

Storage System User Administration Guide

Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS
Modules

VSP N series

Hitachi NAS Platform

Release 13.9.6800

© 2011, 2019 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at <https://support.hitachivantara.com/en-us/contact-us.html>.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

| | |
|--|-----------|
| Preface..... | 4 |
| Related Documentation..... | 4 |
| Accessing product documentation..... | 7 |
| Getting help..... | 7 |
| Comments..... | 7 |
| Chapter 1: Administrator types and responsibilities..... | 9 |
| Read-only users..... | 10 |
| Adding an SMU user (an administrator)..... | 11 |
| Changing an SMU user profile..... | 16 |
| Chapter 2: Changing user passwords..... | 21 |
| Changing your own password..... | 21 |
| Changing another user's password..... | 22 |
| Chapter 3: SMU user authentication..... | 27 |
| Active Directory user authentication..... | 27 |
| Authenticating users from an Active Directory Forest..... | 28 |
| Using Transport Layer Security (TLS) with Active Directory authentication..... | 29 |
| Configuring Active Directory servers..... | 29 |
| Configuring Active Directory groups..... | 35 |
| User authentication through RADIUS servers (HNAS server only)..... | 40 |
| Displaying list of RADIUS servers..... | 41 |
| Adding a RADIUS server..... | 41 |
| Displaying details of RADIUS server..... | 43 |

Preface

This guide explains user management, including the different types of system administrators, their roles, and how to create and manage users. Note that some features apply only to individual platforms and may not be applicable to your configuration.

Virtual Storage Platform G400, G600, G800 and Virtual Storage Platform F400, F600, F800 storage systems can be configured with NAS modules to deliver native NAS functionality in a unified storage platform. The term 'NAS module' in this document also applies to VSP F series, VSP G series, and VSP N series. The unified VSP Gx00 models, VSP Fx00 models, and VSP N series models automatically form a two-node cluster in a single chassis upon installation, with no external cabling required.

Related Documentation

Release Notes provide the most up-to-date information about the system, including new feature summaries, upgrade instructions, and fixed and known defects.

Command Line References

The Command Line Reference provides information on the commands used to manage your system, and includes relevant information on the operation of your hardware and software. Depending on the model of your server or cluster node, refer to the Command Line Reference that is appropriate for your system.

- *NAS Module Server Command Line Reference*
- *Command Line Reference for models 4060, 4080, and 4100*
- *Command Line Reference for models 3080, 3090 and 4040*
- *Command Line Reference for models 5200 and 5300*

Administration Guides

- *System Access Guide* (MK-92HNAS014)—Explains how to log in to the system, provides information about accessing the NAS server/cluster CLI and the SMU CLI, and provides information about the documentation, help, and search capabilities available in the system.
- *Server and Cluster Administration Guide* (MK-92HNAS010)—Provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading software, monitoring servers and clusters, and backing up and restoring configurations.
- *Storage System User Administration Guide* (MK-92HNAS013)—Explains user management, including the different types of system administrator, their roles, and how to create and manage these users.
- *Network Administration Guide* (MK-92HNAS008)—Provides information about the server's network usage, and explains how to configure network interfaces, IP addressing, name and directory services.
- *File Services Administration Guide* (MK-92HNAS006)—Explains about file system formats, and provides information about creating and managing file systems, and enabling and configuring file services (file service protocols).
- *Data Migrator Administration Guide* (MK-92HNAS005) —Provides information about the Data Migrator feature, including how to set up migration policies and schedules.
- *Storage Subsystem Administration Guide* (MK-92HNAS012)—Provides information about managing the supported storage subsystems (RAID arrays) attached to the server/cluster. Includes information about tiered storage, storage pools, system drives (SDs), SD groups, and other storage device related configuration and management features and functions.
- *Snapshot Administration Guide* (MK-92HNAS011)—Provides information about configuring the server to take and manage snapshots.
- *Replication and Disaster Recovery Administration Guide* (MK-92HNAS009)—Provides information about replicating data using file-based replication and object-based replication, provides information on setting up replication policies and schedules, and using replication features for disaster recovery purposes.
- *Antivirus Administration Guide* (MK-92HNAS004)—Describes the supported antivirus engines, provides information about how to enable them, and how to configure the system to use them.
- *Backup Administration Guide* (MK-92HNAS007)—Provides information about configuring the server to work with NDMP, and making and managing NDMP backups.



Note: For a complete list of Hitachi NAS open source software copyrights and licenses, see the *System Access Guide*.

Hardware References

- *Hitachi NAS Platform 3080 and 3090 G2 Hardware Reference* (MK-92HNAS017) — Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- *Hitachi NAS Platform and Hitachi Unified Storage Series 4000 Hardware Reference* (MK-92HNAS030)—Provides an overview of the Hitachi NAS Platform Series 4000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components
- *Hitachi NAS 5000 Series Hardware Reference* MK-92HNAS089—Provides an overview of the Hitachi NAS Platform Series 5000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.
- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.

Best Practices

- *Hitachi NAS Platform Best Practices Guide for NFS with VMware vSphere* (MK-92HNAS028)—This document covers best practices specific to using VMware vSphere with the Hitachi NAS platform.
- *Hitachi NAS Platform Deduplication Best Practice* (MK-92HNAS031)—This document provides best practices and guidelines for using deduplication.
- *Hitachi NAS Platform Best Practices for Tiered File Systems* (MK-92HNAS038)—This document describes the Hitachi NAS Platform feature that automatically and intelligently separates data and metadata onto different Tiers of storage called Tiered File Systems (TFS).
- *Hitachi NAS Platform Data Migrator to Cloud Best Practices Guide* (MK-92HNAS045)—Data Migrator to Cloud allows files hosted on the HNAS server to be transparently migrated to cloud storage, providing the benefits associated with both local and cloud storage.
- *Best Practices for Hitachi NAS Universal Migrator* (MK-92HNAS047)—The Hitachi NAS Universal Migrator (UM) feature provides customers with a convenient and minimally disruptive method to migrate from their existing NAS system to the Hitachi NAS Platform. The practices and recommendations outlined in this document describe how to best use this feature.
- *Hitachi Data Systems SU 12.x Network File System (NFS) Version 4 Feature Description* (MK-92HNAS056)—This document describes the features of Network File System (NFS) Version 4.
- *Hitachi NAS HDP Best Practices* (MK-92HNAS057)—This document lists frequently asked questions regarding the use of Hitachi Dynamic Provisioning.
- *Hitachi Multi-tenancy Implementation and Best Practice Guide* (MK-92HNAS059)—This document details the best practices for configuring and using Multi-Tenancy and related features, and EVS security.
- *Hitachi NAS Platform HDP Best Practices* (MK-92HNAS063)—This document details the best practices for configuring and using storage pools, related features, and Hitachi Dynamic Provisioning (HDP).

- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.
- *NAS Platform ICC with Cisco Nexus Reference Guide* (MK-92HNAS085)—This document describes how to configure Cisco Nexus series switches for use as an ICC (intra-cluster communication) switch.
- *File System Snapshots Operational Best Practice* (MK-92HNAS068)—This document provides operational guidance on file system snapshots.
- *Virtual Infrastructure Integrator for Hitachi Storage Platforms Operational Best Practice* (MK-92HNAS069)—This document provides operational guidance on Hitachi Virtual Infrastructure Integrator for the HNAS platform.
- *Hitachi NAS Platform Replication Best Practices Guide* (MK-92HNAS070)—This document details the best practices for configuring and using HNAS Replication and related features.
- *Hitachi NAS Platform to Hitachi Virtual Storage Platform Unified Gx00 Models Migration Guide* (MK-92HNAS075)—This best practice guide describes how to perform a data-in-place migration of the Hitachi NAS Platform and Virtual Storage Platform (VSP) Gx00 File solution to the VSP Gx00 platform.

Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: <https://knowledge.hitachivantara.com/Documents>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The [Hitachi Vantara Support Website](https://support.hitachivantara.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

[Hitachi Vantara Community](https://community.hitachivantara.com) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Administrator types and responsibilities

This section describes the types of NAS storage system administrators and defines their expected roles in managing the system and the associated storage subsystems.

