logical Unit by using the following CLI command: `iscsilu mount <name>`, where name is the name of the Logical Unit.
5. Reconnect to the Target using the iSCSI Initiator.
6. Rescan disks in Computer Management.

Setting Up iSCSI Targets

An iSCSI Target is a storage element accessible to iSCSI initiators. These targets appear to iSCSI initiators as different storage devices accessible over the network. Titan supports a maximum of 32 iSCSI Targets per EVS and a maximum of 32 iSCSI sessions per Target.

To Add, Delete, or Modify an iSCSI Target

On the **File Services** page, click **iSCSI Targets**.



The table below describes the fields on this screen:

Item / Field	Description
EVS	Select the EVS on which to create the Target.
Name	Identifies the name of the Target.
Comment	Additional information related to the Target.
Globally Unique Name	The Target's name. The name is generated automatically by the Titan SiliconServer, and is unique across the globe.
Logical Units assigned to the selected Target	Lists the Logical Units assigned to the Target.

To add an iSCSI Target:

On the **iSCSI Targets** page, click the **Add>>** button.

BLUE ARC

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

File Services | Home > File Services > Add iSCSI Targets

Add iSCSI Target

Alias

Comment

Secret

☒ Enable Authentication

Access Configuration

Access configuration text currently 0 characters (max is 4096)

EVS

EVS01

Available logical units

Exchange2003

SQL2003

Logical Unit Number

Add LU

Selected logical units

Logical Unit

LUN

Remove LU

Apply

Cancel

The table below describes the fields on this screen:

Item / Field	Description
Alias	The name of the iSCSI Target.
Comment	Additional information on the iSCSI Target.
Secret	The password used to secure the Target from any unauthorized access. The initiator will need to authenticate against this password when connecting to the Target. The secret must be equal to or greater than 12 characters, but less than 17 characters in length.

Enable Authentication	By default, the box is checked. This enables the authentication of the iSCSI Target.
Access Configuration	Enter the desired access configuration parameters. Refer to the Access Configuration table below for details on how to define the Access Configuration List.
EVS	Select the EVS on which to create the iSCSI Target.
Available Logical Units	A list of Logical Units available to assign to the iSCSI Target.
Logical Unit Number	The number assigned to the Logical Unit (LUN) Enter a Logical Unit Number Click Add LU
Selected Logical Units	
Logical Unit	The Logical Unit associated with the Target.
LUN	The Logical Unit Number (LUN) associated with the Logical Unit for this Target. Up to a maximum of 256 Logical Units may be assigned to a Target.

Access Configuration

What to type	Means
Blank or *	All clients can access the target.
Specific address or name. Examples: 10.168.20.2, client.dept.company.com	Only clients with the specified names or addresses can access the target.
Partial address or name using wildcards. Examples: 10.168.*.*, *.company.com	Clients with matching names or addresses can access the target.

To deny access to a specific host, use the no_access or noaccess qualifier. For example, 10.1.2.38(no_access) will deny access to the host with the IP address 10.1.2.38.

To Modify the Properties of an iSCSI Logical Target

1. Select the Target from the list.
2. Click **Properties**.
3. Make the necessary changes on the **iSCSI Target Properties** page.
4. Click **Apply**.

To Delete an iSCSI Target

- 1. Select the Target from the list.
- 2. Click **Delete**.

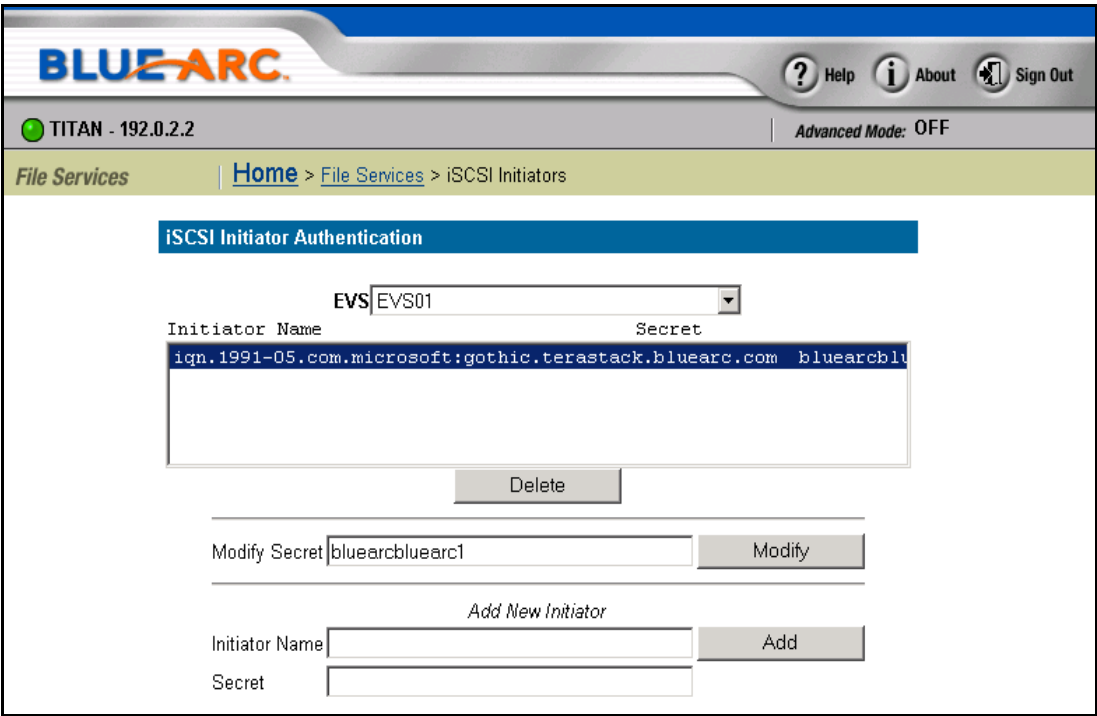
iSCSI Security (Mutual Authentication)

Titan uses the Challenge Handshake Authentication Protocol (CHAP) to authenticate iSCSI Initiators. CHAP requires a “shared secret” known by the Initiator and the Target. Titan also supports mutual authentication where in addition to the Initiator authenticating against the Target on Titan, Titan must also authenticate against the Initiator.

To facilitate with the mutual authentication process, Titan must maintain a list of the Initiators with which it can authenticate and the shared secret for each Initiator.

Configuring Titan for Mutual Authentication

- 1. On the SMU **Home** page, click **File Services**. Then, click **iSCSI Initiator Authentication**.



- 2. Use the drop-down list to select the **EVS** associated with the Target for which mutual authentication is required.
- 3. Enter the **Initiator name**. This is the same name found in the **Change Initiator node name** box on the **Initiator Settings** tab of the Microsoft iSCSI Initiator.

4. Enter the **Secret** for the Initiator. This is the secret which will be entered in the **Initiator Chap Secret** box on the iSCSI Initiator.
5. Click **Add**.
6. If you need to modify a secret, select the Initiator name and secret in the list. Enter a new secret in the **Modify Secret** box. Then, click **Modify**.
7. If you need to delete an Initiator and its secret, select the Initiator name and secret in the list. Then, click **Delete**.

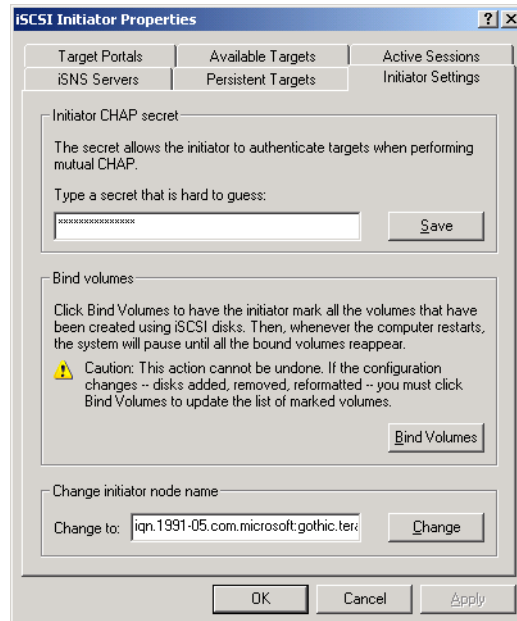
Configuring the Microsoft iSCSI Initiator for Mutual Authentication



Note: For the latest version of Microsoft iSCSI Software Initiator, visit:

<http://www.microsoft.com/>

1. Within the Microsoft's iSCSI Initiator, click the **Initiator Settings** tab.



2. Under the Initiator CHAP secret, enter the secret which allows the Target to authenticate with Initiators when performing mutual CHAP.



Note: The shared secret used to authenticate an Initiator with a Titan should be different from the secret specified when setting up the Target.

3. Click **Save**.
4. Click **OK**.



Note: The **Initiator node name** is the name which should be used as the **Initiator Name** on the iSCSI Initiators page, found under the File Services screen.

Accessing iSCSI Storage

iSCSI Logical Units can be accessed through their Targets using the Microsoft iSCSI Initiator. Discovered through iSNS or through the Target Portal, all iSCSI Targets that are available will be displayed as available Targets by the Initiator.



Caution: Microsoft currently only supports creating a Basic Disk on an iSCSI Logical Unit. To ensure data integrity, do not create a dynamic disk. For more information, refer to the Microsoft iSCSI Initiator User Guide.

An iSCSI Logical Unit will be read-only if its underlying volume is mounted read-only by Titan, or if it is a snapshot copy of another Logical Unit. If a Logical Unit is read-only, then any file systems contained within it will also be read-only. Clients accessing those file systems will not be able to change any part of them, including file data, metadata and system files.

Microsoft Windows 2000 clients cannot mount read-only NTFS file systems, although they can mount read-only FAT and FAT32 file systems. Microsoft Windows 2003 clients can mount read-only FAT, FAT32 and NTFS file systems. If Microsoft Windows clients are required to access read-only NTFS file systems over iSCSI, Microsoft Windows 2003 must be used.

iSCSI MPIO

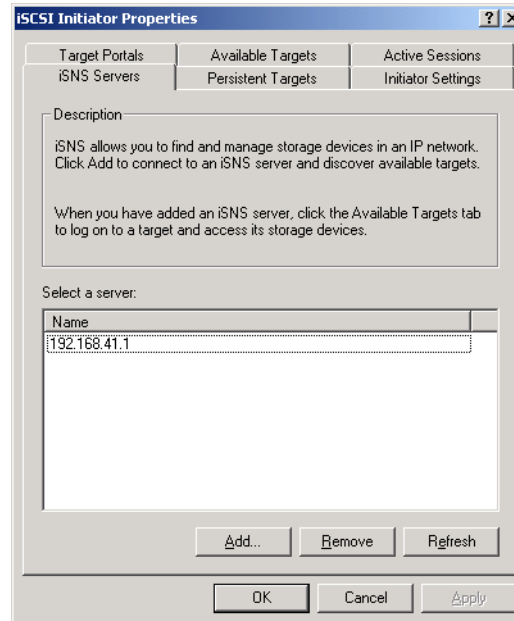
iSCSI MPIO (Multi-path Input/Output) is a technology that uses redundant paths to create logical "paths" between the client and iSCSI storage. In the event that one or more of these components fails, causing the path to fail, multi-pathing logic uses an alternate path so that applications can still access their data.

For example, clients with more than one ethernet connection can use them to establish a multi-path connection to an iSCSI target on Titan. One way it can be used is if one path is redundant, so if one connection fails, the iSCSI session will continue uninterrupted through the remaining paths. Another way the connection can be used is to load-balance the communication to boost performance.

iSCSI MPIO is supported by Microsoft iSCSI Initiator 2.0.

Using iSNS to find iSCSI Targets

1. Using iSNS is the easiest way to find iSCSI Targets on the network. If the network is configured with an iSNS server, configure the Microsoft iSCSI Initiator to use iSNS.
2. Click on the **iSNS Servers** tab.
3. Click **Add**.
4. Enter the iSNS Server's IP Address or DNS name.
5. Click **OK**.



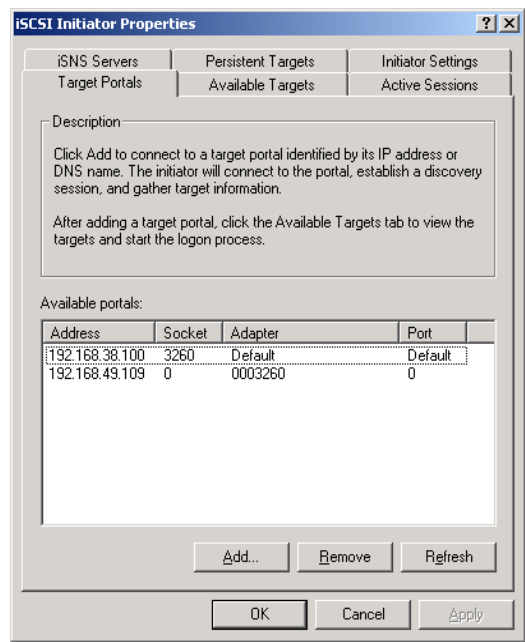
After the iSNS server(s) have been added, all available iSCSI Targets that have been registered in iSNS will appear as available Targets.

Using Target Portals to find iSCSI Targets

If there are no iSNS servers on the network, iSCSI Targets can be found through the use of Target Portals. Add the Titan's file services IP to the Target Portals list to find Targets associated with that server or EVS.

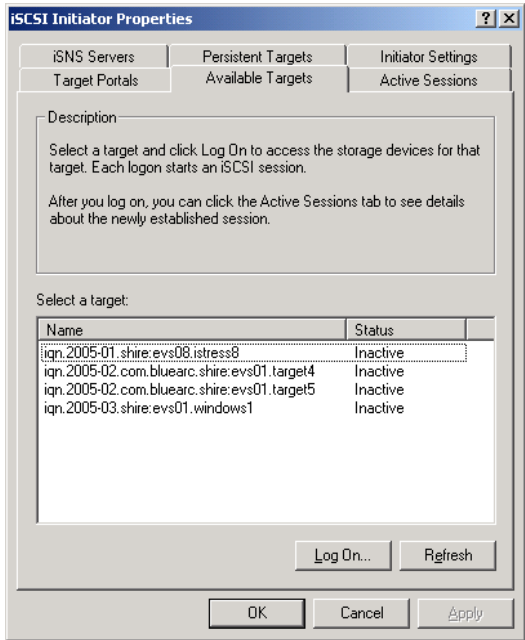
1. Click on the **Target Portals** tab.
2. Click **Add**.
3. Enter the file service IP address for the Titan SiliconServer.

- 4. Click **OK**.



To access available iSCSI Targets

- 1. Click on the **Available Targets** tab.

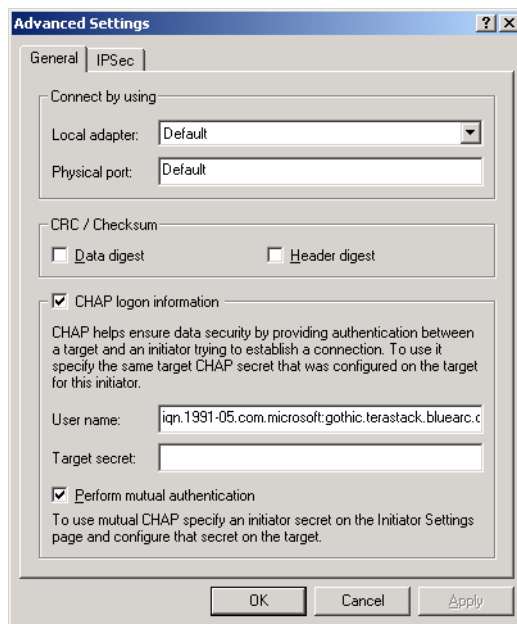


2. Select the Target to which you want to connect. Each logon starts an iSCSI session.



Note: A maximum of 32 iSCSI sessions are allowed per Target.

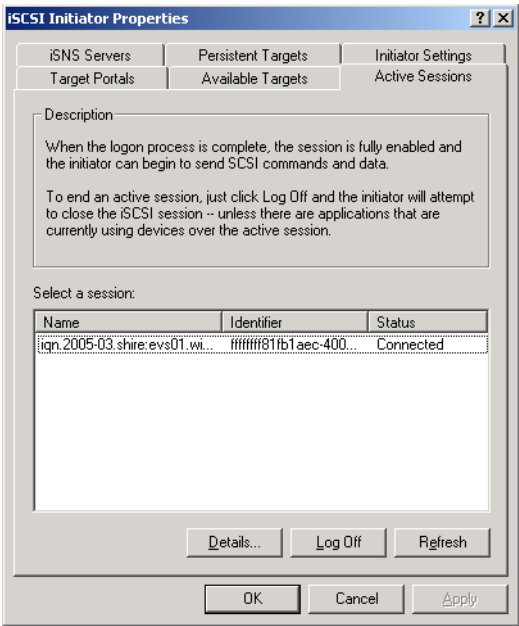
3. Click **Log On**.
4. If authentication is enabled on the Target, click **Advanced...**



5. Check the box for **CHAP logon information**.
6. Enter the Target secret, which is the password configured when the iSCSI Target was created.
7. If Mutual Authentication has been configured, check **Perform mutual authentication**.
8. Click **OK**.
9. On the **Log On Dialog** screen, click **OK**.

To Verify an Active Session

After the connection has been established, click the **Active Sessions** tab to view any details about the newly established session.

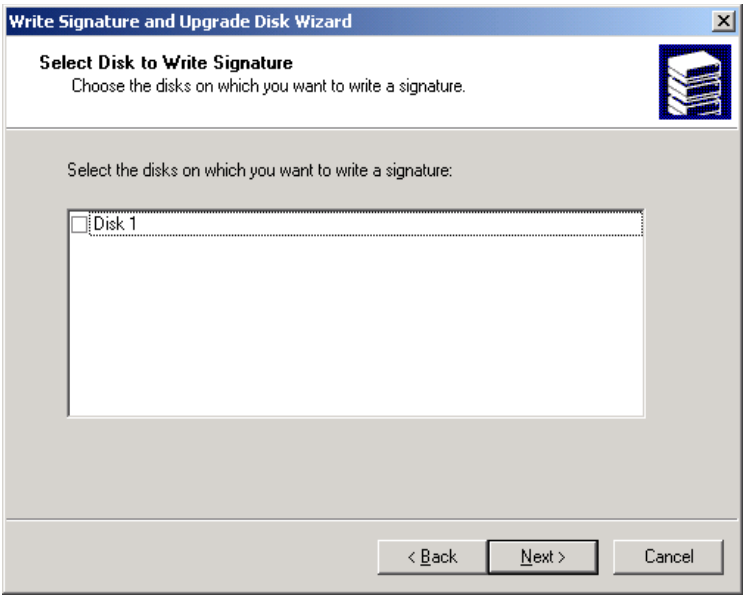


- 1. The Target should appear as **Connected**.
- 2. To end an active session, click **Log Off** and the initiator will attempt to close the iSCSI session if there are no applications currently using the devices.

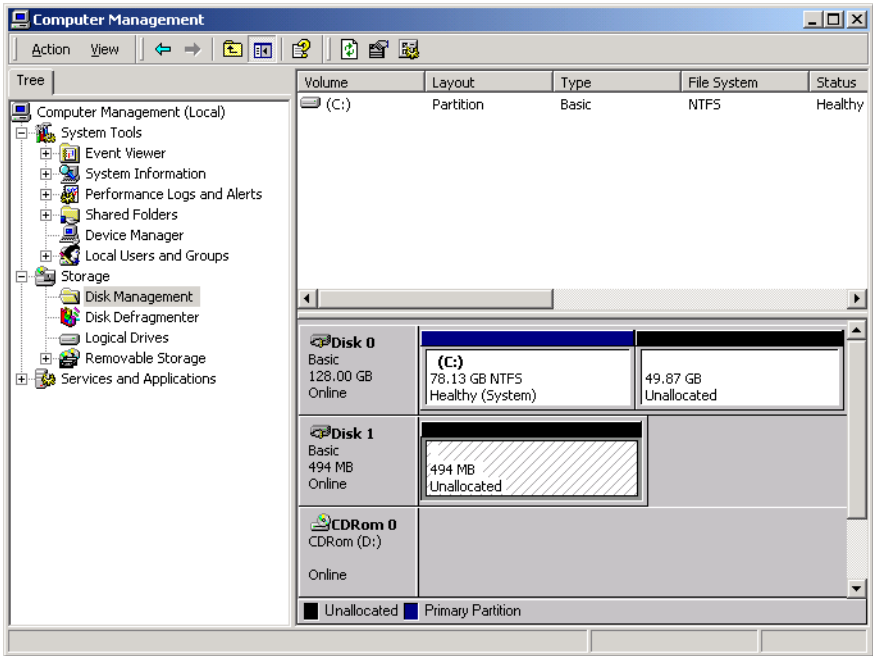
Using Computer Manager to set up your iSCSI storage

The iSCSI “local disk” will need to be configured through **Computer Management**, which can be found in **Control Panel > Administrative Tools**.

- 1. Click on **Disk Management**.
- 2. If this is the first connection to the iSCSI storage, the **Write Signature and Upgrade Disk Wizard** prompt further action.



- 3. Follow the prompts to add the Windows signature to your iSCSI “local disk”.
- 4. Once the **Write Signature Wizard** has been finished, a **Completed** screen should appear.
- 5. Click **Finish**.



- 6. Prepare the disk for use through the Windows disk management tools.

7 Data Protection

Data Protection Overview

The data protection attributes of the file system (file system consistency and NVRAM protection) can be configured by the system administrator to ensure that all the data on the system is protected. The data protection services include snapshots, anti-virus support, data replication, NDMP backup, etc.

The Titan SiliconServer uses a unique hardware based File System, which delivers outstanding performance, and, at the same time, preserves the data in the event of an unexpected failure such as a power loss.

Checkpoints

To guarantee File System consistency, complete and consistent File System images ("checkpoints") are periodically written to the storage subsystem. Additionally, any File System modifications that have started and are not included in an on-disk checkpoint are buffered in NVRAM. An acknowledgement for an operation is only returned to the client once all resulting File System modifications have been buffered in NVRAM and also mirrored if in a cluster. Titan provides [statistics](#) to monitor NVRAM activity.

The checkpoint process ensures that all file system metadata is always internally consistent even after a system failure. In order to ensure File System consistency, a File System "checkpoint" is written to the storage at regular intervals. Every checkpoint is internally consistent. In the event of a system failure, the file system can be "rolled back" to the last successful checkpoint thus ensuring that file system consistency is never lost.

Protecting the Data from Failures

Every request to modify the File System is buffered in NVRAM until the checkpoint containing the modification has been successfully written to the storage. If a system failure occurs, the File System can be rolled back to the last successful checkpoint and then any requests buffered in the NVRAM can be replayed. This ensures that once modification requests have been acknowledged by the server (to the client) they cannot be lost.

Buffering the requests in local NVRAM ensures that software failure or power failure will not result in data loss. Additionally, nodes in a Titan cluster will mirror the contents of their NVRAM to a partner node so that even a single server hardware failure will not result in data loss.

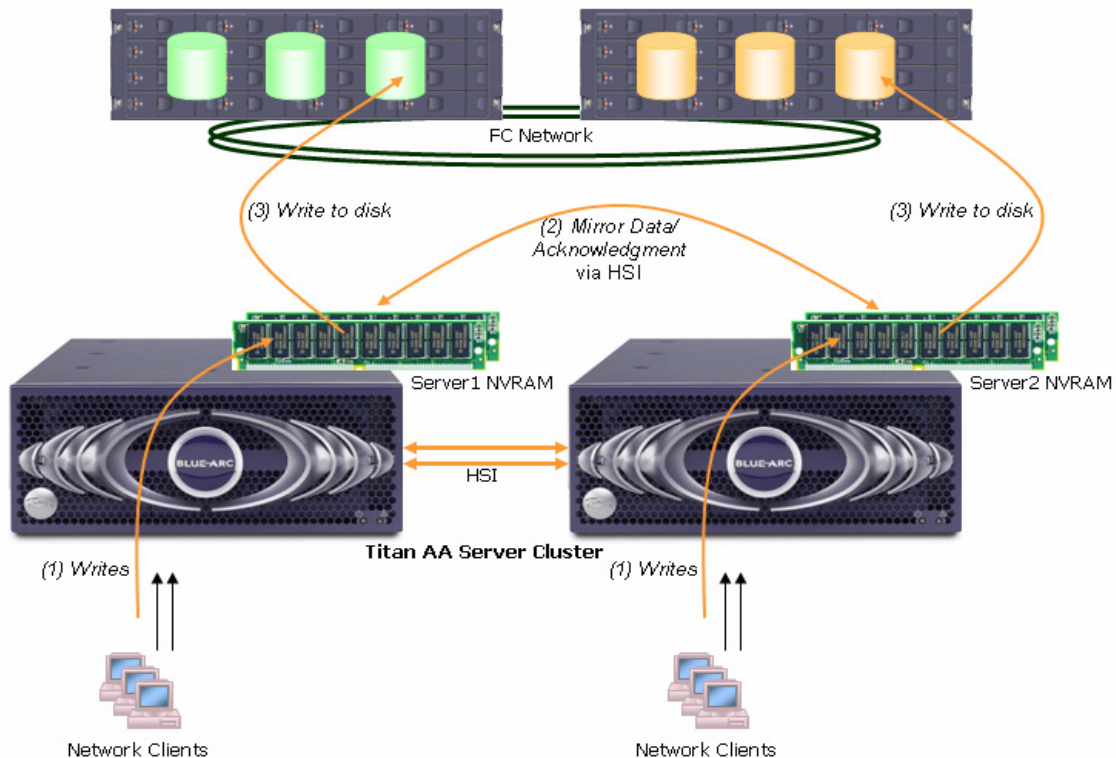
Power Failure Recovery

In the event of a power failure the contents of the NVRAM are preserved (using dedicated battery backup) for a maximum of 72 hours. Once power is restored, the original server can roll back all its File Systems and replay the modifications stored in the NVRAM log.

Buffering in a Cluster Configuration

When Titan is configured as a cluster, in addition to buffering all the File System modifications, each Cluster Node mirrors the NVRAM contents of the other Cluster Node which ensures data integrity in the event of a Cluster Node failure. When a Cluster Node takes over for the failed node, it uses the contents of the NVRAM mirror to complete all File System modifications that were not yet committed to the storage by the failed server.

NVRAM data is mirrored between the Cluster Nodes in this diagram.



FS NVRAM Statistics

[Statistics](#) are available to monitor NVRAM activity. The statistics are updated every ten seconds.

Using Snapshots

Designed for users whose data availability cannot be disrupted by management functions such as system backup and data recovery, snapshots create near-instantaneous, read-only images of an entire file system at a specific point in time. By using snapshots it is safe to create backups from a running system, and allow users to easily restore files that they may have accidentally lost without having to retrieve the data from backup media, such as tape.

Snapshots Concepts

Management functions such as system backups usually take a long time, and consequently the backup program may be copying files to the backup media at the same time that users are modifying those files. This may mean that the backup copies are not a consistent set. A snapshot is a frozen image of a file system, so it is possible to take a backup copy of the snapshot rather than the live File System without worrying about users changing files as they are backed up. The snapshot appears to a network user like a directory tree, and users with the appropriate access rights can retrieve the files and directories that it contains through CIFS, NFS, FTP, or NDMP.

Snapshots preserves disk blocks that are changing in the live file system. A snapshot only contains those blocks that have changed on the live File System since the snapshot was created. This means that the disk space occupied by a snapshot is a fraction of that used by the original File System. Nevertheless, [the space occupied by a snapshot](#) grows overtime as the live file system changes.

Accessing Snapshots

Snapshots are easily accessible from NFS exports and CIFS shares, so that users can restore older versions of files without requiring intervention. The root directory in any NFS export contains a “.snapshot” directory which, in turn, contains directory trees for each of the snapshots. Each of these directory trees consists of a “frozen” image of the files that were accessible from the export at the time the snapshot was taken (access privileges for these files are preserved intact). Similarly, the top-level folder in any CIFS share contains a “~snapshot” folder with similar characteristics. Both with NFS and with CIFS, each directory accessible from the export (share) also contains a hidden “.snapshot” (“~snapshot”) directory which, in turn, contains frozen images of that directory. A global setting can be used to hide “.snapshot” and “~snapshot” from NFS and CIFS clients.



Note: Backing up or copying all files at the root of an NFS export (CIFS share) can have the undesired effect of backing up multiple copies of the directory tree (that is, the current file contents including all the images preserved by the snapshots, e.g. a 10GB directory tree with 4 snapshots would take up approximately 50GB).

If so desired, access to snapshots can be disabled for specific [NFS exports](#) and [CIFS shares](#). This allows the control of who can access snapshot images. For example, create shares for users with snapshots disabled, and then create a second set of shares with restricted privileges, so that administrators can access snapshot images.

Latest Snapshot

Bluearc provides a filesystem view that can be used to access to the "latest snapshot" for a File System. This view automatically changes as new snapshots are taken, but is not affected by changes in the live filesystem. The latest snapshot is the most recent snapshot for the File System, and is accessible through `.snapshot/.latest` (or `~snapshot/~latest`). The latest snapshot can be exported to NFS clients with the path `/.snapshot/latest`. Latest snapshots can also be shared to CIFS clients. When accessing files via the latest snapshot, NFS operations do not use autoinquiry or autoreponse.



Note: The `.latest` ("`~latest`") file designation does not show up in directory listings (i.e. it is a hidden snapshot directory).

Quick Snapshot Restore

Quick Snapshot Restore is a licensed feature for rolling back one or more files to a previous version of a snapshot. The procedure is done at the command line, so for instructions, run `man snapshot` at the CLI or refer to the "Titan CLI Reference."

Quick Snapshot Restore may report that the file cannot be restored, if it has been moved, renamed or hard linked since the snapshot was taken. This should rarely occur but, if seen, indicates that the file cannot be Quick Restored. In this case, the file must be copied from the Snapshot to the live file system normally, that is, without being Quick Restored.

Snapshot Rules

By setting up a snapshot rule, Titan can be scheduled to take snapshots automatically at fixed intervals. Setting up a rule is a two-stage process: first the rule itself is defined, and then one or more schedules are created and assigned to the rule.

To Create Snapshot Rules

1. From the **Home** page, click **Data Protection**. Then, click **Snapshot Rules**.

2. Click **Add**. The following screen will appear:

BLUE-ARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Data Protection | Home > Data Protection > Snapshot Rules

Add a Rule

Name

Queue Size

File System Label	System Drive ID	Capacity	File System Size
vol10	1024	474.57 GB	474.51 GB

In the **Name** field, type a name for the rule (containing up to 30 characters). Do not include spaces or special characters in the name.



Note: The name of the rule determines the names of the snapshots that are generated with it, e.g.

YYYY-MM-DD_HHMM[timezone information].rulename.

If more than one snapshot is generated per minute by a particular rule, the names will be suffixed with .a, .b, .c etc.

For example, a rule with the name 'frequent' generates snapshots called:

2002-06-17_1430+0100.frequent

2002-06-17_1430+0100.frequent.a

2002-06-17_1430+0100.frequent.b... and so on.

3. In the **Queue Size** field, specify the number of snapshots to keep before the system automatically deletes the oldest snapshot. The maximum is 32 snapshots per rule.
4. Select the File System on which to take snapshots, and then click **Apply**.

BLUE-ARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: ON

Data Protection | Home > Data Protection > Snapshot Rules

Snapshot Rules

Existing snapshot rules

Rule name Label	Queue Size	File System
ad	4	vol10

Modify Rule>> Add Rule>> Delete Rule

Existing schedules for the selected rule

Frequency

Every hour at 30 minutes past the hour.

Modify Schedule>> Add Schedule>> Delete Schedule

The **Snapshot Rules** page shows a summary of the details for the rule entered through the **Add a Rule** dialog box on the previous page.

To modify a rule, select it from the **Existing Snapshot Rules** list and click the **Modify Rule** button, re-enter the **Name** and **Queue Size** if necessary and click the **Apply** button.

To delete a rule, select it from the **Existing Snapshot Rules** list and click the **Delete** button.
To assign schedules to snapshot rules

1. Set the frequency with which the system takes snapshots by assigning one or more schedules to a snapshot rule. In the **Snapshot Rules** dialog box, select the rule to which to assign a schedule.
2. Click **Add Schedule**. The **Add a Schedule** dialog box will appear.
3. Choose to take the snapshot on an hourly, daily/weekly, or monthly basis, and then specify the schedule details. If the *crontab* format is familiar, type the schedule in the **Cron string** field and then click **Update GUI from string** to update the dialog box accordingly. For more information on *crontab*, see the *Command Line Reference*.

- 4. In the **List of Email recipients** field, type the Email address of a user to whom the system should send an Email notification each time it takes a snapshot. Enter multiple addresses by separating each one with a semicolon (;). BlueArc recommends that snapshot notifications be sent to at least one user.
- 5. Click **Apply**.

The system automatically deletes the oldest snapshot when the number of snapshots, associated to a snapshot rule, reaches the specified queue limit. However, any or all of the snapshots may be deleted at any time, and new snapshots can be taken.

Managing Snapshots

- 1. From the **Data Protection** page, click **Snapshots**.

BLUEARC

?

Help

i

About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: ON

Data Protection

Home > Data Protection > Snapshots

Snapshots

EVS / File System: EVS01 / All File Systems

change...

Name	File System	Creation Time	Creation Reason
☐ 2004-09-16_0026-0700.ssrule1	vol1	2004-09-16 00:26:00 (PDT)	By Rule
☐ 2004-09-16_0426-0700.ssrule1	vol1	2004-09-16 04:26:00 (PDT)	By Rule
☐ 2004-09-16_0826-0700.ssrule1	vol1	2004-09-16 08:26:01 (PDT)	By Rule
☐ 2004-09-16_1226-0700.ssrule1	vol1	2004-09-16 12:26:00 (PDT)	By Rule
☐ NDMP_AUTO_SNAPSHOT1	vol1	2004-09-16 10:31:57 (PDT)	NDMP Backup

[Check all](#) | [Clear all](#)

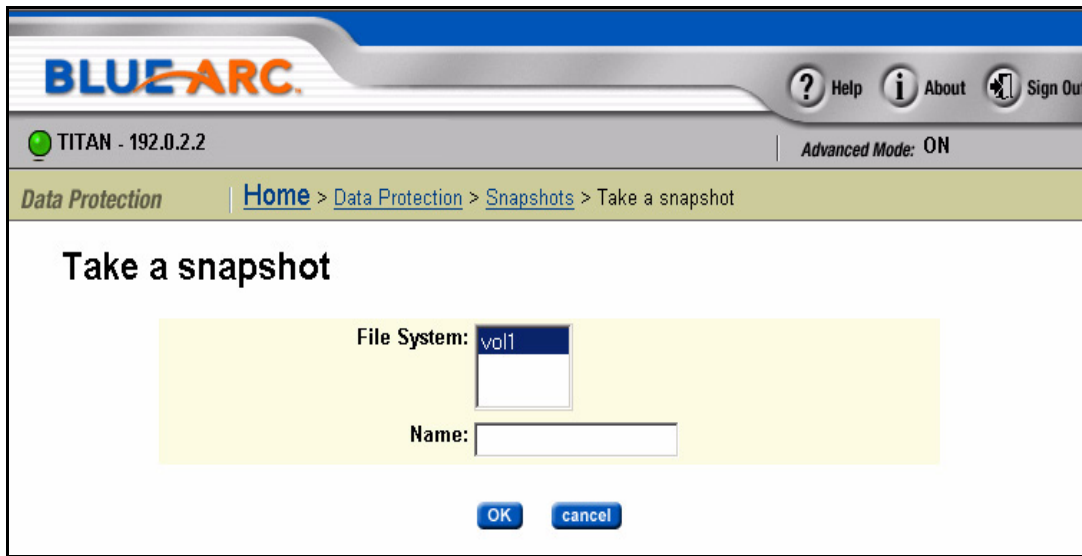
Actions:

delete

Take a snapshot

Snapshot Rules

- 2. Select a specific File System by clicking the **Change** button. When a File System is selected, a list of the associated snapshots will appear.
To delete an individual snapshot, select it and then click **Delete**.
To delete all the snapshots, select **Check All** and then click **Delete**.
To take a new snapshot, click **Take a Snapshot**.



The screenshot shows the BLUE ARC web interface. At the top, there is a header with the BLUE ARC logo and navigation links: ? Help, i About, and a Sign Out button. Below the header, a status bar shows 'TITAN - 192.0.2.2' and 'Advanced Mode: ON'. A breadcrumb trail indicates the current location: Data Protection > Home > Data Protection > Snapshots > Take a snapshot. The main content area is titled 'Take a snapshot' and contains a form with two fields: 'File System:' with a dropdown menu showing 'vol1', and 'Name:' with a text input field. At the bottom of the form are 'OK' and 'cancel' buttons.

3. Select a File System for the snapshot.
4. In the Name field, type a name for the snapshot containing up to 30 characters. Do not include spaces or special characters in the name.
5. Click **OK**.



Note: It is also possible to take a snapshot associated with a rule, without waiting for the next scheduled time. This can be done from the command line interface.

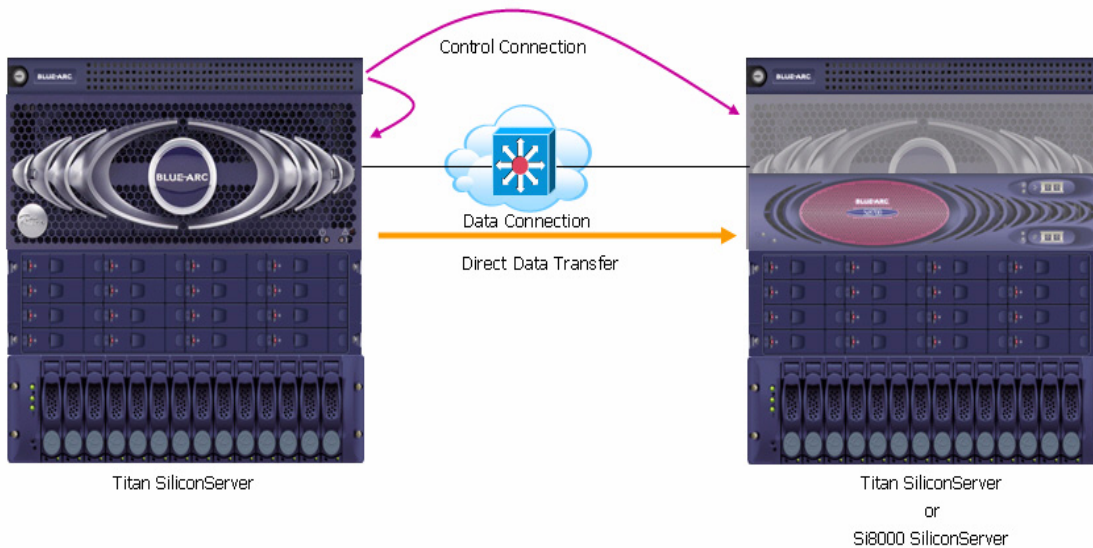
Performing NDMP Backups

Titan supports Network Data Management Protocol (NDMP), an open standard protocol for network-based backup. The purpose of the protocol is to enable a storage management application to control backup and recovery on another device without the backup data being transferred across the network. A standard NDMP configuration is shown in the following diagram:



In the diagram, the storage management application sends backup instructions to the system, which makes a backup copy of data onto tapes in the tape library. The data travels through the Fibre Channel (FC) network, not the Ethernet network. Details of the backup data are sent to the storage management application which is used to recover the data if necessary.

NDMP is used to transfer data between disks and tapes attached to the same server. Data can also be transferred between two separate NDMP servers over an Ethernet connection (in NDMP this is known as a 3-way backup or recovery).



The most common examples of how NDMP can be used are:

- Backing up (recovering) data on a Titan SiliconServer to (from) an Ethernet attached NDMP tape library.
- Backing up (recovering) data on a Titan SiliconServer without a Tape Library to (from) a second BlueArc Storage Server that has a Tape Library attached.
- Using a utility, such as BlueArc's *Accelerated Data Copy (ADC)* or *Data Replication* to copy file systems between BlueArc Storage Servers.

Titan also supports backups done over network protocols such as NFS or CIFS but only NDMP will preserve security settings in a mixed protocol environment including Virtual Volume and quota information.

When using NDMP, Titan uses snapshots to backup data consistently and without being affected by on-going file activity. Snapshots also facilitate incremental backups. However, if so desired, it is also possible to backup data without using snapshots.

Configuring NDMP

This section describes the NDMP configuration and support that the system provides.