- **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access.
- **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.

Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.

- **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices.

Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules.

- **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator.

Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components.

All administrators can connect to the NAS storage system through NAS Manager, the browser-based management utility provided by the system management unit (SMU). Additionally, Global Administrators on an external or virtual SMU can connect to the SMU command line interface (CLI). SMU CLI access is not available on an embedded SMU or a NAS module SMU.

Read-only users: The above roles (when defined for local users or Active Directory groups) can be modified by making them read-only. A read-only user has permission to view most pages of the NAS Manager; however, they are not generally allowed to perform any actions on the NAS Manager that would trigger a system or configuration change.



Note: Server Administrators, Storage Administrators, and Server+Storage Administrators cannot access all of the NAS Manager pages that a Global Administrator can access.

Read-only users

Local users and Active Directory groups can now be given read-only access. A read-only user has permission to view most pages of the NAS Manager; however, they are not generally allowed to perform any actions on the NAS Manager that would trigger a system or configuration change. Based on their defined role, an individual user may or may not perform specific tasks, such as viewing, creating, or modifying files and data. A read-only user may not create, add, or delete files and file systems. Where such actions are not permitted, the corresponding buttons (such as **Add** and **Create**) on the viewed page are disabled. A read-only user retains the scope of their role, such as Global, Storage, Server, or Server plus Storage, and the read-only attribute will not limit which configurations the user may access (except in cases where access to a specific configuration is explicitly defined as limited). All links appropriate to each role are visible on the pages but may be disabled. A global, read-only user can see all configurations. If the system has determined that the logged on user, either a local user or an Active Directory user, has read-only access, the text "read-only" is appended to the user's name in the top-right corner of the page.

Read-only users can view the **Details** pages and see the objects on those pages, but buttons that submit changes, such as the **OK** button, are disabled. Read-only users may use the **Cancel** button on a **Details** page to navigate away from the page.



Note: Once a user is assigned the read-only attribute, their status as read-only may not be changed. To change a user's status from read-only, it is necessary to delete the user or the Active Directory group and re-add them with new read/write privileges.

Read-only user restrictions

Read-only users may not:

- Have CLI access
- Be defined in RADIUS
- Clear or refresh any SMU cache (such as CIFS shares)
- Download data to a local file
- Download diagnostics or configuration data such as quotas and backups
- Browse directories on NAS file systems
- Use any "refresh buttons or links" in a page, but all pages can be refreshed using the F5 shortcut

Inaccessible pages

The following NAS Manager pages are not visible to read-only users:

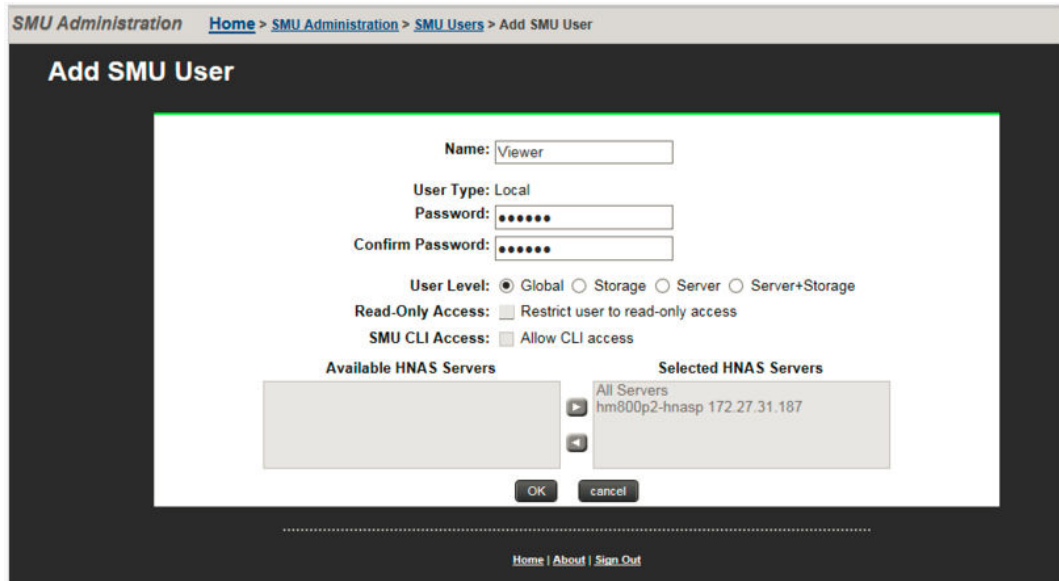
- Send Test Event
- Download diagnostics
- Server Setup Wizard
- Clone Settings
- EVS Migration
- Cluster Wizard
- Reboot Server
- Backup & Restore
- Upgrade Firmware
- File System Relocation
- SMU Setup Wizard
- SMU Backup & Restore
- SMU Shutdown / Restart
- SMU Upgrade

Adding an SMU user (an administrator)


Use NAS Manager to add SMU user accounts for HNAS servers. For systems with NAS modules, use the maintenance utility or an external NAS Manager to create and manage user accounts.



Procedure

1. Navigate to **Home > SMU Administration > SMU Users** to display the **SMU Users** page.
2. Click **add** to display the **Add SMU User** page:



| Field/Item | Description |
|------------|---|
| Name | <p>The name of the new user account. This name will be requested when logging in to the SMU. The rules for user names are:</p> <ul style="list-style-type: none"> ■ For Global administrators only, if the user will access the SMU through the CLI, the user name: <ul style="list-style-type: none"> • Must start with a letter or an underscore, and may consist of up to 31 alphanumeric characters and the underscore (_) and the hyphen (-). • Cannot match certain special purpose names: root, manager, postgres, nobody, or nfsnobody. • Cannot match certain special purpose user ID numbers: for example, those with uid less than 502. ■ For all types of administrators, if the user will access the SMU only through NAS Manager, the user name may consist of alphanumeric characters and/or the underscore (_), the hyphen (-), the equal sign (=), parentheses " (" or ") ", brackets ([or]), the pound sign (#) and the exclamation point (!). ■ Supervisor is a reserved system user name. It is not available as a new user name. |

| Field/Item | Description |
|------------------|--|
| |  Note: If you are using RADIUS realms, and the global administrator will access the SMU using both NAS Manager and the CLI, use the underscore (<code>_</code>) to combine the user name and the realm: for example, <code>johnsmith_realm2</code> . If the global administrator will access the SMU using only NAS Manager, you can use the at sign (<code>@</code>) to combine the user name and the realm: for example, <code>johnsmith@realm3</code> . |
| User Type | <p>The user type is either local or RADIUS.</p> <ul style="list-style-type: none"> ▪ Local users are those whose passwords are locally defined and authenticated in the SMU. ▪ RADIUS users are those whose passwords are defined and authenticated in an external RADIUS servers. The RADIUS administrator must add a user name and password to all RADIUS servers. |
| Password | <p>Enter the password that will be used when this user account logs in. The password cannot exceed 256 characters.</p> <p>This field only applies when the User Type is selected to Local. It does not apply when the RADIUS User Type is selected.</p> |
| Confirm Password | <p>Confirm the password entered in the previous field by entering it in again. Only applies when the Local User type is selected.</p> |
| User Level | <p>Specify the level for the new administrator that you are creating. You can select any one of the following:</p> <ul style="list-style-type: none"> ▪ Global Administrators can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server +Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access. ▪ Storage Administrators manage storage devices, as specified in the administrator profile created by the Global Administrator. Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users. |

| Field/Item | Description |
|---|---|
| | <ul style="list-style-type: none"> ■ Server Administrators manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices. Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules. ■ Server+Storage Administrators manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator. Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components. <div data-bbox="651 877 1393 1024" style="background-color: #e0f2f1; padding: 5px;"> <p> Note: Server Administrators, Storage Administrators, and Server+Storage Administrators cannot access all of the NAS Manager pages that a Global Administrator can access.</p> </div> |
| Read-Only User | <p>Defines the user as read-only. A read-only user may be given Global, Server, Storage or Server+Storage access. Based on their defined role, an individual user may or may not perform specific tasks, such as viewing, creating, or modifying files and data. A read-only user has permission to view most pages of the NAS Manager; however, they are not generally allowed to perform any actions that would trigger a system or configuration change.</p> <div data-bbox="651 1318 1393 1423" style="background-color: #e0f2f1; padding: 5px;"> <p> Note: Read-only users can not access the CLI, and a user with CLI access may not be read-only. If either of these options is checked, the other one is disabled.</p> </div> |
| SMU CLI Access (for Global Administrators only) | <p>If the administrator is allowed to log in and access the SMU CLI of an external SMU, select the SMU CLI Access check box.</p> |
| Available Managed Servers | <p>For Server administrators, Storage administrators, and Server+Storage administrators, lists the servers managed by the SMU to which the administrator has not yet been given management privileges. Not available for Global administrators, because Global administrators are allowed to manage all storage and all servers.</p> |

| Field/Item | Description |
|--------------------------|---|
| Selected Managed Servers | <p>For Server administrators, lists the servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers. Not available for Global administrators, because Global administrators are allowed to manage all storage and all servers.</p> <p>For Storage administrators, lists servers that have attached storage that the administrator can manage. Note that a Storage administrator cannot manage these servers, only the storage attached to these servers.</p> <p>For Server+Storage administrators, lists servers that the administrator can manage. The Server+Storage administrator can also manage the storage attached to these servers.</p> |

3. Enter the user name for the new administrator in the **Name** field.
4. Specify if the administrator login is authenticated locally (by the SMU) or by a RADIUS server by selecting the appropriate **User Type**.



Note: If you are authenticating this user through a RADIUS server, the **Password** and **Confirm Password** fields are not available, and you should skip the next step. You must enter the user passwords into the RADIUS server using the tools available for that server.

5. If the **User Type** is local, specify the initial login password for the new administrator by filling in the **Password** and the **Confirm Password** fields.
6. Specify the user level for the new administrator that you are creating. You can select one of the following:
 - **Global**
 - **Storage**
 - **Server**
 - **Server+Storage**
7. For Global Administrators only, if the administrator is allowed to log in and access the SMU command line interface (CLI) of an external SMU, select the **SMU CLI Access** check box.
8. Using the **Available Servers** and the **Selected Servers** lists, specify the servers the administrator can access or the servers with the storage the administrator can manage.
 - To grant management privileges for a server or the storage attached to a server, move the server from the **Available Servers** list to the **Selected Servers** list.
 - To revoke management privileges for a server or the storage attached to a server, move the server from the **Selected Servers** list to the **Available Servers** list.
 - To move the server between the **Available Servers** and the **Selected Servers** lists, select the server, and use the arrow buttons between the lists.

9. Review the profile, and verify that it is correct.
 - If the profile is correct, click **OK** to save and enable the user profile, and then return to return to the **SMU Users** page.
 - To return to the **SMU Users** page without saving the profile, click **back**.

Changing an SMU user profile

Use NAS Manager to manage SMU user accounts for HNAS servers. For systems with NAS modules, use the maintenance utility or an external NAS Manager to manage user accounts.

Procedure

1. Navigate to **Home > SMU Administration > SMU Users** to open the **SMU Users** page.
2. Click **details** to display the **SMU User Details** page for the user whose profile you want to modify.

The screenshot displays the 'SMU User Details' configuration page. At the top, a breadcrumb trail reads 'SMU Administration > Home > SMU Administration > SMU Users > SMU User Details'. The main content area is titled 'SMU User Details' and contains the following fields and options:

- Name:** A text input field containing 'viewer'.
- User Type:** A dropdown menu set to 'Local'.
- Password:** A text input field with a note: 'Leave empty to retain existing password.'
- Confirm Password:** A text input field.
- User Level:** Radio buttons for 'Global' (selected), 'Storage', 'Server', and 'Server+Storage'.
- Read-Only Access:** A checkbox labeled 'Restrict user to read-only access'.
- SMU CLI Access:** A checkbox labeled 'Allow CLI access'.
- Available HNAS Servers:** An empty list box.
- Selected HNAS Servers:** A list box containing 'All Servers' and 'hm800p2-hnasp 172.27.31.187'.

At the bottom of the form are 'OK' and 'cancel' buttons. Below the form, there is a footer with links: 'Home | About | Sign Out'.

| Item/Field | Description |
|-------------------------------|--|
| Name | Administrator's user name. Cannot be changed. |
| User Type | Describes if the user is authenticated by the SMU itself (local users), or if the user is authenticated by a RADIUS server. |
| Password and Confirm Password | <p>For users authenticated by the SMU only (local users). These fields do not apply for users authenticated by a RADIUS server.</p> <p>The password for the user. Characters are hidden, and the exact same password must be entered in both fields. The password cannot exceed 256 characters.</p> |
| User Level | <p>Displays the user level or type of administrative role.</p> <ul style="list-style-type: none"> ▪ Global Administrators can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access. ▪ Storage Administrators manage storage devices, as specified in the administrator profile created by the Global Administrator. <p>Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.</p> |

| Item/Field | Description |
|------------------------|---|
| | <ul style="list-style-type: none"> ▪ Server Administrators manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices. Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules. ▪ Server+Storage Administrators manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator. Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components. ▪ If the User Type is Local, you can modify the password. ▪ If the User Type is RADIUS, you cannot modify the password, because the password is managed on RADIUS servers. RADIUS users cannot be defined as read-only. ▪ If the User Level is Global, you can select or clear the Allow CLI Access check box. ▪ If the User Level is Storage, Server, or Server+Storage, you can add or remove servers from the user's scope of management. <p>Global users implicitly have access to manage all servers and storage. Non-global users cannot be given CLI access.</p> <p>You cannot change the User Type or User Level of a user. If such a change is needed, delete the old user and create a new user.</p> |
| Read-Only Access | Indicates if a user is defined as read-only, or not. When displaying the details of an existing user, the read-only attribute is shown but cannot be modified. To change the read-only attribute, it is necessary to delete the user and then re-add them. |
| SMU CLI Access | For global administrators only, when the check box is selected, the administrator can access the SMU using the CLI as well as NAS Manager. |
| Available HNAS Servers | Not available for global administrators, because global administrators are allowed to manage all storage and all servers. |

| Item/Field | Description |
|-----------------------|---|
| | <p>For server administrators, storage administrators, and server+storage administrators, lists the HNAS servers managed by the SMU to which the administrator has not yet been give management privileges.</p> <p>The "All Servers" entry is used to allow privileges to all servers managed by the SMU.</p> |
| Selected HNAS Servers | <p>Not available for global administrators, because global administrators are allowed to manage all storage and all servers.</p> <p>For server administrators, lists the HNAS servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers.</p> <p>For storage administrators, lists HNAS servers that have attached storage that the administrator can manage. Note that a storage administrator cannot manage these servers, only the storage attached to these servers.</p> <p>For server+storage administrators, lists HNAS servers that the administrator can manage. The server+storage administrator can also manage the storage attached to these servers.</p> |
| OK | Saves the currently defined user profile and returns to the SMU Users page. |
| Cancel | Returns to the SMU Users page without saving the profile. |

3. Edit the SMU user password.



Note: For users authenticated by the SMU only (local users), not available for users authenticated by a RADIUS server.

To edit the user's password, type the new password in the **Password** and **Confirm Password** fields.

4. For global administrators only, allow or disallow SMU CLI access.

When the check box is selected, the administrator can access the SMU by using the CLI as well as NAS Manager.

5. Specify server and/or storage management rights.

- To grant management privileges for a server or the storage attached to a server, move the server from the **Available Servers** list to the **Selected Servers** list.
- To revoke management privileges for a server or the storage attached to a server, move the server from the **Selected Servers** list to the **Available Servers** list.
- To move the server between the **Available Servers** and the **Selected Servers** lists, select the server, and use the arrow buttons between the lists.

6. Click **OK** to save the profile and return to the **SMU Users** page.

Chapter 2: Changing user passwords

Any logged in user can change their own password. A global administrator can also change the password of any user, whether the user is currently logged in or not.