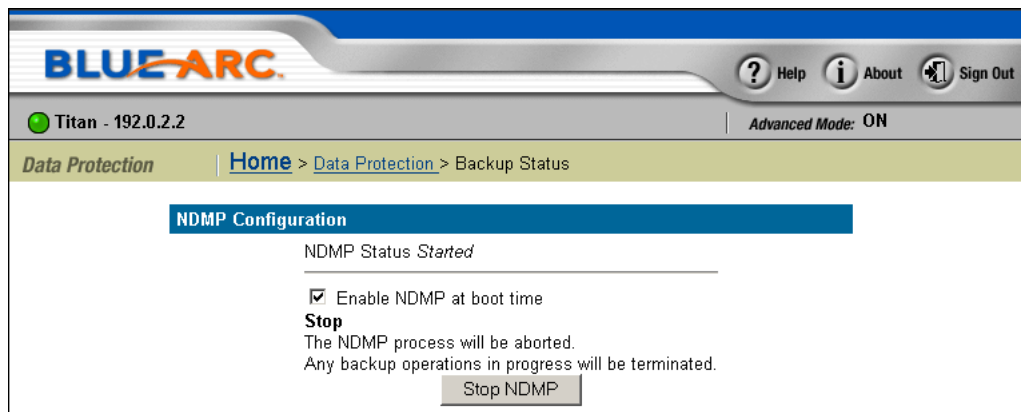


Note: This section does not explain how to set up the storage management application or tape libraries. Consult the documentation that accompanies the application and tape library for setup instructions.

Enabling or Disabling NDMP

NDMP processing status can be checked at any time. NDMP can also be enabled or disabled in mid-session or at system startup.

From the **Home** page, click **Data Protection**. Then, click **Backup Status**.



To enable or disable NDMP processing whenever the system starts, select or deselect **Enable NDMP** at boot time checkbox.

To stop NDMP processing, click **Abort NDMP**.

If the button at the bottom of the dialog box is labeled **Start NDMP**, click it to begin NDMP processing.

It is recommended that all NDMP transfers be terminated using the storage management application before clicking the **Abort NDMP** button. Abort NDMP will immediately stop all NDMP processes. This means that any tapes in use will be left in an untidy state. It may also confuse the storage management application.

Specifying the NDMP User Name, Password, and Version

A user name and password for the primary NDMP user must be defined. Once they are set, they are used to restrict access to NDMP facilities. The storage management application must successfully authenticate against the configured NDMP user account information before it can start a backup or recovery.

The NDMP user name and password set here are likely to be used for most backup, recovery and replication purposes, as they give full access to the files on the system. However, less trusted users can also be allowed to access a restricted set of files (and possibly devices) then an NDMP Restricted User can be used. The SSC command `ndmp-ruser` (see the Command Line Reference) is used to create such users. These user names could for instance be assigned to various users to allow them to use the ADC utility to copy data within limited areas of the file systems. The SSC command `ndmp-ruser-pwd` may be used to change the password for a

selected restricted user.



Note: The user name and password are for NDMP access only, and cannot be used to log in to the system or access files through other routes, such as Windows NT file sharing. However, anyone who knows the user name and password can use an NDMP-enabled storage management application to access data on the system. It is therefore important to keep the NDMP user name and password secure.

For NDMP backups and recoveries, Titan uses the NDMP version 4 protocol by default. If required, Titan can be configured to use version 2 or 3 of the NDMP protocol.



Note: Both [Incremental Data Replication](#) and ADC require NDMP version 3 or 4 to run. Setting the protocol version to 2 will prevent these from running. Set the version to 2 only if required by your backup software.

To Specify the NDMP User Name and Password

1. From the **Home** page, click **Data Protection**.
2. Click **Backup User**.

BLUEARC

TITAN - 192.0.2.2 | Advanced Mode: ON

Data Protection | [Home](#) > [Data Protection](#) > NDMP Configuration

NDMP Configuration

NDMP user name:

NDMP password:

NDMP version:

3. Enter the **NDMP user name**.
4. Enter the **NDMP password**.
5. Enter the **NDMP version**.
6. Click **OK**.



Note: Additional configuration of NDMP can be performed using the `ndmp-option` CLI command. For more information, refer to the *Command Line Reference*.

NDMP Backup Devices

NDMP backup devices, such as tape libraries and auto-changers, require special configuration. Titan monitors its Fibre Channel (FC) links periodically and automatically detects the presence of backup devices. Since Titan could be connected into a Storage Area Network (SAN) shared with other servers, it does not automatically make use of backup devices it detects on its FC links. Backup devices are added to the configuration through the Backup SAN Management page.

Backup SAN Management

From the **Home** page, click **Data Protection**. Then, click **Backup SAN Management**.

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Data Protection

Home > Data Protection > Backup SAN Management

NDMP Device Access

All Tape Devices and Autochangers

ID	Device Type	Serial Number	Location	EVS
800	Tape robot			Any EVS
801	Tape drive	PXA46S1804		Any EVS
802	Tape drive	PXA47S0048		Any EVS

Show

Show All

Allow Access

Yes

Status

OK

NDMP Device Name

Unknown

Fibre Channel Addr

FC Port id: 50050840 001ee000, LUN: 0

Version

2.01

Manufacturer

ATL

Model

P1000 6220051

Assign device to EVS

Sales

Reassign

Deny Access

Forget Device

Refresh

Item / Field	Description
All Tape Devices and Autochangers	Displays the ID, Device Type, Serial Number, Location, and EVS.
Show	Filters the list: Show All , Show Allowed , Show Not Present , Show Denied , Show Tape Drives and Show Autochangers .
Allow Access	Clicking the Deny Access button will deny access to the selected tape device. If Access Allowed is No then NDMP will not attempt to use the corresponding device, and the device will not appear in the Backup > Devices display.  Note: NDMP devices must be assigned to an EVS <i>before</i> access can be allowed to it. A request to "Deny Access" will be rejected if an NDMP client has opened the device. The backup application configuration should be changed to avoid use of the device before clicking "Deny Access".
Status	Current status of the selected device.
NDMP Device Name	This is the name that needs to be entered or selected when configuring the Storage Management Application. If the device is a tape drive and details of its location within a tape library need to be supplied, the Location field in device table can be consulted.
Fibre Channel Address	The Fibre Channel (FC) Port ID (or WWN) and the LUN. If the tape library displays the FC port WWN and device LUNs, it is a way of identifying a specific device.
Version	The device version as returned by the device in response to a SCSI inquiry command.
Manufacturer	Manufacturer of the device.
Model	Device model.

Deny Access - Disables access to a device.

Reassign – This confirms a selection of an alternative EVS assignment.

Forget Device – This will remove the selected device from the list. It is only available if the device has been disconnected from the FC.

Refresh – This requests the software to *discover* any changes in the Fibre Channel connection, i.e. find any newly attached devices and discover any devices that are no longer accessible. If new devices are plugged into the Fibre Channel, use Refresh to identify them.

Assign Device to EVS

Select the **EVS** on which to assign the NDMP device. To allow the tape device sharing among all EVS in a cluster, select **Any EVS**. A device assigned to a specific EVS cannot be shared unless it is reassigned to **Any EVS**.

Tape devices can be shared between EVS under the following conditions:

- ☐ The EVS must be within the same cluster.
- ☐ The tape device is not shared with another BlueArc SiliconServer.
- ☐ The tape device is not shared with another non-BlueArc device.



Note: When an EVS is currently using a tape device, any attempt to use it through a different EVS will prompt a notification that the device is currently in use (i.e. the operation will not be queued).

When a tape device is currently assigned to a particular EVS (i.e. not ANY EVS), any attempt to use it through a different EVS will prompt a notification that the device has not been found.

Verifying NDMP Device Names

To configure a storage management application to work with NDMP, enter the names of the autochangers and tape drives. The device names can be verified through the Backup SAN Management page.

The Location field for each tape drive shows the name of the autochanger that holds the drive and the position of the drive in the autochanger. For example, the location of the first drive in autochanger **/dev/mc_d010** is **/dev/mc_d010 :1**.

To update the display, click **Refresh**.

When the Web Manager cannot determine the location of a tape drive, it shows it as **unknown**. This can happen when:

- The tape library is offline.
- The autochanger does not support the mechanism that the Titan SiliconServer uses to query the tape drive location, or the autochanger has not been setup to accept this query. Where this is the case, compare the serial numbers of the tape drives with displays available in the tape library to verify the drive locations.
- The autochanger and a tape drive within it are attached to different servers. In this case, use the tape drive serial numbers to match the device name shown by one server with the location shown on the other.



Note: Devices will not be available or visible if they have not been enabled through the SAN Management page.

NDMP and Snapshots

The Titan SiliconServer uses [snapshots](#) to backup data consistently and without being affected by on-going file activity. Snapshots also facilitate incremental backups. However, it is also possible to backup data without using snapshots.

Factors to Consider in the Backup Strategy

Snapshots and tape backups complement each other, and there is a strong case for using both backup methods. The following are some factors to consider when designing a backup strategy.

❑ Backing up automatically created snapshots

When backing up a file system that is being actively updated, a snapshot of the file system is much more likely to produce a fully consistent image than backing up the live file system. As a result, NDMP is configured by default to automatically create a snapshot for backup.

❑ Backing up pre-created snapshots

A backup can be taken from a specific snapshot that has been created by rule or by user request.

- ❑ To back up the latest snapshot created under a snapshot rule use the **NDMP_BLUEARC_USE_SNAPSHOT_RULE** environment variable (see *Supported NDMP Environment Variables*).
- ❑ Alternatively, it is possible to request a specific snapshot by explicitly including the snapshot name in the path to back up. Where the path is based on a CIFS share name, indicate the snapshot with **/~snapshot/snapshot_name**; for paths based on an NFS export name, use **/.snapshot/snapshot_name** instead. It is also possible that the CIFS share or NFS export includes a snapshot name.

❑ Backing up databases and iSCSI Logical Units

Typically, special measures are needed when backing up files such as databases and iSCSI Logical Units. The internal structures in these files are tightly coupled with the state of the client software (database manager/iSCSI Initiator) that is controlling the files. Backing up the file half way through a client operation may produce inconsistencies in the backup image that would prevent the client using a recovery of the image. For this reason, any backup of the files needs to ensure that files are in a consistent state when backed up. Snapshots can be used to achieve this, see below for details. The most convenient mechanism is to use a snapshot rule as this avoids having to explicitly specify the name of the snapshot used. However, it is important to ensure that the backups created this way are not deleted too soon. If a snapshot being used for a backup is deleted while the backup is still active then the backup will fail. For more information on backing up and restoring iSCSI Logical Units, refer to the section [Backing Up and Restoring iSCSI Logical Units](#).

To Back Up a Database

1. For databases, shut down the database or use a database-specific command to bring database files into a consistent state.
2. Take a snapshot of the file system.



Note: It is possible to associate the snapshots taken for this purpose with a rule, so that a number of snapshots can be kept. This can be done using the command line interface.

3. Restart the database.
4. Make a backup copy of the snapshot.

All four steps can be scripted to automatically backup at pre-defined times.

Incremental Backups and Snapshots

Taking a full backup of a File System can be time-consuming, so it is a good idea to combine infrequent full backups with regular incremental backups. However, these incremental backups may fail to capture all the changes in the File System, e.g. if the modification time of a file is the determining factor in whether or not to back it up, a backup program will not archive the contents of a directory that has been moved, because the times/dates of the files remain unchanged.

Snapshots provide a solution to this problem. After taking the initial, base backup using a snapshot image, it can be used at incremental backup time to obtain a better picture of changes in the file system. In order to use the snapshots this way, the snapshot must be kept around for as long as the associated backup may be used as the basis for an incremental backup.

Selecting NDMP Snapshot Options

By default, Titan automatically creates a snapshot before it starts a backup operation. The backup then proceeds from the snapshot image rather than the file system. However, if the file system cannot take the snapshot for any reason, the backup proceeds directly from the live file system.

To Configure NDMP Snapshot Options

1. From the **Home** page, click **Data Protection**.
2. Click **Backup Snapshot Options**.

BLUEARC ? Help i About Sign Out

Titan - 192.0.2.2 Advanced Mode: OFF

Data Protection | [Home](#) > [Data Protection](#) > Backup Snapshot Options

NDMP Snapshot options

Automated Snapshot Use:

☐ Do not automatically create snapshots, backup from the live File System

☒ Automatically create snapshots

Automated Snapshot Deletion:

☐ Delete snapshot after use

☐ Delete snapshot after next backup

☒ Delete snapshot when obsolete

Maximum Auto-snapshot retention time Days

Apply Cancel

3. In the **Automated Snapshot Use** section, select whether NDMP should automatically create a snapshot to be backed up. This selection only affects backups or adc copies where the path refers to the live file system. If the backup path already specifies a snapshot or the backup is using a snapshot rule then this option has no effect. The choices are:
 - ☐ Automatically Create Snapshots. This is the recommended choice. A backup of a path referring to the live file system will cause a snapshot to be taken for use in the backup.
 - ☐ Do not automatically Create Snapshots. Backups of live file system will use the live file system directly. If this option is selected, skip Step 4 and click Apply.



Note: If a backup path explicitly contains a snapshot reference then the system does not take a new snapshot, regardless of this setting.

Performing NDMP Backups

4. In the **Automated Snapshot Deletion** section, select when to delete the snapshot. By default, NDMP keeps the snapshot to make incremental backups more accurate. The choices are:
 - ☐ **Delete snapshot after use**

This will delete an automatically created snapshot after the backup, for which it was taken, is completed. To prevent snapshots from being kept for any length of time, select this option for full backups or if the file system is changing very rapidly.
 - ☐ **Delete snapshot after next backup**

This will delete an automatically created snapshot after it has been used as the basis of a new incremental backup. This option is designed to use with "incremental" backup schedules. These schedules with an exception for full backups are based on the immediately previous backup.
 - ☐ **Delete snapshot when obsolete**

This will delete an automatically created snapshot when the next backup of the same level is taken. For instance, the snapshot taken for the full backup will only be deleted when the next full backup is completed. This option is intended to use with "differential" backup schedules. These backup schedules are new differential backups which can be based on the same base backup.
5. In the **Maximum Auto-snapshot retention time** box, enter the number (value between 1 and 40) of days to keep the snapshots before the system deletes them automatically. Usually automatically created snapshots will be deleted according to the rule selected in Step 4. However, if a sequence of backups, using automatically created snapshots, is stopped then snapshots may be left over. The maximum retention time provides a way of tidying up in these circumstances.

Backing Up Virtual Volumes and Quotas

NDMP backups or copies will retain [Virtual Volume](#) and [Quota](#) information if it is not disabled. NDMP is used in the following circumstances:

- NDMP backups to tape libraries.
- File system copies using the ADC utility.
- Data Replication controlled by the SMU.



Note: CIFS or NFS backups will not backup or restore any Virtual Volume or Quota information.

Additional information regarding the Virtual Volume backups or copies:

- Specifying the NDMP environment variable **NDMP_BLUEARC_QUOTAS** as **NO** disables Quota processing on NDMP backups/recoveries and ADC copies.
- Data Replication will copy Virtual Volume and Quota information.

- Configuration information for a Virtual Volume will only be copied if its root is in the backup/copy path.
- Incremental backups and copies, including replication copies, transfer updates of a Virtual Volume if the backup/copy path includes the Virtual Volume root. However, copies and recoveries will not delete Virtual Volumes.



Note: With an Incremental Block-Level Replication (IBR) license these updates can be done as block-level ADC updates.

- If a recovery or copy is merging its contents into an existing Virtual Volume then the Virtual Volume information will also be merged. If a Virtual Volume is recovered/copied to an existing non-empty directory that is not part of the same Virtual Volume, then the existing on-disk settings will be kept.

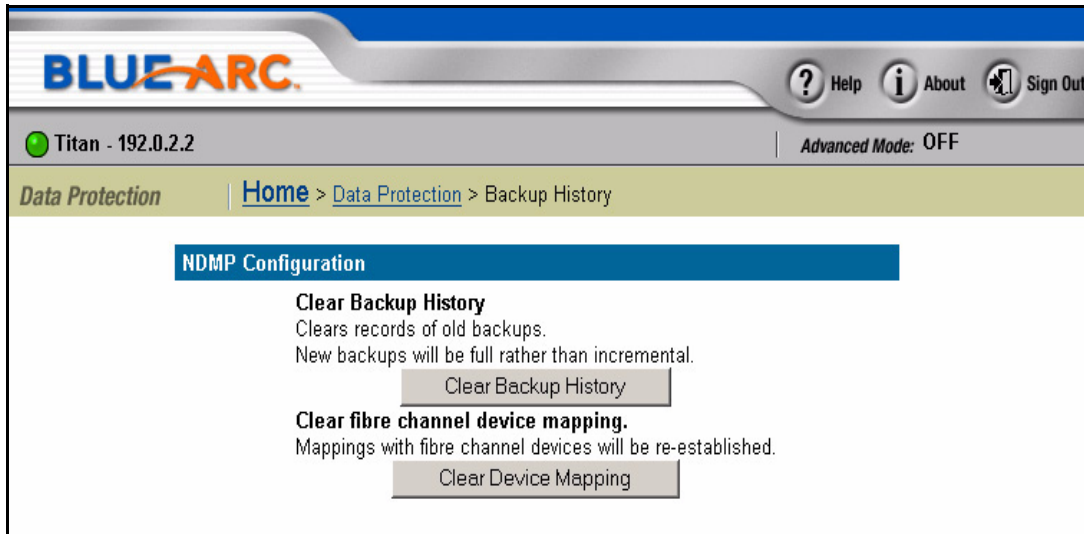
Clearing the Backup History or Device Mappings

To clear the records of old backups that have been made, use the Web Manager. During incremental backups, Titan uses the records of old backups to determine the date and time after which it must back up modified files. If a backup has been lost, clear the records to force a full backup to occur instead of an incremental backup.

Also, the mappings between the tape library devices on the Fibre Channel (FC) and the names of the tape drives and autochangers given in the storage management application can be cleared. When a tape library device is attached to the FC, the device is assigned a number. The number becomes part of the device name. Adding more devices to the FC will not cause the device names to change. When replacing an existing tape library with a new one and keeping the original device names for the new devices, the device mappings must be cleared and then the devices must be re-added in the desired order.

To Clear the Backup History or NDMP Device Mappings

From the **Home** page, click **Data Protection**. Then, click **Backup History**.



Clear Backup History clears records of old backups. New backups will be full rather than incremental.

Clear Device Mapping re-establishes mappings with fibre channel devices.

Using Storage Management Applications

Titan acts as the NDMP host and operates with leading storage management applications. It supports NDMP Version 2, 3 and 4. The BlueArc implementation of NDMP can back up and restore:

- Both Windows and UNIX files from a single storage management application.
- The full attributes of each Windows and UNIX file, including Windows ACLs can save and restore whole volumes and preserve all the file attributes.

Including recovery of a complete backup image, Titan supports recovery of single files or subdirectories or of lists of these. The **Direct Access Recovery (DAR)** mechanism can be used in this case, provided the Storage Management Application supports it. DAR allows NDMP to go directly to the correct place in the tape image to find the data rather than reading the whole image. This can dramatically reduce recovery times.

Supported NDMP Environment Variables

NDMP environment variables can be used to modify backup actions. The storage management application generates most of these variables, and supports additional ones.

DIRECT

Possible value	Notes
y or n	Used on recovery to request Direct Access Recovery (DAR). This may be used when recovering a subset of the full backup. If the storage management application supports use of DAR then the recovery will position the tape to the start of the required data rather than read the complete backup image to find the data. This can save a lot of time in recovery of single files etc. The Storage Management Application may control the setting of this variable. In this case the setting will be based on some form of user interface option or an assessment of the likely efficiency of using DAR. However, in some cases it may be necessary to explicitly add the DIRECT=y variable.

EXCLUDE

Possible value	Notes
Comma-separated list of files or directories	Specifies files or directories to exclude from a backup. By default, none are excluded. When specifying a file or directory, type either: • A full path name, relative to the top-level directory specified in the backup path. The path name must start with a forward slash (/), and an asterisk (*) can be typed at the end as a wildcard character. • A <i>terminal</i> file or directory name, which is simply the last element in the path. The name must not contain any / characters, but it may start or end with the wildcard character *. For example: ENVIRONMENT EXCLUDE "/dir1/tmp*,core,*.o" This command excludes all files and directories that: • Start with the letters tmp in the directory /dir1 • Are called core • End with the characters .o The command is case-sensitive if backing up an NFS export but not if backing up a CIFS share.

EXTRACT

Possible value	Notes
y or n	The default value y causes a recovery operation to extract files from a file list rather than recover the whole backup.

FILESYSTEM

Possible value	Notes
Name of directory to back up	The Storage Management Application will set the FILESYSTEM variable to the name of the path to be backed up.

FUTURE_FILES

Possible value	Notes
y or n	Enables back up of files that were created after the start of the current backup. With NDMP version 2, the inode number that identifies a file can be reused during a backup, thereby causing the backup to fail. By default, therefore, only files created before the start of the backup are backed up. To override this behavior, set the FUTURE_FILES variable to y .

HIST

Possible value	Notes
y or n	The default value y causes file history information to be sent to the storage management application. This enables the display and recovery of the contents of a backup.

LEVEL

Possible value	Notes
0 - 9 , or i	The default value is 0 (full backup). If the value is set to 4 , an incremental backup is taken based on the most recent previous backup of the same FILESYSTEM with level 0 , 1 , 2 , or 3 . If the value is set to i , an incremental backup is taken based on the most recent previous backup of the same FILESYSTEM of any level.

NDMP_BLUEARC_BB_COMPATIBLE

Possible value	Notes
y or n	This is used to request that Titan produces a backup compatible with current Si7500/8000 series server. Note: The ADC issued with the Titan release will automatically add the relevant variable if it recognizes a copy from Titan to an Si7500/8000 series server.

NDMP_BLUEARC_FH_CHARSET

Possible value	Notes
ASCII, ISO8859 or UTF8	Specifies the character set to use when sending file history information to the storage management application. Most file and directory names use characters in the standard ASCII set. If the names of directories and files contain national variant characters outside the ASCII set, it is necessary to decide how to encode these characters when they are sent to the storage management application. Consult the storage management application provider for advice on setting the NDMP_BLUEARC_FH_CHARSET variable. UTF-8 is the most wide-ranging option as it is a mapping of the full Unicode character set, which covers the alphabets of most of the world's languages. ISO8859 (which can also be specified as ISO8859-1) refers to the 8-bit ISO Latin-1 character set and covers all Western European languages. If the path names include characters that cannot be in the chosen character set, then those characters will be encoded as a hexadecimal representation, of the value of the Unicode character enclosed in caret (^) symbols. For instance if using ASCII, the “£” character will be as “^a3^”. To avoid confusion the caret symbol itself is doubled in names in ASCII or ISO8859. Note that this usage varies from that in Si7500/Si8x00 and it may not be possible to explicitly select such files for recovery from old backups.

NDMP_BLUEARC_FH_NAMETYPE

Possible value	Notes
UNIX or NT	Specifies the name type that the system passes to the storage management application in the file history information. NDMP allows files to be described as either UNIX files or NT files. By default, Titan's NDMP implementation describes files under an NFS export as UNIX files and those under a CIFS share as NT files. If the storage management application can handle UNIX-style names only, use the NDMP_BLUEARC_FH_NAMETYPE variable to request UNIX-style names when backing up a CIFS share.

NDMP_BLUEARC_OVERWRITE

Possible value	Notes
ALWAYS or OLDER or NEVER	Used on recovery to indicate if an existing file should be replaced by a file of the same name being recovered. The default setting is ALWAYS , meaning that the backup file will always replace the existing file. OLDER means the existing file will be replaced if it is older than the recovered file. This option does not affect the behavior if either the existing file or the backup file is actually a directory. In this case no overwriting will be done unless both are directories in which case the recovered directory contents are merged into the existing directory.

NDMP_BLUEARC_QUOTAS

Possible value	Notes
y or n	Default value is y which causes NDMP to back up and recover Virtual Volume and Quota information. Set a value of n to disable quota backup or recovery.

NDMP_BLUEARC_READAHEAD_PROCESSES

Possible value	Notes
0 to 10 (In exceptional cases could be increased to as many as 30.)	This variable can control the number of read-ahead processes used when reading directory entries in the backup or copy operation. Remember that each additional readahead process takes up resources, so it is best to limit the number of additional processes unless it makes a significant difference in performance. The default for this value can be set using the “ndmp-option readahead_procs” CLI command. It will be 1 if not set explicitly. A value of 0 will disable directory readahead. This is a reasonable option where file sizes are large. Values from 1 to 10 might be used when reading file systems with smaller files. Where most of the files are very small (16 KB or less) then it may be useful to use 10 processes. In extreme cases, where most of the deepest level directories have only one or two files and those files are very small, it may be useful to increase the amount of second level readahead used with the CLI command “ndmp-option ext_readahead”. If this second level readahead option is set to a higher value such as 10, then setting readahead processes up to a value of 30 might be advisable.

NDMP_BLUEARC_SNAPSHOT_DELETE

Possible value	Notes
IMMEDIATELY LAST or OBSOLETE	This variable overrides the setting of the Automated Snapshot Deletion field in the Backup > Snapshot Options page of the GUI. IMMEDIATELY gives the same effect as “Delete snapshot after use”, LAST is the same as “Delete snapshot after next backup” and OBSOLETE is the same as “Delete snapshot when obsolete”.

NDMP_BLUEARC_TAKE_SNAPSHOT

Possible value	Notes
y or n	Used to override the "Automatic Snapshot Creation" Backup configuration option.

NDMP_BLUEARC_USE_CHANGE_LIST

Possible value	Notes
y or n	Indicates if incremental backups or replications will use a changed object list to direct the search for changed files. If the process were not use the changed object list, it will have to search the entire directory tree looking for changed files. When using the changed object list, the search only passes through those directories that contain changed files. The default setting for this option can be set using the “ndmp-option change_list_incr” CLI command. Where the number of directories that contain changed files covers a relatively small proportion of the file system, the use of changed object lists may significantly reduce incremental backup/replication time. However, the processing of the changed object list itself may take a long time. Therefore, its use is not recommended in situations where there are file changes in many directories.

NDMP_BLUEARC_EXCLUDE_MIGRATED

Possible value	Notes
y or n	Indicates if backups or replications will include files whose data has been migrated to secondary storage. If set to y, the backup or copy will not include files whose data has been migrated to another volume using the Data Migrator facility. The default setting is n, meaning that migrated files and their data will be backed up as normal files. The backup/copy retains the information that these files had originally been migrated.

NDMP_BLUEARC_REMIGRATE

Possible value	Notes
y or n	This variable controls the action on recovering or replicating a file that had been migrated within the original source file system. If set to y, the file will be re-migrated on recovery provided the volume or virtual volume has a Data Migrator path to indicate the target volume. If set to n, all the files and their data will be written directly to the recovery or replication destination volume.

NDMP_BLUEARC_USE_SNAPSHOT_RULE

Possible value	Notes
Snapshot rule name	This variable causes NDMP to back up the latest snapshot created under the specified snapshot rule. This can be used to backup the contents of a snapshot that has been taken at a specific time. For instance it can be used to back up databases. NDMP does not create or delete snapshots if this variable is set. For a successful backup, the snapshot should not be deleted until after the operation has completed. In addition, the snapshot should be kept around long enough to support incremental backups.

NDMP_BLUEARC_AWAIT_IDLE

Possible value	Notes
y or n (Default y)	By default the data management engine imposes an interlock to stop NDMP backups and "adc" copies from the destination of a replication while a replication copy is actively writing data. This is intended to help installations that replicate to a volume and back up from there. However, the lock is held at a volume level and with directory level replication and it may be desirable to override this action. To make use of this replication interlock, it is necessary to specify this rule option on both the replication that is intended to do the waiting, as well as the replication that is waited upon.

NDMP_BLUEARC_SPARSE_DATA

Possible value	Notes
NONE , BASE , or UPDATE	This setting controls the omission of unset or unchanged data when backing up or transferring files. A Block Level Replication license is required to enable this feature. If the setting is NONE (the default) then files are always sent in their entirety including any unset data areas. The BASE setting will omit non-initialized areas of files from the data stream. This is particularly useful for files such as iSCSI LUNs or Database files where significant parts of the files may not have been written. The setting of UPDATE includes the BASE setting features but additionally will send only changed blocks of a file when doing incremental copies or backups. This setting is not recommended as files backed up in this way are only partially included in the backup and cannot be recovered from this single backup - a full correct sequence of backups must be recovered to recreate the file.

NDMP_BLUEARC_SPARSE_FILE

Possible value	Notes
Comma-separated list of files or directories. A list of files similar in format to that specified by the EXCLUDE variable.	Allows control of sparse file/block level incremental processing. If this variable is specified then only files on the list will be considered for sparse transfer.

NDMP_BLUEARC_SPARSE_LIMIT

Possible value	Notes
Numeric value followed by K, M or G signifying Kilobytes, Megabytes or Gigabytes respectively. (For instance, 32M for 32 Megabytes).	Files smaller than the value specified will not be considered for sparse transfer. The default value is 32 MB.

TYPE

Possible value	Notes
dump or tar	Use dump whenever possible. The two backup types use exactly the same environment variables and produce the same backup data on tape. The only difference is in the format of the information sent to the storage management application: dump produces NDMP add directory entry and add node file history information; tar produces NDMP add path file history information.

UPDATE

Possible value	Notes
y or n	The default value (y) causes a record of the backup time to be kept. Future incremental backups can be carried out using this backup as a base.

Specifying File Names

A file name comprises the name of an NFS export or CIFS share followed by a sub-path. Note that file and directory names in an NFS export are case-sensitive, but those in a CIFS share are not. Here are some examples:

- ❑ `/nfsroot/dir1/dir2/file1`
Specifies the file `dir1/dir2/file1` under the NFS export `/nfsroot`.
- ❑ `/ntroot/nt_dir` (or `/NTRoot/NT_DIR`)
Specifies the file `nt_dir` under the CIFS share `/ntroot`.

Special prefixes can be used to further define the file or directory path. If no NFS export or CIFS share is available the path can be based on the volume name as:

`/__VOLUME__/volname/subpath`

If the name of an NFS export is the same as that of a CIFS share, a file name clash may occur. This can be avoided by adding a unique prefix to the name. For example, if `/root` is both an export and a share, differentiate between the two as follows:

`/__EXPORT__/root`

`/__SHARE__/root`

In each case, there are two underscores before and after the prefix keyword, which must be in uppercase characters.

Important Notes

- ❑ NDMP does not specify the format of the backup data on tape. As a result, it is not possible to use NDMP backups to exchange data with other types of servers.
- ❑ An incremental or differential backup, back up changes made since a previous base backup. When asked to do an incremental or differential backup the NDMP code refers to the record of backups to check for such a base backup to compare against. If there is such a backup, and it was a backup of a snapshot, and that snapshot still exists on the system, then the NDMP code executes a “Comparative Incremental” backup, using the original snapshot to identify changes. If the base backup was not of a snapshot, or its snapshot has been deleted, then the only information the code has is the date/time of the backup, and so a “Date-Based Incremental” backup is done.
- ❑ Since the Date-Based incremental backup has no record of the files backed up in the original backup, it cannot identify files that have been deleted in the intervening period. Similarly, if a directory has been moved there is no way of knowing that the contents of the moved directory have changed. Therefore contents of moved directories will not be backed up unless the individual files have themselves changed.”

- ❑ Adding any new equipment to a FC-AL causes the FC-AL to reset, which in turn can leave any attached tape library in an indeterminate state. Similarly, if a failover takes place during a tape backup operation, the tape status may become unknown. While a backup is running, it is therefore advisable not to:
 - ❑ Add devices to the FC-AL loop, or remove them from it.
 - ❑ Reset the partner node in the cluster.
 - ❑ Load any firmware on the partner node in the cluster.
 - ❑ Taking any of these actions causes the FC-AL to reset.
- ❑ In recovery operations the storage management application sends a list of files to recover. If it returns file history information with each file on the list then the list is of practically unlimited length. However, if the storage management application does not include the file history information the list is limited to 1024 names.
- ❑ The maximum tape block size supported is 256 KB.

Compatibility with Other SiliconServers

This section addresses the following two issues:

- ❑ The **copying** of data between a Si7500/Si8x00 series server Titan using the **ADC** utility or the **SMU Replication** function.
- ❑ Recovering an NDMP tape backup image of a Si7500/Si8x00 series server to Titan or vice versa.

Titan uses a backup layout that reflects differences in the underlying file system. However, the Titan NDMP implementation understands the Si7500/Si8x00 series configuration and can:

- ❑ Recover a Si7500/Si8x00 series backup format image from **tape** or through **ADC** copy.
- ❑ If requested, produce a backup image compatible with the older Si7500/Si8x00 series servers.

The ADC program (and hence the SMU replication utility) recognizes the situation where a copy is being made from Titan to a Si7500/Si8x00 series server. ADC will automatically produce a *backward compatible* backup image.

Three possible actions are:

- ❑ **ADC** copies and incremental data replications between Si7500/Si8x00 servers and Titan SiliconServer will be performed correctly *without* requiring any specific action.
- ❑ Tape backups from a Si7500/Si8x00 server can be recovered to Titan *without* any specific action.
- ❑ Tape backups from Titan cannot usually be recovered on Si7500/Si8x00 servers. However, the environment variable, **NDMP_BLUEARC_BB_COMPATIBLE** can be set to **y** to ensure a compatible backup.

There are some differences between the facilities provided by the different file systems and therefore some issues affecting the file attributes copied. These can be summarized as follows:

- ❑ Quota information - Titan allows much more control including *user quotas* etc. Titan quota information can never be transferred back to a Si7500/Si8x00 server.
- ❑ Virtual Volumes and Quota information from a Si7500/Si8x00 server can be transferred to Titan. However, Titan Virtual Volumes only have one base directory so if a Virtual Volumes on a Si7500/Si8x00 server has multiple base directories, then only the first of these will be included in the Titan Virtual Volumes.
- ❑ In the Titan file system, in *mixed security mode*, files have security defined, either by a *CIFS Security Descriptor* or by *Unix Security Mode*. The system uses security mappings to decide what security settings are required in the other system. The Si7500/Si8x00 server files that have both CIFS and Unix security modes set will only retain the *CIFS Security Descriptor* when transferred to Titan.
- ❑ File transfer times for Titan are in nanosecond units and on Si7500/Si8x00 servers in *100* nanosecond units. Transferring files, therefore, from Titan to a Si7500/Si8x00 server and back may cause a very small change in the file times seen.

Policy-Based Data Replication

Titan SiliconServers supports a policy-based data replication. This allows administrators to setup and configure replication jobs independently from other backup strategies using the Web Manager.

Titan SiliconServers can be configured to perform incremental data replications. When a replication policy is first set up, the SMU performs an initial copy of the source volume (or directory) to a target destination. After the initial copies are successful, incremental copies are performed at the scheduled intervals. Incremental block level replication can optionally be used to replicate large files more efficiently. During an Incremental data replication, files that have been changed since the last scheduled replication will be replicated to the target in full. With incremental block-level replication (additional license required), only the changes in files are replicated and not the whole file, thus reducing the amount of data replicated. This reduces the overall replication time.

During replication configuration, a replication policy is setup to identify a source File System, Virtual Volume, or directory, the replication target, and a replication schedule. Pre-replication and post-replication scripts can also be set up during that time. Replication rules are then defined to include various optional settings. These optional settings are explained later in this section.

Incremental Data Replication

The Titan SiliconServer provides support for Incremental Data Replication (IDR). IDR is performed under control of the [System Management Unit](#) (SMU). IDR uses the same data management engine as [NDMP](#) to copy the contents of an entire file system, a [Virtual Volume](#), or an individual directory tree to a replication target. The section [Performing NDMP Backups](#) includes information about NDMP, much of which applies to IDR. Replication is performed incrementally, which means that after the initial copy, only changes in the source volume or directory are actually replicated on the target. Snapshots are used to ensure accuracy of the replication.



Note: In case the snapshot taken prior to the previous replication is lost, the full data set is replicated.

Once a replication policy and schedule is set up, the IDR process will take place automatically at the specified interval. The replicated data can be left in place (and used as a standby data repository). In addition, the replicated file system or directory can be backed up through NDMP to a Tape Library System (TLS) for long-term storage (which can be automated).

The replication target should not be actively used during the replication process. Accessing files during the replication process could prevent those files from being updated. Also any changes applied directly to files at the target might be lost when the file is next updated from the source.

IDR supports the following targets for replication:

- A File System or directory within the same Titan SiliconServer. BlueArc's [Multi-Tiered Storage](#) (MTS) technology ensures that replications that take place within a Titan SiliconServer are performed efficiently, without tying up network resources.
- A File System, Virtual Volume, or directory on another Titan.
- A File System, Virtual Volume, or directory on another SiliconServer model, e.g. the Si8900.

Although the SMU schedules and starts all replications, data being replicated flows directly from source to target without passing through the SMU.

Incremental Block-Level Replication

By default, Incremental Data Replication will copy files that have changed since the last replication in their entirety. With the Block-Level Replication feature enabled, only data blocks in large files that have been written since the last replication will be copied. Depending on the use of files within the source volume, this could substantially reduce the amount of data copied. The Block-Level Replication feature is automatically enabled by installing an IBR license.



Note: Block-Level Replication copies the entire file if the file has multiple hard links.



Note: The Block-Level Replication feature is automatically enabled if the Incremental Block Replication license is present.

Configuring Policy-Based Replication

Configuring a policy-based replication process requires the administrator to setup the following processes.

- ❑ **Replication Policy** - a replication policy identifies the data source, the replication target, and optionally a replication rule. Pre-replication and post-replication scripts can also be set up in the policy page.
- ❑ **Replication Rules** - optional configuration parameters that allow replications to be tuned to enable (or disable) specific functions or to achieve optimal performance.
- ❑ **Replication Schedule** - defines the schedule, timing and policy based on the scheduled date and time.

Creating Replication Policies

The Titan SiliconServer provides a wizard where administrators can add and setup polices for how data replication will occur. The SMU can manage replication jobs from multiple Titan SiliconServers and their associated storage subsystems. Before administrators can add a replication policy the type of server that will be used for storing the replicated data must be determined. You can choose from one of the following policy destination types:

- **Managed Server** - For a server to be considered as managed server, it needs to be entered in the SMU configuration.
- **Not a Managed Server** - A non-managed server is one where the IP Address and username/password of the server is not known by the SMU. Administrators can still select a non-managed server as the target by specifying the IP address along with the username and password.

Choosing the type of Destination SiliconServer

To choose the type of Destination Silicon Server.

1. From the **SMU Home** page, click **Data Protection ->Replication**.

The screenshot shows the 'Policies' screen. At the top, there's a table with columns: Name, SiliconServer, Source (EVS, File System/Path), and Destination (Server, EVS, File System/Path). A single policy 'TestPolicy2' is listed with values: TITAN, EVS01, vol0:/, TITAN, EVS01, vol4:/. Below the table are links for 'Check All' and 'Clear All'. At the bottom, there are 'Actions' (add, remove) and 'Shortcuts' (Replication Rules, Backup User).

Name	SiliconServer	Source EVS	File System/Path	Server	Destination EVS	File System/Path
☐ TestPolicy2	TITAN	EVS01	vol0:/	TITAN	EVS01	vol4:/

[Check All](#) | [Clear All](#)

Actions: [add](#) [remove](#)

Shortcuts: [Replication Rules](#) [Backup User](#)

2. From the **Policies** screen, click the **Add** button. The following screen is displayed.

The screenshot shows the 'Policy Destination Type' screen. It has a header with the BLUE ARC logo and navigation links (Help, About, Sign Out). Below the header, it says 'Titan - 192.0.2.2' and 'Advanced Mode: ON'. The main content area is titled 'Policy Destination Type' and contains a section 'Choose the type of Destination SiliconServer' with two radio buttons: 'Managed Server' (selected) and 'Not a Managed Server'. At the bottom are 'next' and 'cancel' buttons.

BLUE ARC

Titan - 192.0.2.2 Advanced Mode: ON

Data Protection Home > Data Protection > Replication > Policy Destination Type

Policy Destination Type

Choose the type of Destination SiliconServer

☒ Managed Server ☐ Not a Managed Server

[next](#) [cancel](#)

- 3. Click **Managed Server** or **Not a Managed Server** and click the **next** button. Clicking the next button will display the "**Add Policy**" page for type of destination server that was selected.

Replication Policies

Adding a replication policy - managed server

From the **Policy Destination Type** page, click **Next** to display the following page.

Add Policy

Identification

Name:

Source

SiliconServer: Titan

EVS / File System: EVS01 / vol0

change...

Path:

☐ Virtual Volume: None

☒ Directory: /

browse...

Snapshot: None

Destination

SiliconServer: Titan

change...

EVS / File System: EVS01 / wormfs

change...

Path:

☐ Virtual Volume: None

☒ Directory: /

browse...