Note: If the user is authenticated through a RADIUS server, you cannot change the password using NAS Manager or the SMU CLI. You must change the password using the tools and utilities of the RADIUS server.

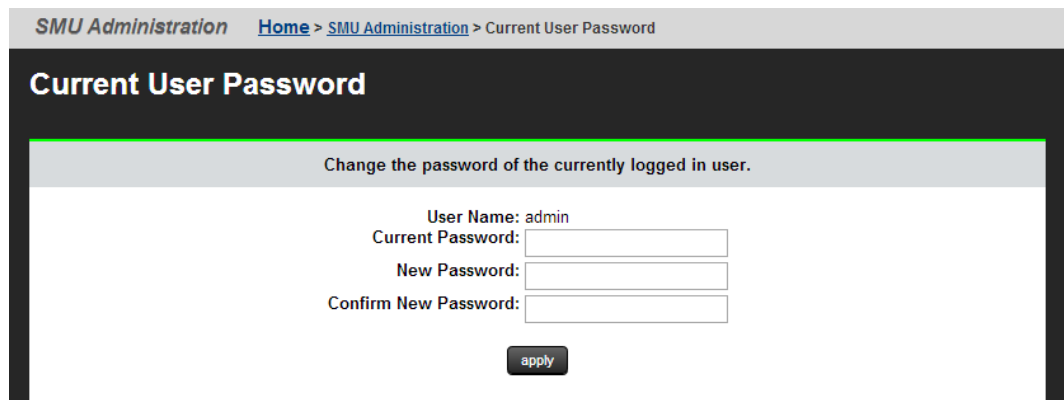
Changing your own password

You can use NAS Manager to change your own password. If your account is authenticated through a RADIUS server, however, your password must be changed using the tools and utilities of the RADIUS server.

- For HNAS servers, use NAS Manager or the SMU CLI to change your password.
- For systems with NAS modules, use an external NAS Manager or the maintenance utility to change your password.

Procedure

1. Navigate to **Home > SMU Administration > Current User Password** to display the **Current User Password** page.



The following table describes the fields on this page:

| Field/Item | Description |
|----------------------|--|
| User Name | Displays your user login name (cannot be changed). |
| Current Password | Displays a series of dots representing the currently specified password (the actual password cannot be displayed). |
| New Password | The new password. The password cannot exceed 256 characters. |
| Confirm New Password | The new password again. Must be exactly the same as what you entered in the New Password field. |
| apply | Saves the new password. |

2. Enter your current password in the **Current Password** field.
If you have forgotten your password, contact a global administrator and ask them to give you a new password. (Passwords are stored in an encrypted form, and are not retrievable or visible by anyone. If a user forgets their password, they must be given a new password, which they can then change.)
3. Enter your new password in the **New Password** field.
4. Enter the new password again in the **Confirm New Password** field.
5. When finished, click **apply** to save the new password.

Changing another user's password

A global administrator can change the password of any user. If the user is authenticated through a RADIUS server, however, the password must be changed using the tools and utilities of the RADIUS server.

- For HNAS servers, use NAS Manager or the SMU CLI to change the user password.
- For systems with NAS modules, use an external NAS Manager or the maintenance utility to change the user password.

Procedure

1. Navigate to **Home > SMU Administration > SMU Users** to display the **SMU Users** page.
2. Click **details** to display the **SMU User Details** page.

SMU Administration [Home](#) > [SMU Administration](#) > [SMU Users](#) > SMU User Details

SMU User Details

Name:

User Type: Local

Password: *Leave empty to retain existing password.*

Confirm Password:

User Level: Global Storage Server Server+Storage

Read-Only Access: Restrict user to read-only access

SMU CLI Access: Allow CLI access

Available HNAS Servers

Selected HNAS Servers

[Home](#) | [About](#) | [Sign Out](#)

| Item/Field | Description |
|-------------------------------|--|
| Name | Administrator's user name. Cannot be changed. |
| User Type | Describes if the user is authenticated by the SMU itself (local users), or if the user is authenticated by a RADIUS server. |
| Password and Confirm Password | <p>For users authenticated by the SMU only (local users). These fields do not apply for users authenticated by a RADIUS server.</p> <p>The password for the user. Characters are hidden, and the exact same password must be entered in both fields. The password cannot exceed 256 characters.</p> |
| User Level | <p>Displays the user level or type of administrative role.</p> <ul style="list-style-type: none"> ▪ Global Administrators can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access. ▪ Storage Administrators manage storage devices, as specified in the administrator profile created by the Global Administrator. <p>Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.</p> |

| Item/Field | Description |
|------------------------|---|
| | <ul style="list-style-type: none"> ▪ Server Administrators manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices. Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules. ▪ Server+Storage Administrators manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator. Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components. ▪ If the User Type is Local, you can modify the password. ▪ If the User Type is RADIUS, you cannot modify the password, because the password is managed on RADIUS servers. RADIUS users cannot be defined as read-only. ▪ If the User Level is Global, you can select or clear the Allow CLI Access check box. ▪ If the User Level is Storage, Server, or Server+Storage, you can add or remove servers from the user's scope of management. <p>Global users implicitly have access to manage all servers and storage. Non-global users cannot be given CLI access.</p> <p>You cannot change the User Type or User Level of a user. If such a change is needed, delete the old user and create a new user.</p> |
| Read-Only Access | Indicates if a user is defined as read-only, or not. When displaying the details of an existing user, the read-only attribute is shown but cannot be modified. To change the read-only attribute, it is necessary to delete the user and then re-add them. |
| SMU CLI Access | For global administrators only, when the check box is selected, the administrator can access the SMU using the CLI as well as NAS Manager. |
| Available HNAS Servers | Not available for global administrators, because global administrators are allowed to manage all storage and all servers. |

| Item/Field | Description |
|-----------------------|---|
| | <p>For server administrators, storage administrators, and server +storage administrators, lists the HNAS servers managed by the SMU to which the administrator has not yet been give management privileges.</p> <p>The "All Servers" entry is used to allow privileges to all servers managed by the SMU.</p> |
| Selected HNAS Servers | <p>Not available for global administrators, because global administrators are allowed to manage all storage and all servers.</p> <p>For server administrators, lists the HNAS servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers.</p> <p>For storage administrators, lists HNAS servers that have attached storage that the administrator can manage. Note that a storage administrator cannot manage these servers, only the storage attached to these servers.</p> <p>For server+storage administrators, lists HNAS servers that the administrator can manage. The server+storage administrator can also manage the storage attached to these servers.</p> |
| OK | Saves the currently defined user profile and returns to the SMU Users page. |
| Cancel | Returns to the SMU Users page without saving the profile. |

3. Enter the new password in the **Password** field.
4. Enter the new password again in the **Confirm Password** field.
5. When finished, click **OK** to save the new password.

Chapter 3: SMU user authentication

When an SMU user administrator attempts to log in, the user ID/password combination is sent to the SMU for authentication. For the SMU, authentication means testing the user ID and password pair, to see if the supplied password matches the stored password for the supplied user ID. Depending on the SMU configuration and the supplied user ID, the SMU may authenticate the user itself (locally), it may authenticate the user through a RADIUS server, or it may authenticate the user through Active Directory. After authorization, the SMU allows the user to perform actions allowed by the user's profile.

Active Directory users are assigned full access rights to the SMU functionality.

For *local and RADIUS* users the user profile details are specified when the user account is created.

The user profile:

- Indicates if the user is to be authenticated locally, or through a RADIUS server.
- Specifies the user's access (privilege) level, meaning it specifies if the user is a:
 - Global administrator.
 - Storage administrator.
 - Server administrator.
 - Server+Storage administrator.
- Specifies the servers the user is allowed to access.
- Specifies if the user has CLI access (for RADIUS and Local Users).

Active Directory user authentication

Active Directory is an LDAP-compliant hierarchical database of objects. It is very popular in enterprise environments and is becoming a de facto standard for user authentication.