Processing Options

Source Snapshot Rule Name: None

Destination Snapshot Rule Name: None

Pre-Replication Script: None

Post-Replication Script: None

User-defined scripts to run before or after each replication. Scripts must be executable, and located in /usr/local/adc_replic/final_scripts.

Replication Rule

Rule Name: None

OK

cancel

Item /Field	Description
Identification	The name of the replication must not contain spaces, or any of the characters: \\<>'!@#E\$%^%&*(){}[] +=?:;,~` .'

Source	• SiliconServer: The name of the SiliconServer where the replication will be created. • EVS/File System: The name of the EVS and File System to which the replication is mapped. Click change... to change the EVS/File System. • Path: select the Virtual Volume by using the drop-down list. Or select the directory and enter the path.
Destination	The destination of the replication storage is configured to point to a managed server: • SiliconServer: The name of the SiliconServer where the replication will be created. Click change... to change the destination to a different server. • EVS/File System: The name of the EVS and File System to which the replication is mapped. Click change... to change the EVS/File System. • Path: select the Virtual Volume by using the drop-down list. Or select the directory and enter the path. Click change... to change the destination to a different server.
Processing Options	Pre-/Post-Replication Script: This is a user-defined script to run before or after each replication. Scripts must be located in /usr/local/adc_replic/final_scripts. The permissions of the scripts must be set to "executable".
Replication Rule	Optional configuration parameters that allow replications to be tuned to enable (or disable) specific functions or to achieve optimal performance.

1. Enter the Name of the policy in the Identification section. Provide a unique name the will identify this particular policy.
2. Enter the replication source parameters. The replication source identifies the currently managed server and allows selection of EVS, File System and path.
3. Enter the replication destination parameters. The replication destination allows selection of EVS, File System and path.
4. Specify the Source [Snapshot Rules](#) name. If a snapshot rule is specified for the source File System, it is used to perform the replication.
5. Specify the Destination [Snapshot Rules](#) name. If a snapshot rule is specified for the destination File System, it is used to perform the replication.
6. Specify any pre or post-scripts you plan to use. The pre replication scripts will be executed before the replication process begins and the post-scripts will executed at the conclusion of the replication process.
7. Select a Rule Name to associate this particular replication policy.

When all the fields are complete press the **OK** button.

Adding a replication policy - non-managed server

The procedure for adding replication policies for a non-managed server is very similar to the way managed servers are configured.



Note: Administrators should be authorized to use a non-managed server access and store replication data.

From the **Policy Destination Type** page, click **Next** to display Policy Identification page. When the Not Manage Server option is selected, the following screen is displayed.

BLUE-ARC

?

 Help

i

 About

Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

Data Protection

Home > Data Protection > Replication > Policy Destination Type > Add Policy

Add Policy

Identification

Name:

Source

SiliconServer: Titan

EVS / File System: EVS01 / vol0

change...

Path:

☐ Virtual Volume:

None

☒ Directory:

browse...

Destination

File Serving IP Address / Host Name:

File System:

Path:

NDMP User Name:

NDMP User Password:

Processing Options

Source Snapshot Rule Name:

None

Pre-Replication Script:

None

Post-Replication Script:

None

User-defined scripts to run before or after each replication. Scripts must be located in /usr/local/adc_replic/final_scripts.

Replication Rule

Rule Name:

None

OK

cancel

Item / Field	Description
Identification	The name of the replication must not contain spaces, or any of the characters: \\<>'!"@#E\$%^%&*(){}[]+=?:,;~` .'

Source	❑ SiliconServer: The name of the SiliconServer where the replication will be created. ❑ EVS/File System: The name of the EVS and File System to which the replication is mapped. Click change... to change the EVS/File System. ❑ Path: select the Virtual Volume by using the drop-down list. Or select the directory and enter the path.
Destination	The destination of the replication storage is configured to point to a not managed server: ❑ File Serving IP Address / Host Name: The name of the SiliconServer where the replication will be created. Click change... to change the destination to a different server. ❑ File System: The name of the File System to which the replication is mapped. ❑ Path: select the Virtual Volume by using the drop-down list. Or select the directory and enter the path. Click change... to change the destination to a different server. ❑ NDMP User Name: The name of the NDMP user for which the replication target is created. ❑ NDMP Password: Set the password for the selected NDMP user used to authenticate against the replication target.
Processing Options	Pre-/Post-Replication Script: This is a user-defined script to run before or after each replication. Scripts must be located in /usr/local/adc_replic/final_scripts. The permissions of the scripts must be set to "executable".
Replication Rule	Parameters that allow replications to be tuned for optimal performance.

1. Enter the Name of the policy in the Identification section. Provide a unique name the will identify this particular policy.
2. Enter the replication source parameters. The replication source identifies the currently managed server and allows selection of EVS, File System and path.
3. Enter the replication destination parameters. The replication destination allows selection of the following:
 - File Serving IP Address/Host Name
 - File System
 - Path
 - NDMP User Name
 - NDMP User Password

4. Specify the Source [Snapshot Rules](#) name. If a snapshot rule is specified for the source File System, it is used to perform the replication
5. Specify any pre or post-scripts you plan to use. The pre replication scripts will be executed before the replication process begins and the post-scripts will be executed at the conclusion of the replication process.

Snapshot Rules

If a replication policy is configured to use a snapshot rule, then when the replication begins no snapshot will be taken. Rather, the replication will use the most recent snapshot associated with the rule as the source of the replication. Snapshot rules are typically used when the replication includes a database or some other system that needs to be stopped in order to capture a consistent copy. The data management engine expects a snapshot will be taken as a result of an external command that may have been issued by the pre-replication script. In addition, to perform incremental replications, the data management engine needs the snapshot used during the previous replication.

Note the following:

- If no snapshot exists in the rule, then the data management engine issues a warning message and performs a full replication using an automatically created snapshot that is deleted immediately after the copy.
- If the snapshot taken during the previous replication has been deleted, a full copy is to be done instead of an incremental.

Custom Replication Scripts

Replication scripts are custom-written to perform specific functions. These scripts can be run prior to or after each replication. It is possible to specify scripts to execute each time an incremental replication is made. Under normal conditions, there's no need to use pre-replication and post-replication scripts and snapshot rules. The replication engine will take care of snapshot implementation to ensure proper incremental replication.

However, in the case of database or other applications that require a consistent state, the best practice would be to use the pre-replication and/or post-replication scripts and snapshot rules together.

- The pre-replication script is executed to completion before the replication is started.
- The post-replication script is executed after a successful replication.

Potential uses of pre-replication and post-replication scripts are illustrated in the following examples:

To backup a database

A pre-replication script can be used to backup database files. Typically, this pre-replication script will need to:

1. Shut down the database to bring it into a consistent or quiescent state.
2. Take a snapshot of the file system using a snapshot rule.
3. Restart the database.

To backup data from the replication target

The post-replication script can be used to perform incremental (or full) backups from the replication target after each incremental replication has completed. Backing up from the replication target (rather than the original volume or directory) minimizes the performance impact on network users.

After a replication copy has succeeded, the snapshots associated with previous copies on the source can be deleted. However, it is very important not to delete the snapshot associated with the last successful copy until the next successful copy has been completed.

Updating the "latest" snapshot

If the contents of the replication target are being shared or exported through the [Latest Snapshot](#) then it may be desirable to update the view of the target after the replication is complete. The latest snapshot shows the contents of the most recently created snapshot on the file system. While a replication is in progress no changes currently being recorded will appear in the shared or exported snapshot. Once the replication is complete, a post-replication script can take a new snapshot on the target file system. This will result in an immediate update of the view of the shared or exported latest snapshot, giving immediate access to the updates made by the replication.

Replication Rules

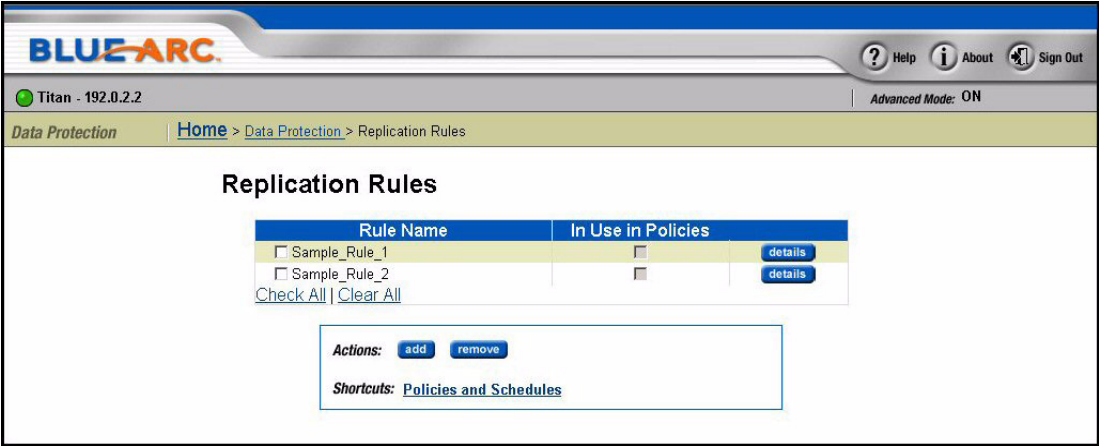
The **Replication Rules** page lists all existing rules and allows new rules to be created. Replication rules are optional configuration parameters that allow replications to be tuned to enable or disable specific functions or to achieve optimal performance.

Using Replication rules allow control of values such as the number of read-ahead processes, minimum file size used in block replication, when snapshots are deleted and if replications will include migrated files. The Titan SiliconServer is configured with default values which should be optimal in most cases. However, these values can be changed to customize replication performance characteristics based on the data set.

To view the Replication Rules

From the **Home** page, click **Data Protection**. Then, click **Replication Rules**.

The fields on this screen are described in the table below:



Item /Field	Description
Rule Name	Displays the name given to the Rule. This is assigned when the Rule is created, and is used to identify the Rule when creating or configuring policies.
In Use by Policies	A check in the box indicates that the rule is being used by one or more policies.
Details	Click the details button next to the rule to view the complete details regarding it. Select a Rule and click remove to delete it

To add a Replication Rule

From the **Home** page, click **Data Protection**. Then, click **Replication Rules**.

1. Click **Add**. The **Add Rule** page appears.

The fields on this screen are described in the table below:

Item / Field	Description
Name	Name of replication rule.
Description	Description of what the replication rule does.
Files to Exclude	Specifies files or directories to exclude from a replication. By default, none are excluded. When specifying a file or directory, type either: ☐ A full path name, relative to the top-level directory specified in the replication path. The path name must start with a forward slash (/), and an asterisk (*) can be typed at the end as a wildcard character. ☐ A <i>terminal</i> file or directory name, which is simply the last element in the path. The name must not contain any / characters, but it may start or end with the wildcard character *.

Block Replication Minimum File Size	Block replication minimum file size controls the minimum file size that is used for block replication. For instance, if this option is set to 64 MB and the source data file is 63 MB and the system determines only 1 MB of the source file has changed, then the entire source file (63MB) will be replicated. In contrast if the source file is 65 MB and only a small portion of that 65 MB file has changed, then only the delta will be replicated. This option is only functional if the Incremental-Block license is present. The drop down list options available are: 256 K, 512 K, 1, 2, 4, 8, 16, 32, 64 or 128 MB
Use Changed Directory List	Indicates if incremental backups or replications will use a changed object list to direct the search for changed files. If the process was not use the changed object list, it will have to search the entire directory tree looking for changed files. When using the changed object list, the search only passes through those directories that contain changed files.  Note: Using the change object list is likely to improve performance in some cases, such as situations where there are sparse changes. However it could also make performance worse in other cases where there are many changes throughout the directory structure).
Number of Read Ahead Processes	This option controls the number of read-ahead processes used when reading directory entries during a replication. The default read-ahead values will usually be suitable for most replications. However, where the file system is made up of many small files, the amount of time spent reading directory entries increases proportionately. In these cases, adding additional processes may speed up the replication operation.  Note: Each additional read-ahead process takes up system resources, so it is best to limit the number of additional processes unless it makes a significant difference in performance.

Pause While Replication(s) Finish Writing	By default the data management engine imposes an interlock to stop "NDMP" backups and "adc" copies from the destination of a replication while a replication copy is actively writing data. This is intended to help installations that replicate to a volume and back up from there. However, the lock is held at a volume level and with directory level replication and it may be desirable to override this action. To make use of this replication interlock, it is necessary to specify this rule option on both the replication that is intended to do the waiting, as well as the replication that is waited upon. As a best practice, create one rule with this option enabled and have each participating Replication Policy enable the same rule. Then, schedule the Policy "that waits" to run after the Policy that is "waited upon".
Take a Snapshot	Used to override the "Automatic Snapshot Creation" Backup configuration option.  Note: Snapshots are used as an integral part of the algorithm for incremental replication. The default option must be chosen in order to make incremental replication copies. However, when making a complete copy of a directory disable the snapshot generation option. Different files will be copied at different times so if the source file system is changing and there are dependencies between different files on the system then inconsistencies may be introduced.
Delete the Snapshot	This variable determines when snapshots are deleted. IMMEDIATELY gives the same effect as "Delete snapshot after replication is done", LAST preserves snapshot for use with incremental replications and OBSOLETE will delete an automatically created snapshot when the next backup of the same level is taken.  Note: Changing the "Delete Snapshot" options can adversely effect the replication process and therefore, it's recommended that this option only be changed at the direction of BlueArc Global Services.

Migrated File Exclusion	Indicates if the replications will include files whose data has been migrated to secondary storage. If set to enable, the replication will not include files whose data has been migrated to another volume using the Data Migrator facility. The default setting is disable, meaning that migrated files and their data will be replicated as normal files.
Migrated File Remigration	This option controls the action at the destination when the source file had been migrated. If set to enabled, the file will be re-migrated when written to the destination volume provided the volume or virtual volume has a Data Migrator path to indicate the target volume. If set to disabled, all the files and their data will be written directly to the replication destination volume.

Replication Files to Exclude Syntax

Replication "Files to Exclude" statements, each containing a number of expressions identifying which directories or files to exclude from the replication can be written using the following guidelines:



Note: BlueArc recommends creating the "Files to Exclude" list before the initial replication copy, and not changing it unless necessary. When running incremental updates, changes in the Files to Exclude list do not act retrospectively. For instance suppose the Files to Exclude list initially excludes "*.mp3". Then no files with the .mp3 extension will be migrated. If the replication or rule is then changed such that files with the mp3 extension are no longer excluded, then any new or changed mp3 files will be replicated. However, any mp3 files that haven't changed since the previous replication copy will not be replicated.

- The asterisk "*" can be used as a wildcard character to qualify path and filename values. When used in a path value, "*" is only treated as a wildcard if it appears at the end of a value, e.g. /path*. In a filename value, **a single** "*" can appear at the beginning and or the end of the value. e.g *song.mp*, *blue.doc, file*.
- Parentheses (), spaces, > greater than and quotation marks (") are allowed around a filename or path list but they will be treated as literal characters.
- Path and filename can be defined together but must be separated by a comma (.). e.g. /subdir/path*, *song.doc, newfile*, /subdir2
- The forward slash (/) is used as a path separator. As such, it must not be used in a filename list.

Replication Schedules

After a Replication Policy has been defined, it must be scheduled to run. Replications can be scheduled and rescheduled at any time and with any of the available scheduling option.

Replication Schedules Overview:

- **Periodic replication:** replications will occur at preset times. Periodic replications can be setup to run daily, weekly, monthly or at intervals specified in number of hours or days.
- **Continuous replication:** a new replication job starts after the previous one has ended. The new replication job can start immediately or after a specified number of hours.
- **One time replication:** a replication job is set-up to run a specific time.

When planning Replication Schedules, it is recommended to schedule them to run during off-peak times such as nights or over the weekends. After a replication has started, additional replications for the same policy cannot be started until the current one has completed. However, it is possible to start multiple concurrent replication, each for its own policy.

To view Scheduled Replications

From the **Home** page, click **Data Protection**. Then, click **Replication**.

BLUE-ARC

?

 Help

i

 About

✕

 Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

Data Protection

Home > Data Protection > Replication

Replication for Titan

Policies

Name	SiliconServer	Source EVS	File System/Path	Server	Destination EVS	File System/Path	
☐ TestPolicy2	Titan	EVS01	vol0:/	Titan	EVS01	vol4:/	details
☐ policy1	Titan	EVS01	vol0:/dean_replication	Titan	EVS01	vol1:/replication1	details

Check All | Clear All

Actions: [add](#) [remove](#)

Shortcuts: [Replication Rules](#) [Backup User](#)

Schedules

ID	Policies	Next Run	Interval	Last Status	
☐ 5	policy1	06/07/2005 14:30	DAILY		details

Check All | Clear All

Actions: [add](#) [remove](#)

Shortcuts: [Replication Status & Reports](#)

The fields on this screen are described in the table below:

Item /Field	Description
Id	Displays the ID assigned to the Replication Policy.
Policies	Displays the name given to the Replication Policy.
Next Run	Displays the month, date, year and time for the next scheduled replication run for this policy.
Interval	Displays the frequency at which the replication has been scheduled to run.
Last Status	Displays a light indicator for successful and failed replication jobs. A green light represents a successful replication job has completed. Failed replication jobs will display a red light and the reason for failure.  Note: In case of a replication failure, the next time a replication is started the data management engine attempts to restart the failed replication instead of starting a new replication.

Actions	Click Add to add a new schedule from the Add Replication Schedule page. Click Remove to clear a selected schedule from the list.

To add a Replication Schedule

- 1. From the **Home** page, click **Data Protection**. Then, click **Replication**.
- 2. Under **Schedules**, click **add** schedule a new replication. The following screen appears.

BLUE ARC

?

 Help

i

 About

Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

Data Protection

 | [Home](#) > [Data Protection](#) > [Replication](#) > Add Schedule

Add Schedule

Policy

Replication Policy:

TestPolicy2

Timing

Time of Initial Run:

23:59

 (24 hour time)

Date of Initial Run:

06/06/2005

Date of Final Run: (optional)

Current SMU Date and Time: 06/06/2005 16:19

Schedule

☒

daily

 - based on the scheduled date and time.

☐ Every hours - based on the scheduled date and time.

☐ Continuous. Pause hours between runs.

☐ Once, at the scheduled date and time.

☐ Inactive

A replication policy must be set up before a replication job can be scheduled.

Item	Description
Replication Policy	Select a replication policy from the drop-down menu.

Time of Initial Run	Enter the scheduled run time in a 24 hour setting (i.e. 11:59 PM will be entered as 23:59). The current SMU date and time are provided below for reference.
Date of Initial Run	From the calendar next to the field, select the start date for the policy's initial run. The selected date appears on the field.
Date of Final Run	From the calendar next to the field, select the start date for the policy's final run. The selected date appears on the field. This is an optional setting.
Schedule	☐ When selecting the first option, pick a pre-set rule of: <i>daily</i>, <i>monthly</i>, or <i>weekly</i> from the drop-down menu. ☐ Select the second option to specify replication jobs in number of hours or days. ☐ Select the third option to have a new replication job start after the previous one has ended. The new replication job can start immediately or after a specified number of hours. This option also allows you to specify a "pause" between replications. ☐ Selecting the fourth option guarantees that the policy is scheduled to run only once. This is the date and time for the next replication. ☐ Selecting the fifth option causes the replication schedule to be placed in a inactive (paused) state.  Note: If an excess amount of time elapses between replication runs then: ☐ Snapshots may take up a larger amount of space. ☐ By default, replication-defined snapshots are purged after 7 days (configurable to 40 days). That means waiting 8 or more days between replication runs could result in a full replication.

1. Click **OK** to add the schedule and return to the **Replication** page.
2. Click **cancel** to clear the screen and return to the **Replication** page.

To modify a Replication Schedule

Once defined, schedules can be easily modified to meet the changing requirements of the Replication Policies. When modifying a schedule, the scheduled date and time, as well as the interval in which the schedule will run can be changed.

1. From the **Replication** page, select a schedule to modify.
2. Click **details**.

BLUE ARC ? Help i About Sign Out

TITAN-ST - 192.0.2.2 Advanced Mode: ON

Data Protection | [Home](#) > [Data Protection](#) > [Replication](#) > Modify Schedule

Modify Schedule

Policy

Replication Policy: Archive01
 Next Run: 02/08/2006 23:59
 Last Status: ☒ No Status [View Latest Report](#)

Immediate Actions

Recovery Options

Timing

Schedule Time: 23:59
 Schedule Date: 02/08/2006
 Date of Final Run:

☐ Reschedule
 Time: (24 hour time)
 Date: (date)
 Final Run: (optional)

Current SMU Date and Time: 02/08/2006 18:50

Schedule

☒ - based on the scheduled date and time.
☐ Every hours - based on the scheduled date and time.
☐ Continuous. Pause hours between runs.
☐ Once, at the scheduled date and time.
☐ Inactive

3. To start the selected Replication Policy immediately, click **run now**.
4. If the previous replication attempt failed, click restart to **restart** the replication or, if available, **rollback** the target file system to the snapshot taken after the last successful replication.

5. To define a new starting date and time for the selected schedule, click **re-schedule** and enter the new values in the appropriate fields.
6. To change the schedule's interval, configure the schedule to repeat either daily, weekly, or monthly, or configure the schedule to run **Continuously, Once Only**. Select **Inactive** to pause a replication job.
7. Click **OK** to apply the changes or **cancel** to discard them, and return to the **Replication** page.



Note: A replication job cannot be started if a previous instance of the same job is still in progress. In this case, the replication is skipped, and an error is logged.

Scheduling Incremental Replications

Incremental replications rely on the existence of the snapshot taken during the previous replication. If this snapshot no longer exists, the data management engine has to perform a full replication. The data management engine automatically preserves the snapshots it needs for replication. However, replication-defined snapshots are purged after 7 days (configurable to 40 days via "Replication Schedule"). A full replication could occur in the following scenarios:

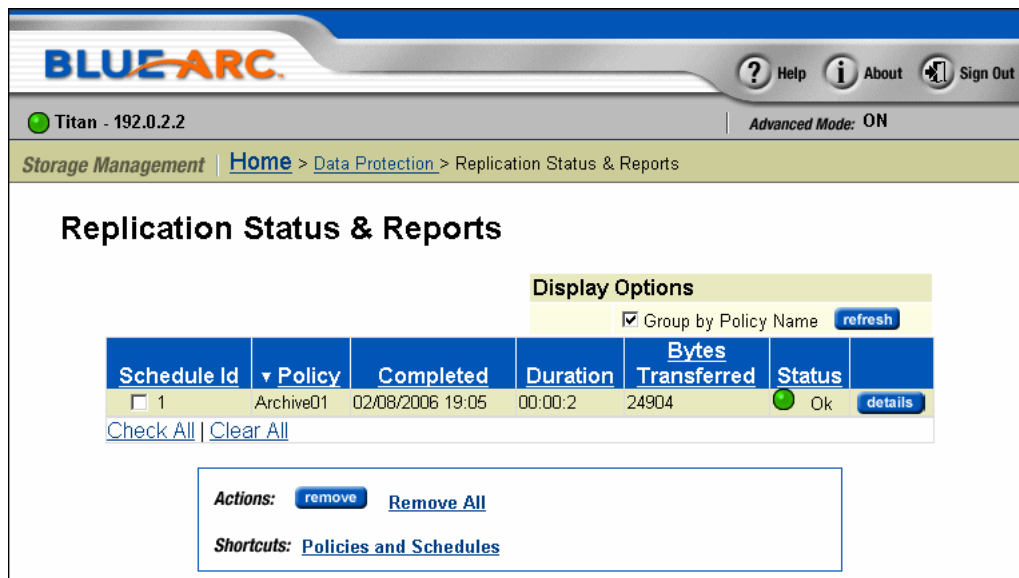
- "Periodic" or "Once Only" schedule but not running frequently (waiting 8 or more days between replication runs could result in a full replication).
- Deleting the schedule of policy and then rescheduling at a much later date (the snapshots will have been purged when the schedule is deleted).
- Scheduling a "Date of Final Run", then re-using the schedule/policy weeks after the final run finished (the snapshots will have been purged after the "final run").

The schedule section shows the age of the snapshot to be used for replication. If the snapshot doesn't exist, then indicates that a 'full replication' is performed.

Replication Status & Report

The **Replication Status & Reports** page displays a list of replication jobs that are in progress or that have been completed. Replication Reports also includes a number of reporting details on files replicated, amount of data replicated, success or failure status, etc. If a schedule is deleted, the reports associated with it are also deleted.

The replication report Status column displays the results of the replication job (successful or failed). Reports can also be beneficial for analyzing the effects of a particular incremental replication policy. This is particularly true when replicating across a WAN by viewing the Report Summary page. The information contained in the Report Summary provides a detailed view of the replication job results. This information can be used to make adjustments in the replication policy and schedule that can improve the overall replication efficiency.



BLUEARC

Titan - 192.0.2.2 | Advanced Mode: ON

Storage Management | [Home](#) > [Data Protection](#) > Replication Status & Reports

Replication Status & Reports

Display Options

☒ Group by Policy Name [refresh](#)

Schedule ID	Policy	Completed	Duration	Bytes Transferred	Status
☐ 1	Archive01	02/08/2006 19:05	00:00:2	24904	Ok details

[Check All](#) | [Clear All](#)

Actions: [remove](#) [Remove All](#)

Shortcuts: [Policies and Schedules](#)

The fields on this screen are described in the table below.

Item	Description
Schedule ID	Displays the ID number for the completed replication.
Policy	Displays the policy's name.
Completed	Displays the month, date, year and time when the replication was completed.
Duration	The amount of time it took for the replication schedule to run.
Bytes Transferred	Displays the volume of data in Bytes that were replicated.
Status	Displays the status on whether the replication was successfully completed.

To view Replication Reports

- 1. From the **Home** page, click **Data Protection**. Then, **Replication Status & Reports**.
- 2. Select the completed replication of interest and click **details** next to it. The following page is displayed.

Replication Report

Report Summary

Replication Policy:

Schedule ID:

Status:

Frequency:

policy1

5

Ok

DAILY

Start Time:

End Time:

Duration:

06/04/2005 14:30

06/04/2005 14:45

00:15:54

Server / EVS:

Amount Replicated:

Titan / EVS01

0 bytes

Received notify_connect (Connection established): version: 4:
Connected to Bluearc NDMP session 8

Progress (14:30:00): Transfer Started
Msg (type 0, id 5281) NDMP(7): Starting replication (policy1) of files to /vol1/replication1

Msg (type 0, id 5280) NDMP(8): Starting level 10 replication (policy1) of file system /vol0/dean_replicatio

Writing restart file /usr/local/adc_replic/replication_policies/policy1/adc_restart
Progress (14:35:21): Transferred 3094 megabytes (9872 kilobytes / second)
Progress (14:40:42): Transferred 6788 megabytes (11781 kilobytes / second)
Backup Operation operation halted (Successful):
NDMP(8): replication (policy1) of /vol0/dean_replication complete (0 warning(s), 0 error(s))

Operation complete
File recovered: /
Recovery Operation operation halted (Successful):
NDMP(7): replication (policy1) to /vol1/replication1 complete (0 warning(s), 0 error(s))

Progress (14:45:52): Transfer Terminated: 10491 megabytes
Time elapsed: 00:15:52
Average tranfer rate: 11284 kilobytes / second
Operation complete
Elapsed time: 0 hours, 15 minutes, 54 seconds.

The transfer is complete.

Item	Description
Replication Policy	Displays the completed replication policy's name.
Schedule ID	Displays the replication schedule ID.
Status	Indicates whether the replication was successfully completed.
Frequency	Displays how often the Policy is scheduled to run.

Start Time	Displays the date and time when the replication began.
End Time	Displays the date and time when the replication ended.
Duration	Displays the time taken to complete the replication.
Server/EVS	Displays the EVS on which the Source and Destination File System reside.
Bytes Transferred	Displays the volume of data in Bytes that were replicated.

Troubleshooting Replication Failures

If a replication fails with errors, identify the source of the problem and ensure that it has been cleared. Listed below are some possible scenarios where a replication job can fail and possible solutions that may resolve the problem.

- ❑ The destination volume is offline.

In this case, bring the volume back online before the replication can continue.

- ❑ The destination volume was full.

In this case, clear up more space in the destination.

- ❑ One of the volumes involved may have been unmounted.

In this case, remount the volume before the replication can continue.

- ❑ SMU was rebooted while a replication job was in progress.

In this case, the replication will abort but will restart the next scheduled replication job when comes back on line.



Note: Without any further action upon a replication failure, the replication will continue as expected on its next scheduled run. However, this will recopy any changes already copied during the failed replication attempt.

Clicking the *Run Now* button will cause the failed replication to be restarted immediately and will avoid recopying most of the data.

To Manually Restart a Failed Replication

If a replication has failed, the replication will be restarted normally when it is next scheduled to run. To restart the replication before the next scheduled replication interval, it will need to be restarted manually. Do the following to manually restart a failed replication.

1. Move to the SMU **Home** page.
2. From the **Data Protection** heading, click on **Replication** to view the main replication page.
3. From the Schedules table, click on the **Details** button for the failed replication to view the Replication Schedule page.
4. Click the **Restart** button to start the replication again.

To Rollback an Incomplete Replication

When a replication between a source and target file system successfully completes, a snapshot is taken of the target to preserve the state of the file system. If a subsequent replication fails because the source file system is offline, it may be desirable to restore the target to the state of the last successful replication. Do the following to rollback the target file system to the state of the last successful replication.

1. Move to the SMU **Home** page.
2. From the **Data Protection** heading, click on **Replication** to view the replication page.
3. From the Schedules table, click on the **Details** button for the failed replication to view the Replication Schedule page.
4. Click the **Rollback** button to rollback the target file system to the state of the last successful replication.

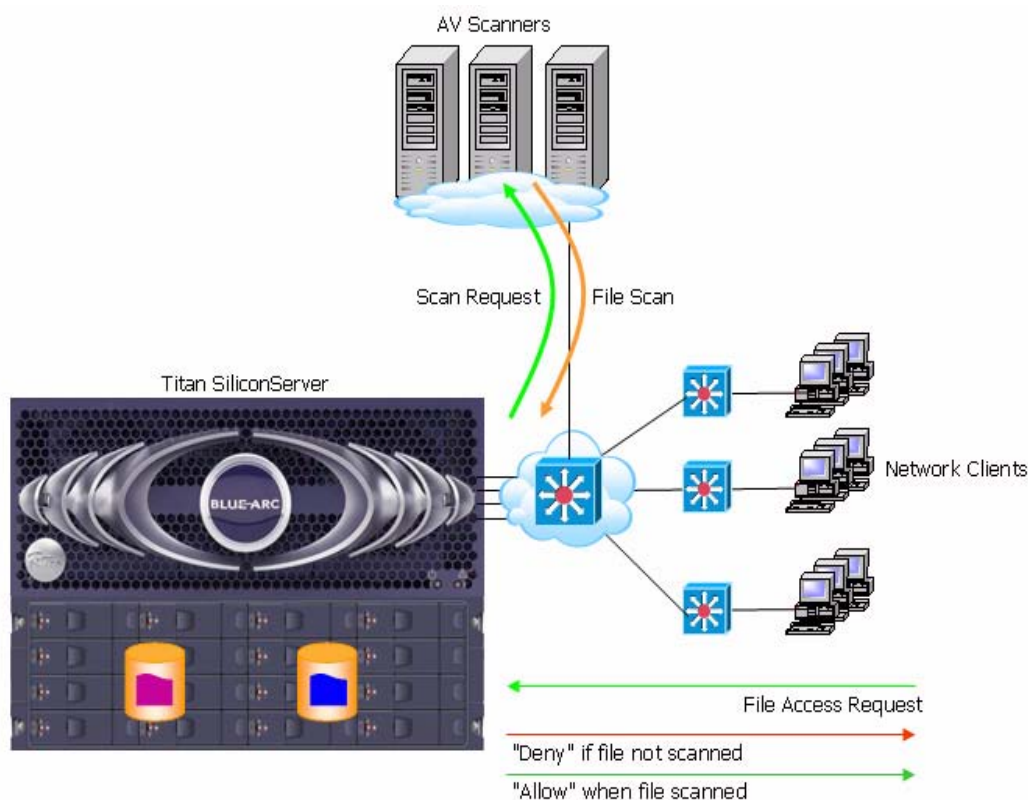
Virus Scanning

As the spread of viruses increases, organizations are looking for solutions that can detect and quarantine them. To address this growing issue, BlueArc is working with industry leading anti-virus (AV) software vendors to ensure that the Titan SiliconServer integrates into an organization's existing AV solutions and without requiring special installations of AV software and servers.

The Titan architecture reduces the effect of a virus because the file system is hardware-based. This prevents viruses from attaching themselves to or deleting system files that are required for server operation. However, viruses can still propagate and infect users' data files that are stored by the server. To reduce the effect that a virus may have on users' data, BlueArc recommends that anti-virus is configured for Titan to protect users' data and that anti-virus software runs on all user workstations.



Note: Titan provides a means by which to connect with existing Virus Scan Engines on the network. Titan does not perform any scanning of the files per se.



Virus Scanning Overview

Virus Scanning is enabled and configured per [EVS](#). Only files accessed using the CIFS protocol are scanned. If a file has not been verified by a Virus Scan Engine as clean, it will need to be scanned before it can be accessed. However, scanning for viruses when a client is trying to access the file can take time. To reduce this latency, files are automatically queued to be scanned as soon as they are created or modified, and then closed. Queued files are scanned promptly, expediting the detection of viruses in new or modified files and making it unlikely that a virus infected file will remain dormant on the system for a long period of time.

The Titan maintains a list of file types, the Inclusion List, that allows the administrator to control which files are scanned (e.g. .exe, .dll, .doc, etc.). The default Inclusion List includes most file types commonly affected by viruses.

Multiple Virus Scan Engines can be configured to enhance performance and high-availability of the server. If a Virus Scan Engine fails during a virus scan, Titan automatically redirects the scan to another Virus Scan Engine.



Caution: When virus scanning is enabled, Titan must receive notification from a Virus Scan Engine that a file is clean before allowing access to the file. As a result, if virus scanning is enabled and there are no Virus Scan Engines available to service the virus scans, CIFS clients may experience a temporary loss of data access. To ensure maximum accessibility of data, configure multiple Virus Scan Engines to service each EVS on which virus scanning has been enabled.

If virus scanning is temporarily disabled, files will continue to be marked as needing to be scanned. In this way, if virus scanning is re-enabled, files that were changed will be re-scanned the next time they are accessed by a CIFS client.

Titan provides [statistics](#) to monitor virus scanning activity.

Configuring Virus Scanning

To configure virus scanning, the following steps are required:

1. Configure the Virus Scan Engine(s).
2. Enable anti-virus support on Titan.
3. Optionally disable virus scanning on selected [CIFS shares](#).

Supported Platforms

- ❑ Symantec Anti Virus Scan Engine (SAVSE) 4.3
- ❑ McAfee® VirusScan® with RPC support 7.1.0
- ❑ Sophos Antivirus for NetApp 1.0.1
- ❑ Trend Micro ServerProtect 5.31 with RPC support

Important Information on Virus Scanning Configuration

- ❑ The account used to start the scanning services on the Virus Scan Engine must be added to Titan's [Backup Operator Local Group](#). A link to the **Local Groups** configuration page can be found on the bottom of the **Virus Scanning** page.
- ❑ When installing a Virus Scan Engine, select to use the RPC protocol when prompted.
- ❑ When configuring McAfee VirusScan, set the action to "Clean infected files automatically", then to "Delete infected files automatically".
- ❑ Sophos Antivirus reports repaired .zip files as an "infected file" and not a "clean scan" as the other Scan Engines.

After installation and configuration has been complete, the Virus Scan Engine will automatically self-register with Titan.

For additional details on preparing the Virus Scan Engine software for use, refer to the Virus Scan Engine installation instructions.

To Enable Virus Scanning on the Titan SiliconServer

From the **Data Protection** page, click **Virus Scanning**.

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: ON

Data Protection

Home > Data Protection > Virus Scanning

Virus Scanning

EVS[EVS01]

☒ Enable Virus Scanning

Registered Virus Scanners

Name	IP Address	Domain	Status
RING	192.168.41.5	shire	Ok

Deregister Scanner

Request Full Scan

☒ Scan All File Types

File types to scan

ACE
ACM
ACV
ACX
ADT

Delete

Delete All

Reset Defaults

Extension

Add to Inclusion List

Apply

Cancel

1. Select the **EVS** on which to enable virus scanning.
2. Check the box for **Enable Virus Scanning**. This will enable the virus scanning services on the Titan or the selected EVS. Virus Scanning can be disabled on individual shares by unchecking the Enable Virus Scanning box in the **Add Shares** screen.



Note: It is important that at least one Virus Scan Engine is registered in the box.

3. Click **Apply**.



Tip: Optionally, virus scanning can be disabled on selected **CIFS shares**.

To Take a Virus Scan Engine Out of the Configuration

When the IP address of a Titan SiliconServer is added to a Virus Scan Engine's list of RPC clients, the Virus Scan Engine will automatically register itself with the Titan SiliconServer. Virus Scan Engines will also automatically deregister themselves when their local virus scanning service is restarted, stopped, or when the IP address of the Titan SiliconServer is removed from the Virus Scan Engine's IP address list. However, if a Virus Scan Engine fails, it may not automatically deregister itself. Therefore, the **Deregister Scanner** button removes the failed Virus Scan Engine out of the Titan Registered Virus Servers list.



Note: The *Deregister Scanner* button should only be used with failed Virus Scan Engines.

Controlling Which File Types Are Scanned

Titan maintains a list of file types, the *Inclusion List*, that allows the administrator to dictate which files are scanned (e.g. .exe, .dll, .doc, etc.). The default *Inclusion List* includes most file types commonly affected by viruses.

Selecting **Scan All File Types** will cause all files to be scanned.



Caution: The default Inclusion List contains the most commonly used file types. BlueArc recommends that the anti-virus software vendor be contacted for an up-to-date list of file types that should be included for scanning and to modify the Inclusion List accordingly. BlueArc accepts no responsibility for viruses introduced through file types that are not listed.

To Add a file type in the list of **Files types to scan**, enter the extension in **Extension**. Then, click **Add to Inclusion List**.

To delete a file type, select it from the list. Then, click **Delete**.

To delete all file types, click **Delete All**.

To revert back to the original list of files types to scan, click **Reset Defaults**.

The **default** file extension inclusion list is as follows:

ACE, ACM, ACV, ACX, ADT, APP, ASD, ASP, ASX, AVB, AX, BAT, BO, BIN, BTM, CDR, CFM, CHM, CLA, CLASS, CMD, CNV, COM, CPL, CPT, CPY, CSC, CSH, CSS, DAT, DEV, DL, DLL, DOC, DOT, DVB, DRV, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTT, HTW, HTX, IM, INF, INI, JS, JSE, JTD, LIB, LGP, LNK, MB, MDB, MHT, MHTM, MHTML, MOD, MPD, MPP, MPT, MRC, MS, MSG, MSO, MP, NWS, OBD, OBT, OBJ, OBZ, OCX, OFT, OLB, OLE, OTM, OV, PCI, PDB, PDF, PDR, PHP, PIF, PL, PLG, PM, PNF, PNP, POT, PP, PPA, PPS, PPT, PRC, PWZ, QLB, QPW, REG, RTF, SBF, SCR, SCT, SH, SHB, SHS, SHT, SHTML, SHW, SIS, SMM, SWF, SYS, TD0, TLB, TSK, TSP, TT6, VBA, VBE, VBS, VBX, VOM, VS?, VSD, VSS, VST, VWP, VXD, VXE, WBT, WBK, WIZ, WK?, WML, WPC, WPD, WS?, WSC, WSF, WSH, XL?, XML, XTP, 386

Forcing Files to be Rescanned

With the appearance of a new virus and release of anti-virus software updates, it is important to re-scan all files, including those that have not changed since the last time they were scanned.

1. From the **Home** page, click **Data Protection**. Then, click **Virus Scanning**.
2. Click **Request Full Scan**. This flags all file types in the *Inclusion List* to be re scanned the next time a user attempts to access them.

8 Scalability and Clustering

Scalability and Clustering Overview

The Titan SiliconServer can be configured for standalone operation or as a two-node Active/Active (A/A) High-Availability (HA) cluster. Through shared storage and centralized management, multiple Titan SiliconServers and HA clusters can be joined together as a logical unit called a Server Farm. File services are virtualized, allowing them to be migrated to any Titan within the same HA cluster or Server Farm. Titan supports file services through special entities called Enterprise Virtual Servers.