After Active Directory connection settings and groups have been configured for the SMU, it will allow logins from enabled users who supply their Active Directory name and password. This is typically the same name and password that the user would use to log into Windows and other enterprise applications. Unlike SMU local and RADIUS user names, Active Directory user names are case-insensitive. Active Directory passwords are case-sensitive and cannot be changed from the SMU; they are maintained in the Active Directory server. NAS Manager accepts user names in the following formats:

| Description | Format |
|--|-----------------------------------|
| User logon name (pre-Windows 2000) | administrator |
| NetBIOS domain name and user logon name (pre-Windows 2000) (*) | COMPANY\administrator |
| User Principal Name | administrator@support.company.com |

(*) Not supported with the SMU CLI access.

Instead of maintaining a separate set of user details, the administrator can use an Active Directory enterprise user database. Active Directory groups can be granted access to the SMU. Then, AD users that belong to these groups, can log into the SMU using their usual name and password.

Groups of Active Directory users can have their access restricted to certain roles. For example, giving an Active Directory group a 'server' level access, will restrict all the users that belong to such group to be able to only manage HNAS servers. They won't be able, for example, to make any changes related to SMU administration.

Although the SMU supports RADIUS and Active Directory for external authentication, they are mutually exclusive; it is not possible to have them both configured for external authentication at the same time.

When a login attempt is made, the SMU first tries to authenticate the credentials as a local user. If that fails, and Active Directory is configured, they are authenticated as an Active Directory user.

Active Directory authentication requests are sent to servers in the configured sequential order. If a successful connection cannot be made to the first server or a referral error is returned, it attempts to contact the second server and so on. When a connection is made and an authentication response received (either positive or negative) it is treated as definitive. It does not then contact further servers because all servers are assumed to belong to the same Active Directory forest.

Authenticating users from an Active Directory Forest

For user authentication the SMU supports **Active Directory Forest** by using Active Directory **Global Catalog** feature. When Global Catalog is configured, all Active Directory groups, which are granted access to the SMU directly and indirectly (via the chain of membership), must have 'Universal' scope. This guarantees that Active Directory group membership details, required to verify user's access, are available to the SMU via Global Catalog connection.

Using Transport Layer Security (TLS) with Active Directory authentication

TLS is a cryptographic protocol which provides security between applications over a network.

For Active Directory authentication, the SMU supports up to TLS 1.2. It negotiates with the domain controller to use the highest version of TLS which is common to both.

Configuring Active Directory servers

Global Administrators can provide information to configure, modify, and list Active Directory (AD) servers for authentication on the **Active Directory Servers** page.

Before you begin

To enable Active Directory, the SMU administrator needs to know the following information:

- The name of the domain or forest from which the Active Directory users and groups will access the SMU.
- The LDAP distinguished name and password of an Active Directory user that has read access to users and groups on the Active Directory servers. This is referred to as the Search User. The user can search for users or groups under the supplied base distinguished name.
- The addresses of one or more Active Directory servers that maintain the users and groups for the domain or forest. Each AD server must be from the same domain unless Global Catalog is enabled in which case each AD server must be from the same Forest. If DNS servers have been configured for the SMU, then when a Forest DNS name or Domain DNS name is set in the **find servers** dialogue box, the SMU should be able to automatically discover these server addresses via the **find** button in the **find servers** dialogue box. SRV records must be setup for **find servers** to find the Active Directory servers.
- The Active Directory group or groups whose members are to be given the right to log into the SMU. To guarantee that membership will work properly with any AD server when Global Catalog is enabled, all the groups must be Universal groups.
- If RADIUS was previously in use and it is to be replaced by Active Directory, then the RADIUS configuration must first be removed before Active Directory can be configured. This is done from the **Home>SMU Administrator>RADIUS Servers** page by clicking the **remove all settings** button. No RADIUS user will be able to log into the SMU after this is done.



Note: On the NAS system, local users and Active Directory groups can be given read-only access. A read-only user has permission to view most pages of the NAS Manager; however, they are not generally allowed to perform any actions on the NAS Manager that would create a system or configuration change.

Procedure

1. Navigate to **Home > SMU Administrator** to display the **Active Directory Servers** page.
2. To authenticate with a Forest rather than with a Domain, mark the Global Catalog checkbox. As a result, the Global Catalog ports 3268 or 3269 will be used in all AD connections initiated by SMU.

Active Directory Servers

Connection

Global Catalog

Connection Port

LDAP port 389 unencrypted

LDAP port 389 using TLS

LDAPS port 636

Connections

Connection Attempts: per server

Timeout for Connection Attempts: seconds

Search Credentials

Distinguished Name:

The account used for searching the directory. Example: cn=SearchUser,cn=Users,dc=example,dc=com

Password:

User Search

Base Distinguished Name: ▼ Add

Include Entire Directory

▲ Move Up
✕ Remove
▼ Move Down

The SMU will search for users under the directory tree specified by the Base Distinguished Name.
Example: dc=example,dc=com

Group Search

Base Distinguished Name: Use User Search Settings

▼ Add

Include Entire Directory

▲ Move Up
✕ Remove
▼ Move Down

The SMU will search for groups under the directory tree specified by the Base Distinguished Name.
Example: dc=example,dc=com

Servers

IP Address or DNS Name: find servers or ▼ Add

▲ Move Up
✕ Remove
▼ Move Down

Groups

Groups with access to the SMU: No groups.

The following table describes the fields on this page:

| Field/Item | Description |
|---------------------------------|--|
| Connection | |
| Global Catalog | To connect to an Active Directory Forest, the Global Catalog box must be checked. |
| Connection port | <p>The port and encryption method to use when connecting to an Active Directory server.</p> <p>Non-Global Catalog options are:</p> <ul style="list-style-type: none"> ▪ port 389 unencrypted ▪ port 389 encrypted using START TLS ▪ port 636 encrypted using LDAPS <p>Global Catalog options are:</p> <ul style="list-style-type: none"> ▪ port 3268 unencrypted ▪ port 3268 encrypted using START TLS ▪ port 3269 encrypted using LDAPS |
| Connections | |
| Connection Attempts | The maximum number of times that the SMU attempts to connect to each Active Directory server when a connection fails. |
| Timeout for Connection Attempts | The maximum time in seconds that the SMU waits when connecting to an Active Directory server before failing with a time out. |
| Search Credentials | |
| Distinguished Name | The LDAP distinguished name for a user that has search capabilities. |
| Password | The password for the search user. |
| User Search | |
| Base Distinguished Name | The root of an Active Directory subtree of entries from where the SMU searches for users. The maximum number of Base Distinguished Names is 5. During authentication, all Base Distinguished Names are scanned. The order can be changed with Move Up and Move Down buttons. |
| Include Entire Directory | If checked, the entire Active Directory forest will be searched for user details. During authentication, all the Base Distinguished Names are scanned with the Entire |

| Field/Item | Description |
|--------------------------|--|
| | Directory being the last. This option is only available when Global Catalog is configured. |
| Group Search | |
| Use User Search Settings | If checked, the Base Distinguished Names from User Search section will be used. |
| Base Distinguished Name | The root of an Active Directory subtree of entries from where the SMU searches for groups. The maximum number of Base Distinguished Names is 5. This list is used by the find group utility which searches groups in the Active Directory domain or forest. The utility scans Base Distinguished Names in the order they appear in the list. The order can be changed with Move Up and Move Down buttons. |
| Include Entire Directory | If checked, the Entire Directory is scanned after all configured Base Distinguished Names. This option is only available when Global Catalog is configured. |
| Servers | |
| IP Address or DNS Name | The address of one or more Active Directory servers for the domain. Each AD server must be from the same domain unless Global Catalog is enabled in which case each AD server must be from the same Forest. The maximum number of servers is 20. |
| find servers | A utility which queries DNS to show the list of available Active Directory servers for the domain or forest. The NAS Manager lists the Active Directory servers in order of their response time (quickest first). If you add them in the same order, the SMU attempts to authenticate users against the fastest responding servers first. |
| Forest DNS Name | When Global Catalog is configured, the find servers utility expects the DNS name of the Active Directory Forest. Clicking on find button, will find all the Active Directory servers that support Global Catalog. |
| Domain DNS Name | When Global Catalog is not configured, the utility expects the DNS name of the Active Directory Domain. Clicking on find button, will find all the Active Directory servers in that Domain. |
| Add | Add an Active Directory server after you have entered its fully qualified domain name or IP address. |
| Move Up | If there is more than one server, use these buttons to prioritize the list. |

| Field/Item | Description |
|-------------------------------|---|
| Move Down | |
| Remove | Remove a server from the list. |
| apply | Submit the page and save all the settings to the SMU database. |
| Groups | |
| Groups with access to the SMU | Shows groups with access to the SMU. Active Directory users who belong to these groups can access the SMU. |
| Modify groups | Click to go to the Active Directory Groups page, where you can add groups. |
| Actions | |
| remove all settings | Removes all Active Directory server settings, including server list, connection settings, search user credentials and groups. After this action, Active Directory users can no longer log into the SMU. |