Enterprise Virtual Servers

Enterprise Virtual Servers (EVS) appear to network clients as actual file servers. Like a physical server, these virtual servers are configured with IP addresses, have CIFS shares and NFS exports for file sharing, and contain file systems. Network clients access EVS as unique, individual servers, while the administration of EVS is localized to the server or cluster hosting them. A single Titan server or HA cluster can support up to eight EVS.

To increase availability of file services provided by EVS, Titans can be configured as a High Availability (HA) cluster. In an HA cluster, EVS can be balanced across the Cluster Nodes based on the load and data access patterns of the individual Cluster Nodes. If one of the Cluster Nodes should fail, all EVS in the cluster are automatically migrated to the remaining node.

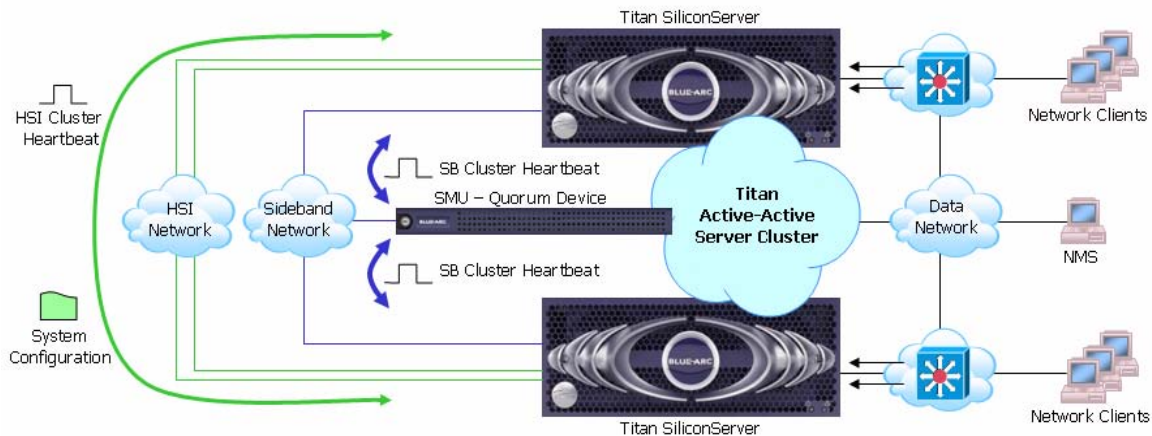
Titans can be configured together as a Server Farm. Server Farms are collections of Titan servers and/or HA clusters with a shared Storage Pool. EVS that are hosted on the Server Farm can be migrated to any other server or HA cluster in the farm.

Shared Storage Pool

Every server in a HA cluster or Server Farm must share the same pool of storage. This ensures that when EVS move from one server to another, whether due to an automatic failover in a HA cluster or a manual migration of EVS amongst servers in a Server Farm, the target server has access to the storage served by the EVS.

High Availability Clusters

The Titan SiliconServer supports two-node Active/Active (A/A) clusters. In A/A cluster configurations, each server can host independent EVS, which can service network requests simultaneously. Should either of the servers fail, the EVS from the failed node will automatically migrate to the remaining server. Network clients will not typically be aware of the failure and will not experience any loss of service, though the cluster may operate with reduced performance until the failed server is restored. After the server is restored and is ready for normal operation, the EVS can be migrated back to the original server.



A license is required to set up an A/A cluster. Contact BlueArc to purchase an A/A cluster license. For more information on how to enter the license key(s), see ["To Add a License Key"](#).

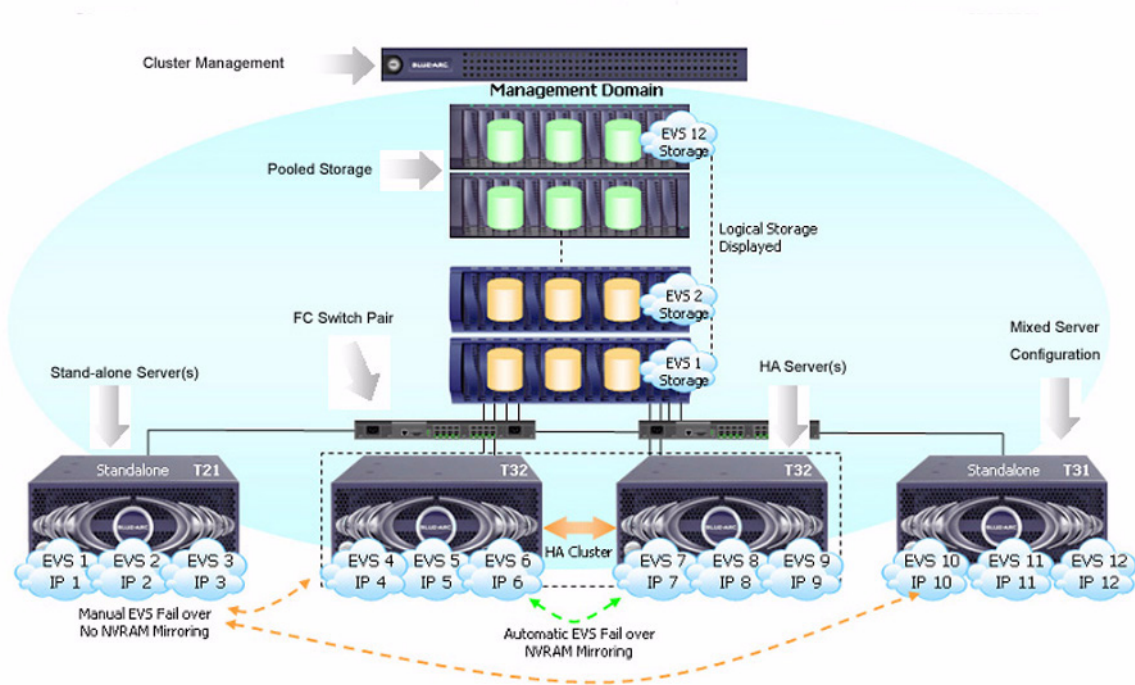
Server Farms

A Server Farm is a collection of standalone Titan SiliconServers or HA clusters in which all storage resources are combined in a shared Storage Pool. Each server or cluster in the Server Farm can host up to a maximum of 8 EVS. EVS can be easily migrated between the servers and clusters in the Server Farm through the SMU. There are three primary reasons to configure a Server Farm:

- **Maximum performance** - When maximum data throughput is required, EVS can be migrated to a high-end Titan or one on which no other EVS resides. This will ensure that the EVS enjoys the fully dedicated resources of a single Titan SiliconServer.
- **Load balancing** - Heavily used EVS can be migrated to less-busy Titans, or to higher-end Titans which support greater server capacity, resulting in more efficient use of available resources.
- **Failure recovery** - In the event of a catastrophic failure of any standalone server, EVS hosted by the failed server can be brought online on any other server or cluster in the Server Farm.

A single SMU is used to manage every server and cluster within the Server Farm. The SMU hosts the management network for the Server Farm and provides quorum services for up to eight HA clusters. Managed devices must be located in the same data center, not distributed across a campus or MAN environment.

The following is a typical representation of a Server Farm, containing two standalone servers and an HA cluster:



The following table distinguishes the properties of an HA cluster and a Server Farm:

Properties	HA Cluster	Server Farm
Can belong to a Server Farm	Yes	No
EVS migration under server failure	Automatic	Manual
NVRAM mirroring between servers	Yes	No

Maximum number of Titan servers	2	There are no restrictions on the number of servers except that an SMU can only manage 8 Quorum Devices; so the Server Farm will have to be arranged accordingly.
Shared SMU	For central management; cluster quorum	For central management; EVS Migration
Shared Storage Pool	Yes	Yes

Using Enterprise Virtual Servers

Titan SiliconServer can have up to eight Enterprise Virtual Servers (EVS). Likewise, an Active/Active (High-Availability) Cluster can have up to eight EVS. An EVS can be added, deleted, and changed based on the evolving needs of the network.

Creating an EVS

EVS must be created and configured before they can be used. First, EVS must be created and assigned an IP address. Then, in order for an EVS to provide file services, it must be assigned to one or more file systems.

To add an EVS

1. From the **Home** page, click **SiliconServer Admin**. Then, click **EVS Management**.
2. Click **Add EVS**. The **Add EVS** page appears.

BLUE ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

SiliconServer Admin | Home > SiliconServer Admin > Add EVS

Add EVS

Label

IP Address

Subnet Mask

Port

Apply Cancel

3. Enter a **Label** for the EVS.
4. Enter the **IP Address** of the EVS.
5. Enter the **Subnet Mask**.
6. Select the **Port** to which the EVS will be assigned.
7. Click **Apply**.

Assign a File System to an EVS

After the EVS has been created, it must be assigned a file system. Only when a file system is unmounted can it be assigned to an EVS.

- 1. From the **Home** page, click **Storage Management**. Then, click **Silicon File Systems**.
- 2. Click **details** next to the file system that will be assigned to the EVS.
- 3. The **File System Details** screen will appear. Next to **Current EVS**, select the EVS to which the file system will be assigned.

EVS

Select an EVS:  

Status:

Security: [Unknown](#)

- 4. Click **assign**.
 - 5. The File System will now appear as having been assigned to the EVS on the **Silicon File Systems** page. The File System is ready to be mounted.
 - 6. Check the box next to the File System **Label**.
 - 7. Click **mount**.
- The File System should appear as **Mounted** in the **Status** column.

EVS Management

The **EVS Management** page allows EVS to be added, deleted, enabled, and disabled.

BLUE ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

SiliconServer Admin | [Home](#) > [SiliconServer Admin](#) > EVS Management

EVS Management

Type	Label	First IP Address	Status	Enabled	Cluster Node
Admin Services	Titan	192.0.2.2	online	Yes	TITAN-1
File Services	EVS01	192.168.38.100	online	Yes	TITAN-1
File Services	EVS02	192.168.38.101	online	Yes	TITAN-1
File Services	EVS03	192.168.38.102	online	Yes	TITAN-2
File Services	EVS04	192.168.38.103	online	Yes	TITAN-2
File Services	EVS05	192.168.38.104	online	Yes	TITAN-1
File Services	EVS06	192.168.38.105	online	Yes	TITAN-2

Modify Label Disable EVS Restart EVS

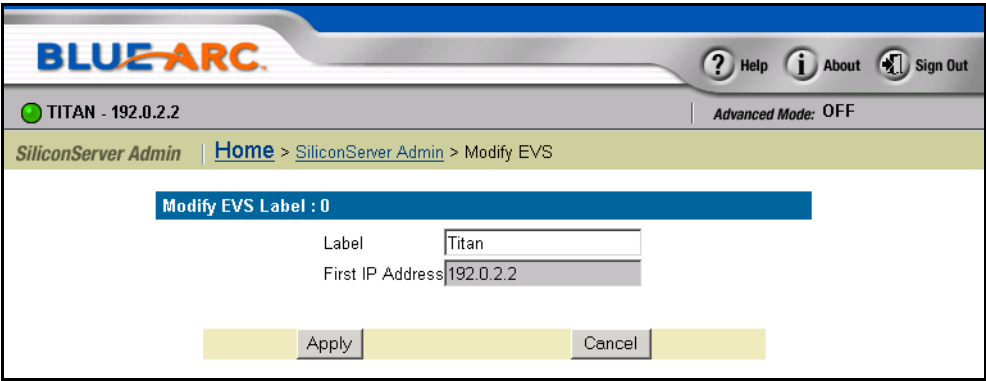
Add EVS Delete EVS

Item	Description
Type	Type of service (administration or file).
Label	The EVS label. The label is used to help identify the different configured EVS.
First IP Address	EVS can have multiple IP addresses. This displays the first IP address assigned to the EVS.
Status	Service status: Online: Up and capable of providing services. Offline: Not running. While offline, EVS are inaccessible.

Enabled	Indicates whether the EVS is enabled. If enabled, then the EVS is online and will start automatically if the server is rebooted. Click Disable EVS to disable the EVS. If not enabled, then the EVS is offline and will not start automatically if the server is rebooted. Click Enable EVS to enable the EVS.
Cluster Node	Cluster Node hosting this service.

To change an EVS label

- 1. On the **SiliconServer Admin** page, click **EVS Management**.
- 2. Click **Modify Label**.
- 3. On the **Modify Label** page, enter the new label for the cluster services.



- 4. Click **Apply**.
- Click **Cancel** to clear the screen.

To delete an EVS

- 1. On the **SiliconServer Admin** page, click **EVS Management**.
- 2. Select the desired EVS.
- 3. Click **Disable EVS**.
- 4. Click **Delete EVS**.



Note: Deleting an EVS does not affect the file system owned by the EVS. Once the EVS has been deleted, assign the file system to another EVS to make it available for use.

Titan High Availability Clusters

The following section details how Titan SiliconServers can be formed as clusters to expand their functionality.

Clustering Concepts

Titan clustering provides the following functions:

- Nodes in a Titan cluster can simultaneously host multiple EVS, allowing both servers to be *active* at the same time, each providing file services to clients.
- The cluster monitors the health of each server through redundant channels. Should one server fail, the other can take over its functions transparently to network clients, so no loss of service will result from the failure.
- The cluster provides a cluster-wide replicated registry, containing configuration for both servers in the cluster.

Cluster Nodes

Each Titan SiliconServer that is a member of a cluster is referred to as a Cluster Node. In a cluster, EVS can be hosted simultaneously on both Cluster Nodes. Titan clustering keeps file services separate from the Cluster Node on which these services reside. Network users use IP addresses that are associated with the EVS rather than with the Cluster Nodes. This allows for seamless, automatic failover, or EVS migration, from one Cluster Node to another.

The Quorum Device (QD)

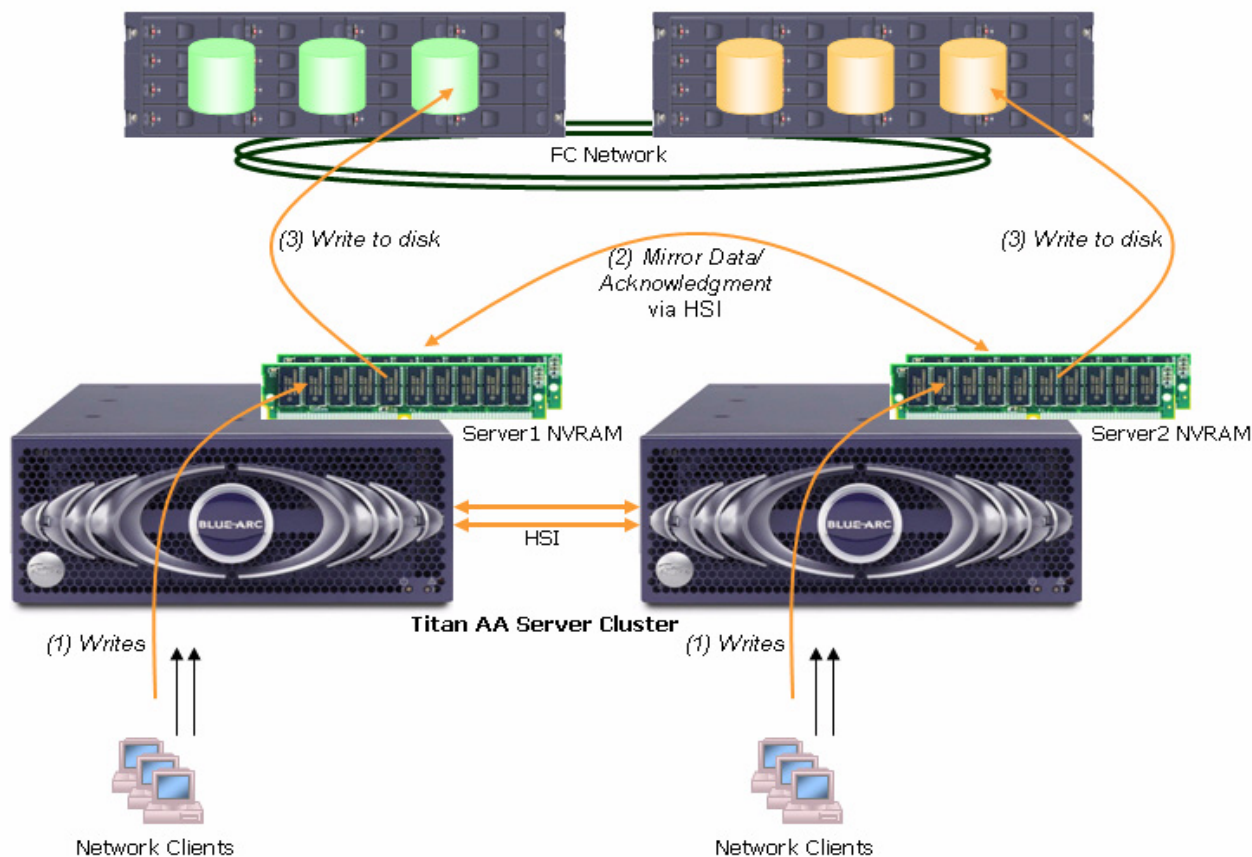
A Quorum Device (QD) allows the cluster to survive a node-to-node cluster communication failure and preserves a copy of the *registry*, which contains the cluster's configuration. The QD resides and runs on the [System Management Unit](#) (SMU). The SMU can provide QD services for up to eight clusters in a Server Farm. Refer to [Managing the Quorum Device](#) for more information.

Titan clustering makes use of a *Majority Voting Quorum* scheme, which is augmented by the QD. The majority voting quorum ensures that only one server can access a file system, thus preserving data integrity. Each Cluster Node and the QD act as voting nodes in the majority voting quorum scheme. Only when a Cluster Node has quorum will it be allowed access to a file system. Normally, the two active nodes in the cluster can constitute a quorum and maintain the integrity of the file systems. However, under certain failure scenarios, both Cluster Nodes will attempt to use the same storage (this is typically referred to as a *network partition*, a condition in which each Cluster Node has lost communication with the other node). In this case, the QD will “vote” for one of the servers, allowing it to maintain quorum and thus granting it exclusive access to the storage. If there is no partition between servers, the QD does not participate in any elections.

Although the registry is replicated across both Cluster Nodes, there are certain failure scenarios which could result in the loss of recent configuration changes (this problem is referred to as *amnesia*, a condition where configuration changes are lost because of other failures). The SMU preserves a copy of the registry, thus ensuring that configuration changes are always replicated.

Data Protection

Titan buffers file system data in **NVRAM** until it is written to disk, to protect it from failures including power loss. When the Titan SiliconServer is configured as a cluster, each Cluster Node mirrors the NVRAM of the other node, thus ensuring data consistency in the event of a hardware failure of a Cluster Node. When a Cluster Node takes over for a failed node, it uses the contents of the NVRAM mirror to complete all data write transactions that were not yet committed to disk by the failed node.



Cluster Topology

All cluster elements (i.e. the Cluster Nodes and the QD) are typically connected through the **private management network**. This keeps cluster traffic off the enterprise network, and isolates it from potential congestion resulting from heavy data access loads.

Cluster Nodes are also connected directly using the *High Speed Interconnect* (HSI). This dedicated network consists of dual redundant Gigabit Ethernet (GE) links, and is used for clustering traffic and data protection, i.e. NVRAM mirroring.

Creating a Cluster

Configuring two Titan SiliconServers to operate in a cluster requires the following steps:

1. Ensure that one of the servers has an A/A cluster license.
2. Configure, or “promote”, the licensed server to A/A cluster mode.
3. Add a second server by “joining” it to the A/A cluster.
4. Add one or more EVS to the cluster.
5. Distribute the EVS amongst the Cluster Nodes.



Note: In order to maximize the performance in the cluster, the EVS should be distributed in such a way as to even the network client load between them.

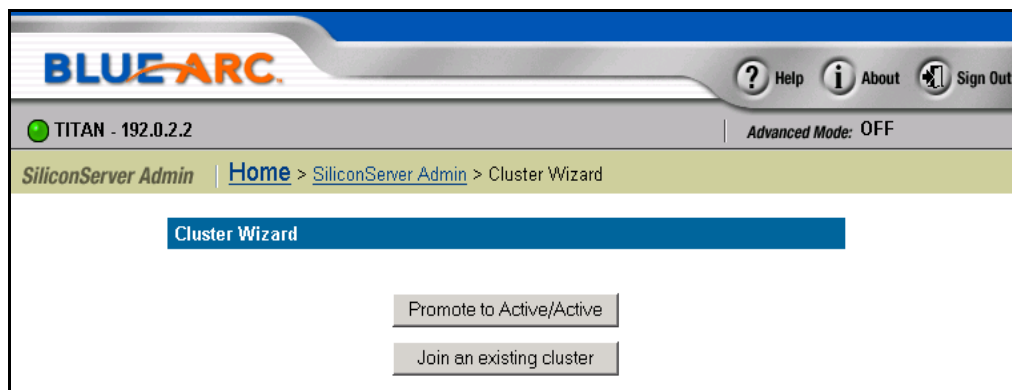
Using the Cluster Wizard

In Cluster Wizard, a server can be configured as an Active/Active Cluster Node and a server can also be configured to join an existing cluster.

Whether creating a new cluster or joining a node to an existing cluster, a Cluster Node [IP address](#) must be defined. The Cluster Node IP address is used to maintain heartbeat communication between Cluster Nodes and between the Cluster Nodes and the Quorum Device (QD). Due to the importance of the heartbeat communication, the Cluster Node IP address should be assigned to the 10/100 management port connected to the private management network, keeping the heartbeats isolated from normal network congestion.

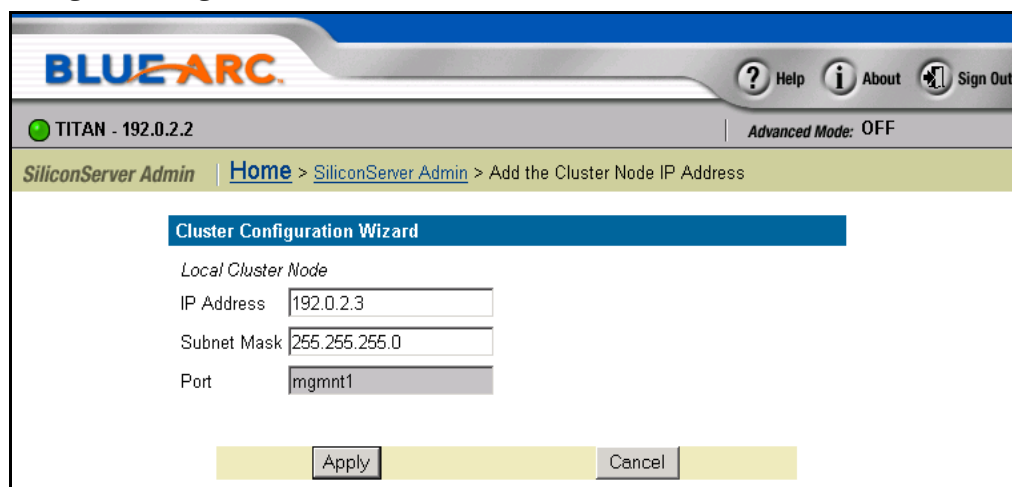
To configure the first Cluster Node

1. From the Home page, click SiliconServer Admin. Then, click **Cluster Wizard**.
2. Click **Promote to Active/Active**.



The screenshot shows the BlueArc SiliconServer Admin interface. The top navigation bar includes the BlueArc logo, a status bar showing 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF', and links for Help, About, and Sign Out. The breadcrumb trail is 'SiliconServer Admin > Home > SiliconServer Admin > Cluster Wizard'. The main content area is titled 'Cluster Wizard' and contains two buttons: 'Promote to Active/Active' and 'Join an existing cluster'.

3. Enter the Cluster Node **IP Address** and **Subnet Mask**. The **Port** is automatically assigned to mgmnt1.



The screenshot shows the BlueArc SiliconServer Admin interface for the 'Cluster Configuration Wizard'. The top navigation bar is identical to the previous screenshot. The breadcrumb trail is 'SiliconServer Admin > Home > SiliconServer Admin > Add the Cluster Node IP Address'. The main content area is titled 'Cluster Configuration Wizard' and contains a section for 'Local Cluster Node' with three input fields: 'IP Address' (192.0.2.3), 'Subnet Mask' (255.255.255.0), and 'Port' (mgmnt1). At the bottom, there are 'Apply' and 'Cancel' buttons.

- Click **Apply**.

BLUE ARC

TITAN - 192.0.2.2 | Advanced Mode: OFF

SiliconServer Admin | Home > SiliconServer Admin > Create Cluster

Cluster Configuration Wizard

Cluster Name:

Available Quorum Devices

Name	Status	Supported Version(12)
SMU-TITAN	Unconfigured	Supported Version(12)

Apply Cancel

- To change the default server name, enter a new **Cluster Name**.
- Select a **Quorum Device** from the list.
- Click **Apply**.

The server will automatically reboot.

To join an existing Cluster through the CLI

It is easiest and most expedient to join a node to a cluster when it is being configured for the first time.



Caution: When joining a node to a cluster, the cluster's configuration will overwrite the configuration information of the joining node, causing any prior configuration changes to be lost including IP addresses and file system bindings.

The following details the steps necessary to join a node to a cluster using the Web Manager GUI.

- Connect to the built-in RS232 port of the unconfigured Titan SiliconServer that will join the cluster as described in [Using the Command Line Interface](#).

- 2. When the server boots for the first time, it will prompt for cluster membership and request information about the cluster being joined.

Prompt	Description
Is this node joining a cluster	To join the cluster, enter y
Enter cluster node IP address	Enter the Cluster Node IP address to assign to the joining node. This IP address will be assigned to the mgmnt1 port which is the 10/100 Ethernet port.
Enter cluster node IP mask	Enter the network mask for the joining node's Cluster Node IP.
Enter the cluster name	Enter the name of the cluster to join. This is the cluster name and should not be confused with the DNS name. i.e. <i>Titan</i> should be entered rather than <i>192.0.2.2</i>

The node will automatically join the cluster during boot.

To join an existing cluster through Web Manager

The following details the steps necessary to join a node to a cluster using Web Manager.

- 1. From the **Cluster Wizard** screen, click the **Join an existing cluster** button.
- 2. Enter the Cluster Node IP address and subnet mask for this new Cluster Node. The IP address will automatically be assigned to the mgmnt1 port.
- 3. Click **Apply**.
- 4. Select a cluster from the available list.
- 5. Click **Apply**.

The server will automatically reboot.

Managing a Cluster

The following sections explain how to manage the cluster including cluster services (file services and server administration) and the physical elements which form the cluster (cluster nodes and the quorum device).

Configuring the Cluster

On the **SiliconServer Admin** page, click **Cluster Configuration**.

The screenshot shows the 'Cluster Configuration' page in the SiliconServer Admin interface. The page has a blue header with the 'BLUE-ARC' logo and navigation links for Help, About, and Sign Out. Below the header, a status bar shows 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF'. The main content area is titled 'Cluster Configuration' and displays the following information:

- Cluster Mode:** Active/Active (A/A)
- Cluster Name:** TITAN (in a text input field)
- Overall Status:** Cluster ONLINE
- Cluster Health:** Robust
- Buttons:** 'Rename Cluster' (disabled)
- Quorum Device Section:**
 - Name:** SMU-TITAN
 - IP Address:** 192.0.2.1
 - Status:** Owned
 - Owner:** TITAN-2
 - Buttons:** 'Add Quorum>>' (disabled), 'Remove Quorum' (disabled)

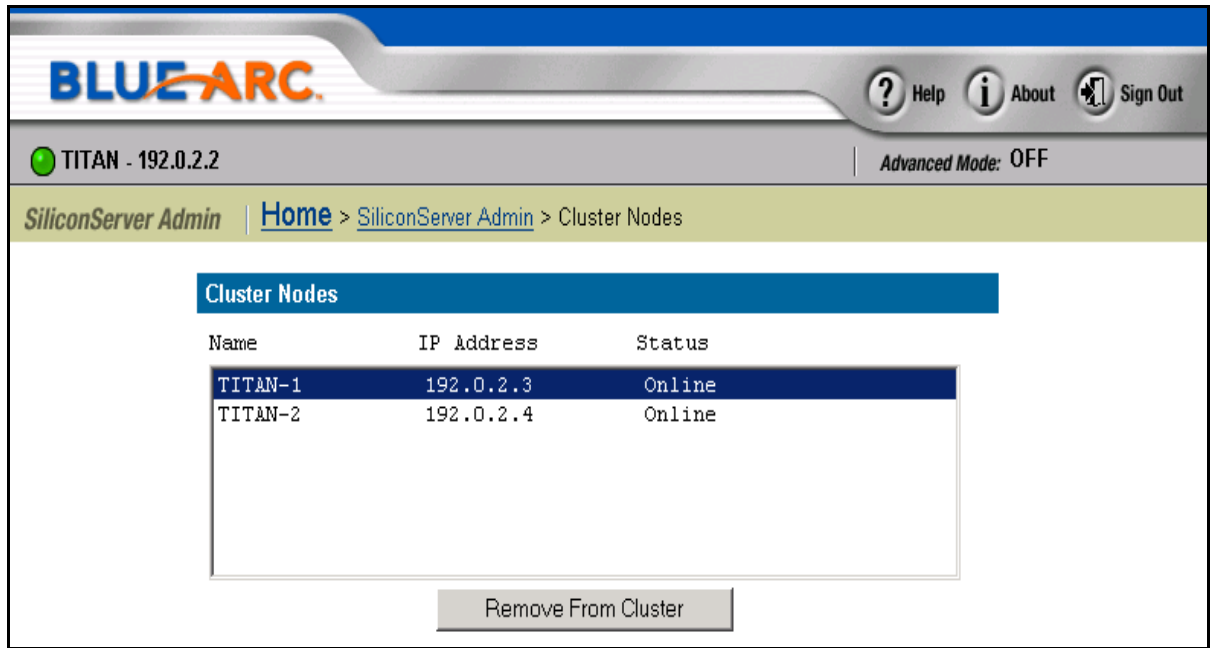
Item	Description
Cluster Mode	Single node or Active/Active (A/A).
Cluster Name	Name of cluster.
Overall Status	Overall cluster status (online or offline).
Cluster Health	Cluster health: - Robust - Degraded
Quorum Device	
Name	Name of server hosting the QD (i.e. the SMU on which the QD resides).
IP Address	IP address of server hosting the QD (i.e. the SMU on which the QD resides).
Status	QD status: - Configured - the QD is attached to the cluster, but the QD's vote is not needed, i.e. a cluster of 1. - Owned - the QD is attached to the cluster and owned by a specific node in the cluster. - Not up - the QD cannot be contacted. - Seized - the QD has been taken over by another cluster.
Owner	Cluster Node that currently "owns" the QD.

If you need to add or remove the cluster’s QD, click the appropriate button (**Add Quorum>>** or **Remove Quorum**).

If the QD is removed from the cluster, the port will be released back to SMU’s pool of QDs and ports.

Managing Cluster Nodes

From the **SiliconServer Admin** page, click **Cluster Nodes**.



This screen shows the following:

Item	Description
Name	Name of Cluster Node.
IP Address	IP address of Cluster Node.

Status	Status of Cluster Node: • Online. The Cluster Node is a part of the cluster and is exchanging heartbeats with the other cluster members. • Offline. The Cluster Node is no longer exchanging heartbeats with the other cluster members. This may be caused by a reboot, or the Cluster Node may be have suffered a fault condition. Services cannot be migrated to this Cluster Node while in this state. • Dead. No heartbeats have been seen from this Cluster Node for a significant amount of time. Services cannot be migrated to another Cluster Node while in this state. • Unknown. The node has not been online since the cluster was started.

To remove or break a cluster, select the Cluster Node that needs to be removed then click the **Remove From Cluster** button.



Note: A Cluster Node can only be removed if it is not hosting any administrative services. If services are hosted by the Cluster Node, they need to be migrated to a different Cluster Node before the node can be removed.

Managing the Quorum Device

Quorum Device services are provided by the SMU. While servers and clusters in a Server Farm are managed by a single SMU, an SMU can provide quorum services for up to eight clusters in a Server Farm. To do so, the SMU hosts a pool of eight available QDs. When a new cluster is formed, a QD must be assigned to the cluster. Once assigned to the cluster, the QD is “owned” by that cluster and is no longer available. Removing a QD from a cluster releases its ownership and returns the service to the pool of available QDs.

Each instance of the QD service can be viewed and configured by using the `quorumdev` command in the SMU’s CLI interface.

Using the `quorumdev` command

The Quorum Device (QD) is a process running on the SMU and is managed using the `quorumdev` CLI command. Access to the SMU’s CLI is available using SSH as follows:

1. Connect to the SMU using SSH with the *manager username* and *password*.
2. Choose ‘exit to SMU shell’.
3. Log in as *root* (type ‘su -’, when prompted enter the configured root password).

4. At the prompt run '**service quorumdev**' with the appropriate option, i.e. **start**, **stop**, **status**, **unconfigure** or **restart**.

[1-8]: If specified, the command works on the appropriate *instance* of the quorum device.

- ❑ **start**: starts any QD process not currently running.
- ❑ **stop [1-8]**: stops the quorumdev process.
- ❑ **restart [1-8]**: stops and then starts the quorumdev process.
- ❑ **unconfigure [1-8]**: removes the current cluster configuration settings, so that the quorum device can be assigned to a new cluster or the same cluster following an error. After unconfiguring, the quorum device has to be restarted.
- ❑ **status [1-8]**: reports the quorum devices current status, e.g. quorumdev is running, quorumdev process not running. If the QD is owned by a cluster, additional information about the cluster is also visible such as the cluster name and unique ID.



Caution: Incorrect usage of the stop, restart, or unconfigure options may disrupt QD services provided to clusters throughout a Server Farm.

Cluster Name Space

When deployed on a Titan SiliconServer, the Cluster Name Space (CNS) allows separate and physically discrete file systems to appear as a single logical file system, i.e. a unified file system. This virtualizes multiple storage elements, allowing network clients to access them through a single CIFS share or NFS export.

Like a file system, at the top of the CNS tree is a root directory. Subdirectories can then be created under the root directory. The root directory and subdirectories in the CNS tree are virtual directories. Access to these virtual directories is read-only. Only Titan's physical file systems support read-write access. Physical file systems can be made accessible under any directory in the CNS tree by creating a File System Link. File System Links associate the virtual directory in the CNS tree with physical file systems.

Any directory in the CNS can be exported or shared, making the CNS, and the underlying physical file systems, accessible for use by network clients. The creation and configuration of the CNS can be done either through the Web UI (described below) or the CLI.

Once shared or exported, the CNS will be accessible through any EVS in the server or cluster. As a result, it is not necessary to access a file system through the IP address of the specific EVS to which the file system is associated. Consequently, file systems linked into the CNS can be relocated between the EVS on the server or cluster transparently and without requiring the client to update its network configuration. This can be useful to help distribute load between servers in a cluster, allowing heavily used file systems to be relocated to servers that are better able to support the load.

The typical configuration for CNS is also the most simple. After the root directory of the CNS has

been created, create a single CIFS share and NFS export on the CNS root. Then, add a File System Link for each physical file system under the root directory. In such a configuration, all of the server's storage resources will be accessible to network clients through a single share or export, and each file system will be accessible through its own subdirectory.

Windows and Unix clients can take full advantage of the storage virtualization provided by CNS because directories in the virtual name space can be shared and exported directly. However, there is no support for creating FTP mount points or iSCSI Logical Units through the name space. As a result, FTP clients and iSCSI Initiators communicate directly with individual EVS and their associated file systems. This also means that if a file system containing FTP mount points or iSCSI Logical Units is relocated to a different EVS, connectivity will need to be reestablished through the new EVS.



Tip: For the best results, FTP mount points and iSCSI Logical Units should be added to file systems that are not part of a Cluster Name Space.



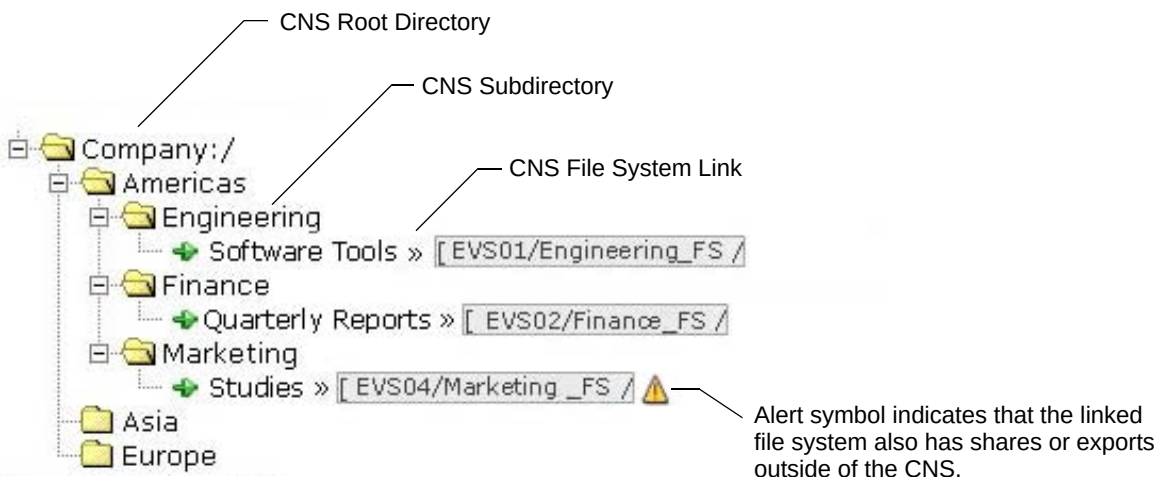
Note: CNS is a licensed feature. To create a Cluster Name space, a CNS license must be installed. To purchase a CNS license, please contact BlueArc.

CNS Topology

The CNS has a tree-like directory structure, much like a real file system. The CNS can be viewed through the CLI or the Web UI, and shows all of the configured directories and File System Links.

To View an Existing Name Space

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.



- At the top of the name space is the root directory.
- Under the root directory are a number of subdirectories. In this example topology, one subdirectory has been created for each physical file system.
- Under each subdirectory is a File System Link. A File System Link associates a directory with a specific file system. The EVS to which the file system is associated is also shown.

Creating a Cluster Name Space

A CNS contains a root directory, File System Links, and, optionally, subdirectories. The first step required to configure CNS is to create the root directory.

To Create a CNS Root Directory

Use this procedure to create a root directory. All that is needed is a name.

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. In the **CNS Root Label** text box, type in a name.
4. From the box at the bottom of the page, click on **OK** to create the CNS.

In order for the CNS to be available to clients, a CIFS share and/or an NFS export must be created for it. For instructions, see ["To Setup a CIFS Share,"](#) or ["To Add an NFS Export."](#)

To Create a CNS Directory

Directories are an optional configuration element for CNS. They can be created under the root directory or under other subdirectories in the CNS tree. Directories give structure to the CNS, allowing granular control over the organization of physical file system resources.

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. From the box at the bottom of the page, click on **Add Directory** to view the Add CNS Directory page.
4. From the **Select a Parent for the Directory** options box, select a location in the CNS tree where the new directory must be added.
5. In the **Subdirectory Name** text box, type in a name for the directory.
6. Click **OK** to create the directory.
7. If needed, repeat to add more directories.

To Create a File System Link

File System Links make physical file systems accessible through the CNS. A File System Link can be associated with either the root directory or a subdirectory in a physical file system. Once created, a File System Link will appear as a directory in the CNS. The directory name seen by a

client will be the name given to the File System Link. A client navigating through CNS and into a File System Link will see the contents of the directory that was linked.

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. From the box at the bottom of the page, click on **Add Link** to view the Link File System page.
4. In the **Link Name** text box, type a name for the link.
5. At the **From CNS Directory** options box, select a location in the CNS tree for the link.
6. Select the file system to link by clicking **Change** on the **To File System** options box. Then, select the desired file system to link.
7. To link a specific directory in the physical file system, rather than the root directory which will link the entire file system, enter the directory to link in the **Path on File System** text box, or click **browse...** to search for one.
8. From the bottom of the page, click **OK** to create the File System Link.

Editing a Cluster Name Space

After a CNS has been created, any part of it can be changed, except for renaming the root directory.

To Delete a Cluster Name Space

Deleting a CNS will permanently erase it. Deleting a CNS will not affect the physical file systems accessible through the CNS. However, once the CNS has been deleted, it may be necessary to restore access to the file system by sharing or exporting the file system through its EVS.

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. From the CNS directory tree, select the CNS root directory.
4. From the box at the bottom of the page, click **Remove** to open a confirmation message box.
5. Click **OK** to delete the CNS.

To Rename a CNS Directory

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. From the CNS directory tree, select the directory that needs to be edited.
4. From the box at the bottom of the page, click on **Modify** to view the Modify CNS Directory page.

5. In the **Subdirectory Name** text box, type in a new name for the CNS directory.
6. From the bottom of the **Enter a New Directory Name** options box, click **Apply** to open a confirmation message box.
7. Click **OK** to rename the directory.

To Move a CNS Directory

Moving a CNS directory from one location in the CNS to another can be done at any time.

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. From the CNS directory tree, select the directory that needs to be moved.
4. From the box at the bottom of the page, click on **Modify** to view the Modify CNS Directory page.
5. From the **Select a Parent for the Directory** options box, select a new location in the tree for the directory.
6. From the bottom of the options box, click **Apply** to open a confirmation message box.
7. Click **OK** to move the directory.

To Delete a CNS Directory

Deleting a CNS directory will permanently remove it and all of its subdirectories and File System Links. Deleting CNS directories will not affect physical file systems on the server.

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. From the CNS directory tree, select the directory that needs to be deleted.
4. From the box at the bottom of the page, click on **Remove** to open a confirmation message box.
5. Click **OK** to delete the directory.

To Edit a File System Link

The name and location in the CNS can be changed.

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. From the CNS tree, select the link that needs to be changed.
4. From the box at the bottom of the page, click on **Modify** to view the Modify File System Link page.
5. If the link name must be changed, use the **Link Name** text box to make the change.

6. If the parent directory must be changed, then from the **Select a New Parent Directory** options box, select a new location in the CNS tree.
7. From the bottom of the page, click **OK** to add or change the CNS link.

To Delete a File System Link

Deleting a File System Link will erase the link from the CNS. The actual file system associated with the link will not be deleted.

1. Move to the SMU **Home** page.
2. From the **File Services** heading, click on **CNS** to view the CNS page.
3. From the CNS tree, select the link that needs to be deleted.
4. From the box at the bottom of the page, click **Remove** to open a confirmation message box.
5. Click **OK** to delete the link.

Considerations when using CNS

Be aware of the following when using CNS:

- A single name space is supported per server or cluster.
- CNS does not support hard links or 'move' operations across the individual file systems. These operations are fully supported, but only within a single physical file system, i.e. the part of the CNS tree under a File System Link.
- Relocating file systems under the CNS may interrupt CIFS access to the file system being relocated. To minimize interruption, relocate file systems when they are idle. For more information, see "[To Relocate a Silicon File System](#)".

Migrating an EVS

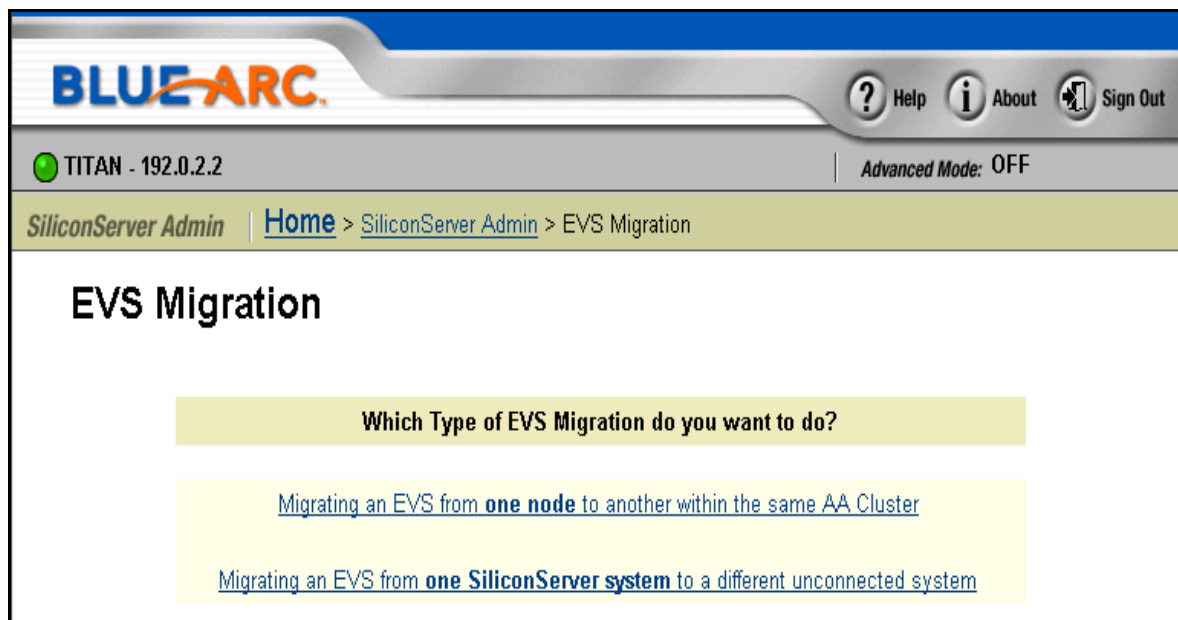
While automatic migration of EVS occurs as part of the failover resiliency provided in HA clusters, EVS can be manually migrated across any server or cluster within a Server Farm.

Migrating an EVS within an HA Cluster

EVS can be migrated to a different Cluster Node, or all EVS can be migrated to a preferred mapping. EVS to Cluster Node mappings can be preserved, if desired.

To migrate EVS between servers of the same HA cluster

1. From the **SiliconServer Admin** page, click **EVS Migrate**.



Note: This screen will only appear if the SMU is managing multiple Titan SiliconServers in a Server Farm. Otherwise, clicking **EVS Migrate** will immediately launch the **EVS Migrate** page shown in step 2.

- Click the first option, **Migrating an EVS from one node to another within the same AA Cluster.**

The **EVS Migrate** page appears with several options:

BLUE ARC

TITAN - 192.0.2.2 | Advanced Mode: OFF

SiliconServer Admin | Home > SiliconServer Admin > EVS Migrate

EVS Migrate

☒ Migrate all cluster services from Node TITAN to Node TITAN

☐ Migrate EVS EVS01 to Node TITAN

☐ Migrate all EVS to Preferred Migration Mapping:

EVS Name	Current Node	Preferred Node
EVS01	TITAN	

Save the Current Mapping as Preferred Mapping:

To migrate all EVS between Cluster Nodes

- Select the **Migrate all cluster services from Node ___ to Node ___** radio button.
- Using the drop-down menu, select the Cluster Node from which to migrate all EVS.
- Select the Cluster Node to which the EVS will be migrated.
- Click **Migrate**.

To migrate EVS to a Cluster Node

- Select the **Migrate EVS ___ to Node ___** radio button.
- Using the drop-down menu, select the EVS to migrate to a Cluster Node.
- Select the Cluster Node to which the EVS will be migrated.
- Click **Migrate**.

To save a Preferred EVS to Cluster Node Mapping

Saving the **Preferred Migration Mapping** helps restore EVS mappings to Cluster Node. For example, if a failed Cluster Node is being restored, the preferred migration mapping can be used to easily restore the original cluster configuration.

1. Migrate the EVS between the Cluster Nodes until the preferred mapping has been defined. The current mapping will be displayed in the list box.
2. Select the **Migrate all EVS to Preferred Migration Mapping** radio button.
3. Click **Save**.

To migrate all EVS to a Preferred Mapping

1. Select the **Migrate all EVS to Preferred Migration Mapping** radio button.
2. Click **Migrate**.

Migrating an EVS within a Server Farm

Migration within a Server Farm is supported under the following conditions:

- ☐ When both the source and destination server are online.
- ☐ If the source server is offline and the destination server is online.
- ☐ The EVS does not contain any file systems that are linked into a CNS tree.



Note: After migrating EVS between servers in a Server Farm, the assignment of tape drives and tape autochanger devices to EVS must be manually adjusted. Any tape devices that were specifically assigned to the migrated EVS will have become unassigned. Tape devices that had been assigned to "any EVS" on the source server will remain assigned to "any EVS" on the source server. Tape devices must not be assigned to EVSs on more than one server.

Preparing for EVS Migration

EVS contain most of the settings needed to support client access to the storage. However, certain settings, like DNS, Windows NT domain or Active Directory, etc. are functions of the server or cluster hosting the EVS, and not the EVS itself. When preparing to migrate an EVS from one server or cluster to another, it is important to make sure that the target settings can properly support the EVS being migrated to it. To prepare a server or cluster to receive a new EVS, settings from the source server can be applied to it through Server Cloning. For information about specific settings that can be cloned, refer to [Cloning from another Titan SiliconServer](#).

To Clone Server settings

1. Select the *target* of the EVS migration as the SMU's *managed server*.

- From the **Home** page, click **SiliconServer Admin**. Then, click **Clone SiliconServer Settings**.

The screenshot shows the 'Clone SiliconServer Settings' page in the BLUEARC SiliconServer Admin interface. The page header includes the BLUEARC logo, navigation links (Help, About, Sign Out), and a status bar indicating the current server is 'TITAN - 192.0.2.2' with 'Advanced Mode: OFF'. The breadcrumb trail shows the path: Home > SiliconServer Admin > Clone SiliconServer Settings. The main content area is titled 'Clone SiliconServer Settings' and contains a form with a dropdown menu labeled 'Clone the selected configuration from:' showing 'TITAN - 192.168.41.210' and a text field labeled 'to: TITAN-1'. At the bottom are 'back', 'next', and 'cancel' buttons.

- Select the server currently hosting the EVS that will be migrated from the **Clone the selected configuration from** drop-down menu.
- Click **next**.
- Select the settings that should be migrated to the *target* server.



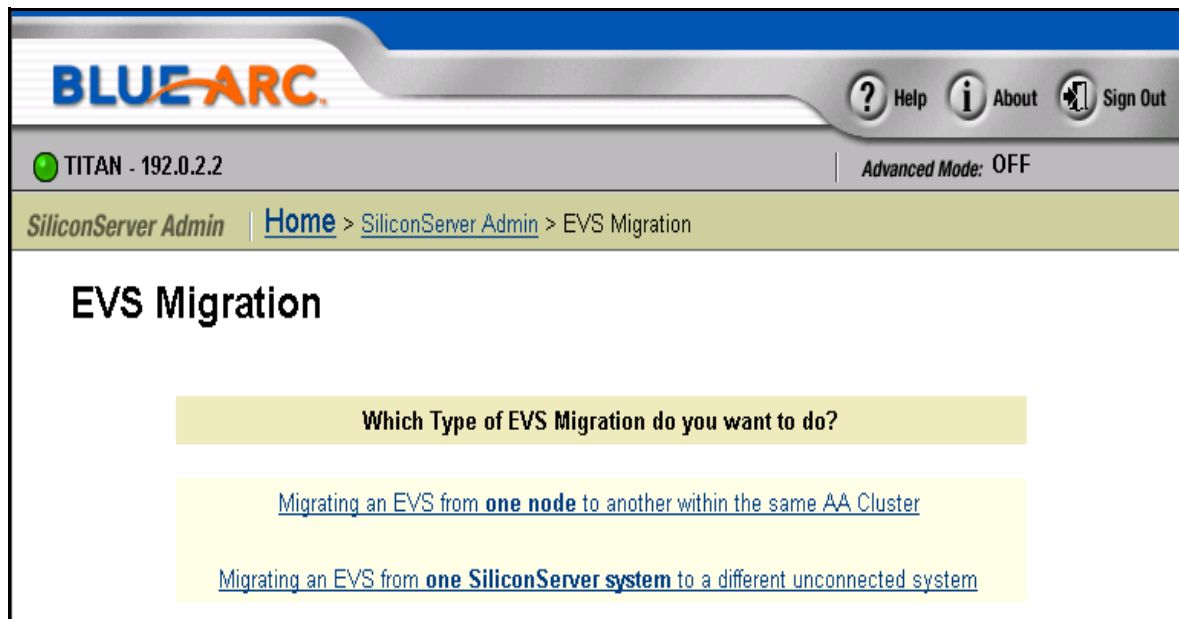
Caution: Settings selected for cloning will **overwrite** the currently defined settings on the target server. If the existing configuration needs to be preserved, do not specify those settings to be cloned.

- Click **OK** to initiate the Server Cloning of the specified settings.

Once the server has been prepared through Server Cloning, it is ready to have the EVS migrated to it.

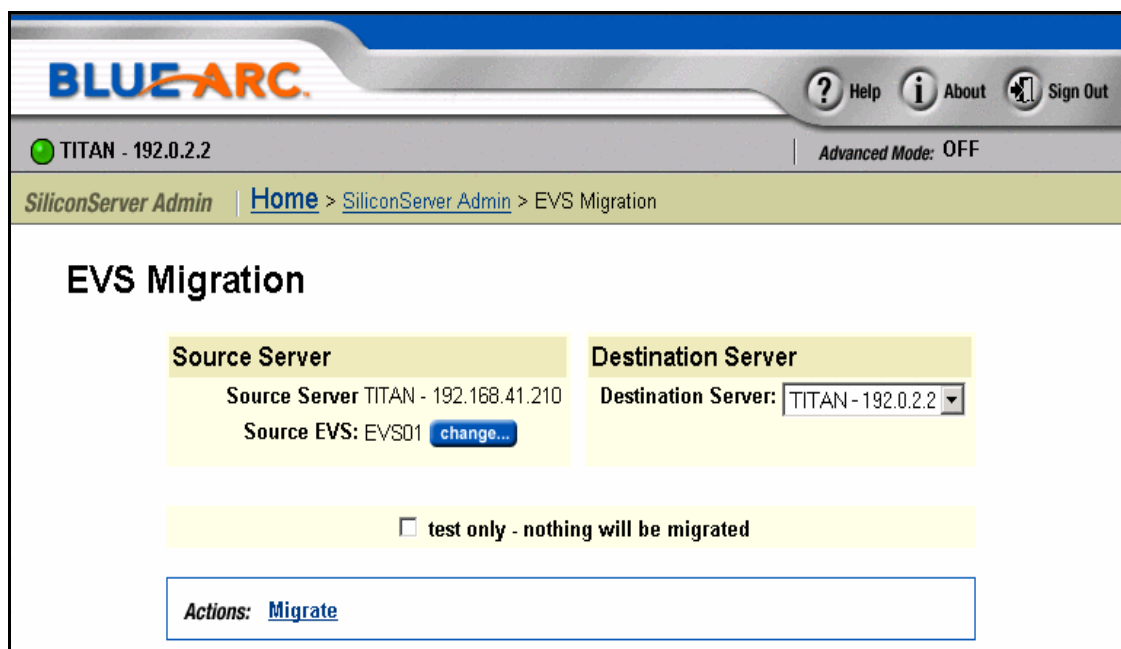
To migrate an EVS within a Server Farm

1. From the **SiliconServer Admin** page, click **EVS Migrate**.



Note: This screen will only appear if the current managed server is an HA cluster. Otherwise, clicking **EVS Migrate** will immediately launch the **EVS Migration** page shown in step 2.

- Click the second option, **Migrating an EVS from one system to a different unconnected system**. The EVS Migration page appears:



BLUE ARC

Help About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

SiliconServer Admin | Home > SiliconServer Admin > EVS Migration

EVS Migration

Source Server

Source Server TITAN - 192.168.41.210

Source EVS: EVS01 [change...](#)

Destination Server

Destination Server: TITAN - 192.0.2.2

☐ test only - nothing will be migrated

Actions: [Migrate](#)

- Select the desired EVS on the source server or select a different source server by clicking **Change....**
- Using the drop-down menu in the **Destination Server** field, select the server to which the EVS should be migrated.
- To test the migration before committing the change, click **Test Only**. This will ensure that the EVS migration is possible.
- Click **Migrate**.



Note: If the source server is offline or doesn't function, migration will be performed using an existing backup. The following warning will appear in such a case:

The specified source server is currently offline.
 If you migrate it in this state the EVS will be migrated from backed up configuration.
 The original configuration of this EVS cannot be removed from the source server, if this server comes back online there will be duplicate IP addresses and names causing conflicts on the network.
 The last backup file for the source server was taken: 02/22/2005 07:34

9 Status & Monitoring

Status & Monitoring Overview

Web Manager provides integrated and complete storage management of the Titan SiliconServer and its storage subsystem. Color-coded status information on the various devices installed on the BlueArc Storage System is provided through the management screens. In addition, Titan provides a comprehensive event logging and alerting mechanism, which can notify the system administrator as well as BlueArc Global Services as soon as a problem occurs. Alerts are issued through email, SNMP, Syslog, and Windows pop-ups.

BlueArc Storage System Status

Web Manager provides a flexible, customizable, and easy to use interface, providing the status of each managed device in the BlueArc Storage System. Ethernet connected auxiliary devices can be added as managed objects in the [System Monitor](#), and the status of these devices will be displayed. The System Monitor page provides a central management console for the management and status monitoring of all devices that comprise the BlueArc Storage System.

Using the Server Status Console

Summary status information pertaining to the Titan SiliconServer that is the *currently managed server* can be viewed from the Web Manager's server console, in the home page of the Titan SiliconServer.

The screenshot shows the 'Server Status Console' for 'Titan - 10.2.21.113'. The interface includes a status LED, volume capacity indicators, current data throughput, and alerts for critical, severe, and warning errors.

Server name and IP address of the *currently managed server*.
This drop-down box can be used to select another managed server.

Summary server status.
Clicking the LED loads the **System Monitor** page.

Volume Nearest Capacity:
2 % **View**

Disk percentage of used space on the File System (volume) that is nearest to full capacity.
The LED shows how close this File System is to its configured size limits:

- ☐ **Green** = File System within limits
- ☐ **Yellow** = File System reached / crossed warning threshold
- ☐ **Orange** = File System reached / crossed critical threshold

Clicking **View** loads the **Silicon File Systems**

Current Data Throughput:

	Rx	Tx	
Net:	0	0	Mbps
FC:	0	0	Mbps

Current data throughput from both the network and the Fibre Channel links.
These are instantaneous values (in MB/s) sampled every 60 seconds.

Alerts:

Critical	Severe	Warning
0	1	30

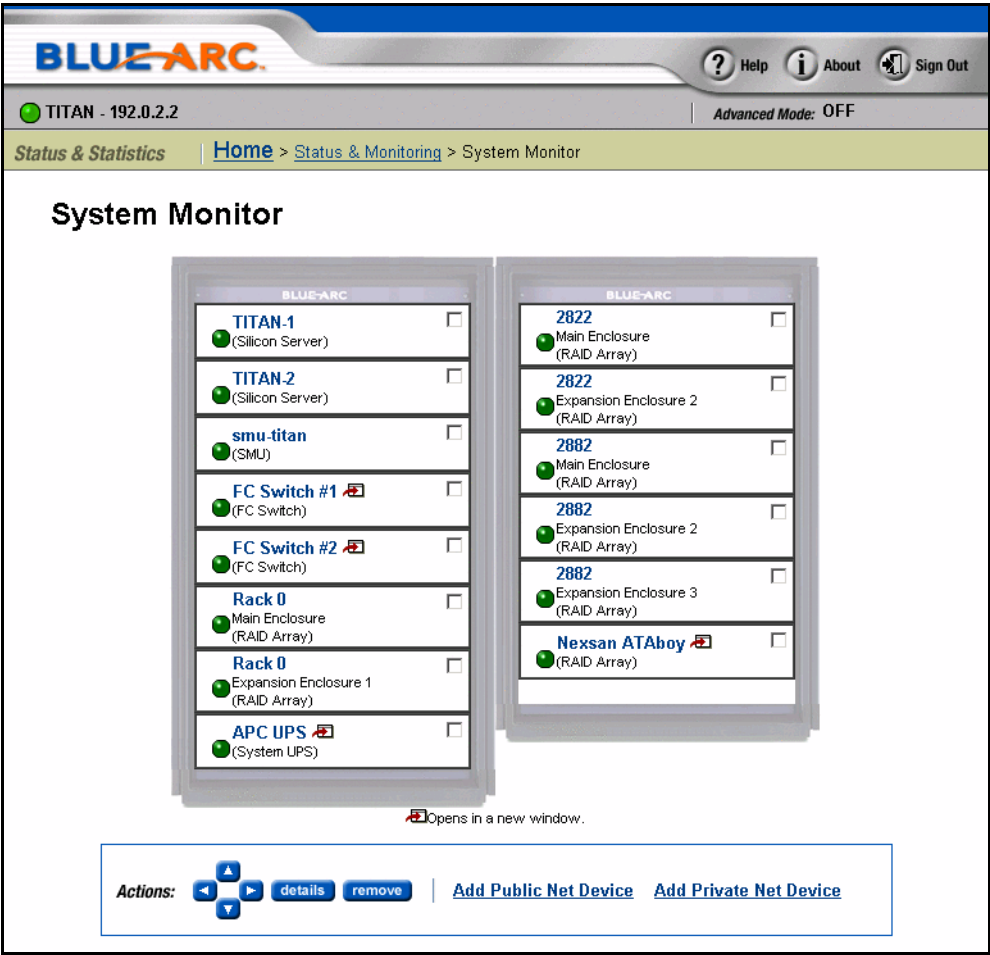
Critical errors, in the past 24 hours, in the event log.
Clicking the red LED loads the **Event Log** page, showing all critical errors.

Severe errors, in the past 24 hours, in the event log.
Clicking the orange LED loads the **Event Log** page, showing all severe errors.

Warnings, in the past 24 hours, in the event log.
Clicking the yellow LED loads the **Event Log** page, showing all warnings.

Checking the System Status

To display the components contained within the system and view the status of the Titan SiliconServer that is the *currently managed server*, from the **Status & Monitoring** page, click the **System Monitor** item. The following screen will be displayed:



This page represents graphically, the main components that make up the system (e.g. the server itself, storage enclosures, etc.), it shows their status, and provides links to more information (see table below).

Status information is cached by the SMU and refreshed every 60 seconds; so it may take this long to see changes in the System Monitor.

When displaying status of a device using a colored LED, the following conventions apply:

Color	Status	Means that the item is
	Information	Is operating normally and not displaying an alarm condition
	Warning	Needs attention, but does not necessarily represent an immediate threat to the operation of the system
	Severe Warning	Has failed in a way that poses a significant threat to the operation of the system
	Critical	Requires immediate attention. The failure that has occurred is critically affecting system operation

A system can contain the following basic components:

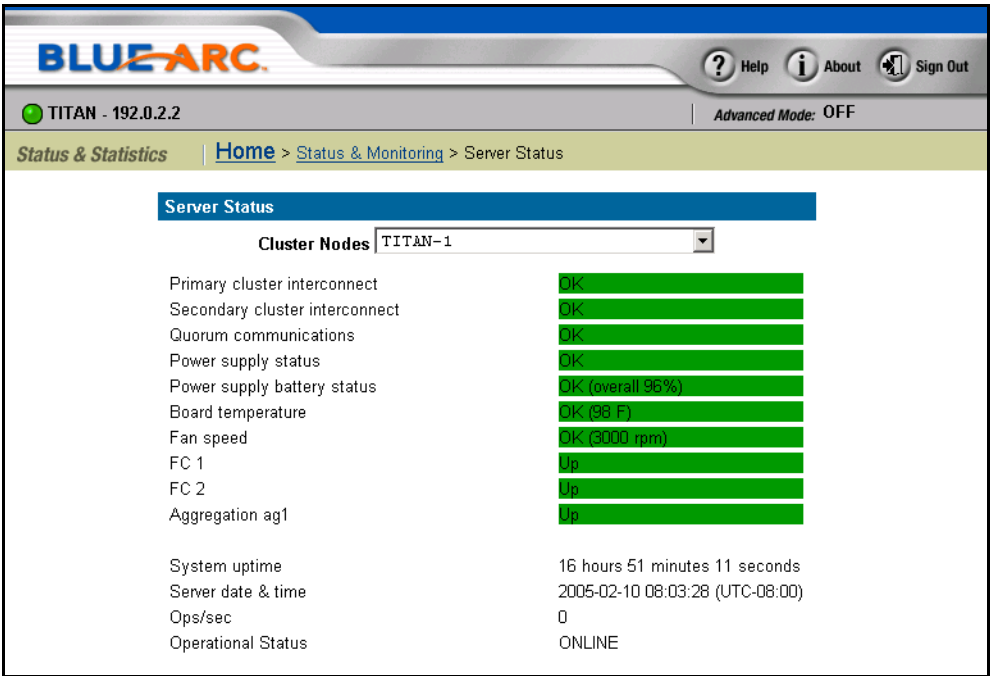
Component	Description	Action when clicking the <i><u>component</u></i>	Action when clicking the <i><u>details</u></i> button
Titan SiliconServer	This component provides multiple Gigabit Ethernet interfaces to the network and multiple Fibre Channel interfaces to the main enclosure. In high availability configurations, there are two servers.	Loads the Server Status page.	
Main Enclosure	An FC-14 , SA-14 , or FC-16 main enclosure contains disk slots, dual power supplies, and dual RAID controllers.	Loads the enclosure status page.	Loads the System Drives page.
Expansion Enclosure	An FC-14 , SA-14 , or FC-16 expansion enclosure does not contain any RAID controllers.	Loads the enclosure status page.	Loads the System Drives page.
SMU	The System Management Unit	Loads the SMU System Status page.	
System Power Unit	This component is also known as an <i>uninterruptible power supply</i> (UPS).	Loads the UPS Status page.	Loads the UPS Configuration page.

NDMP Backup Devices	Titan monitors its FC links every 60 seconds, and automatically detects the presence of backup devices and adds them to the system monitor. Since Titan could be connected into a FC network shared with other servers, it does not automatically make use of backup devices found on its FC links. Backup devices are added to the configuration through the SAN Management (for backup devices) page.	Loads the NDMP Devices page.	Loads the Backup SAN Management page.
Other Components	Any component can be added to the system monitor. If the device supports a web-based management interface, the management interface can be launched directly from the server management interface.	Loads the embedded management utility for the device. For example, for an AT-14 or AT-42 storage enclosure, it loads the Home page for the device.	Loads either the Add Public Net Device or the Add Private Net Device page. Settings for the component can be changed from this page.

To change the position of any of the items on this screen, select the item (place a tick in the checkbox) and use the **arrows** in the **Action** box.

Checking the Status of a Server Unit

From the **Status & Monitoring** page, click **Server Status**.



The table below describes the items on this screen:

Item	Description
Primary cluster interconnect	The status of the first cluster interconnect link.
Secondary cluster interconnect	The status of the second cluster interconnect link.
Quorum communications	The status of the link connecting the Cluster Nodes to the Quorum Device.
Power supply status	The status of the power to the server.
Power supply battery status	The status of the power supply's battery.
Board temperature	The status and temperature of the internal server boards. If there is a problem, check the fan speed and server environment temperature.
Fan speed	The status and speed of the fan.

FC 1, FC 2	The status of the Fibre Channel links. The number of links that appear is based on the version of SiliconServer blades installed.
Aggregation ag1	The status of the Gigabit Ethernet interfaces (or port aggregations).
System uptime	The time that has elapsed since the server was last switched on or reset.
Server date and time	The date and time configured on the server. To change these, click the Set date and time hyperlink.
Ops/sec	The average number of operations per second completed.
Operational status	Displays ONLINE when the server has fully booted.



Note: In a cluster, the Server Status page has the server status of the first Cluster Node. To view your second Cluster Node, select the second Cluster Node from the drop-down list.

Checking the Status of a Power Unit

In the **SiliconServer Admin** page, click **UPS Status**. The following dialog box will appear:

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

SiliconServer Admin | [Home](#) > [SiliconServer Admin](#) > UPS Status

System Power Unit

IP	Status	Charge	Runtime Remaining
192.0.2.23	On Line	100.0%	22 minutes

This screen displays the following:

This field	Shows
IP	The IP address of the System Power Unit.

Status	Indicates whether or not the unit is currently supplying battery power to the system, and whether or not the batteries are low or need replacing.
Charge	The percentage of battery capacity that is currently available.
Runtime Remaining	The number of minutes for which the System Power Unit is capable of providing battery power to the system.

Checking the Status of a Storage Unit

Titan supports the following RAID storage subsystems:

- [FC-14](#) storage used for Tier 1 and Tier 2 storage.
- [FC-16](#) storage used for Tier 1 and Tier 2 storage.
- [SA-14](#) storage used for Tier 3 storage.
- [AT-14](#) storage used for Tier 3 and Tier 4 storage.
- [AT-42](#) storage used for Tier 4 storage.

Checking the Status of a FC-14 or SA-14 Storage Unit

The storage subsystem management provides management of:

- The RAID controllers (if enclosure is a SCE)
- The LRC modules (if enclosure is a SEE)
- Batteries
- Power Supplies
- Temperature Sensors
- Fans
- The Disk drives

To Check the Status of a FC-14 or SA-14 storage enclosure

1. From the **Home** page, click **Storage Management**. Then, click **RAID Racks**.
2. Check the box next to the name of the Storage Enclosure to view the status.

3. Click **details**.

BLUEARC

?

Help

i

About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Storage Management | [Home](#) > [Storage Management](#) > [RAID Racks](#) > RAID Rack Details

RAID Rack Details

Identification

Name:

2822

Rack WWN:

60:0a:0b:80:00:12:df:a4:00:00:00:00:41:fe:89:b7

Configuration

Media Scan Period:

0

days

Cache Block Size:

☐ 4 KB

☒ 16 KB

Controllers

Controller A (192.168.38.35):

Status:

Online

Mode:

Active

Firmware:

05.42.10.00

Controller B (192.168.38.36):

Status:

Online

Mode:

Active

Firmware:

05.42.10.00

Batteries

Battery 0

Status:

OK

Location:

Controller Slot A

Age:

259 Day(s)

Life Remaining:

460 Day(s)

Battery 1

Status:

OK

Location:

Controller Slot B

Age:

259 Day(s)

Life Remaining:

460 Day(s)

Power Supplies

PSU 0:

OK

PSU 1:

OK

PSU 2:

OK

PSU 3:

OK

Temperature Sensors

Temperature Sensor 0:

OK

Temperature Sensor 1:

OK

Temperature Sensor 2:

OK

Fans

Fan 0:

OK

Fan 1:

OK

Fan 2:

OK

Fan 3:

OK

Physical Disks

Overall Physical Disk Status:

OK

Actions:

apply

Change Password

Shortcuts:

[Physical Disks](#)

[Active Tasks](#)

[Event Log](#)

[System Drives](#)

Item /Field	Description
Identification	Rack Information: • Name: Name of the FC-14 RAID Rack. Enter a new RAID Rack name which is used to identify the FC-14 RAID Rack. • WWN: Worldwide name for the FC-14 RAID Rack. • Media Scan Period: The number of days over which a complete scan of the System Drives will occur. • Cache Block Size: 4 KB or 16 KB. By default, the cache block size is 16 KB. Setting the cache block size to 4 KB may result in reduced performance with file systems configured with 32 KB block size. Click the OK button to apply any changes to the RAID Rack Identification.
Controllers	The information for each RAID Controller: • Status: The Status of the RAID Controller • Mode: The Mode of the RAID Controller • Firmware: The firmware of the RAID Controller
Batteries	The information for each Battery within the RAID Rack: • Status: Green – OK, Amber – Warning, Red – Severe. • Location: The location of the batteries within the RAID Rack. • Age: The number of days which the batteries have been in the RAID Rack. • Life Remaining: The number of days remaining until the batteries should be replaced.
Power Supplies	The status of the Power Supply Units (PSU) within the RAID Rack.
Temperature Sensors	The temperature (Temperature Sensor) within the RAID Rack.
Fans	The Status of the Fans within the RAID Rack.
Physical Disks	The summary of the Physical Disks within the RAID Rack.

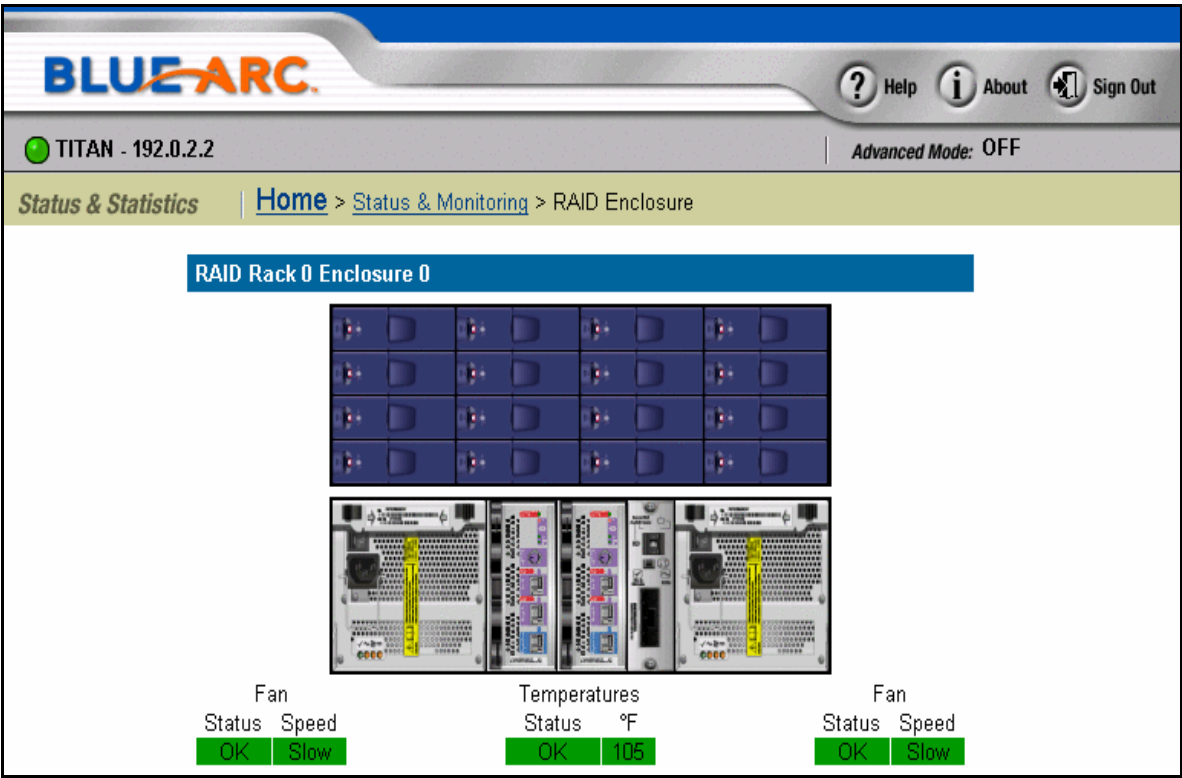
Checking the Status of an FC-16 Storage Unit

The storage subsystem management provides management of:

- The Storage enclosure
- The Power supplies
- The RAID controllers (if enclosure is a SCE)
- The LRC modules (if enclosure is a SEE)
- The Disk drives

To Check the Status of a FC-16 storage enclosure

From the **Home** page, click **Status & Monitoring**. Then, click **System Monitor**. On the **System Monitor** page, click the FC-16 enclosure to view the status.



To display the concise information on a component, hold the mouse pointer over it for a few seconds.

To view detailed information on a RAID controller or physical disk, click the physical disk.

The upper half of the dialog box shows the *physical disks* associated with the RAID racks. The color of a disk indicates its status.

BlueArc Storage System Status

Status Color	Description
Gray	The disk is not present in the enclosure or it has not been configured.
Blue	The disk is present and, if there is no overlay, functioning normally and part of a System Drive. The Web Manager may qualify this status with the following overlays: - The words Hot Spare indicate that a disk is not part of a System Drive but is available, to rebuild it, in the event of disk failure. - An amber overlay indicates that the System Drive is currently rebuilding. - A red overlay indicates that the System Drive has failed.

Checking the Status of an AT-14 or AT-42 Storage Unit

From the **System Monitor** page, click on the AT-14 or AT-42 enclosure to be configured. Click on the **Home** page link from the page on the left hand side.

BLUE ARC ALL OK

Friendly name - 'AT14-40000050'
11:25:10 Saturday 24-Feb-2001

> > > MAIN MENU
HOME
RAID INFORMATION
SYSTEM INFORMATION
CONFIGURE RAID
CONFIGURE VOLUMES
CONTROLLER ADMIN.
CONFIGURE NETWORK
QUICK START
LOG OFF

PSU Blower 1 Controller 0 Controller 1 PSU Blower 0

PSU 1 Temperature 37°C PSU 0

Disk1	Disk2	Disk3	Disk4	Disk5	Disk6	Disk7	Disk8	Disk9	Disk10	Disk11	Disk12	Disk13	Disk14
Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Array #1 (scan)	Pool Spare	Array #1 (scan)

The storage subsystem management provides management of:

- Power Supplies

- RAID Controllers
- Temperature
- Physical Disks

Checking the Status of the SMU

To view the current status of the SMU, from the **SMU Administration** page, click **SMU Status**.

BLUEARC

?

Help

i

About

Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

SMU Administration | [Home](#) > [SMU Administration](#) > [SMU Status](#)

SMU Status

Service	Status	Action
SMU Titan Proxy	OK	restart
Quorum Device	OK	restart

Top

7:22am up 1 day, 18:37, 1 user, load average: 0.00, 0.05, 0.02
198 processes: 197 sleeping, 1 running, 0 zombie, 0 stopped
CPU states: 3.3% user, 0.9% system, 0.2% nice, 11.5% idle
Mem: 1028672K av, 954820K used, 74052K free, 9104K shrd, 110776K buff
Swap: 2040244K av, 0K used, 2040244K free 327156K cached

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	%CPU	%MEM	TIME	COMMAND
19231	root	16	0	1188	1184	828	R	43.5	0.1	0:01	top
1	root	8	0	520	520	452	S	0.0	0.0	0:03	init
2	root	8	0	0	0	0	SW	0.0	0.0	0:00	keventd
3	root	19	19	0	0	0	SWN	0.0	0.0	0:00	ksoftirqd CPU0

SMU Disk Usage (df)

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda5	27G	3.6G	21G	15%	/
/dev/sda2	4.8G	3.3G	1.3G	71%	/BlueArcData
/dev/sda1	45M	12M	31M	27%	/boot
none	502M	0	502M	0%	/dev/shm

The **SMU Status** page displays the **services** available, the current **status** of each service and the option to **restart** each service if necessary:

Services	Description
SMU Titan Proxy	Used to allow communication from the SMU to Titan SiliconServers.
Quorum Device	Used by a Cluster which has become <i>partitioned</i> by a network failure, to determine which partition is allowed to talk to the storage.

In the **Status** column, the desired state of these services is OK.

If any of these services are not running correctly, an error message will be displayed. To solve this error message, click **restart**.

Top

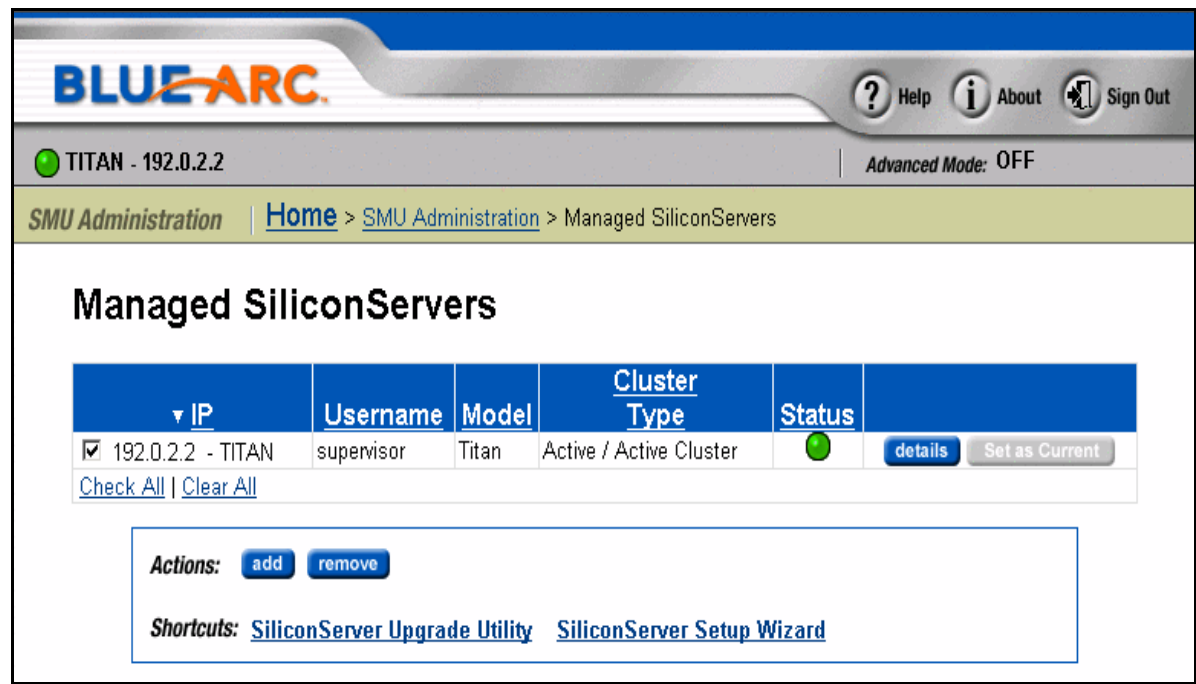
The information contained in the Top box represents the status of the SMU's Operating System. This is the actual output gathered from the Unix 'top' command and indicates the current running status of the SMU's internal processes.