3. Configure the following settings for the connections as required:
 - **Connection Port** - The port and encryption method to use when connecting to an Active Directory server. The options are: 'LDAP port 389 unencrypted', 'LDAP port 389 using TLS ' and 'LDAPS port 636'. In Global Catalog configuration, the options are: 'LDAP port 3268 unencrypted', 'LDAP port 3268 using TLS' and 'LDAPS port 3269'. The default value is 'LDAP port 389 using TLS' and for Global Catalog 'LDAP port 3268 using TLS'.
 - **Connection Attempts** - The maximum number of times that the SMU attempts to connect to each Active Directory server when a connection fails. The default value is four attempts.
 - **Timeout for Connection Attempts** - The maximum time in seconds that the SMU waits when connecting to an Active Directory server before failing with a timeout. The default value is 60 seconds.
4. Enter the **Distinguished Name**.
This is the Distinguished Name of the Search User, an existing user that has permission to access Active Directory. An Search User DN would typically contain common name (cn) and possibly organization unit (ou) attributes as well as the domain components. The domain components should match those used in the Base Distinguished Name. An example Search User DN is "*cn=ldapguest,cn=users,dc=example,dc=com*".
5. Enter the **Password** of the Search User (an existing user that may access the directory).

6. Enter the **Base Distinguished Names for User Search**

These names must be entered in LDAP distinguished name (DN) format which consists of a sequence of "attribute=value" pairs separated by comma. The Base Distinguished Name should contain the domain component (dc) attributes for the organization's domain or forest. For the domain *example.com* it would be "*dc=example,dc=com*". The name may also contain organization unit (ou) attributes. These Base Distinguished Names will be used to search for user details during authentication. No more than 5 Base Distinguished Names can be configured.

When Global Catalog is configured, to search in the entire Active Directory forest, click on **Include Entire Directory** checkbox.

7. Enter the **Base Distinguished Names for Group Search**

By default, this is set to the same values as the Base Distinguished Names for User Search. To override these values, for example to make a narrower search, click on the **Use User Search Settings** checkbox to deselect it and add at least one Base Distinguished Name.

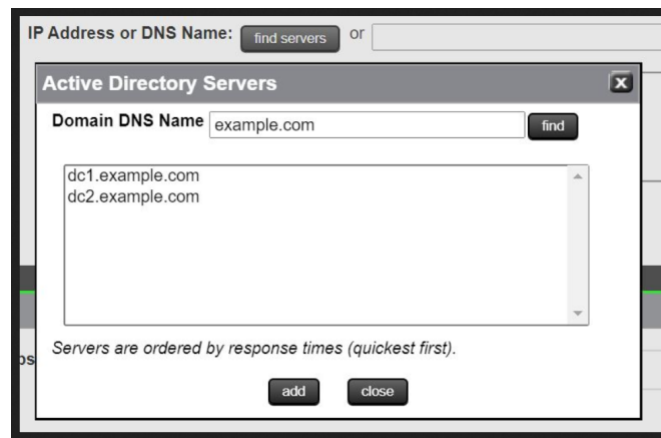
8. There are two ways to add Active Directory servers.

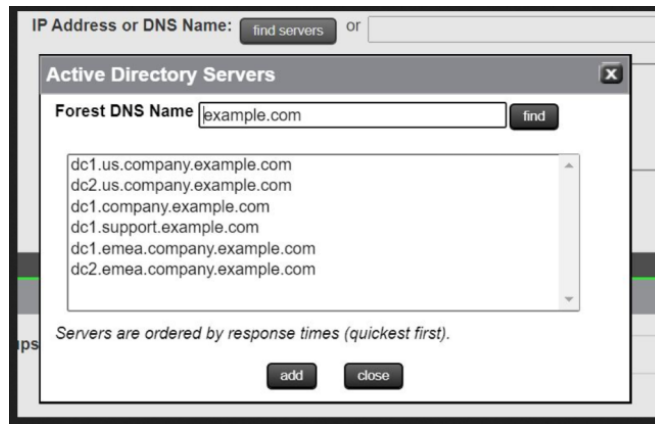
- Enter the fully qualified domain name of the server or its IP address and click **Add**.
- Click **find servers**. The NAS Manager will try to determine the DNS name of the Active Directory domain or forest from the Base Distinguished Names set for User Search. The value can be overridden manually. For an Active Directory forest setup, the DNS name of the Active Directory forest is expected. For an Active Directory domain, the DNS name of the domain is expected. Click on the **find** button to get the list of Active Directory servers in order of their response time (quickest first). If you add them in the same order, the SMU attempts to authenticate users against the fastest responding servers first.



Note: A DNS server or servers must be configured for the SMU (under Name Services) for **find servers** to work.

- Select one or more servers and click **add** to add them to the list. No more than 20 Active Directory servers can be configured at a time.
- When you are finished, click **close** to return to the **Active Directory Servers** window.





9. If there is more than one server, the list can be prioritized using **Move Up** or **Move Down** buttons.
10. Click **Apply** to submit this page and save all the settings to the SMU database. The SMU will perform a connection test to check that it can access the configured servers with the supplied details. It will also check for potential issues with configuration, for example whether a configured Base Distinguished Name exists in the Active Directory domain or forest. In case of an issue, a warning will be displayed. This gives the user the opportunity to either modify the settings or acknowledge that the settings are correct and save them as they are.

Any information, warnings and errors related to Active Directory configuration or authentication are logged to `/var/opt/smu/log/mgr/mgr.log` and `/var/opt/smu/log/mgr/security.log`

Configuring Active Directory groups

Before Active Directory users can log into the SMU, you must configure one or more Active Directory groups. After a group has been added and saved, members of that group can log into the SMU using their Active Directory name and password. Active Directory users belonging to the subgroups of the configured group also have SMU access. In Global Catalog configuration, all the groups must be of scope Universal. CLI access via Active Directory primary group is not supported for Global Catalog configurations.

Before you begin

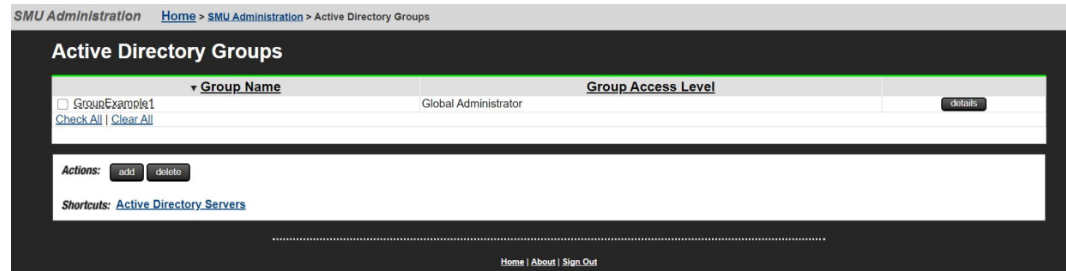
Note that the administrator is only able to configure groups after Active Directory servers have been added on the **Active Directory Servers** page.

Procedure


1. Navigate to the **Home > SMU Administrator > Active Directory Groups** to display the **Active Directory Groups** page.

This page shows all Active Directory groups that have been added. Note that Active Directory groups are given a group access level. A group can be constrained by this access level such that it can only reconfigure settings related to the server or the storage or for read-only access.