SMU Disk Usage (df)

The information contained in the SMU Disk Usage (df) box represents output of the Unix command 'df'. This provides details of the space used in each of the partitions of the SMU's Hard Disk.

Monitoring Multiple Servers

Titan SiliconServers including other SiliconServers can be managed from the SMU. To display all of the currently managed Titan SiliconServers, click **Managed SiliconServers** from the **SMU Administration** page.



The screen displays the following:

Item / Field	Description
IP Address	The IP address of the server. This should be the Administration Services IP address as used on the private management network e.g. 192.0.2.x
Username	The username used to access the Titan SiliconServer.
Model	The model type, e.g. Titan.
Cluster Type	The cluster type, e.g. Single Node, Active/Active Cluster.
Status	The current status of the SiliconServer: Green indicates that the server is operating normally (i.e. not showing an alert condition)
	Amber is displaying a warning (e.g. operating normally, however, action should be taken to maintain normal operation)
	Red indicates a critical condition (e.g. the server is no longer functioning).

Details	A link to a page displaying detailed information used to contact or to manage the server.
Set as Current	Select the server as the <i>currently managed server</i> .

In the **Actions** frame, managed servers can be added (**Add**) or removed (**Remove**) from the displayed list.

To remove one or more servers, check the appropriate box or use **check all** to remove all servers. Then, click **Remove**.

Titan SiliconServer Statistics

Titan provides extensive statistics that can be used to monitor server operation. This includes:

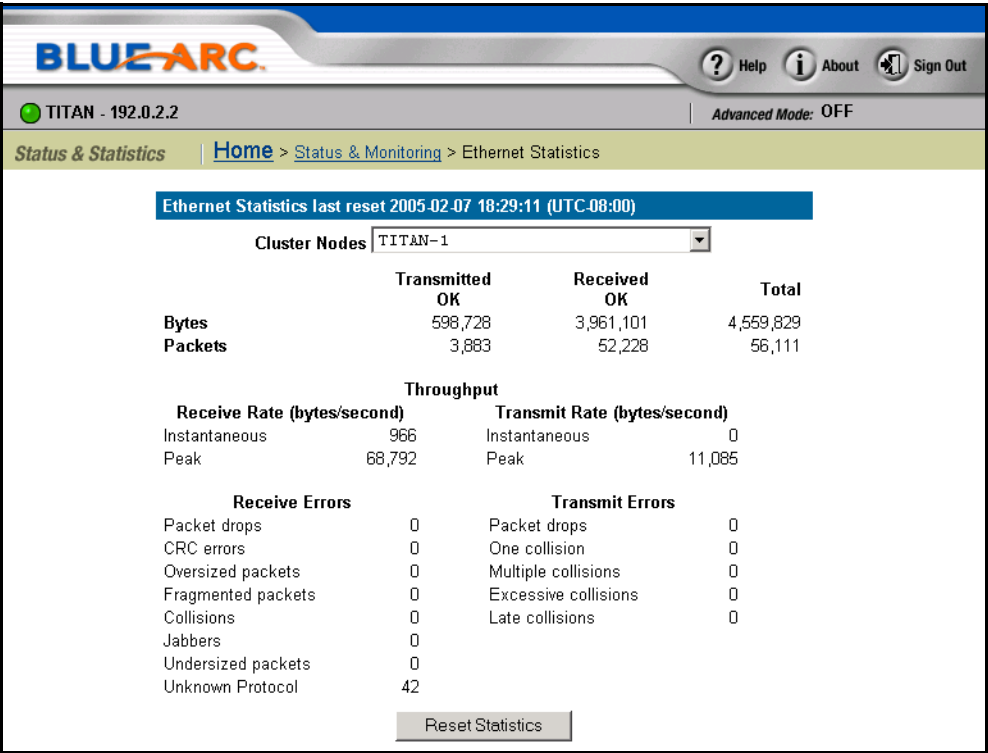
- Networking (Ethernet and TCP/IP)
- Fibre Channel
- File access protocols (CIFS, NFS, and FTP)
- Block access protocols (iSCSI)
- Management access (Telnet, SSC, and SNMP)
- Virus scanning

Ethernet Statistics

The [Ethernet](#) statistics display the activity since the last Titan reboot or since the Ethernet statistics were last reset. Both per-port and overall statistics are available. The statistics are updated every ten seconds. In addition, a histogram which shows the number of bytes/second received and transmitted over the last few minutes is also available.

To View Ethernet Statistics

From the **Status & Monitoring** page, click **Ethernet Statistics**.



Item/Field	Description
Cluster Nodes	If configured as a cluster, select the Cluster Node on which to view the Ethernet statistics.
Transmitted	The total numbers of bytes and packets successfully transmitted.
Received	The total numbers of bytes and packets successfully received.
Total	The total number of bytes and packets successfully transmitted and received
Throughput	The receive and transmit rates for both current (instantaneous) and peak throughput.
Receive Errors	The total number of errors received per source.
Transmit Errors	The total number of errors transmitted per source.

The **Reset Statistics** button will reset all the values to zero.

To view Per Port Ethernet Statistics

From the **Status & Monitoring** page, click **Ethernet Statistics (per port)**. This will generate statistics for each defined port.

The screenshot displays the BLUE ARC web interface for monitoring a Titan SiliconServer. The page title is "Ethernet Statistics" and it shows data for cluster node "TITAN-1". The interface includes a navigation bar with "Home", "Status & Monitoring", and "Per Port Ethernet Statistics". The main content area is divided into several sections: "Cluster Nodes" (TITAN-1), "ag1" (Last Reset Time: 2005-02-07 18:29:12 UTC-08:00), "Link Status" (Up), "Bytes" (Transmitted OK: 575,466; Received OK: 3,845,455; Total: 4,420,921), "Packets" (Transmitted OK: 3,721; Received OK: 50,714; Total: 54,435), "Receive Throughput Rate (bytes/second)" (Instantaneous: 5,264; Peak: 68,792), "Transmit Throughput Rate (bytes/second)" (Instantaneous: 3,858; Peak: 11,085), "Receive Errors" (Packet drops, CRC errors, Oversized packets, Fragmented packets, Collisions, Jabbers, Undersized packets, Unknown Protocol: all 0), "Transmit Errors" (Packet drops, One collision, Multiple collisions, Excessive collisions, Late collisions: all 0), "MAC Addresses" (00-30-17-00-66-c4), and "Reset statistics for port" (Reset button). A "Reset All Ports" button is also present at the bottom. The page footer includes "Physical Ports Ethernet Statistics" and a link to "Physical Ports Ethernet Statistics".

Ethernet Statistics	
Cluster Nodes	TITAN-1
ag1	
Last Reset Time	2005-02-07 18:29:12 (UTC-08:00)
Link Status	Up
Bytes	
Transmitted OK	575,466
Received OK	3,845,455
Total	4,420,921
Packets	
Transmitted OK	3,721
Received OK	50,714
Total	54,435
Receive Throughput Rate (bytes/second)	
Instantaneous	5,264
Peak	68,792
Transmit Throughput Rate (bytes/second)	
Instantaneous	3,858
Peak	11,085
Receive Errors	
Packet drops	0
CRC errors	0
Oversized packets	0
Fragmented packets	0
Collisions	0
Jabbers	0
Undersized packets	0
Unknown Protocol	0
Transmit Errors	
Packet drops	0
One collision	0
Multiple collisions	0
Excessive collisions	0
Late collisions	0
MAC Addresses	00-30-17-00-66-c4
Reset statistics for port	Reset
Reset All Ports	
Physical Ports Ethernet Statistics	

Item/Field	Description
Cluster Nodes	If configured as a cluster, select the Cluster Node which to view the Ethernet statistics.
Last Reset Time	The timestamp when the Ethernet statistics were taken.
Link Status	Status of the link: Up or Down .
Bytes	The total numbers of bytes and packets successfully transmitted.
Packets	The total numbers of bytes and packets successfully received.
Receive Throughput Rate (bytes/second)	The receive rates for current (instantaneous) and peak throughput.
Transmit Throughput Rate (bytes/second)	The transmit rates for current (instantaneous) and peak throughput.
Receive Errors	The total number of errors received: Packet drops, CRC Errors, Oversized packets, Fragmented packets, Collisions, Jabbers, Undersized packets, Unknown Protocol
Transmit Errors	The total number of errors while transmitting: Packet drops, one collision, multiple collisions, excessive collisions, and late collisions.
MAC Addresses	The MAC address for each link aggregation.

The **Reset** button will reset all the statistics of the selected port to **zero**.

The **Reset all ports** button will reset all the statistics on all ports to **zero**.

This page will refresh every 10 seconds.

To view a Histogram showing Ethernet activity

From the **Home** page, click **Status & Monitoring**. Then, click **Ethernet History**. Both per-port and overall histograms are available. The screen displays the number of bytes/second received and transmitted. If configured as a cluster, select the Cluster Node for which to view the Fibre Channel History.

TCP/IP Statistics

The TCP/IP statistics display the activity since the last Titan reboot or since the TCP/IP statistics were last reset. Both per-port and overall statistics are available. The statistics are updated every ten seconds.

To view TCP/IP statistics

From the **Status & Monitoring** page, click **TCP/IP Statistics**.

BLUE ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Status & Statistics | [Home](#) > [Status & Monitoring](#) > TCP/IP Statistics

TCP/IP Statistics

Cluster Nodes: TITAN-1

TCP Connections		TCP Segments		UDP Packets	
Currently Open	2	Transmitted	307	Transmitted	2,618
Maximum Open	2	Received	198	Received	4,632
Total Opened	9	Retransmitted	0	Unknown Port	319
Failed Connections	0	Invalid	0	Invalid	319

ICMP Packets		IP Packets	
Transmitted	0	Transmitted	0
Received	0	Received	57
		Unknown Protocol	0
		Invalid	57

Reset Statistics

Item/Field	Description
Cluster Node	If configured as a cluster, the Cluster Node to which the TCP/IP Statistics correspond is displayed.
TCP Connections	Currently Open: the number of currently open connections. Maximum Open: the peak number of open connections. Total Opened: the number of connections opened since the last reset. Failed Connections: the number of failed incoming and outgoing connections.

TCP Segments	Transmitted: the number of transmitted TCP segments. Received: the number of received TCP segments. Retransmitted: the number of retransmitted TCP segments. Invalid: the number of segments received with invalid TCP checksums.
UDP Packets	Transmitted: the number of transmitted UDP packets. Received: the number of received UDP packets. Unknown Port: the number received on a port with no UDP listener. Invalid: the number received with invalid UDP checksums.
ICMP Packets	Transmitted: the number of transmitted ICMP packets. Received: the number of received ICMP packets.
IP Packets	Transmitted: the number of transmitted IP packets. Received: the number of received IP packets. Unknown Protocol: the number of unknown protocol packets. Invalid: the number of invalid IP packets.

The **Reset Statistics** button will reset the values in this dialog box.

To view Per Port TCP/IP Statistics

From the **Status & Monitoring** page, click **TCP/IP Statistics (per port)**. This will generate the detailed statistics for each of the defined ports. The **Reset** button will reset all the statistics of the selected port to **zero**. This screen will refresh every 10 seconds.

? Help
i About
Sign Out

TITAN - 192.0.2.2
Advanced Mode: OFF

Status & Statistics
Home > Status & Monitoring > Per Port TCP/IP Statistics

TCP/IP Statistics

Cluster Nodes
TITAN-1

	ag1	ag2
Last Reset Time	2005-02-07 18:29:12 (UTC-08:00)	2005-02-07 19:13:37 (UTC-08:00)
TCP Segments		
Transmitted	314	0
Received	290	0
Retransmitted	0	0
Invalid	0	0
UDP Packets		
Transmitted	2,706	0
Received	4,723	0
Unknown Port	337	0
Invalid	337	0
ICMP Packets		
Transmitted	0	0
Received	0	0
IP Packets		
Transmitted	0	0
Received	57	0
Unknown Protocol	0	0
Invalid	57	0

Reset statistics for port
Reset
Reset

Reset All Ports

Physical Ports TCP/IP Statistics

Item /Field	Description
Cluster Node	If configured as a cluster, select the Cluster Node on which to display the TCP/IP Statistics.
Last Reset Time	The timestamp when the TCP/IP Statistics was taken.
TCP Segments	Transmitted: the number of transmitted TCP segments. Received: the number of received TCP segments. Retransmitted: the number of retransmitted TCP segments. Invalid: the number of segments received with invalid TCP checksums.

UDP Packets	Transmitted: the number of transmitted UDP packets. Received: the number of received UDP packets. Unknown Port: the number received on a port with no UDP listener. Invalid: the number received with invalid UDP checksums.
ICMP Packets	Transmitted: the number of transmitted ICMP packets. Received: the number of received ICMP packets.
IP Packets	Transmitted: the number of transmitted IP packets. Received: the number of received IP packets. Unknown Protocol: the number of unknown protocol packets. Invalid: the number of invalid IP packets: • The header checksum is invalid. • The length field is too long for the packet. • The source address is invalid. • The destination address is invalid (this is the most common error condition).

The **Reset** button will reset all the statistics of the selected port to **zero**.

The **Reset all ports** button will reset all the statistics on all ports to **zero**.

To view TCP/IP Detailed Statistics

From the **Status & Monitoring** page, click **TCP/IP Detailed Statistics**.



?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Status & Statistics

Home > Status & Monitoring > Detailed TCP/IP Statistics

Detailed TCP/IP Statistics

Cluster Nodes TITAN-1

IP Errors

Invalid Header Field 0

Oversized Segment 0

Invalid Source Address 61

Invalid Option 0

TCP Errors

Invalid Checksum 0

UDP Errors

Short Packet 0

Invalid Checksum 0

This field	Shows the number of

Cluster Nodes	If configured as a cluster, select the Cluster Node on which to display detailed TCP/IP Statistics.
IP Errors	
Invalid Header Field	IP errors from an invalid header field.
Oversized Segment	Fragmented TCP packets greater than the MTU size when re-assembled. The transmitting source made an error or the packet was corrupted in transit.
Invalid Source Address	IP packets with an invalid source address. This can be caused by DHCP broadcast requests using the source address 0.
Invalid Option	IP packets that were not decoded because the IP option length was invalid. The transmitting source made an error or the packet was corrupted in transit.
TCP Errors	
Invalid Checksum	Invalid TCP packet checksums. The transmitting source made an error or the packet was corrupted in transit.
UDP Errors	
Short Packet	UDP packets that were too short for the UDP header or length. The transmitting source made an error or the packet was corrupted in transit.
Invalid Checksum	Invalid UDP packet checksums. The transmitting source made an error or the packet was corrupted in transit.

Fibre Channel Statistics

The Fibre Channel (FC) statistics display the activity since the last Titan reboot or since the FC statistics were last reset. Both per-port and overall statistics are available. The statistics are updated every ten seconds. In addition, a histogram which shows the number of bytes/second received and transmitted over the last few minutes is also available.

To view a histogram showing FC activity

From the **Home** page, click **Status & Monitoring**. Then, click **Fibre Channel history**. The screen displays the number of bytes/second received and transmitted. If configured as a cluster, select the Cluster Node for which to view the Fibre Channel History.

To view the Fibre Channel statistics

From the **Home** page, click **Status & Monitoring**. Then, click **Fibre Channel Statistics**.

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Status & Statistics

Home > Status & Monitoring > Fibre Channel Statistics

Fibre Channel Statistics

Cluster NodesTITAN-1

Throughput

Receive Rate (bytes/second)

Transmit Rate (bytes/second)

Instantaneous0

Instantaneous19,568

Peak98,816

Peak17,325,528

Total471,040

Total78,393,648

I/O Requests

Disk Reads

Disk Writes

Total Requests206

Total Requests22,116

Total Responses206

Total Responses22,115

Total Requests & Responses

Total Errors

Requests61,207

Loss of Signal0

Responses61,206

Bad Receive Character1,020

Cache

Loss of Sync5

Hits39,217

Link Fail6

Misses205

Receive EOFa0

I/O Status Counters

Discarded Frames0

Failed0

Bad CRCs0

Resubmitted0

Protocol Errors0

Congestion

Instantaneous0

Peak over 24 hours0

Ave. over 24 hours0

Reset Statistics

Item/Field	Description
Cluster Nodes	If configured as a cluster, select the Cluster Node on which to view the Fibre Channel Statistics.
Throughput	The number of data bytes received and transmitted per second on the FC: Instantaneous and Peak.
I/O Requests	The number of read and write requests that the attached storage devices have received and sent: Total Requests and Total Responses.
Total Requests and Responses	The total number of requests received and responses transmitted.

415

Titan SiliconServer

Cache	The number of hits (requests that the cache has served) and misses (requests not served by the cache and passed to the storage subsystem).
I/O Status Counters	The numbers of failed and resubmitted input and output requests.
Total Errors	The number of errors logged at the Fibre Channel interface.

The **Reset Statistics** button will reset all the values to **zero**.

To view Per Port Fibre Channel Statistics

From the **Status & Monitoring** page, click **Fibre Channel Statistics (per port)**.

BLUE ARC TITAN - 192.0.2.2 Advanced Mode: OFF

[Status & Statistics](#) | [Home](#) > [Status & Monitoring](#) > Per Port Fibre Channel Statistics

FC stats per port

Cluster Nodes: TITAN-1

	FC 1	FC 2
Receive Throughput Rate (bytes/second)		
Instantaneous	0	0
Peak	98,816	35,328
Total	314,368	156,672
Transmit Throughput Rate (bytes/second)		
Instantaneous	0	0
Peak	17,325,528	40,176
Total	49,944,704	31,755,936
Total Errors		
Loss of Signal	0	0
Loss of Sync	0	5
Receive EOFa	0	0
Bad CRCs	0	0
Bad Receive Character	510	510
Link Fail	6	0
Discarded Frames	0	0
Protocol Errors	0	0
Congestion		
Instantaneous	0	0
Peak over 24 hours	0	0
Ave. over 24 hours	0	0

[Reset Statistics](#)

This page will display the statistics for each of the defined ports.

Item/Field	Description
Cluster Nodes	If configured as a cluster, select the Cluster Node to view the Fibre Channel Statistics.
Receive and Transmit Throughput Rate (bytes/second)	The number of data bytes received and transmitted per second on the FC: Instantaneous and Peak.
Total Errors	The number of errors logged at the Fibre Channel interface.

The **Reset** button will reset all the statistics, of the selected port, to **zero**. This page will refresh every 10 seconds.

File and Block Protocol Statistics

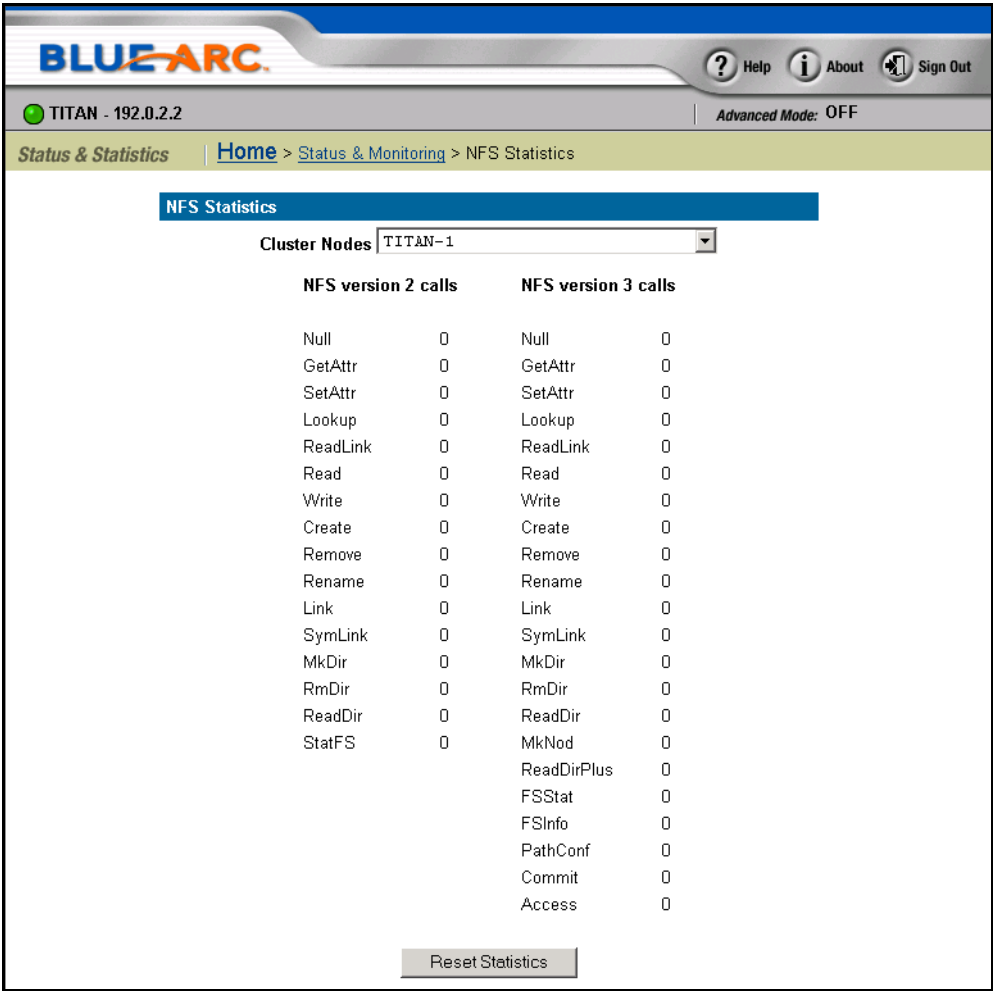
Titan provides statistics to monitor data access via the following network protocols:

- [Network File System](#) (NFS)
- [Common Internet File System](#) (CIFS)
- [File Transfer Protocol](#) (FTP)
- [Internet Small Computer System Interface](#) (iSCSI)

NFS Statistics

The **NFS** statistics display the activity since the last Titan reboot or since the NFS statistics were last reset. The statistics are updated every ten seconds.

From the **Home** page, click **Status & Monitoring**. Then, click **NFS Statistics**.



The number of current clients and the number of NFS calls that clients have sent to the server are shown in the **NFS Statistics** page.

Request	Description
Null	Does nothing, except to make sure the connection is up.
GetAttr	Retrieves the attributes of a file or directory.
SetAttr	Sets the attributes of a file or directory.
Lookup	Looks up a file name in a directory.

ReadLink	Reads the data associated with a symbolic link.
Read	Reads data from a file.
Write	Writes data to a file.
Create	Creates a file or symbolic link.
Remove	Removes a file.
Rename	Renames a file or directory.
Link	Creates a hard link to an object.
SymLink	Creates a symbolic link.
MkDir	Creates a directory.
RmDir	Removes a directory.
ReadDir	Reads from a directory.
StatFS	Gets dynamic file system state information.
MkNod	Creates a special device node (device file or named pipe).
ReadDirPlus	Performs an extended read from a directory.
FSStat	Gets dynamic file system state information.
FSInfo	Gets static file system state information.
PathConf	Retrieves POSIX information for the file system.
Commit	Commits the cached data on the server to stable storage.
Access	Gets the file security accesses for a file.

The **Reset** button will reset all the values to zero.

CIFS Statistics

The **CIFS** statistics display the activity since the last Titan reboot or since the CIFS statistics were last reset. The statistics are updated every ten seconds.

From the **Home** page, click **Status & Monitoring**. Select **CIFS Statistics**.



In addition to showing the number of current clients, this statistics page displays the number of CIFS calls that clients have sent to the server.

The CIFS calls are listed in the table below:

Call	Description
Chkpth	Checks that the specified directory path exists.
Close	Closes a file.
Create	Creates a new file or opens an existing one.
Dskattr	Retrieves file system attributes.
Echo	Pings the server.
FindClose	Closes a CIFS FindFirst subfunction.

Flush	Instructs the server to flush cached information on a file.
Getatr	Retrieves the attributes of a file or directory.
Link	Creates a hard link to an object.
LockingX	Locks or unlocks a range of bytes in a file.
Lseek	Sets the file pointer to a given offset in the file.
Mkdir	Creates a new directory.
Mknew	Creates a new file.
NegProt	Negotiates the protocol with which the client and server will communicate.
NTcancel	Cancels an outstanding operation.
NTcreateX	Creates a new file or opens an existing one.
NTtrans	Multifunction command for operating subfunctions.
NTtranss	Multifunction command for operating subfunctions.
Open	Creates a new file or opens an existing one.
OpenX	Creates a new file or opens an existing one.
Read	Reads data from a file.
ReadBraw	Reads a block of data with no CIFS header.
ReadX	Reads data from a file.
Rename	Renames a file or directory.
Rmdir	Removes a directory.
Search	Lists the files in a directory.
SessSetupX	Logs the client in to a CIFS session.
Setatr	Sets the attributes of a file or directory.
TconX	Connects the client to a file system resource.
Tdis	Breaks a connection that a TconX call previously established.
Trans	Multifunction command for operating subfunctions.
Trans2	Multifunction command for operating subfunctions.
UlogoffX	Breaks a connection that a SessSetupX call previously established.

Unlink	Deletes a file.
Write	Writes data to a file.
WriteBraw	Write a block of data with no CIFS header.
WriteClose	Writes data to a file and then closes the file.
WriteX	Writes data to a file.

All values can be reset to zero by clicking **Reset**.

FTP Statistics

The [FTP](#) statistics are displayed since Titan was last started or when it was last reset. The Web Manager updates the FTP statistics every ten seconds.

BLUE-ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Status & Statistics | [Home](#) > [Status & Monitoring](#) > FTP Statistics

FTP Statistics last reset 2005-02-07 18:30:01 (UTC-08:00)

Cluster Nodes

Sessions		Commands	
Current Active Sessions	0	Commands Issued from Clients	0
Total Sessions	0	Total Replies Sent to Clients	0
Current Active Transfers	0	Total Bytes Received in Commands	0
		Total Bytes Sent in Replies	0
Files		Data Bytes	
Files Incoming for Active Sessions	0	Data Bytes Incoming for Active Sessions	0
Total Files Incoming	0	Total Data Bytes Incoming	0
Files Outgoing for Active Sessions	0	Data Bytes Outgoing for Active Sessions	0
Total Files Outgoing	0	Total Data Bytes Outgoing	0

Item / Field	Description
Sessions	
Current Active Sessions	FTP sessions that are currently active.

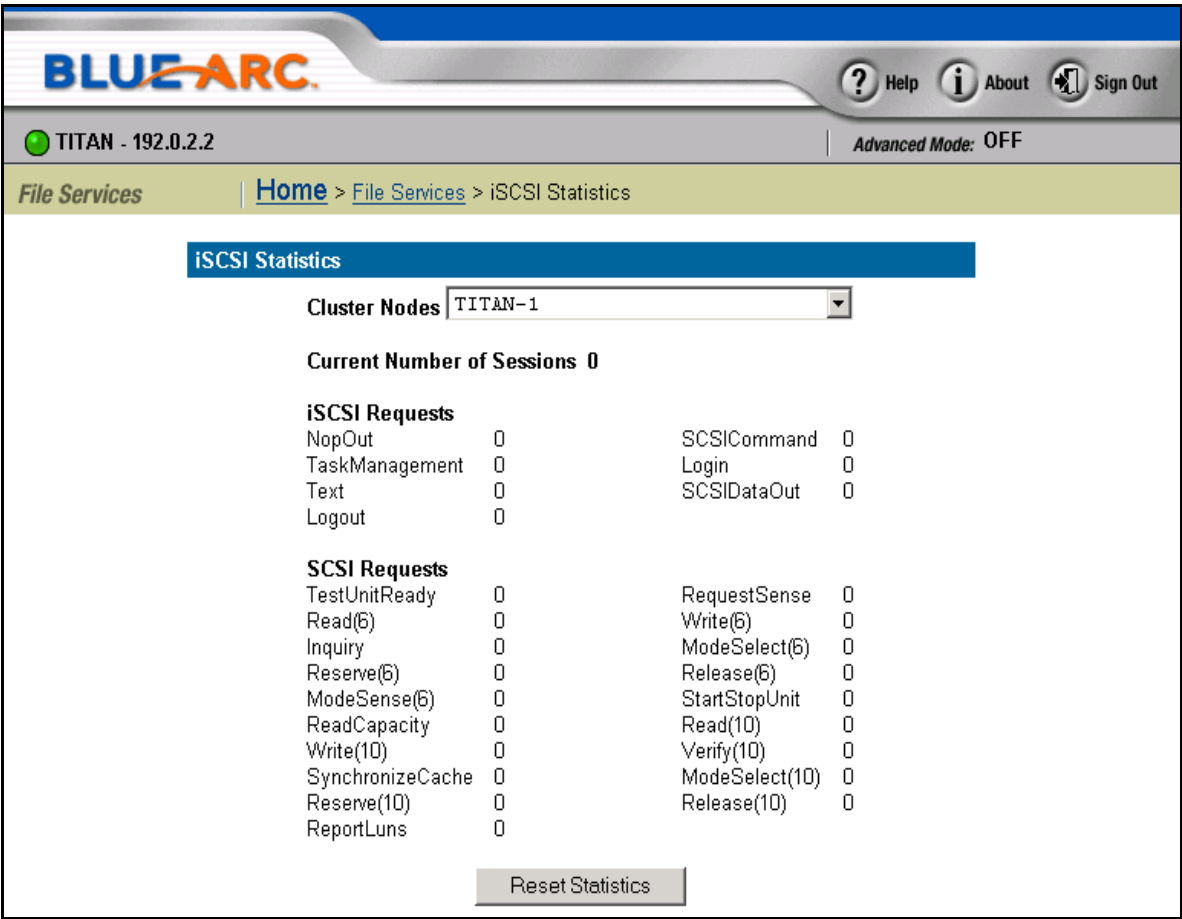
Total Sessions	FTP sessions that clients have conducted since you last started the server ore reset the statistics.
Current Active Transfers	FTP transfers that are currently active.
Commands	
Commands Issued from Clients	Commands that clients have sent to the FTP server.
Total Replies Sent to Clients	Replies that the FTP server has sent to clients.
Total Bytes Received in Commands	Bytes in commands that clients have sent to the FTP server.
Total Bytes Sent in Replies	Bytes in replies that the FTP server has sent to clients.
Files	
Files Incoming for Active Sessions	Files that clients have transferred to the FTP server in currently active sessions.
Total Files Incoming	Files that clients have transferred to the FTP server since you last started the server or reset the statistics.
File Outgoing for Active Sessions	Files that the FTP server has transferred to clients in currently active sessions.
Total Files Outgoing	Files that the FTP server has transferred to clients since you last started the server or reset the statistics.
Data Bytes	
Data Bytes Incoming for Active Sessions	Bytes of data that clients have transferred to the FTP server in currently active sessions.
Total Data Bytes Incoming	Bytes of data that clients have transferred to the server since you last started the server or reset the statistics.
Data Bytes Outgoing for Active Sessions	Bytes of data that the FTP server has transferred to clients in currently active sessions.
Total Data Bytes Outgoing	Bytes of data that the server has transferred to clients since you last started the server or reset the statistics.

The **Reset** button will reset all the values of the FTP Statistics to **zero**.

iSCSI Statistics

The **iSCSI Statistics** page will provide you with an overall view and summary of the iSCSI and SCSI requests on a Cluster Node.

From the **Home** page, click **Status & Monitoring**. Then, click **iSCSI Statistics**.



To view the iSCSI Statistics on specific Cluster Node, use the drop-down list to select it. The screen will automatically refresh with the current iSCSI and SCSI statistics.

To reset all the statistics to zero, click the **Reset Statistics** button.

Item / Field	Description
Current Number of Session	The number of iSCSI sessions currently hosted by Titan.
iSCSI Requests	
NopOut	No operation.

Task Management	Requests used for task management functions.
Text	Requests used to negotiate behavior.
Logout	Logout requests
SCSICommand	Carries a SCSI Command
Login	Login requests
SCSIDataOut	Requests containing SCSI data.
SCSI Requests	
TestUnitReady	Tests that the target is ready to receive commands.
Read(6)	Reads data.
ModeSelect(6)	Configure SCSI behavior.
Release(6)	Releases (unlocks) a Logical Unit reservation.
StartStopUnit	Warm reboots the target.
Read(10)	Reads data.
Verify(10)	Verifies data.
ModeSelect(10)	Configure SCSI behavior.
Release(10)	Releases (unlocks) a Logical Unit reservation.
RequestSense	Requests state information.
Inquiry	Requests device information.
Reserve(6)	Reserves (locks) a Logical Unit for exclusive access.
ModeSense(6)	Requests SCSI configuration information.
ReadCapacity	Reads the size of Logical Unit.
Write(10)	Write data.
SynchronizeCache	Flushes cached data to disk.
Reserve(10)	Reserves (locks) a Logical Unit for exclusive access.
ReportLuns	Retrieves a list of available Logical Units.

Data Access and Performance Statistics

Titan provides ways to monitor the impact network clients have on internal resources. In particular, Titan provides:

- [Server and file system load statistics](#)
- [FS NVRAM usage statistics](#)

Server and File System Load (Ops per second)

In addition to Ethernet and Fibre Channel throughput statistics, Titan's performance can also be measured by how many operations per second (ops/sec) it is performing. Through the Web UI, a graphic representation of the number of ops/sec it is performing can be viewed. Ops/sec can be viewed at two levels:

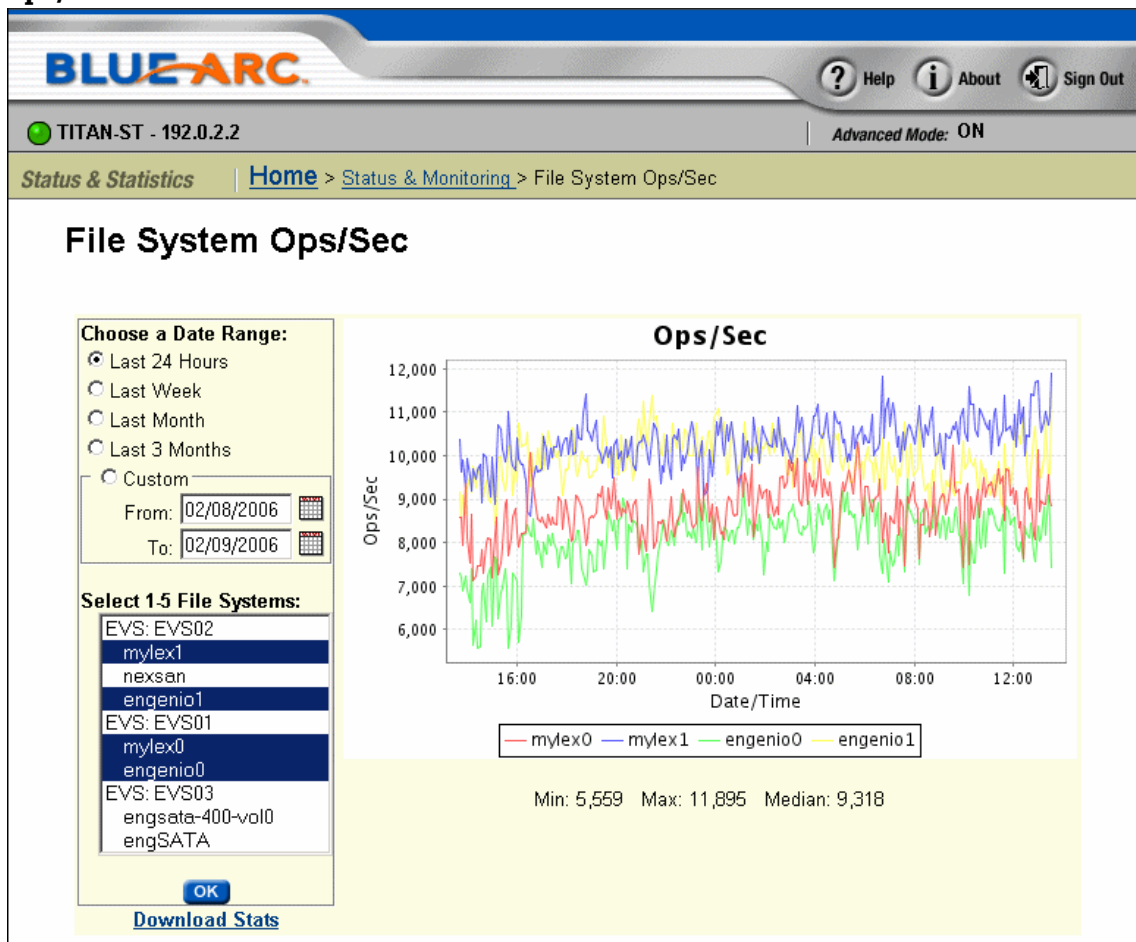
- The total number of operations performed by a specific Titan SiliconServer.
- The number of operations performed by individual file systems.

The total operations on a server will essentially be an aggregate of the individual ops performed by all Silicon File Systems hosted by that server.

Understanding the performance profile of servers and individual file systems is especially useful in environments where more than one SiliconServer is installed, whether as an A/A cluster or in a server farm. In such installations, EVS or file systems can be relocated to more equally distribute the load among the available servers.

To view ops/sec statistics

From the **Home** page, click **Status & Monitoring**. Then, click **Node Ops/Sec** or **File System Ops/Sec**.



If File System Ops/sec was selected, select between one and five file systems to view under **Select 1-5 File Systems**. Hold down the Ctrl key while clicking to select more than one file system.

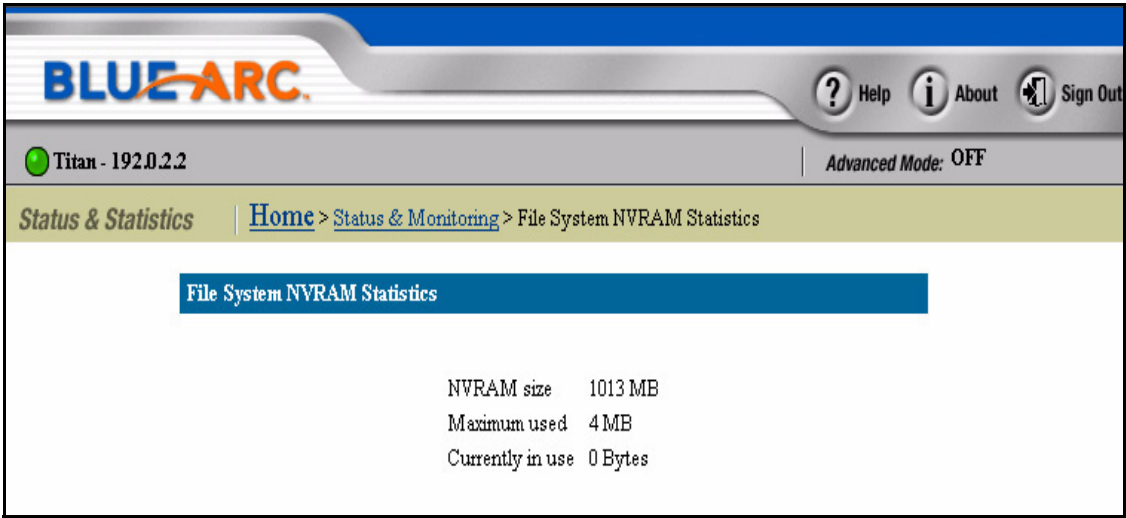
Statistics can be viewed based on a specified range. Customize the date range by selecting an option under **Choose a Date Range**.

The statistics can be downloaded into .csv format by clicking the **Download Stats** link.

FS NVRAM Statistics

The [FS NVRAM](#) Statistics page will provide you with an indication as to NVRAM activity.

From the **Home** page, click **Status & Monitoring**. Then, click **File System NVRAM Statistics**.



Item /Field	Description
NVRAM size	Size of NVRAM buffer, used to preserve data for disk-modifying operations until written to disk.
Maximum used	High water mark for NVRAM buffer usage (in bytes).
Currently in use	Current NVRAM buffer usage (in bytes).

Management Statistics

Titan provides the following management statistics:

- [Access Management Statistics](#) for Telnet, SSC, and [SNMP](#)
- [Virus Scanning Statistics](#)

Access Management Statistics

The Telnet and SSC management statistics are displayed since Titan was last started or when it was last reset. The Web Manager updates the management statistics every ten seconds.

From the **Home** page select **Status & Monitoring** then select one of the items in the **Management Access Statistics** section, i.e. Telnet, or SSC; a screen similar to the following will

be displayed:



This statistic	Shows
Sessions	
Current Active Sessions	The number of sessions that are currently in progress.
Max Sessions	The peak number of concurrent sessions.
Total Sessions	The total number of sessions.
Rejected Sessions	The number of failed attempts to establish a connection. A connection may fail because the client does not have the required permissions or because the maximum number of concurrent sessions is in progress.
Frames	
Frames Transmitted	The number of frames (packages of information transmitted as single units) that the system has sent to clients.
Frames Received	The number of frames that clients have sent to the system.
Data Bytes	

Bytes Transmitted	The number of data bytes that the system has sent to clients.
Bytes Received	The number of data bytes that clients have sent to the system.

SNMP Management Statistics

The [SNMP](#) management statistics are displayed since Titan was last started or when it was last reset. The Web Manager updates the management statistics every ten seconds.

From the **Status & Monitoring** page, click **SNMP Management Statistics**.



Item /Field	Shows the number of
Input	
Packets	SNMP packets the agent has received.
Bad Community Names	SNMP messages received using an unknown community name.

Too Bigs	Protocol Data Units (PDUs) received containing an error-status field value of tooBig
Bad Values	PDUs received containing an error-status field value of badValue.
General Errors	PDUs received containing an error-status field value of genErr.
Total Set Varbinds	MIB objects successfully altered because of valid SNMP Set-Request PDUs.
Get Nexts	Get-Next PDUs received and processed.
Get Responses	Get-Response PDUs received and processed.
ASN Parse Errors	Abstract Syntax Notation (ASN) errors found in SNMP messages received.
Bad Versions	Packets received for an unsupported SNMP version.
Bad Community Uses	SNMP messages received representing an operation not allowed by the SNMP community named in the message.
No Such Names	PDUs received containing an error-status field value of nosuchName.
Read Onlys	PDUs received containing an error-status field value of ReadOnly. This value is used to detect incorrect SNMP implementations.
Total Request Varbinds	MIB objects successfully retrieved because of valid SNMP Get-Request and Get-Next PDUs.
Get Requests	Get-Request PDUs received and processed.
Set Requests	Set-Request PDUs received and processed.
Traps	Trap PDUs received and processed.
Output	
Packets	SNMP packets the agent has sent.
No Such Names	Sent PDUs receiving an error-status field value of noSuchName.
General Errors	Sent PDUs receiving an error-status field value of genErr.
Get Nexts	Get-Next PDUs sent.
Get Responses	Get-Response PDUs sent.
Too Bigs	Sent PDUs receiving an error-status field value of tooBig.
Bad Values	Sent PDUs receiving an error-status field value of badValue.

Get Request	Get-Request PDUs sent.
Set Requests	Set-Request PDUs sent.
Traps	Trap PDUs sent.
Drops	
Silent Drops	PDUs delivered but silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests.
Proxy Drops	PDUs delivered but silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned.

Virus Scanning Statistics

The **Virus Statistics** page will provide you with an indication as to virus scanning activity. From the **Home** page, click **Data Protection**. Then, click **Virus Statistics**.

BLUE ARC ? Help i About Sign Out

TITAN - 192.0.2.2 Advanced Mode: OFF

Data Protection | [Home](#) > [Data Protection](#) > Virus statistics

Virus Statistics last reset 2005-01-26 07:01:33 (UTC-08:00)

EVS EVS01

Number of virus scans 0

Number of clean scans 0

Number of errored scans 0

Additional statistics:

Number of infections found 0

Action taken:

Number of infections repaired 0

Number of files deleted 0

Number of files quarantined 0

Reset Statistics

Item	Description
Number of virus scans	Number of times files are scanned for viruses.
Number of clean scans	Number of times files are scanned with no viruses detected.
Number of errored scans	Number of times a failure occurred while scanning a file.
Additional statistics: (not supported on every Virus Scan Engine)	
Number of infections found	Number of times files are scanned and detected infections are found.
Number of infections repaired	Number of times the Virus Scan Engine has been able to repair infections found.
Number of files deleted	Number of deleted files because they contain irreparable infections.
Number of files quarantined	Number of files quarantined because they contain irreparable infections.

Reset Statistics will reset all values to zero.

Event Logging and Notification

The Titan SiliconServer provides a comprehensive event logging and alert mechanism. In addition, auxiliary devices in the storage subsystem automatically direct any events and SNMP traps to Titan, or can be configured to do so.

All event messages generated by Titan (including those issued by its auxiliary devices) are logged into an event log, which can be downloaded and cleared by the system administrator. The event log provides a record of past events that have occurred on the server that can be used for trend/fault analysis.

Titan can be configured for automated notification on pre-defined severity categories, including daily summary and status notification. With automated notification enabled, the system will notify selected personnel when an event is generated according to the level of severity of the event. With BlueArc's 24x7 Global Services, the automated notifications allows BlueArc Global Services personnel to pro-actively monitor the health of the system and address any issues that may occur on the system.

Using the Event Log

Titan continuously monitors the temperatures, fans, power supply units, and disk drives in the cabinet. Each time an event occurs (e.g. a disk failure or a possible breach of security, the system records it in an event log). The event log can be viewed, filtered, and saved as a permanent record.

The log can contain a maximum of 10,000 events. Once the event log limit has been reached, each new event replaces the oldest event in the log.

To view and filter the event log

1. From the **Home** page, click **Status & Monitoring**. Then, click **Event Log**.

The screenshot shows the BlueArc Titan web interface. At the top, the BlueArc logo is on the left, and navigation links (Help, About, Sign Out) are on the right. Below the logo, the system status is shown as 'Titan - 192.0.2.2' and 'Advanced Mode: OFF'. The breadcrumb trail is 'Home > Status & Monitoring > Event Logs'. The main section is titled 'Event Log Management' and contains search criteria filters: 'Display Order' (Newest First), 'Event Category' (All), and 'Event log severity' (Information, Warning, Severe, Critical, all checked). There are buttons for 'Refresh Log', '<<', and '>>'. Below the filters is a table of event log entries with columns: ID, Severity, Date, Time, and Event. The table contains 13 entries, mostly 'INFORMATION' level events related to user logins, logouts, and system status reports. At the bottom, the current time is displayed as '2004-09-16 01:41:47 (UTC)' and there are buttons for 'Download Entire Log' and 'Clear Event Log'.

ID	Severity	Date	Time	Event
1310	INFORMATION	2004-09-16	01:41:46	User supervisor has logged in from https:192.0.2.1
1311	INFORMATION	2004-09-16	00:57:42	User supervisor has logged out from https:192.0.2.1
1310	INFORMATION	2004-09-16	00:42:15	User supervisor has logged in from https:192.0.2.1
1311	INFORMATION	2004-09-16	00:37:02	User supervisor has logged out from https:192.0.2.1
1310	INFORMATION	2004-09-16	00:04:55	User supervisor has logged in from https:192.0.2.1
1282	INFORMATION	2004-09-15	23:57:31	PSU battery 1 low voltage started charging
1311	INFORMATION	2004-09-15	23:33:12	User supervisor has logged out from https:192.0.2.1
4064	INFORMATION	2004-09-15	23:19:24	Fibre channel congestion report: [2] 0% (average over 24 hours) 0% (peak)
4064	INFORMATION	2004-09-15	23:19:23	Fibre channel congestion report: [1] 0% (average over 24 hours) 0% (peak)
1031	INFORMATION	2004-09-15	23:14:46	Established contact with monitored device goblin

In a cluster, select the Cluster Node for which to display the log. The default is the first Cluster Node. To view the other Cluster Node, select from the drop-down list (**Cluster Nodes**) the other Cluster Node.

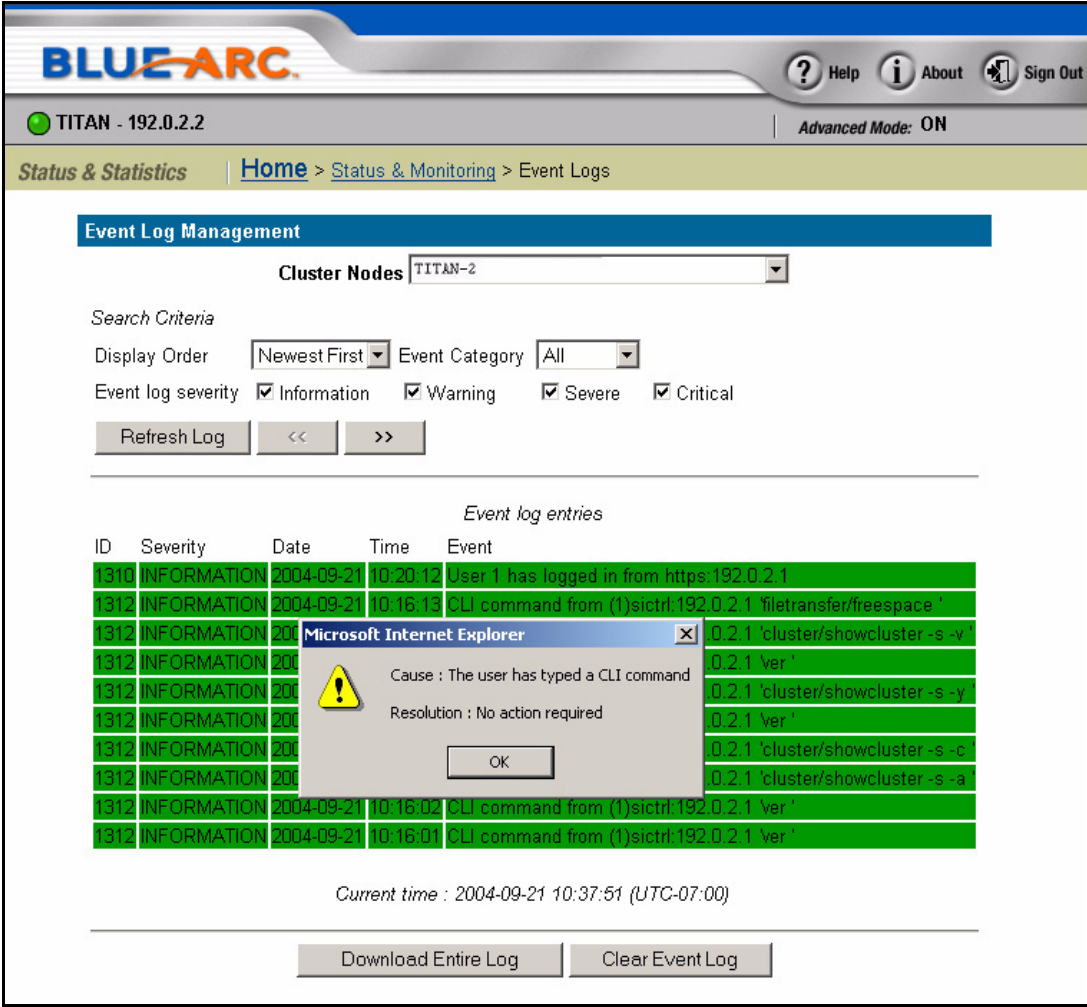
- 2. In the **Display Order** field, select display order to sort the events chronologically by **Newest First** or **Oldest First**.
- 3. Select the **Event Category: All, System, or Security**.
- 4. Check one or more of the boxes in **Event log severity: Information, Warning, Severe, and Critical**.

Severity	Status	Color
Information	Green	
Warning	Yellow	
Severe	Orange	
Critical	Red	

- 5. The **Refresh Log** button will regenerate the log according to the criteria selected.
- 6. The **Page Forward** and **Page Back** buttons allow the events to be viewed one page at a time.

Event Logging and Notification

- Click an event for more details. A dialog box will be displayed with the **cause** and **resolution**.



BLUE ARC

TITAN - 192.0.2.2 Advanced Mode: ON

Status & Statistics | [Home](#) > [Status & Monitoring](#) > Event Logs

Event Log Management

Cluster Nodes: TITAN-2

Search Criteria

Display Order: Newest First Event Category: All

Event log severity: ☒ Information ☒ Warning ☒ Severe ☒ Critical

Refresh Log << >>

Event log entries

ID	Severity	Date	Time	Event
1310	INFORMATION	2004-09-21	10:20:12	User 1 has logged in from https:192.0.2.1
1312	INFORMATION	2004-09-21	10:16:13	CLI command from (1)sictrl:192.0.2.1 'filetransfer/freespace '
1312	INFORMATION	2004-09-21	10:16:02	CLI command from (1)sictrl:192.0.2.1 'cluster/showcluster -s -v '
1312	INFORMATION	2004-09-21	10:16:02	CLI command from (1)sictrl:192.0.2.1 'cluster/showcluster -s -y '
1312	INFORMATION	2004-09-21	10:16:02	CLI command from (1)sictrl:192.0.2.1 'cluster/showcluster -s -c '
1312	INFORMATION	2004-09-21	10:16:01	CLI command from (1)sictrl:192.0.2.1 'cluster/showcluster -s -a '
1312	INFORMATION	2004-09-21	10:16:02	CLI command from (1)sictrl:192.0.2.1 'ver '
1312	INFORMATION	2004-09-21	10:16:01	CLI command from (1)sictrl:192.0.2.1 'ver '

Current time : 2004-09-21 10:37:51 (UTC-07:00)

Download Entire Log Clear Event Log

Microsoft Internet Explorer

Cause : The user has typed a CLI command

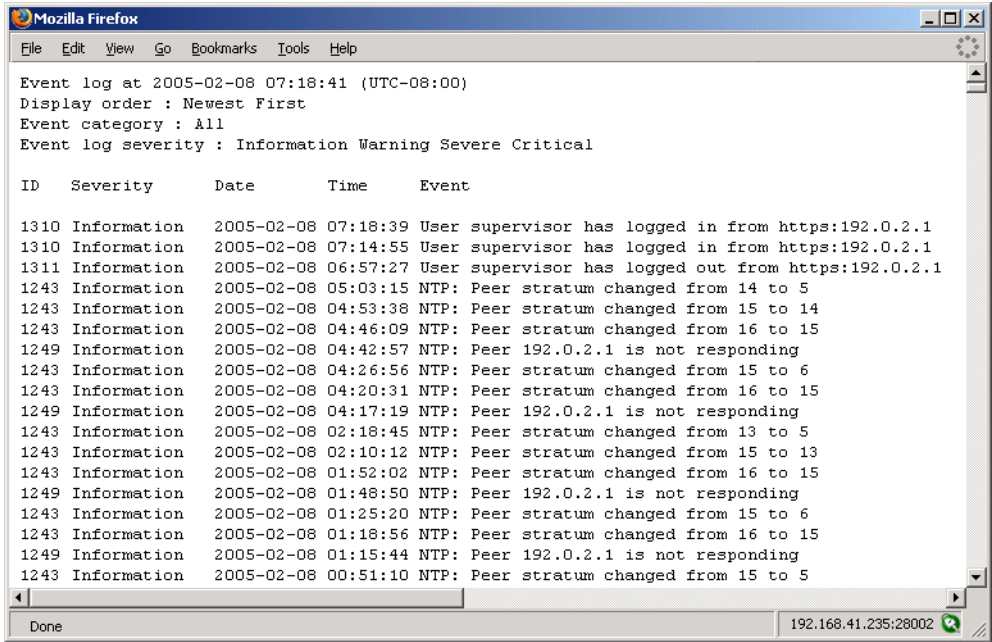
Resolution : No action required

OK

To empty the log, click **Clear Event Log**.

To archive the event log

1. On the **Event Log Management** dialog box, click **Download Entire Log**.



2. From the browser page, **print** the log or **save** it as a text file on a local PC.

Setting up Event Notification

It is possible to set up Titan so that it automatically notifies selected users when particular types of system events occur. Once warned of an event, these users can run the Web Manager to diagnose the problem from anywhere with a direct connection or virtual private link to the network that contains the system.

The event notification may take four forms:

1. An **Email message**, which the system sends through an SMTP server. See [Configuring Email Alerts](#) for more information.
2. A **WinPopup message**, for display on Windows NT/2000/2003/XP computers. See [Setting Up WinPopup Notification](#) for more information.
3. An **SNMP trap**, to notify a central Network Management Station (NMS) of any events generated by the server, for example HP OpenView. See [Sending SNMP Traps](#) for more information.
4. A **Syslog** alert, enables the user to send alerts from a Titan Server to a UNIX's system log, (the UNIX system must also have its *syslog daemon* configured to receive remote syslog messages). See [Setting Up Syslog Notification](#) for more information.



Note: With any of the event notifications, it is recommended to set a notification frequency of Immediately for the most serious alert types (Critical and Severe) and to send these alerts to at least two users.

Email Alerts

Titan can be configured to send emails to specified recipients to alert them on system events. Setting up email alerts requires configuring:

- **SMTP Servers:** The servers on the network to which Titan should email alerts.
- **Email Profiles:** Email profiles allow distribution groups to be created so email recipients are properly notified based on alert threshold criteria.

To Configure Email Alerts

From the **Home** page, click **Status & Monitoring**. Then, click **Email Alerts Setup**.

The screenshot shows the BlueArc Titan web interface. The top navigation bar includes the BlueArc logo, a status bar showing 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF', and links for Help, About, and Sign Out. The breadcrumb trail is 'Home > Status & Monitoring > Email Alerts Setup'. The main heading is 'Email Alerts Setup'. Below this, there is a section for 'SMTP Servers' with two input fields: 'SMTP Primary Server IP/Name' containing '192.0.2.1' and 'SMTP Secondary Server IP/Name' containing 'mail.bluearc.com'. An 'apply' button is below these fields. A message states 'No Profiles have been created'. At the bottom, there is an 'Actions' section with 'add' and 'delete' buttons and a link 'Create BlueArc Support Profile'. A 'Shortcuts' section contains a link 'Configure Email Forwarding'.

The fields on this screen are described in the following table:

Field	Description
SMTP Primary Server IP/ Name	Type the host name or IP address of the primary mail server. The server specified as the SMTP Server will be used for email alert notification. If the Primary SMTP Server is offline, the Silicon Server will re-direct email notifications to the defined SMTP Secondary Server.  Tip: As the Titan SiliconServer should always be in contact with the SMU, it is recommended that the SMU's eth1 IP address be defined as the Primary SMTP server. The SMU can be configured for email forwarding and relay any messages to the public mail server.
SMTP Secondary Server IP/ Name	Type the host name or IP address of the secondary mail server. Email alerts are redirected to this server if the Primary SMTP Server is unresponsive.

Click **Create BlueArc Support Profile** to create the email profile used by BlueArc Global Services so that they can be notified about errors and critical events that occur on the server.

Once the email servers have been defined, click **apply**.

Click **add** to add a new email profile.

Click **delete** to delete the selected profile.

Email Profiles

Titan allows the option of classifying email recipients in specific profiles so that recipients can receive customized alerts with the depth of focus they require.

For instance, profiles can define the different tiers of user responsibility for the server, wherein recipients in one profile will only receive alerts on Critical events, while recipients in a second profile receive alerts on Warning and Critical events, and recipients in a third get summary emails on all events with extensive details. In a large user group, dividing them into separate profiles saves time and simplifies event notification.

To add an Email Profile

- 1. From the **Home** page, click **Status & Monitoring**.
- 2. Click **Email Alerts Setup**.

3. Click **add**.

BLUE ARC

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Status & Statistics | [Home](#) > [Status & Monitoring](#) > [Email Alert Configuration](#) > Add Email Profile

Add Email Profile

Profile Name:

☐ Uuencode Diagnostic Emails

☐ Send HTML Emails

☐ Send Empty Emails

☐ Disclose Email details to the recipients

☐ Send a Daily Status Email at midnight

☐ Ignore NDMP Events in immediate emails

Max. Email Length

Send Emails for Critical Events:

Never

Send Emails for Severe Events:

Never

Send Emails for Warning Events:

Never

Send Emails for Information Events:

Never

Send Summaries At:

08:30

 hh:mm (24 hour)

None

 hh:mm

Recipients

X

Add Recipient:

Add

OK

cancel

The fields on this screen are described in the following table:

Field	Description
Profile Name	Select a name for the profile being created.
Uuencode Diagnostic Emails	Select this checkbox to <i>uuencode</i> the email attachments with the mail that the server automatically sends when it restarts after an unplanned shutdown. This message contains diagnostic information that may help recipients to identify the cause of the problem. By uuencoding the message any virus scanning software at the recipient's site will be bypassed.
Send HTML Emails	Select this checkbox to receive emails in HTML format. HTML emails are easier to read compared to plain text mails, and there is easy access to the web UI since the server name in the Email is <i>clickable</i> .
Send Empty Emails	By default, the Send Empty Emails button will be checked. Empty summary emails will be sent to the specified recipient when this is selected. To avoid sending empty summarized Emails, remove the check in the box.

Disclose Email Details to the recipient	By default, the Disclose Email details to the recipient button will be checked. Detailed emails containing restricted or confidential information (account names, IP addresses, portions of user data, etc.) will be sent to the specified recipient. To avoid sending detailed emails, remove the check in the box.
Send a Daily Status Email	By default, the Send a Daily Status Email button will be checked. Detailed emails containing logs of server performance and battery health, descriptive information regarding the health of the server and storage subsystem, and the current space utilization of the file systems will be sent to the specified recipient. To avoid sending Daily Status Emails, remove the check in the box.
Ignore NDMP events in immediate emails	Select to prevent emails from being sent when events are generated by the NDMP backup system.
Max. Email Length	Limit the size of the email by designating the maximum number of bytes it can contain. It must be stated numerically, such as: 32768.
Send Emails for Critical Events	Select the preferred option for the chosen recipient from the drop-down menu: • Immediately • Never
Send Emails for Severe Events	Select the preferred option for the chosen recipient from the drop-down menu: • Immediately • Summary • Never
Send Emails for Warning Events	Select the preferred option for the chosen recipient from the drop-down menu: • Immediately • Summary • Never
Send Emails for Information Events	Select the preferred option for the chosen recipient from the drop-down menu: • Immediately • Summary • Never
Send Summaries At	Set the time when the emails should be sent. Set the exact time (hh:mm) in a 24-hour format (i.e. 2 PM will be set as 14:00). A second summary can also be sent by entering a time in the second box.
Recipients	Displays the current recipient's Email Address .
Add Recipient	Enter the Email Address of the recipient about to be added to the profile.

Click **X** to delete the selected recipient from the current profile.

Click **add** to add the specified recipient to the current profile.

When the profile has been fully defined, click **OK** to create the email profile.

Use the **cancel** button to discard the changes or return to the **Email Alerts Setup** page.

Managing Email Alerts and Profiles

The **Email Alerts Setup** page can be used to delete a profile or modify its properties.

To modify Email Alerts and Profiles

1. From the **Home** page, click **Status & Monitoring**.
2. Click **Email Alerts Setup**.
3. Select the desired profile to be modified or deleted by selecting the checkbox next to it in the **Profile Name** column.
4. Click **details** corresponding to the selected profile.
The **SMTP Email Profile** screen appears.
5. Modify the profile by selecting the desired alert option from the drop-down menus or the checkboxes.

Click **X** to delete the selected recipient from the current profile.

Click **add** to add the specified recipient to the current profile.

Click **cancel** to discard the latest modifications.

When all the fields have been completed in the **SMTP Email Profile** screen, click **OK** to return to the **Email Alerts Setup** screen.



Note: The **SMTP Primary Server IP/Name** should always point to SMU's Private IP address, while the **SMTP Secondary Server IP/Name** should always point to the company's main SMTP server.

Daily Status Emails

The Titan Storage System is composed of many different components. To get an accurate description of the overall status of the various components of the storage system, two daily status emails are generated: one from Titan, and the other from the SMU.

Titan's Daily Status Email

Titan's Daily Status Email contains logs of server performance and battery health, descriptive information regarding the health of the server and storage subsystem, and the current space utilization of the file systems.

Titan's Daily Status Email is sent to all recipients in all mail profiles in which the **Send a Daily Status Email at midnight** option has been selected.

SMU's Daily Status Email

SMU's Daily Status Email contains a list of the SMU's managed servers and their current firmware versions. It also contains the SMU's current software version. The SMU server names as well as the Silicon Server names are links that can be 'clicked' to manage the specified server. The email also provides the ID, Model, Type (single node, cluster, etc.), and Status information on Silicon Servers.

SMU Diagnostics Emails

The SMU will send all of its configured email recipients a diagnostic email when any of the following events occur:

- ❑ The SiliconServer has unexpectedly reset.
- ❑ When a high number of bad blocks have been identified on any FC-14 or SA-14 RAID Rack in the storage subsystem.
- ❑ If enabled, once per day at a specified time.

These diagnostic emails contain details on the servers and storage managed by the SMU. As the details in these diagnostic mails can be useful to BlueArc Global Services should their assistance be required, it is strongly advised to include alerts@bluearc.com as one of the email recipients.

It is also recommended to enable **Monthly BlueArc Emails**. When enabled, a full set of server, SMU, and storage diagnostics are emailed to BlueArc on the first of every month. These provide an archive of the complete configuration of the storage system, which can aid in the detection of problems, provide a wealth of information to BlueArc Global Services should a problem occur, and, if necessary, the restoration of a known good configuration should it be required.

To Configure the SMU's Diagnostic Emails

From the **SMU Administration** page, click **Diagnostic Emails**.

The screenshot shows the 'Diagnostic Email Configuration' page within the BlueArc Titan web interface. The page has a blue header with the BlueArc logo and navigation links for Help, About, and Sign Out. Below the header, a status bar shows 'Titan - 192.0.2.2' and 'Advanced Mode: ON'. The main content area is titled 'Diagnostic Email Configuration' and contains two sections. The first section, 'Diagnostic Emails', has a yellow background and includes fields for 'Enable Daily Emails' (checked), 'Time' (08:30), 'Send Email From' (smu-titan.shire), 'Email Subject' (Diagnostics_smu-titan.s), 'HTML Format' (checked), and 'Send Emails To' (jgallagher@shire.bluearc.com, pbland@shire.bluearc.com). A note below the email list states 'alerts@bluearc.com is recommended'. The second section, 'Monthly BlueArc Emails', has a white background and includes a checkbox for 'Enable' (recommended) and a 'Send to' field (alerts@bluearc.com). At the bottom of the page are 'apply' and 'test' buttons.

The table below describes the fields on this screen:

Item / Field	Description
Enable Daily Emails	Check this to enable the Daily Status Email report.
Time	Set the time when the emails should be sent. Set the exact time (hh:mm) in a 24 hour format (i.e. 2:00 P.M. will be set as 14:00).
Send Email From	The host name or other identifier that uniquely identifies the SMU from which the email will be sent.
Email Subject	Enter an easily recognizable subject line for the Daily Status email report.
HTML Format	Select to have the status email sent in HTML format. If this is not selected, emails will be sent in plain text.
Send Emails To	Enter the email addresses of all the recipients.
Monthly BlueArc Emails	Check to send a monthly diagnostic email to BlueArc. This email will send a copy of all server, SMU, and storage array configuration to BlueArc. This information is kept private and will only be referenced if a service call is placed with BlueArc Global Services.

Use the **down arrow** button to add more email addresses.

Use the **X** button to delete selected email addresses.

Use the **apply** button to register the additions, changes on the screen.

Setting Up WinPopup Notification

1. From the **Home** page, click **Status & Monitoring**. Then, click **Windows Popups** Setup.

The screenshot shows the BlueArc Titan web interface. The header includes the BlueArc logo, a status bar showing 'Titan - 192.0.2.2' and 'Advanced Mode: OFF', and navigation links for Help, About, and Sign Out. The main navigation bar shows 'Status & Statistics' and 'Home > Status & Monitoring > Windows Popups'. The 'Event Notification' section contains dropdown menus for 'Notification frequency' (Critical alerts, Severe alerts, Warning alerts, Information alerts) all set to 'Never'. Below this is a text area for 'Windows popup recipients' with buttons for 'Delete Recipient' and 'Delete All Recipients'. At the bottom, there is a 'New windows popup recipient' input field with an 'Add Recipient' button, and a green bar with 'Apply' and 'Cancel' buttons.

The fields on this screen are described in the following table:

Field	Description
Notification Frequency	Select the <i>notification frequency</i> for each type of alert.
New Windows popup recipient	In the New Windows popup recipient box, add the required user names or computer names and click the Add Recipient button. (Do not enter the IP addresses of the selected computers.)
Delete Recipient	To delete a recipient, select it from the <i>Windows popup recipients</i> list and click the Delete Recipient button.
Delete All Recipients	To delete all recipients click the Delete All Recipients button.

2. When all fields have been completed, click **Apply**.

On Windows 2000, Windows 2003, or Windows XP computers, no further setup is needed to receive and display popups. However, on Windows 98 computers, winpopup.exe must be running to display the popups.

Setting Up an SNMP Agent

The Simple Network Management Protocol (SNMP) is a standard protocol used for managing different devices connected to a network. An SNMP agent can be set up so that Network Management Stations (NMS) or SNMP managers can access its management information. Titan supports SNMP versions 1 and 2c.

SNMP Statistics

[Statistics](#) are available to monitor SNMP activity since Titan was last started or its statistics were reset. The statistics are updated every ten seconds.

The Management Information Base

The SNMP agent maintains a 'database' of information called a *Management Information Base* (MIB). Data in the MIB is organized in a treelike structure. Each item of data has a unique object identifier (OID), which is written as a series of numbers separated by dots-- known as the ASN.1 notation.

BlueArc's SNMP agent not only supports the MIB-II specification as described in RFC1213, but also provides the BlueArc Enterprise MIB module, making management facilities available beyond those in the MIB-II specification. Download BlueArc's Enterprise MIB module from the SMU, or contact *BlueArc Global Services* for the latest BlueArc Enterprise MIB module.

BlueArc's Enterprise MIB module is compiled for SNMP v2c, and is defined in two modules, BLUEARC-SERVER-MIB and BLUEARC-TITAN-MIB.



Note: When loading (compiling) the BlueArc enterprise MIB module in IBM's Tivoli management application, the MIB module is loaded by selecting **Tools > MIBs > SNMPv2 > Load** page options as opposed to the **Tools > MIBs > Load page** option.

Implementing SNMP Security

By default, the SNMP agent does not permit access to the *Management Information Base* (MIB). Access is enabled by specifying:

- The *version* of the SNMP protocol with which requests must comply.
- The *community names* of the SNMP hosts and their associated access levels.
- The *IP address or name* of hosts from which requests may be accepted (or just choose to accept requests from any host).

Configuring SNMP

From the **SiliconServer Admin** page, click **SNMP Access Configuration**.

BLUE ARC

?

 Help

i

 About

Sign Out

Titan - 192.0.2.2

Advanced Mode: OFF

SiliconServer Admin | [Home](#) > [SiliconServer Admin](#) > SNMP Management Access

Management Access Configuration

☐ Disable agent

☐ Process SNMPv1 requests only

☐ Process SNMPv2c requests only

☒ Process SNMPv1 and SNMPv2c requests

☐ Send Authentication Trap

No Community Names

Add Community

Add

☐ Accept SNMP packets from any host

☒ Accept SNMP packets from authorized hosts

No Host Names

Add Host

Add

Accept SNMP packets on port number:

161

Send traps to port number:

162

Receive traps on port number:

162

Apply

Cancel

Item /Field	Description
SNMP Protocol Support	Using the options at the top of the page, select the <i>version</i> of the SNMP protocol with which hosts must comply when sending requests to the agent. Alternatively, choose to <i>disable</i> the SNMP agent altogether.
Send Authentication Trap	Select this checkbox if the SNMP agent is to send a trap in the event of an authentication failure (caused, for example, by the SNMP host using an incorrect community string when formulating a request).

Add Community	Type the name of a community that is to access the MIB. Community names are case-sensitive. It is recommended that at least one entry for the community public be defined. When all the details have been entered click Add.
Accept SNMP Packets	In the bottom half of the dialog box, choose whether to accept SNMP requests from any host or from authorized hosts only. To permit requests from authorized hosts only, type the IP address of a host in the Add Host field and then click Add. If Titan is to work with a name server, the name of the SNMP host can be given, rather than its address.
Send traps	To <i>send</i> traps to a specific port number, enter the port number in the specified field.
Receive traps	To <i>receive</i> traps on a specific port, enter the port number in the specified field

When all fields have been completed, click **Apply**.

Sending SNMP Traps

A trap is unsolicited information that the SNMP agent sends to a manager. It enables the agent to alert the manager to some unusual system event. The SNMP agent supports the limited number of built-in traps defined below.

Trap name	Indication
AuthenticationFailure	The SNMP agent received a request from an unauthorized manager. Either the manager used an incorrect community name or the agent has been setup to deny access to the manager.
ColdStart	The SNMP agent has started or been restarted.
LinkUp	The status of the Ethernet link has changed from Down to Up.

To set up SNMP notification

From the **Home** page, click **Status & Monitoring**. Then, click **SNMP Traps Setup**.

BLUEARC

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: OFF

Status & Statistics

 | [Home](#) > [Status & Monitoring](#) > SNMP Alerts

Event Notification

Notification frequency

Critical alerts

Never

 Severe alerts

Never

Warning alerts

Never

 Information alerts

Never

Community Host

Delete Recipient

Delete All Recipients

New SNMP recipient

Community

Host

Add

Item /Field	Description
Notification Frequency	By using the drop-down list, select the notification frequency for each type of alert.

New SNMP Recipient	Type the name of the SNMP community in the <i>New SNMP recipient</i> , Community field, (community names are case-sensitive) and click the Add button. Read and Write communities names must be defined. In the Host field, type the IP address of an SNMP host to associate with the selected community. If the system has been setup to work with a name server, type the name of the SNMP host rather than its address.
Delete Recipient	To delete a recipient, select it from the <i>Community</i> list and click the Delete Recipient button.
Delete All Recipients	To delete all recipients click the Delete All Recipients button.

Setting Up Syslog Notification

From the **Home** page, click **Status & Monitoring**. Then, click **Syslog Alerts Setup**.

BLUE ARC

?

 Help

i

 About

Sign Out

TITAN - 192.0.2.2

Advanced Mode: ON

Status & Statistics

Home > Status & Monitoring > SysLog Alerts

Event Notification

Notification frequency

Critical alerts

Immediately

 Severe alerts

Immediately

Warning alerts

Immediately

 Information alerts

Immediately

Syslog recipients

172.16.10.154

10.1.2.101

Delete Recipient

Delete All Recipients

New syslog recipient

Add Recipient

Apply

Cancel

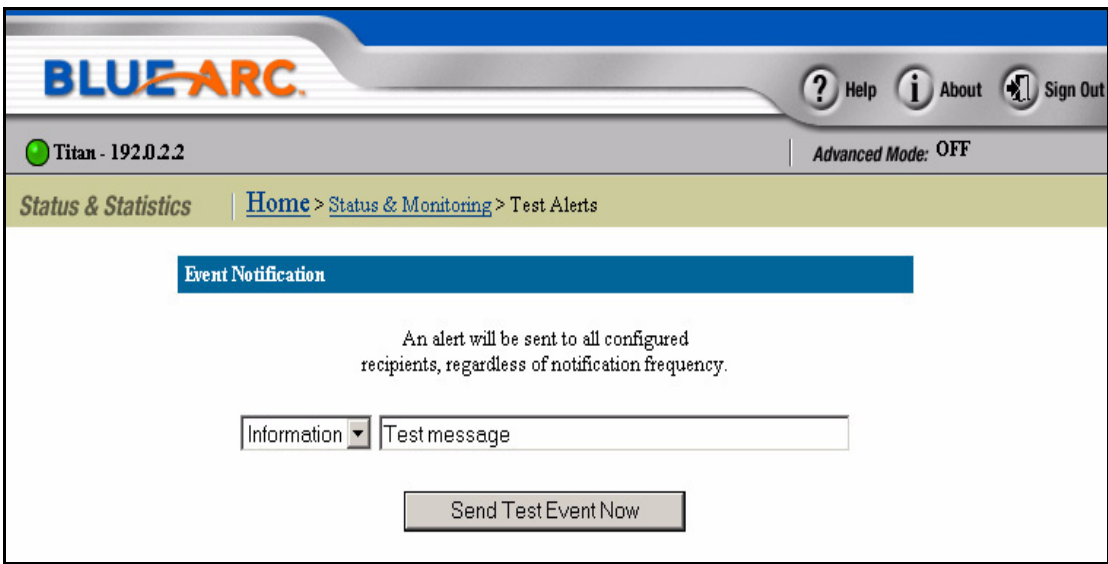
The fields on this screen are described in the following table:

Field	Description
Notification Frequency	Select the notification frequency for each type of alert.
New Syslog Recipient	Type the name of the recipient in the <i>New Syslog recipient</i> field, and click the Add Recipient button.
Delete Recipient	To delete a recipient, select it from the <i>Syslog recipients</i> list and click the Delete Recipient button.
Delete All Recipients	To delete all recipients click the Delete All Recipients button.

Testing the Alert Configuration

After setting up the alert configuration, send a test alert to all the recipients that were selected

1. From the **Home** page, click **Status & Monitoring**. Then, click **Send Test Event**.



The screenshot shows the BlueArc Titan web interface. At the top, there's a header with the BlueArc logo and navigation links: Help, About, and Sign Out. Below the header, a status bar shows 'Titan - 192.0.2.2' and 'Advanced Mode: OFF'. The main navigation area includes 'Status & Statistics' and a breadcrumb trail: 'Home > Status & Monitoring > Test Alerts'. The central content area is titled 'Event Notification' and contains the text: 'An alert will be sent to all configured recipients, regardless of notification frequency.' Below this text, there is a dropdown menu currently set to 'Information' and an adjacent text input field containing 'Test message'. At the bottom of this section is a button labeled 'Send Test Event Now'.

2. Select a **type** of message to send from the drop down page, *information/warning/critical*, and then enter a **test message** in the empty box.
3. Click **Send Test Event Now**.

10 Maintenance Tasks

Maintenance Tasks Overview

Various administration tasks for the Titan SiliconServer, such as firmware upgrades, system configuration backup and restore, etc. are explained in this section.

Checking Version Information

When requesting technical support, it is important to have version information about Titan firmware and hardware.

To display version information for a Titan SiliconServer

From the **SiliconServer Admin** page, click **Version Information**.



?

 Help

i

 About

Sign Out

Titan - 192.0.2.2

Advanced Mode: ON

SiliconServer Admin | [Home](#) > [SiliconServer Admin](#) > Version

Version Information

Server Version

Software: 4.1.873b (Fri Jul 1 18:10:15 2005)

Hardware: Titan (TITAN1FC100087)

Module Versions

board	NIM
titanbootrom	T8 release (Tue Jul 22 12:40:10 2003)
nim	4.1.873b release (Fri Jul 1 18:10:15 2005)
nimhw	release 506 (Tue May 10 01:32:52 2005)
Serial Number	B0412079 (Tue Jan 4 11:32:47 2005)

board	FSA
titanbootrom	T8 release (Tue Jul 22 12:40:10 2003)
fsm	4.1.873b release (Fri Jul 1 17:32:52 2005)
Serial Number	B0411345 (Sat Jan 8 09:49:36 2005)

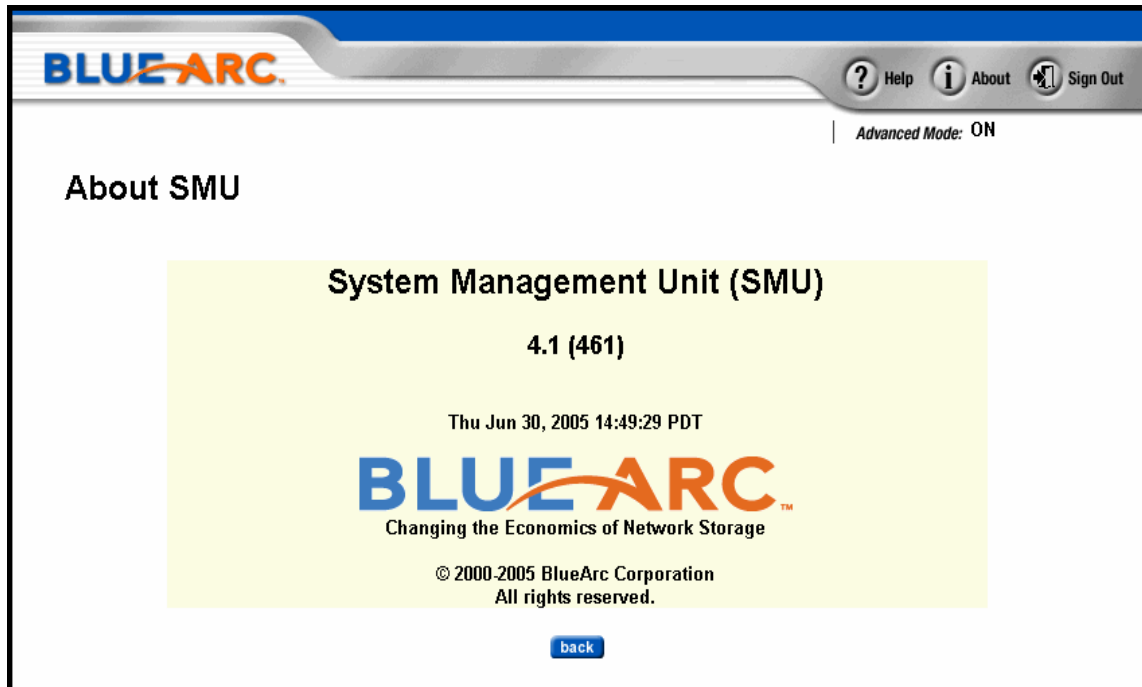
board	FSB
fsmhw	release 612 (Tue Jun 28 07:49:46 2005)
Serial Number	B0411246 (Sun Nov 21 15:33:12 2004)

board	SIM
titanbootrom	T8 release (Tue Jul 22 12:40:10 2003)
sim	4.1.873b release (Fri Jul 1 17:33:36 2005)
simhw	release 606 (Mon May 23 02:22:43 2005)
Serial Number	B0412037 (Sat Jan 8 07:08:11 2005)

If configured as a cluster, select the Cluster Node from the drop-down list to view the current version information.