If an Active Directory user is member of more than one configured groups in the SMU, then their access level will be derived by combining the access level for all configured Active Directory groups. For example, if a user is a member of one group defined with storage level, but is also a member of a group with server level, then that user will have server+storage access to the SMU.



The following table describes the fields on this page:


| Field/Item | Description |
|---------------------------|--|
| Group Name | <p>Group Name is the user-friendly name of an Active Directory group existing on the Active Directory server.</p> <p>The full Distinguished Name for a group can be viewed by hovering the mouse over the group name. The sort order of the table can be changed by clicking over a column heading.</p> |
| Group Access Level | <p>Shows the group access level. This defines the access level given to Active Directory users who are members of the group when they log onto the SMU. On an external or virtual SMU, if the Group Access Level is Global, then group members are given SMU CLI access. SMU CLI access is not available on an embedded SMU or a NAS module SMU.</p> <p>This column also displays those Active Directory groups assigned the read-only attribute. A read-only group has permission to view most pages of the NAS Manager, but they are not allowed to perform any actions that would trigger a system or configuration change.</p> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p> Note: Read-only users can not access the CLI, and a user with CLI access may not be read-only. If either of these options is checked, the other one is disabled.</p> </div> |
| details | Click the details button in the right-hand column to view details of the associated group. |
| Check All | Checks all boxes under Group Name . |
| Clear All | Clears all checked boxes under Group Name . |

| Field/Item | Description |
|---------------------------------|---|
| add | Click to add a group. Takes you to the Add Active Directory Group page. |
| delete | Existing groups can be deleted by checking the box in left-hand column and clicking the delete button. The user is asked for confirmation before deleting. If all groups are being deleted, the user is warned that no Active Directory users will be authenticated. |
| Active Directory Servers | Takes you to the Active Directory Servers page. |

2. Click **add** and use the **Add Active Directory Group** page to add groups.

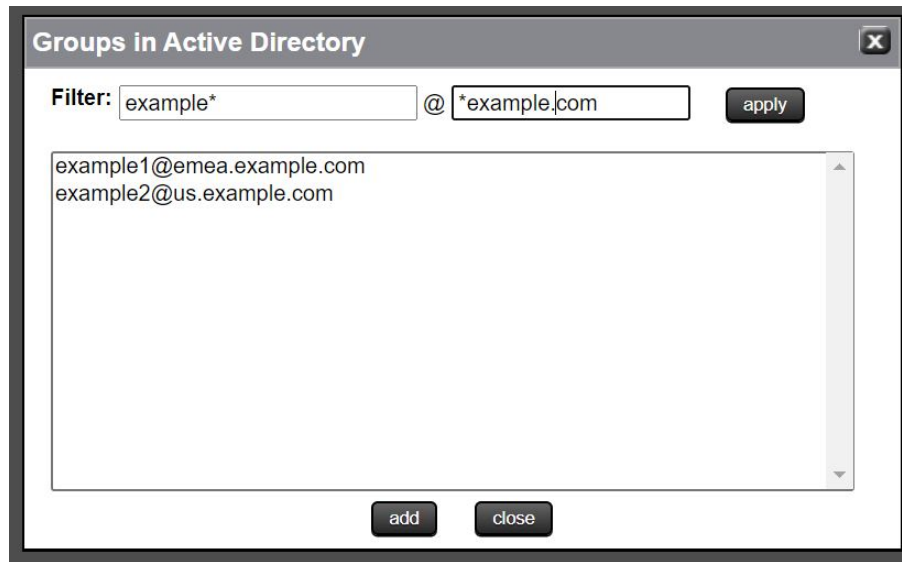
The following table describes the fields on this page:

| Field/Item | Description |
|------------------------------|---|
| Base Distinguished Name | The root of an Active Directory subtree of entries from where the SMU searches for groups. Base Distinguished Names are defined on the Active Directory Servers page. |
| Group Distinguished Name | The LDAP Distinguished Name of a group to add. Groups can be added one at a time, by entering each Distinguished Name and then pressing the OK button. A maximum of 100 groups can be added. Alternatively, groups can be added by using the find group button. |
| find group | Queries the Active Directory to show the list of available groups. The list can be filtered by entering a partial group name and/or a partial domain DNS name. A maximum of 1000 group names is displayed. |
| User Level for Group Members | The user levels that can be assigned to group members are the same as those that can be assigned to local or RADIUS users and have the same meanings. The default is Global , but the level can be modified by selecting one of the other radio buttons. |

| Field/Item | Description |
|------------------|--|
| Read-Only Access | <p>Users in a read-only group may log into the SMU and have permission to view most pages of the NAS Manager; however, they are not allowed to change anything. The Active Directory Group Details page will not allow the read-only attribute to be modified. The group would need to be deleted and re-added to change this attribute.</p> <div data-bbox="721 485 1393 709" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: Users in a group with the read-only attribute can not access the CLI, and a user with CLI access may not be read-only. For complete details on read-only access, please see the section, <i>Read-only users</i>, in the <i>NAS Storage System User Administration Guide</i>.</p> </div> |
| OK | Click to save the group details. The SMU checks that the group exists in Active Directory. If the group does not exist (or if the SMU failed to access any AD server) the user is asked for confirmation that they still wish to save it. After saving the group, the updated group list page is displayed. |
| cancel | Cancels input. |

3. There are two ways to add groups:

- Enter the full Distinguished Name for the group (for example "CN=Mygroup,CN=users,DC=example,DC=com") and click the **add** button. Special characters: *comma, semi-colon, backslash, and leading/trailing spaces* within the group name have to be escaped with a "\" backslash character.
- Click the **find group** button.
 - Groups that exist under the configured Base Distinguished Names are displayed in a window. The full Distinguished Name for a group can be viewed by hovering the mouse over the group name. The order of the groups matches the order of the Base Distinguished Names. The list can be filtered by entering a partial group name and/or partial domain DNS name. The "*" wildcard character is supported anywhere in the filter string. The filter is case insensitive. The left-hand box of the filter will be matched anywhere in the group name. The right-hand box, if it does not start with "*", will be matched at the beginning of the domain DNS name. A maximum of 1000 group names is displayed. Select a group from the list. Only one group can be added at a time.
 - Click **add** to add the group's Distinguished Name to this page.
 - Click **close** to return to the **Active Directory Groups** page without selecting a group from the list.



4. Select a User Level to be assigned to members of the group.
CLI access is given to members of all groups configured with the **Global** level.
Active directory users are given the same access level to all managed HNAS servers.
5. Click **OK** to save the group.

NAS Manager will warn if the group is not found in Active Directory, giving the user the opportunity to modify the group.

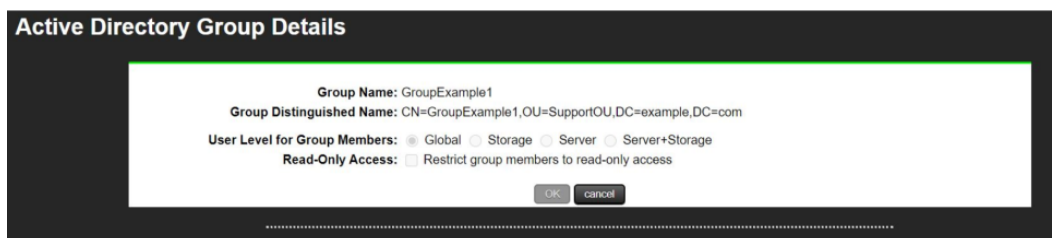
Any information, warnings and errors related to Active Directory configuration or authentication are logged to `/var/opt/smu/log/mgr/mgr.log` and `/var/opt/smu/log/mgr/security.log`

On returning to **Active Directory Groups** page, the current list of configured groups is displayed.



6. Click the **details** button in the right-hand column to view details of a previously configured group.

When displaying the group details, the SMU checks that the group exists in Active Directory and displays a warning if it does not exist or if the SMU could not access an Active Directory server. The user level cannot be modified once the group has been added. In order to modify the user level, the group would have to be deleted, then added again. Click the **cancel** button to return to the **Active Directory Groups** page.