To display version information for the SMU

From the **Web Manager** home page, click the **About** button at the top right corner of the screen.



Saving and Restoring the Server's Configuration

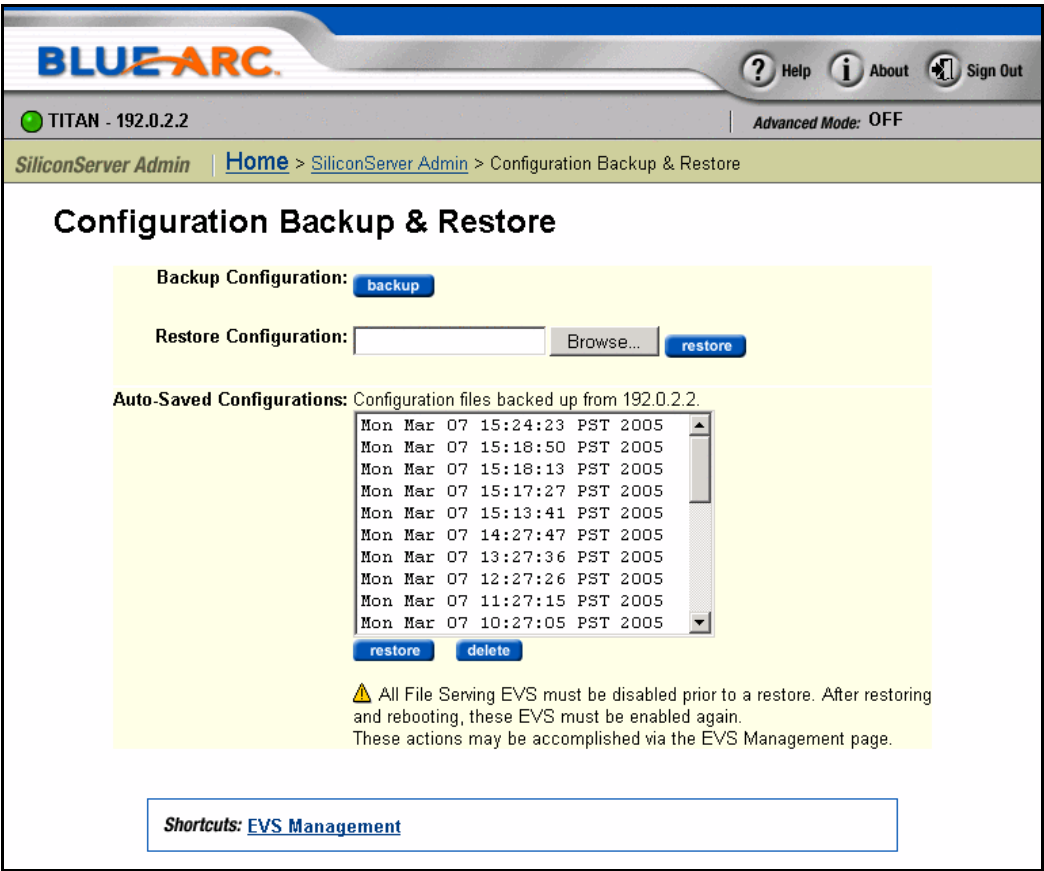
The [System Management Unit \(SMU\)](#) automatically saves the configuration of all managed servers on a periodic basis. The configuration can be backed up at any time and saved files can be archived on a PC or workstation. Configuration files maintained on the SMU, or archived on a different system, can be restored to the Titan SiliconServer.



Caution: Restored configurations may have different (older) passwords. Update these settings on the Managed SiliconServers page if necessary after rebooting the server. If it is not updated, the SMU may fail to connect to Titan.

To Backup the SiliconServer Configuration

1. From the **SiliconServer Admin** page, click **Configuration Backup & Restore**.



2. Click **backup**.
3. Choose a location to store/archive the configuration.
4. Click **OK**.

To Restore the SiliconServer Configuration from Backup

Do the following to restore the server's configuration settings from a backup file:

1. Click the **EVS Management** link and [disable the EVS](#) before restoring the configuration.
2. Click **browse...** to find and select a configuration file (e.g. registry_data.gz) for the Restore Configuration field.
3. Click the **restore** button. The file will be uploaded to Titan.
4. Reboot the server for the changes to take effect.

If the configuration has been restored to the original server, the storage will be available once the reboot is complete. If the configuration is being restored to a different server, as in the case of disaster recovery, the storage may not be immediately available after the reboot. In such a case, the Storage Pools may be displayed as being assigned to "another cluster". To make the storage available, three steps are required:

- ❑ Run `span-assign-to-cluster` from the CLI to associate the Storage Pools with the server. For more information, run `man span-assign-to-cluster` at the CLI.
- ❑ Allow access to the Storage Pools. For more information, see "[To Allow Access to a Storage Pool](#)".
- ❑ Assign the file systems to an EVS. If the file system is not currently associated with an EVS, this assignment can be performed on the File System Details page. See "[To View the Details of a File System](#)".

Auto-Saved Configurations

The SMU automatically saves and maintains a two-week "rolling" archive of all of its managed servers' configuration files. The archive consists of:

- ❑ Hourly backups for the current day (a maximum of 24 files).
- ❑ Daily backups for two weeks (a maximum of 14 files).

To Restore from the Auto-Saved SMU Archive

Do the following to restore the server's configuration settings from the list of configuration backups preserved on the SMU:

1. Click the **EVS Management** link and [disable all EVS](#) before restoring the configuration.
2. From the list of archived backups, select a configuration file to restore.
3. Click the **restore** button. The file will be uploaded to Titan.
4. Reboot the server for the changes to take effect.

To Delete an Auto-Saved Configuration file

To delete an Auto-Saved Configuration file, select it from the displayed list. Then, click **delete**.

Saving and Restoring the SMU's Configuration

The SMU's configuration information is preserved automatically on the SMU. This configuration can be backed up and, if necessary, restored to the same or different SMU. Restoring the SMU's configuration from backup is the quickest way to recover from a failure should a problem occur with the SMU.

High Availability environments can deploy a Standby SMU. When an SMU is configured with a separate Standby unit, the SMU can regularly archive copies of its configuration on the Standby. In the event of a failure, the archived configuration can be restored on the Standby SMU, enabling rapid recovery of all administrative functions and quorum services provided by the failed SMU.

Standby SMU

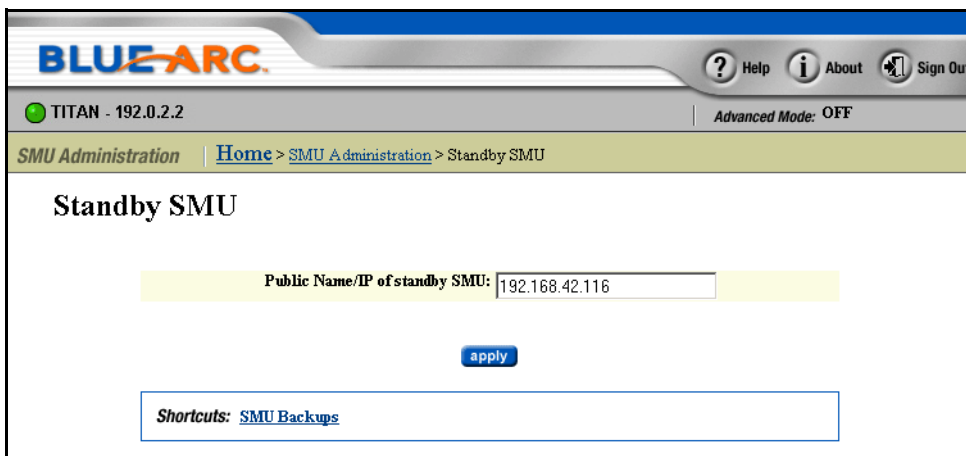
An SMU is configured as a standby during the installation phase. The setup procedure will prompt whether the SMU being configured should be made a standby SMU. If so, a custom IP address must be specified for the Standby to use on the private management network. For more information on the SMU installation procedure, refer to the *SMU Quick Start Guide*.

The Standby SMU's public IP address is added to the configuration of the Primary SMU. This allows the Primary to identify the SMU on which it can archive copies of its configuration.

Configuring the Standby SMU

The following setup must be performed on the Primary SMU.

1. From the **Home** page, click **SMU Administration**. Then, click **Standby SMU**.



The screenshot shows the BlueArc TITAN web interface. The top navigation bar includes the BlueArc logo, a status indicator for TITAN - 192.0.2.2, and links for Help, About, and Sign Out. Below the navigation bar, the breadcrumb trail reads: SMU Administration > Home > SMU Administration > Standby SMU. The main heading is "Standby SMU". A form field labeled "Public Name/IP of standby SMU:" contains the value "192.168.42.116". Below the form field is an "apply" button. At the bottom, there is a "Shortcuts:" section with a link to "SMU Backups".

2. Enter the host name or IP address of the Standby SMU in the **Public Name/IP of standby SMU** field. This IP address must be the **eth0**, not the **eth1** IP address of the Standby SMU.

- 3. Click **apply**.

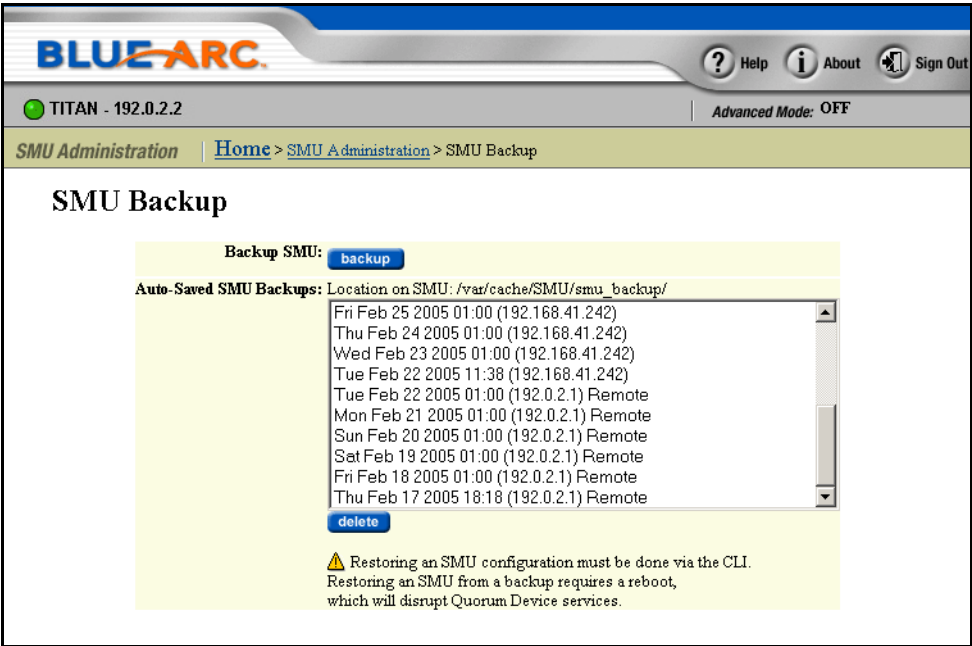
Copies of the SMU's configuration database will start being archived daily on the Standby.

Verifying Operation of the Standby SMU

Once the Standby SMU has been defined, it is important to make sure copies of the Primary's configuration database are being properly archived.

To verify proper archiving of the Primary's configuration, enter the URL of the Standby SMU into your browser, and go to the following page:

From the **Home** page, click **SMU Administration**. Then, click **SMU Backup**.



The configuration backups in the list are identified by the **eth0** IP address of the SMU on which the backup was performed. Additionally, archives that have come in from a Primary SMU will indicate that they are **Remote**.

Backing up the SMU Configuration

The best way to preserve a copy of the SMU's configuration is by installing a Standby SMU. Short of that, the SMU's configuration can be backed up manually. The SMU automatically archives its own configuration, but if the SMU fails those backups would not be recoverable.

Automatic Backup of the SMU Configuration

The SMU is set up to have its configurations backed up automatically. The SMU backups are created:

Saving and Restoring the SMU's Configuration

- Once every day at 1:00 AM.
- Within 20 minutes of the SMU being rebooted.

While the SMU backups are performed automatically, manual backups can be created, and existing backups can be viewed or [deleted](#) from the SMU Backup screen.

Saving the SMU Configuration Manually

1. From the **Home** page, click **SMU Administration**. Then, click **SMU Backup**.
2. Click **backup**.
3. Choose a location (on your PC) to store/archive the configuration.
4. Click **OK**.

A copy of that backup is also kept on the SMU. And if configured with a Standby SMU, that backup file will also be sent to the Standby.

Restoring SMU Backups

In the event of an SMU's failure, an archived copy of its configuration can be restored to another SMU, enabling it to come up with the saved configuration. If a Standby SMU has been configured, it contains all the backups from the Primary SMU, and it can be activated to take place of the Primary. If a Standby SMU was not configured but a saved configuration is still available, a new SMU unit can be installed, and the configuration restored from the old unit.

After the SMU's configuration has been restored, the status of any in-progress replications at the time the backup took place may be reflected on the main replication page. This may result in seeing a replication as being in-progress, even if the schedule hasn't yet been run after the configuration restore. In this case, the status will be properly updated during the next scheduled run of the Replication Policy.



Caution: The replacement SMU will assume the same IP address as the original SMU. To eliminate the possibility of accidental outage, it is recommended to remove the network connections from the old SMU to prevent the possibility of an IP conflict.

Restoring the SMU's configuration must be done through the SMU's Command Line Interface. To restore the SMU configuration, do the following:

1. Connect to the SMU using SSH with the *manager* username and password.
2. Choose 'exit to SMU shell', if prompted to do so.
3. Log in as root, i.e. 'su -'.
When prompted enter the configured root password.
4. Change into the directory in which the configuration backups reside. The value for <SMU_IP> should be the IP address of the eth0 interface on the Primary SMU.
`cd /var/cache/SMU/smu_backup/<SMU_IP>/`

5. Retrieve a list of available configuration backups to restore by typing:
`ls -l`
6. Identify the desired package, typically the most recent backup, and restore it by typing:
`/usr/local/smu_packages/restore.sh ./<filename>.zip`
7. Reboot the SMU by typing:
`reboot`

Deleting the SMU's Backup Configuration Files

1. From the **Home** page, click **SMU Administration**. Then, click **SMU Backup**.
2. From the dated list in the **Auto-Saved SMU Backups** field, select the particular backup that must be deleted.
3. Click **delete**.

Upgrading System Software and Firmware

The System Management Unit (SMU) software and Titan SiliconServer firmware can be upgraded to a newer release.



Note: SMU software and Titan Server firmware are upgraded at the same time. It is necessary to verify that the server's flash has sufficient space for the new firmware file to be uploaded. If there is insufficient space, erase one of the old image files before proceeding.

Upgrading SMU Software

To upgrade the SMU software:

1. Before proceeding with the upgrade process, connect to the SMU through the **serial port**.
2. Login as '**root**' (when prompted, enter the password).
3. From the command prompt enter:
`lilo -R backup`
4. Reboot the SMU by typing:
`reboot`
5. The SMU will boot into backup mode in a few minutes.
6. Login as '**root**'.
7. Insert the **Upgrade CD** and close the CD ROM drive, wait 5 seconds.

Upgrading System Software and Firmware

8. From the prompt, mount the CD ROM by typing:
`mount /mnt/cdrom`
9. To start the upgrade process, type:
`/mnt/cdrom/autorun`
10. The upgrade process will start. This process will take approximately 15 minutes.



Note: During the SMU upgrade process, a cluster, which is using the SMU as a Quorum Device, may generate the following Severe Event. This is to be expected and may be ignored:

Severe: Lost communication with the Quorum Device.

11. When the upgrade is complete, the SMU will automatically reboot.
12. Manually eject the CD during the reboot (click the CD drive's button on the front of the SMU).



Note: To eject the CD through the SMU's command prompt, (logged in as root) type:

```
umount /mnt/cdrom  
eject cdrom
```

13. The SMU will boot up using the new build.



Note: After the SMU upgrade process, the SMU may report Titan as 'out of contact' or 'version mismatch error', this is expected and is not a problem. The Titan SiliconServer can be upgraded as soon as the SMU has rebooted. However, the Titan Server will not be managed by the SMU during the SMU upgrade process.

Upgrading Titan Server Firmware

A Titan SiliconServer can store up to three firmware packages in flash memory. Any one of these images can be selected to run automatically when Titan is rebooted. Such a package is known as the default package. The package being run on Titan at any given time is known as the current package.

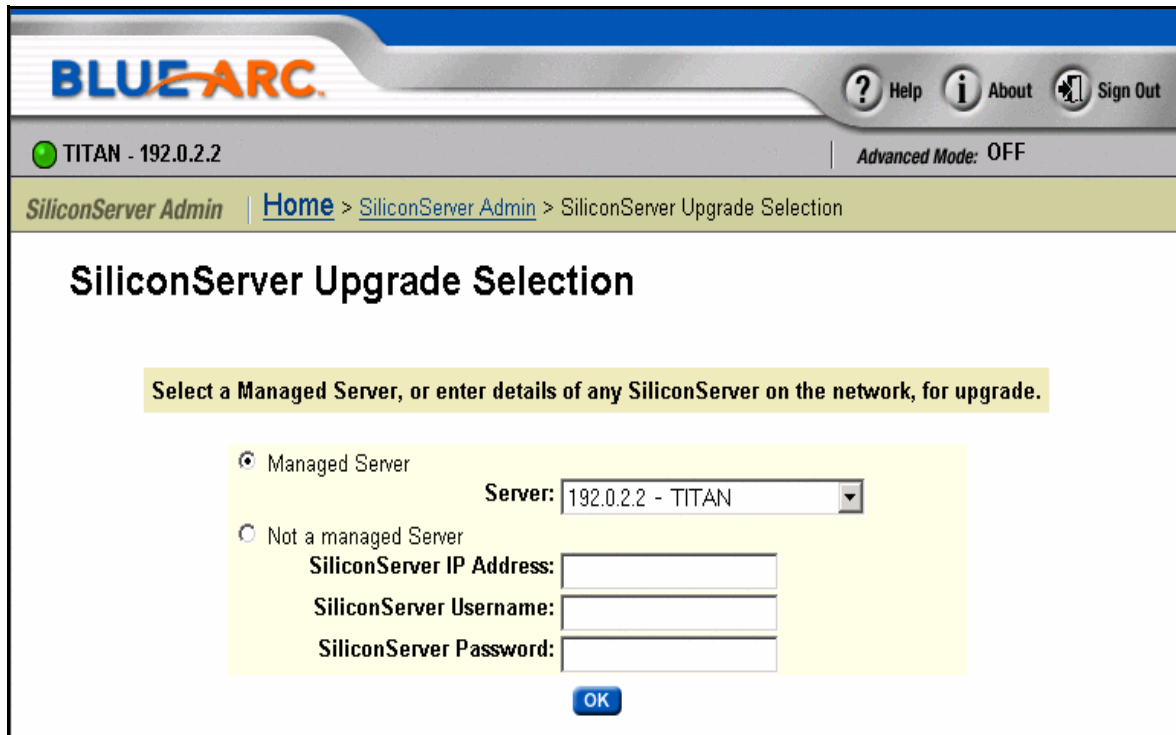
When BlueArc releases a new version of the server firmware, it can be uploaded to flash memory, ready to be set as the default package for Titan. The sections below explain how a package can be uploaded and designated as the default package.



Note: Contact BlueArc Global Services for instructions on how to obtain the latest firmware version.

A firmware package can be uploaded to Titan if it is or is not listed by the SMU as a Managed Server.

1. From the **SiliconServer Admin** page, click **Upgrade Firmware**.



The screenshot shows the BlueArc web interface. At the top, the BlueArc logo is on the left, and navigation links for Help, About, and Sign Out are on the right. Below the header, a status bar shows 'TITAN - 192.0.2.2' and 'Advanced Mode: OFF'. A breadcrumb trail reads 'SiliconServer Admin | Home > SiliconServer Admin > SiliconServer Upgrade Selection'. The main heading is 'SiliconServer Upgrade Selection'. Below this, a yellow box contains the instruction: 'Select a Managed Server, or enter details of any SiliconServer on the network, for upgrade.' There are two radio buttons: 'Managed Server' (selected) and 'Not a managed Server'. Under 'Managed Server', there is a 'Server:' label and a dropdown menu showing '192.0.2.2 - TITAN'. Under 'Not a managed Server', there are three input fields labeled 'SiliconServer IP Address:', 'SiliconServer Username:', and 'SiliconServer Password:'. An 'OK' button is at the bottom of the form.

2. On the **SiliconServer Upgrade Selection** page, use the radio button to select whether the server is or is not a managed server.
 - ❑ If the server is a **Managed Server**, use the drop-down list to select the correct server to upgrade the firmware package.
 - ❑ If the server is **Not a managed server**, enter the **IP Address, Username, and Password** of the SiliconServer.

3. Click **OK**.

The screenshot shows the 'Titan Package Upload: 192.0.2.2' page. At the top, there's a header with the 'BLUEARC' logo and navigation links: '? Help', 'i About', and 'Sign Out'. Below the header, a status bar shows 'Titan - 192.0.2.2' and 'Advanced Mode: OFF'. The main breadcrumb trail is 'SiliconServer Admin | Home > SiliconServer Admin > SiliconServer Upgrade Selection > Titan Package Upload'. The title 'Titan Package Upload: 192.0.2.2' is prominently displayed. The form area has a light yellow background and contains the following elements: a label 'Enter the path of a file to upload', a 'Free Flash Space: 84.23MB' indicator, an 'Upgrade File:' text input field with a 'Browse...' button, two checked checkboxes labeled 'Set As Default Package:' and 'Reboot The SiliconServer(s) On Completion:', and two buttons at the bottom: 'apply' and 'cancel'.

On the Titan Package Upload page, enter the path where the firmware image can be found next to Upgrade File. Use **Browse...** to assist in locating the firmware image.

Item/Field	Description
Free Flash Space	The amount of free flash space available. If there is not sufficient space to upload the package, delete older package files through the Manage Packages page.
Upgrade File	Type the path to the upgrade file or click Browse to search for it.
Set As default Package	Check the box to set the uploaded file as the default package.
Reboot Server on Completion	Check the box to reboot Titan once the package has been uploaded.



Caution: If configured in a cluster, the package will be uploaded to each Cluster Node. If a reboot is requested, **both** Cluster Nodes will reboot.

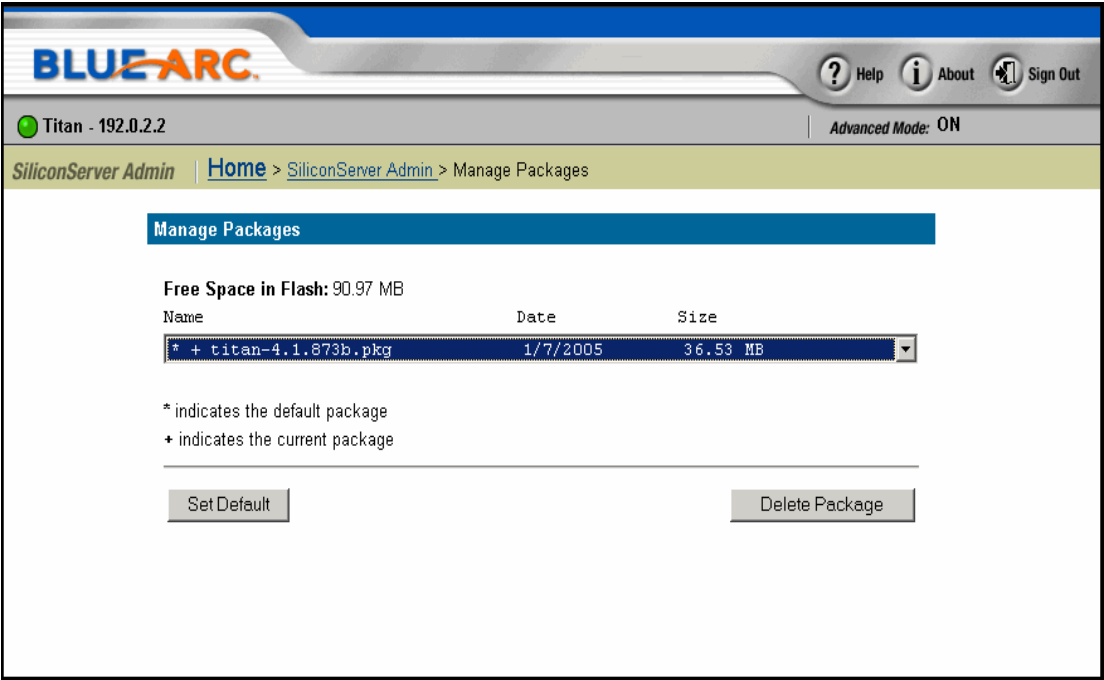
4. When all the fields have been completed, click **Apply**.

The Web Manager monitors the progress of the upload (and reboots, if requested), which may take several minutes to complete. Do not reset the server or turn off the power during this process. If the server has been chosen not to reset automatically, but the new package has been designated as default, then, once the upload has completed, reboot to enable the new firmware as default.

If there has been a problem with the uploading the new firmware package, the package will not be enabled as the default package and the server will not reboot.

Managing Titan Firmware Packages

Firmware packages can be viewed, modified or deleted on the **Manage Titan Packages** page. From the **SiliconServer Admin** page, click **Manage Titan Packages**.



Note: If configured as a cluster, select the Cluster Node from the drop-down list to view the list of managed packages.

Item / Field	Description
Free Space	The amount of free space in flash.
Package List	Lists all the available packages in flash.
Set Default	Select the required package and click the Set Default button.

Delete Package	To delete a package, select it from the list and click the Delete Package button.

Providing an SSL Certificate

Both the Titan and SMU are pre-configured with default SSL certificates. These default certificates should provide an acceptable level of security for most users. For added security, this certificate may be replaced with a certificate signed by a Certificate Authority (e.g. Verisign).

Requesting and Generating Certificates

To request a certificate from a certificate authority (CA):

1. Generate a custom private key [optional].
2. Generate a Certificate Signing Request (CSR).

Generating a Private Key

The SMU already contains a default private key from which a CSR may be generated. It uses default BlueArc values:

- Common Name (CN) uses the SMU’s hostname but other values are BlueArc specific e.g. OU=., O=BlueArc, L=San Jose, ST=CA, C=US
- Valid for 3650 days (10 years).
- Key length of 2048 bits.

To view these values by displaying the SMU's default certificate, type the following at the SMU CLI:

```
cert-showall.sh
```

If other values *must* be used, a custom private key may be generated via the following steps:

1. Log onto the SMU (through ssh or through its serial port) as the user manager, then type:
`sudo cert-gencustom.sh`

Enter the manager user’s password when prompted.

2. Prompts will appear, requesting details of the following: (Hit enter to accept the default values.)
Organizational Unit (OU)
Organization (O)
Location (L)
State (ST)
Country (C)
Valid Period (in days)
Key Size (e.g. 1024, 2048 - must be divisible by 64).
3. After confirming the input, a new private key and self-signed certificate will be generated.
4. Restart the web server (tomcat) when prompted so that it may pick up the new SSL certificate.
5. Close and restart any browsers used to connect to the SMU. This is required to purge the browser of any previously negotiated SSL session values.

When logging into the SMU Web UI, the new SSL Certificate should be provided.

6. Now propagate the new SSL certificate to all managed servers.
Go to Home > SMU Administration > Managed SiliconServers.
For each server, click "details" and then "OK".

A backup of this private key and certificate (i.e. the whole keystore) may be made for safekeeping.

1. Log onto the Web UI.
2. Go to Home > SMU Administration > SMU Backup
3. Click "backup" and save the resulting zip file to safe and secure location.

The zip file contains a full backup of the SMU's configuration information. The file "smu.keystore" within the zip file contains the SMU's private key.

Generating a Certificate Signing Request (CSR)

A Certificate Signing Request is a file that contains the encoded information needed to request a certificate from an authority. After generating the Certificate Signing Request, it can be submitted to the authority. For example, on Verisign's Web site at <http://www.verisign.com/>, paste the Certificate Signing Request into the Web page.

To generate a CSR

1. Log onto the SMU (through ssh or through its serial port) as the user manager, then type:
`sudo cert-gencsr.sh`

Enter the manager user's password when prompted.

2. Copy-and-paste the CSR that was displayed after step 1. That data should be provided to the Certificate Authority.

Alternatively, the same information may be copied off the SMU via the file:
`/var/cache/SMU/certreq.csr`.

Acquiring a SSL Certificate from a Certificate Authority (CA)

At this point, the CSR can be submitted to a Certificate Authority such as Verisign, Thwate, etc. The details of how to do this are beyond the scope of this document.

When acquiring a certificate from a CA has been completed, move ahead to the section [Installing and Managing Certificates](#).

Installing and Managing Certificates

Once a certificate has been obtained from the CA, follow the instructions below to install it.

To Install a Certificate

First, copy the certificate provided by the CA to the SMU (for example, scp to `/home/manager/server.cer`). If necessary, also provide the CA's Trusted Certificate Chain as a file (e.g. `/home/manager/veritas.pem`). The SMU already includes popular CA Trust Chains, so step 2 may typically be skipped. To view these popular CA's, see Sun's documentation:
<http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html#cacerts>



Note: The content of the certificate and trust chain files should only start with "-----BEGIN" and end with "-----END CERTIFICATE-----".

1. Log onto SMU (through `ssh` or it is serial port) as user manager.
2. First, import the CA's Trusted Certificate Chain; this may require multiple files/chains, so repeat as necessary:
`sudo cert-importtrustchain.sh <path to trust chain file> <unique alias>`

When prompted, enter the manager user's password.

An example Intermediate CA trust chain may be found at:
<http://www.verisign.com/support/install2/intermediate.html>



Note: Any alias may be used so long as it's unique. If the alias already exists, you will be prompted to replace the old certificate or cancel the import.

3. Next, the signed "Certificate Reply" from the CA may imported (replacing the default SMU SSL certificate):
`sudo cert-importcert.sh <path to cert file>`

4. Restart the web server (tomcat) when prompted so that it may pick up the new SSL certificate. When prompted to overwrite the existing certificate, enter 'y'
5. To view and verify the contents (SSL certificate and Trust Chain) of the keystore, type:
`sudo cert-showall.sh`
6. Close and restart any browsers used to connect to the SMU. This is required to purge the browser of any previously negotiated SSL session values.

When logging into the SMU web UI, the new SSL Certificate should be provided.

7. Now propagate the new SSL certificate to all managed servers.
Go to Home > SMU Administration > Managed SiliconServers.
For each server, click "details" and then "OK".

Restore the Default SMU Certificate

If troubles are encountered when trying to create/import an SSL certificate, the SMU's default certificate may be restored.

To Restore the Default Certificate

At any time a custom SSL certificate with the default, self-signed certificate, can be replaced.

1. Log onto SMU (through `ssh` or it is serial port) as user manager and type:
`sudo cert-gendefault.sh`

Enter the manager password when prompted.

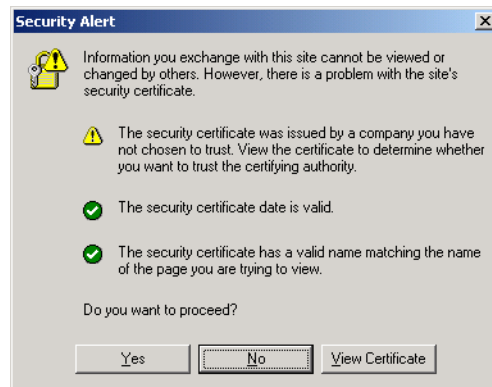
2. Restart the web server (tomcat) when prompted so that it may pick up the new SSL certificate.
3. Close and restart any browsers used to connect to the SMU. This is required to purge the browser of any previously negotiated SSL session values.

When logging into the SMU web UI, the new SSL Certificate should be provided.

4. Now propagate the new SSL certificate to all managed servers.
Go to Home > SMU Administration > Managed SiliconServers.
For each server, click "details" and then "OK".

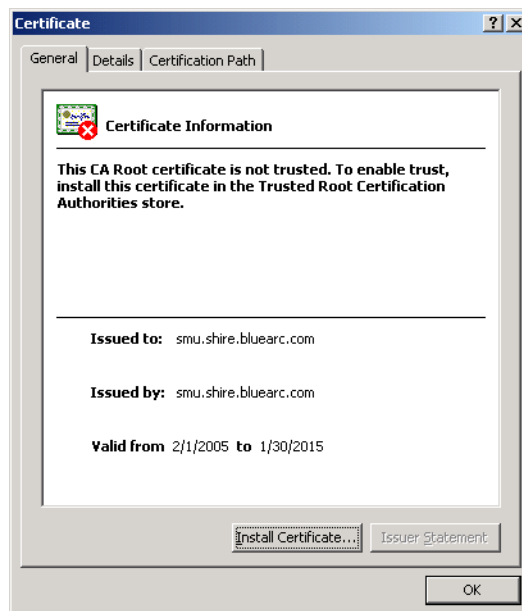
Accepting Self-Signed Certificates

If a self-signed certificate has been installed, users receive a security alert similar to the following when they first access the Web Manager over a secure connection:



Although users can click **Yes** to proceed, the alert reappears when they next run the Web Manager. To suppress the alert, users must choose to trust the certifying authority.

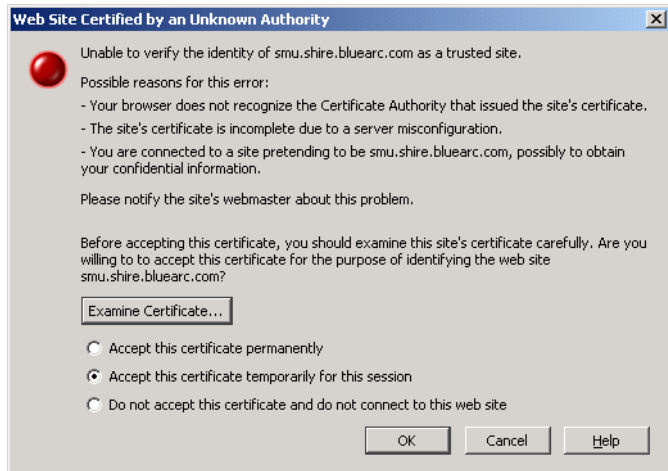
In Internet Explorer, from the Security Alert dialog box, click **View Certificate** to display the certificate:



Click **Install Certificate**, and then follow the on-screen instructions to install the certificate in the *Trusted Root Certification Authorities* store.

Mozilla-based browsers will see an alert message similar to the following. Selecting **Accept the**

certificate permanently will suppress the alert in future sessions.



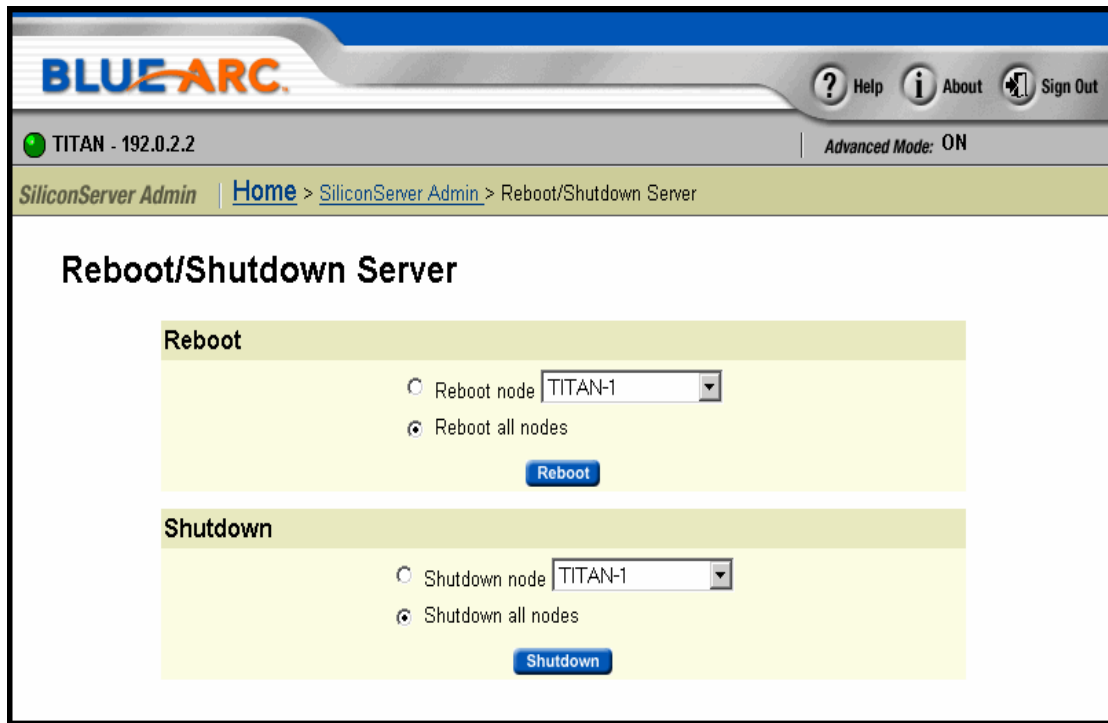
Shutting Down / Restarting the System

During normal operation, first shut down the server before turning off the power. The shutdown process flushes the data in the cache to disk as a safeguard against the risk of data loss.

Shutting Down / Resetting the Titan SiliconServer

To reset or shut down the server:

1. From the **Home** page, click **SiliconServer Admin**. Then, click **Reboot/Shutdown Server**. If configured as a cluster, all Cluster Nodes will reset or shut down.



2. Click **Reset** or **Shutdown**. Wait a few minutes for the system to shut down in an orderly fashion.



Note: After shutting down the server, disconnect it from the power supply.

To shut down the server in preparation for shipping:

Titan is fitted with dual redundant PSU modules, each of which contain a battery that is used to power the NVRAM in the event of loss of power to the server. These batteries should not be allowed to fully discharge, as this increases the chances of failure of the battery pack.



Note: Improper shutdown will result in the batteries supplying the NVRAM and if the server is left too long in this state, then the batteries will end up fully discharged.

To shutdown Titan properly before it is shipped, or before it is to be left un-powered for any length of time:

1. [Using the Command Line Interface](#), run the command "shutdown --ship". For more information, refer to *Using the Command Line Interface (CLI)*.
2. Power down the Titan SiliconServer by switching off both PSU modules.

3. Check that the NVRAM status LED on the FSB module is off. The server is now fully shutdown.
4. If the NVRAM status LED is on (either green or amber), then remove both PSU modules simultaneously for at least 10 seconds and replace.



Note: If the Titan SiliconServer fails to shutdown properly or to verify that the NVRAM has not entered the battery powered back up state when the PSUs are switched off, verify that both PSU modules are removed (refer to step 4).

Shutting Down / Restarting the SMU

If it is necessary to shutdown or restart the SMU, this screen provides three options. From the **SMU Administration** page, click **SMU Reset / Shutdown**.

The **Restart** button will restart the SMU *application* software, but not the SMU server. After the application has started up, the application will return to the login page.

The **Reboot** button will restart the SMU application and the server. It will close down all processes on the server and all connections from other hosts. When it has rebooted, which may take up to five minutes, the browser will return to the login page.

The **Shutdown** button will shutdown everything running on the SMU server, close all connections, and bring the SMU server to a state in which it may safely be powered down. In all cases, the SiliconServer(s) listed as *Managed Servers* will continue to function as normal.

Default Username and Password

	Username	Password
SMU Web Manager	<i>admin</i>	<i>bluearc</i>
SMU CLI	<i>manager</i>	<i>bluearc</i>
SMU Entering this specific username and password will provide unlimited access on the SMU.	<i>root</i>	<i>bluearc</i>
Titan SiliconServer (CLI)	<i>supervisor</i>	<i>supervisor</i>