The following table describes the fields on this page:

| Field/Item | Description |
|------------------------------|---|
| Group Name | The LDAP Common Name attribute of the group. |
| Group Distinguished Name | The LDAP Distinguished Name attribute of the group. |
| User Level for Group Members | The user levels that can be assigned to group members are the same as those that can be assigned to local or RADIUS users and have the same meanings. The default is Global , but the level can be modified by selecting one of the other radio buttons. |
| OK | No details can be modified for a group, so the OK button is disabled. |
| cancel | Returns to the Active Directory Groups page. |

User authentication through RADIUS servers (HNAS server only)

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service.

RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The SMU acts as a RADIUS client component that communicates with the RADIUS server to validate logins. The RADIUS server is usually a background process running on a Unix or Microsoft Windows server.

RADIUS serves three functions:

- Authenticates users or devices before granting them access to a network.
- Authorizes those users or devices for certain network services.
- Accounts for usage of those services.

The RADIUS server compatibility is as follows:

- For IPv4 only, works with FreeRADIUS 2.1 or Windows 2003 Internet Authentication Service (IAS).
- For IPv6, requires FreeRADIUS 2.2 or Windows 2008 Network Policy Server (NPS).

Configuring user authentication through a RADIUS server requires the following:

- The RADIUS server must be set up and operational.
- The SMU must be able to communicate with the RADIUS server using the network.
- You must know the RADIUS server's:
 - IP address or DNS name.
 - Authentication port.
 - Shared secret for the SMU.

You can specify and prioritize multiple RADIUS servers for authentication.



Note: The SMU contacts RADIUS servers in order of priority; the SMU will always try to contact higher priority servers before lower priority servers, and you cannot map SMU users to authenticate through a specific RADIUS server. If you specify an incorrect secret or there are network problems that prevent the SMU from communicating with the highest priority RADIUS server, the SMU will try to contact the secondary RADIUS server, then the third RADIUS server, then the next server, until the SMU has tried to contact all the RADIUS servers in the list.

Displaying list of RADIUS servers

Procedure

1. Navigate to **Home > SMU Administration > RADIUS Servers**.

The screenshot shows the 'RADIUS Servers' configuration page. At the top, there is a breadcrumb trail: 'SMU Administration > Home > SMU Administration > RADIUS Servers'. The main heading is 'RADIUS Servers'. Below it is a table with the following columns: 'RADIUS Server', 'IP Address/DNS Name', 'Port', 'Protocol', 'Timeout (seconds)', and 'Retry Count'. There are three rows of servers listed: 'RadServ01', 'RADIUS02', and 'R-Server03'. The 'R-Server03' row is selected with a checked checkbox. Each row has a 'details' button to its right. Below the table are links for 'Check All' and 'Clear All'. A note states: 'RADIUS servers are tried in the order listed above.' At the bottom, there are 'Actions' for 'Increase Priority', 'Decrease Priority', 'remove', and 'add'. A 'Shortcuts' section contains a link to 'SMU Users'.

| RADIUS Server | IP Address/DNS Name | Port | Protocol | Timeout (seconds) | Retry Count | |
|--|---------------------|------|----------|-------------------|-------------|---------|
| <input type="checkbox"/> RadServ01 | | 1812 | PAP | 3 | 3 | details |
| <input type="checkbox"/> RADIUS02 | | 1812 | PAP | 3 | 3 | details |
| <input checked="" type="checkbox"/> R-Server03 | | 1812 | PAP | 3 | 3 | details |

Check All | Clear All

RADIUS servers are tried in the order listed above.

Actions: [Increase Priority](#) [Decrease Priority](#) [remove](#) | [add](#)

Shortcuts: [SMU Users](#)

Adding a RADIUS server

Procedure

1. Navigate to **Home > SMU Administration > RADIUS Servers** to display the **RADIUS Servers** page.

2. Click **add** to display the **Add RADIUS Server** page.

SMU Administration [Home](#) > [SMU Administration](#) > [RADIUS Servers](#) > Add RADIUS Server

Add RADIUS Server

RADIUS Server IP Address or DNS Name:

Shared Secret:

Port:

Protocol: PAP

Timeout: (seconds)

Retry Count:

| Field/Item | Description |
|--------------------------------------|---|
| RADIUS server IP address or DNS name | <p>To connect with the RADIUS server, specify an IPv4 or IPv6 address, or a host name (host name is not recommended). An IP address is preferred, both because it eliminates the dependency on the network DNS sever(s), and to improve login performance.</p> <p>The SMU Network Configuration page (navigate to Home > SMU Administration > SMU Network Configuration) shows the active IP addresses. It is recommended that IPv4 on eth0 and the current IPv6 addresses be added to the "allowed client" list on each RADIUS server. For more information on setting up the SMU Network Configuration for IPv6, see the <i>Network Administration Guide</i>.</p> |
| Shared Secret | <p>Specify the shared secret.</p> <p>Some RADIUS Servers limit the length of the shared secret and require that it be comprised only of characters that can be typed on a keyboard which uses only 94 out of 256 possible ASCII characters.</p> |

| Field/Item | Description |
|---------------|---|
| | <p>If the shared secret must be a sequence of keyboard characters, choose shared secrets that are at least 22 characters long and consisting of a random sequence of upper and lower case letters, numbers, and punctuation.</p> <ul style="list-style-type: none"> ▪ To ensure a random shared secret, use a computer program to generate a random sequence at least 22 characters long. Windows 2008 Server allows you to generate a shared secret when adding the RADIUS client. ▪ The SMU will support a shared secret from 1 up to 128 characters. ▪ Use a different shared secret for each RADIUS server-RADIUS client pair. |
| Port | Specify the RADIUS server authentication port. The default RADIUS server authentication port is 1812, but you should check with the RADIUS server administrator to make sure that 1812 is the correct port. |
| Protocol | The protocol for the RADIUS server. |
| Timeout | Specify the timeout, which is the number of seconds the SMU waits before retrying (retrying is re-transmitting the authentication request to the same RADIUS server). The default is 3 seconds. If the timeout is reached and there is no response from the first RADIUS server in the list, the SMU attempts another retry. |
| Retry Count | Specify the retry count. The default is 3. When the retry limit is reached, the SMU sends the request to the next RADIUS server in the list. When the retry limit for the second server is reached, the SMU attempts to reach the next server in the list, until there are no more servers to try. If there are no more servers to try, the user cannot be authenticated, and the login fails. |
| OK | When you are done making changes, click OK to test connectivity and save the configuration for this RADIUS server and return to the RADIUS Servers page. |
| cancel | Exits without saving the configuration. |

Displaying details of RADIUS server

Procedure

1. Navigate to **Home > SMU Administration > RADIUS Server** to display the **RADIUS Server** page.
2. Select a RADIUS server, and click **details** to display the **RADIUS Server Details** page.

SMU Administration [Home](#) > [SMU Administration](#) > [RADIUS Servers](#) > RADIUS Server Details

RADIUS Server Details for R-Server03

RADIUS Server IP Address or DNS Name: R-Server03

Shared Secret:

Port:

Protocol: PAP

Timeout: (seconds)

Retry Count:

[Check Connectivity](#)

| Field/Item | Description |
|--------------------------------------|---|
| RADIUS server IP address or DNS name | The RADIUS server IP address or DNS name. |
| Shared Secret | The shared secret, displayed with asterisks. |
| Port | The RADIUS server authentication port. |
| Protocol | Protocol associated with the RADIUS server. |
| Timeout | The number of seconds the SMU waits before retrying (retrying is re-transmitting the authentication request to the same RADIUS server). If the timeout is reached and there is no response from the first RADIUS server in the list, the SMU attempts another retry. |
| Retry Count | When the retry limit is reached, the SMU sends the request to the next RADIUS server in the list. When the retry limit for the second server is reached, the SMU attempts to reach the next server in the list, until there are no more servers to try. If the timeout is reached, and there are no more servers to try, the user cannot be authenticated, and the login fails. |
| Check connectivity | Click to check the connectivity status of the RADIUS server. |

Hitachi Vantara



Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact