HITACHI
Inspire the Next

Hitachi NAS Platform

Storage Systems User Administration

Release 12.3

Hitachi Data Systems

MK-92HNAS013-04

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at https://portal.hds.com.

Notice: Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

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

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Data Systems Legal Department for any export compliance questions.

Contents

Preface

In PDF format, this guide explains user management, including the different types of system administrators, their roles, and how to create and manage these users.

Contacting Hitachi Data Systems

2845 Lafayette Street
Santa Clara, California 95050-2627
U.S.A.
https://portal.hds.com
North America: 1-800-446-0744

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.

Administration Guides

- *System Access Guide* (MK-92HNAS014)—In PDF format, this guide 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)—In PDF format, this guide provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading firmware, monitoring servers and clusters, the backing up and restoring configurations.
- *Storage System User Administration Guide* (MK-92HNAS013)—In PDF format, this guide 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)—In PDF format, this guide 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)—In PDF format, this guide 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) —In PDF format, this guide provides information about the Data Migrator feature, including how to set up migration policies and schedules.
- *Storage Subsystem Administration Guide* (MK-92HNAS012)—In PDF format, this guide 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)—In PDF format, this guide provides information about configuring the server to take and manage snapshots.
- *Replication and Disaster Recovery Administration Guide* (MK-92HNAS009) —In PDF format, this guide 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)—In PDF format, this guide 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)—In PDF format, this guide provides information about configuring the server to work with NDMP, and making and managing NDMP backups. Also includes information about Hitachi NAS Synchronous Image Backup.
- *Command Line Reference* Opens in a browser, and describes the commands used to administer the system.

⚠ **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 G1 Hardware Reference* (MK-92HNAS016)—Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- *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 Series 4000 Hardware Reference* (MK-92HNAS030) (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 High-performance NAS Platform* (MK-99BA012-13)—Provides an overview of the NAS Platform 3100/NAS Platform 3200 server hardware, and describes how to resolve any problems, and replace potentially faulty parts.

Best Practices

- *Hitachi USP-V/VSP Best Practice Guide for HNAS Solutions* (MK-92HNAS025)—The HNAS practices outlined in this document describe how to configure the HNAS system to achieve the best results.
- *Hitachi Unified Storage VM Best Practices Guide for HNAS Solutions* (MK-92HNAS026)—The HNAS system is capable of heavily driving a storage array and disks. The HNAS practices outlined in this document describe how to configure the HNAS system to achieve the best results.
- *Hitachi NAS Platform Best Practices Guide for NFS with VMware vSphere* (MK-92HNAS028)—This document covers VMware best practices specific to HDS HNAS storage.
- *Hitachi NAS Platform Deduplication Best Practice* (MK-92HNAS031) —This document provides best practices and guidelines for using HNAS 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.
- *Brocade VDX 6730 Switch Configuration for use in an HNAS Cluster Configuration Guide* (MK-92HNAS046)—This document describes how to configure a Brocade VDX 6730 switch for use as an ISL (inter-switch link) or an ICC (inter-cluster communication) switch.
- *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 NAS Platform Storage Pool and HDP Best Practices* (MK-92HNAS048)—This document details the best practices for configuring and using HNAS storage pools, related features, and Hitachi Dynamic Provisioning (HDP).
- *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 Platform Hitachi Dynamic Provisioning with HNAS v12.1* (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 HNAS Multi-Tenancy and related features, and EVS security.

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 Web Manager, the browser-based management utility provided by the system management unit (SMU). Additionally, Global Administrators can connect to the SMU command line interface (CLI).

⚠ **Note:** Server Administrators, Storage Administrators, and Server+Storage Administrators will not be able to access all the Web Manager pages that a Global Administrator can access.

- □ Adding an SMU user (an administrator)
- □ Changing an SMU user profile

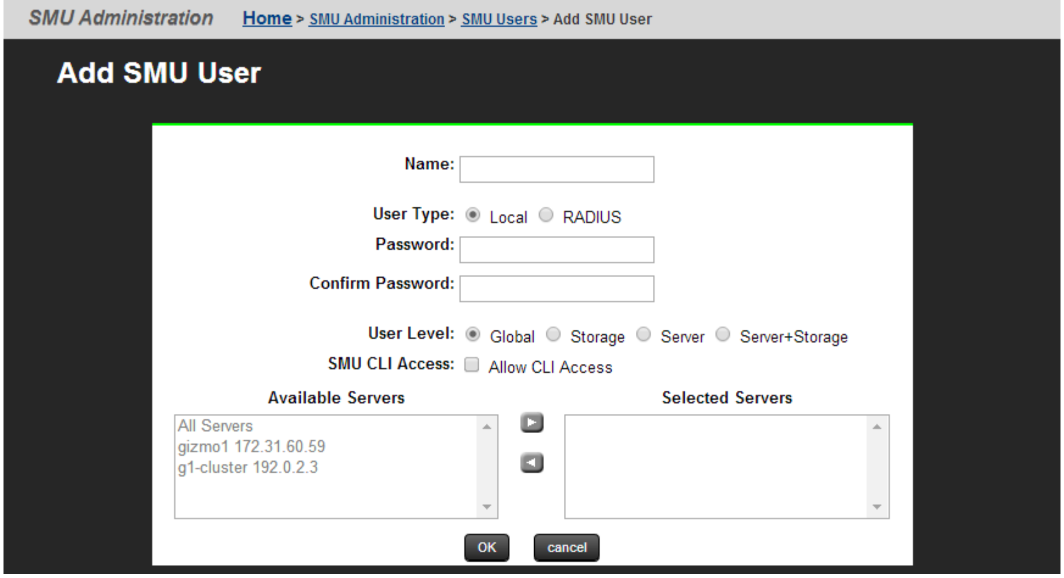
Adding an SMU user (an administrator)

To add an SMU user (a NAS storage system administrator):

Procedure

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

2. Click **add** to display the **Add SMU User** page:



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

Add SMU User

Name:

User Type: ● Local ○ RADIUS

Password:

Confirm Password:

User Level: ● Global ○ Storage ○ Server ○ Server+Storage

SMU CLI Access: □ Allow CLI Access

Available Servers: All Servers, gizmo1 172.31.60.59, g1-cluster 192.0.2.3

Selected Servers:

Field/Item	Description
Name	The name of the new user account. This name will be requested when logging in to the SMU. The rules for user names are: • For Global administrators only, if the user will access the SMU through the CLI, the user name: ○ Must start with a letter or an underscore, and may consist of 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 Web 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 (!). **Note:** If you are using RADIUS realms, and the global administrator will access the SMU using both Web Manager and the CLI, use the underscore (_) to combine the user name and the realm: for example `johnsmith_realm2`. If the global administrator will access the SMU using only Web Manager, you can use the at sign (@) to combine the user name and the realm: for example `johnsmith@realm3`.
User Type	The user type. User types are either **local** or **RADIUS**. • 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

Field/Item	Description
	administrator must add a user name and password to all RADIUS servers.
Password	Enter the password that will be used when this user account logs in. The password cannot exceed 256 characters. This field only applies when the User Type is selected to Local. It does not apply when the RADIUS User Type is selected.
Confirm Password	Confirm the password entered in the previous field by entering it in again. Only applies when the Local User type is selected.
User Level	Specify the level for the new administrator that you are creating. You can select any one of the following: • **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. ⚠ **Note:** Server Administrators, Storage Administrators, and Server+Storage Administrators will not be able to access all the Web Manager pages that a Global Administrator can access.
SMU CLI Access (for Global Administrators only)	If the administrator is allowed to log in and access the SMU CLI of an external SMU, fill in the **SMU CLI Access** check box.
Available Servers	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

Field/Item	Description
	available for Global administrators, because Global administrators are allowed to manage all storage and all servers.
Selected Servers	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. 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. For Server+Storage administrators, lists servers that the administrator can manage. The Server+Storage administrator can also manage the storage attached to these servers.
OK	When the profile is complete and correct, click **OK** to save and enable the user profile, and then return to the **SMU Users** page.
cancel	Closes the page without saving the profile, and returns to the **SMU Users** page.

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 will not be available, and you should skip the next two steps, but you must enter the user passwords into the RADIUS server using the tools available for that server.

5. If the **User Type** is local, enter the password for the new administrator in the **Password** field.
6. If the **User Type** is local, confirm the password for the new administrator in the **Confirm Password** field.
7. Specify the initial login password for the user by filling in the **Password** and the **Confirm Password** fields.
8. Specify the user level for the new administrator that you are creating.

   You can select one of the following:
   - **Global Administrator**
   - **Storage Administrator**
   - **Server Administrator**
   - **Server+Storage**
9. For Global Administrators only, if the administrator is allowed to log in and access the SMU command line interface (CLI) of an external SMU, fill the **SMU CLI Access** check box.
10. 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.

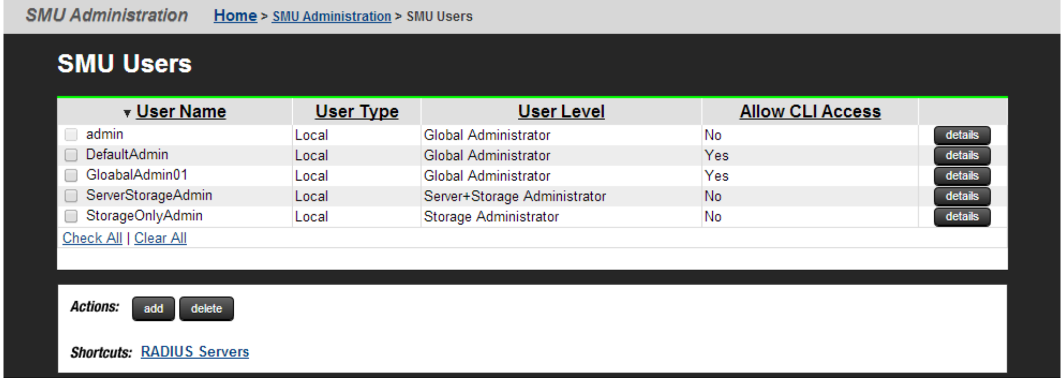
- To grant management privileges for a server or the storage attached to a server, move the server from the **Available Servers** list to the **Selected Servers** list.
- To revoke management privileges for a server or the storage attached to a server, move the server from the **Selected Servers** list 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.

11. 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

Procedure

1. Navigate to **Home > SMU Administration > SMU Users** to open the **SMU Users** page.



SMU Administration Home > SMU Administration > SMU Users

SMU Users

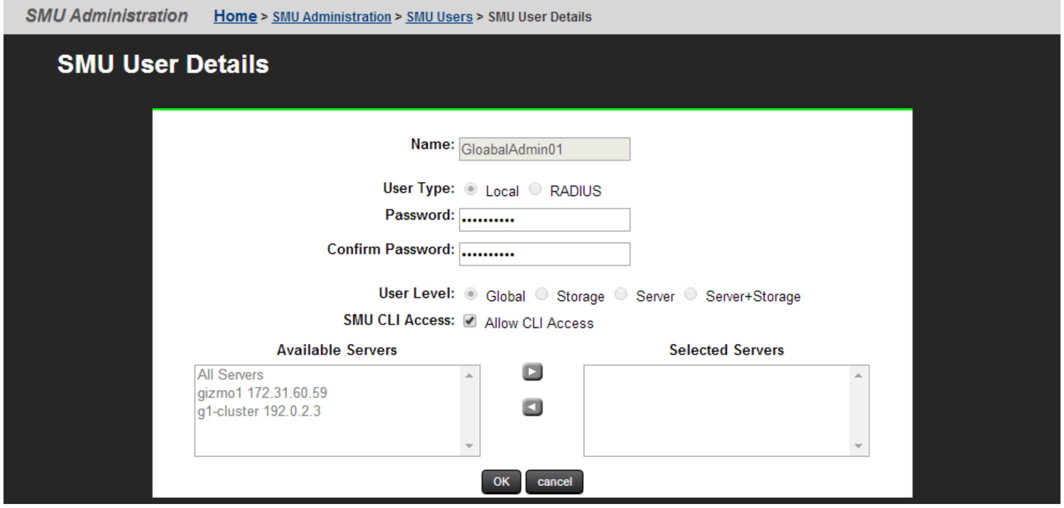
▾ User Name	User Type	User Level	Allow CLI Access	
□ admin	Local	Global Administrator	No	details
□ DefaultAdmin	Local	Global Administrator	Yes	details
□ GloabalAdmin01	Local	Global Administrator	Yes	details
□ ServerStorageAdmin	Local	Server+Storage Administrator	No	details
□ StorageOnlyAdmin	Local	Storage Administrator	No	details

Check All | Clear All

Actions: add delete

Shortcuts: RADIUS Servers

2. Click **details** to display the **SMU User Details** page for the user whose profile you want to modify.



SMU User Details

Name: GloabalAdmin01

User Type: ● Local ○ RADIUS

Password: ....

Confirm Password: ....

User Level: ● Global ○ Storage ○ Server ○ Server+Storage

SMU CLI Access: ☑ Allow CLI Access

Available Servers: All Servers, gizmo1 172.31.60.59, g1-cluster 192.0.2.3

Selected Servers:

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	For users authenticated by the SMU only (local users). These fields do not apply for users authenticated by a RADIUS server. 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.
User Level	Displays the user level or type of administrative role. • **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

Item/Field	Description
	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. • If the User Level is Global, you can enable or disable the **Allow CLI Access** check box. • If the User Level is server, storage, or server+storage, you can add or remove servers from the user's scope of management. Global users implicitly have access to manage all servers and storage. Non-global users cannot be given CLI access. 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.
SMU CLI Access	For global administrators only, when the check box is filled, the administrator can access the SMU using the CLI as well as Web Manager.
Available Servers	Not available for global administrators, because global administrators are allowed to manage all storage and all servers. For server administrators, storage administrators, and server +storage administrators, lists the servers managed by the SMU to which the administrator has not yet been give management privileges. The "All Servers" entry is used to allow privileges to all servers managed by the SMU.
Selected Servers	Not available for global administrators, because global administrators are allowed to manage all storage and all servers. For server administrators, lists the servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers. 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. For server+storage administrators, lists servers that the administrator can manage. The server+storage administrator can also manage the storage attached to these servers.
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 filled, the administrator can access the SMU using the CLI as well as Web 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. When you are done making changes, click **OK** to save the profile and return to the **SMU Users** page.

2

Changing the password for a currently logged in user

⚠ **Note:** If the user is authenticated through a RADIUS server, you cannot change their password using Web Manager or the SMU CLI, you must change those user's passwords using the tools/utilities for the RADIUS server.

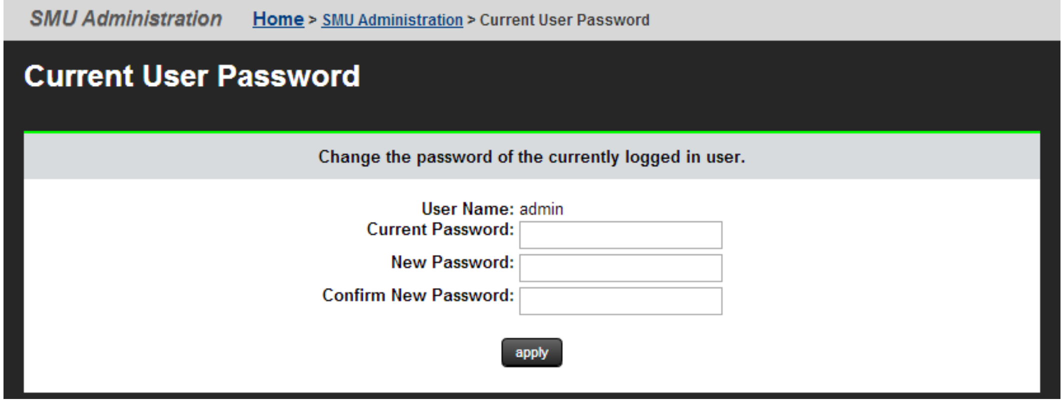
Any logged in user can change their own password. A global administrator can also change the password of any user, whether the user is currently logged in or not.

Changing your own password

Note: If your log in is authenticated through a RADIUS server, you cannot change their password using the SMU, you must change it using the tools/utilities for the RADIUS server.

Procedure

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



SMU Administration   Home > SMU Administration > Current User Password

Current User Password

Change the password of the currently logged in user.

User Name: admin
Current Password:
New Password:
Confirm New Password:

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 new password and closes the page.

2. Enter your current password in the **Current Password** field.

   If you have forgotten you 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.

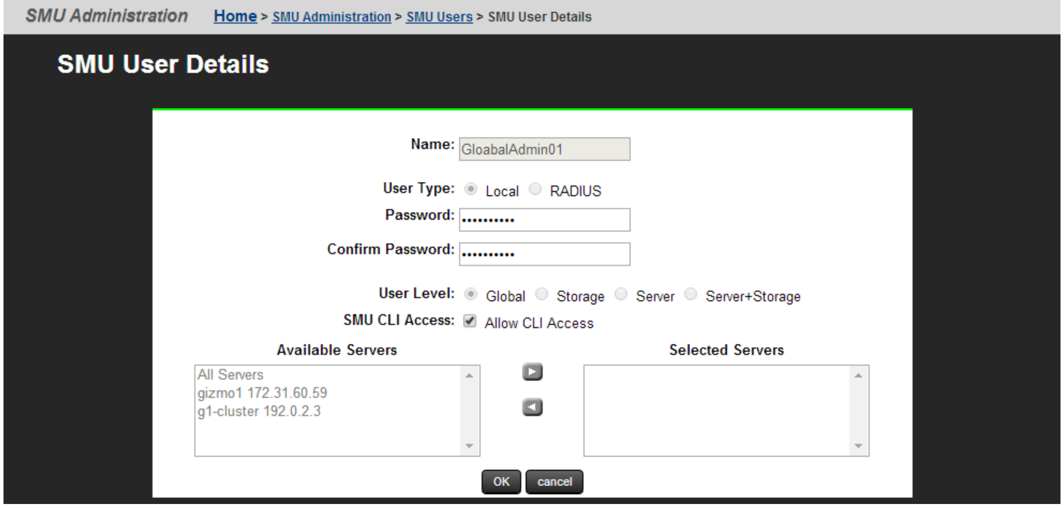
5. When finished, click **apply** to save the new password.

Changing another user's password

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: GloabalAdmin01

User Type: ● Local ○ RADIUS

Password: ••••••••••

Confirm Password: ••••••••••

User Level: ● Global ○ Storage ○ Server ○ Server+Storage

SMU CLI Access: ☑ Allow CLI Access

Available Servers:
All Servers
gizmo1 172.31.60.59
g1-cluster 192.0.2.3

Selected Servers:

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	For users authenticated by the SMU only (local users). These fields do not apply for users authenticated by a RADIUS server. 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.
User Level	Displays the user level or type of administrative role. • **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

Item/Field	Description
	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. • If the User Level is Global, you can enable or disable the **Allow CLI Access** check box. • If the User Level is server, storage, or server+storage, you can add or remove servers from the user's scope of management. Global users implicitly have access to manage all servers and storage. Non-global users cannot be given CLI access. 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.
SMU CLI Access	For global administrators only, when the check box is filled, the administrator can access the SMU using the CLI as well as Web Manager.
Available Servers	Not available for global administrators, because global administrators are allowed to manage all storage and all servers. For server administrators, storage administrators, and server +storage administrators, lists the servers managed by the SMU to which the administrator has not yet been give management privileges. The "All Servers" entry is used to allow privileges to all servers managed by the SMU.
Selected Servers	Not available for global administrators, because global administrators are allowed to manage all storage and all servers. For server administrators, lists the servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers. 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. For server+storage administrators, lists servers that the administrator can manage. The server+storage administrator can also manage the storage attached to these servers.
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.

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).

- □ Displaying list of RADIUS servers
- □ Adding a RADIUS server
- □ Displaying details of RADIUS server

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.

Once 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.

There are a number of benefits for SMU users. The administrator does not need to maintain a separate set of user details, because the SMU can just make use of the Active Directory enterprise user database. Users can login using their usual name and password instead of having to remember a separate set of credentials for the SMU. And instead of configuring access for individual users, the SMU administrator just has to specify the Active Directory *groups* whose members have login rights.

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

Active Directory is used for authentication but not for authorization. All Active Directory users are assigned "global" access rights to the SMU. There is no user's access (privilege) level.

Note: There is no CLI access to the SMU provided for Active Directory users.

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, 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 have identical content.

Configuring Active Directory servers

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

Prerequisites

In order to enable Active Directory use, the SMU administrator needs to know the following information:

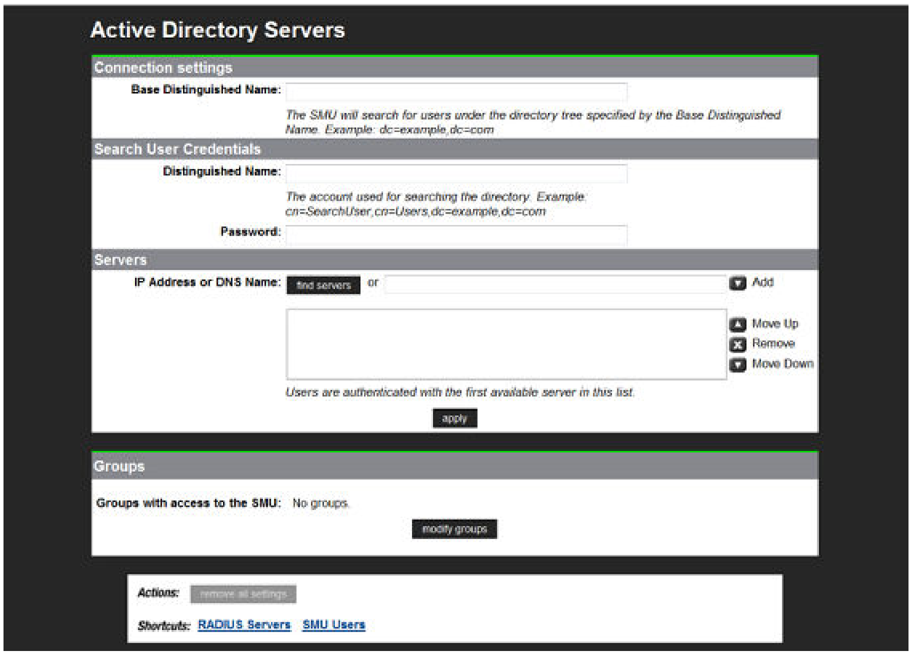
- The domain in which the Active Directory users and groups that will access the SMU are located.
- The LDAP distinguished name and password of an Active Directory user that has read access to users and groups on the Active Directory servers. This is referred to as the Search User. The user can search 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. The content of all configured servers must be identical. If DNS servers have been configured for the SMU, then the SMU should be able to automatically discover these server addresses via the **find servers** button on the setup page. SRV records must be setup in order 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.
- 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.

Procedure

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

2. Enter the **Base Distinguished Name**.

   This name must be entered in LDAP distinguished name (DN) format which consists of a sequence of "attribute=value" pairs separated by comma or semi-colon. The Base Distinguished Name should contain the domain component (dc) attributes for the organization's domain. So for the domain *example.com* it would be "*dc=example, dc=com*". The name may also contain organization unit (ou) attributes.



Active Directory Servers

Connection settings

Base Distinguished Name:

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

Search User Credentials

Distinguished Name:

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

Password:

Servers

IP Address or DNS Name:

Users are authenticated with the first available server in this list.

Groups

Groups with access to the SMU: No groups.

The following table describes the fields on this page:

Field/Item	Description
Connection settings	
Base Distinguished Name	The LDAP root location for users and groups. The name is recommended to contain just the domain components.
Search User Credentials	
Distinguished Name	The LDAP distinguished name for a user that has search capabilities.
Password	The password for the search user.
Servers	
IP Address or DNS Name	The address of one or more Active Directory servers for the domain. Each server should hold identical content.
find servers	Queries DNS to show the list of available Active Directory servers for the domain.

Field/Item	Description
Add	Add an Active Directory server after you have entered its fully qualified domain name or IP address.
Move Up **Move Down**	If there is more than one server, use these buttons to prioritize the list.
Remove	Remove a server from the list.
apply	Submit the page and save the connection settings and server list 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. 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".*

4. Enter the **Password** of the Search User (an existing user that may access the directory).

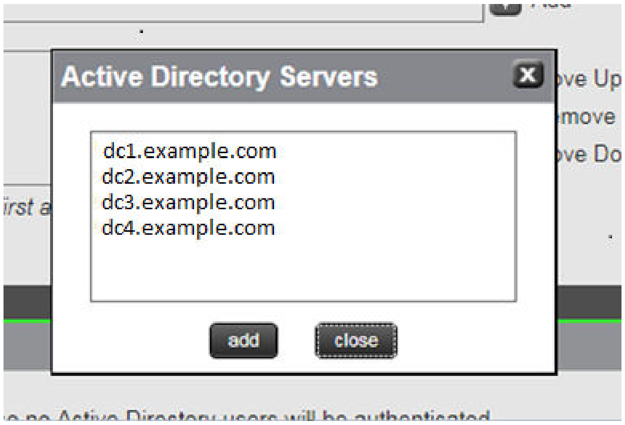
5. There are two ways to add Active Directory servers.

- Enter the fully qualified domain name or IP address of the server, and click **Add**.
- Click **find servers**.The list of discovered servers is displayed.

Note: The 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.



dc1.example.com
dc2.example.com
dc3.example.com
dc4.example.com

6. If there is more than one server, the list can be prioritized using **Move Up** or **Move Down** .
7. Click **Apply** to submit this page and save the connection settings and server list to the SMU database.
   The SMU will perform a connection test to check that it can access the configured servers with the supplied details and display a warning if the SMU cannot, giving the user the opportunity to modify the settings or to 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

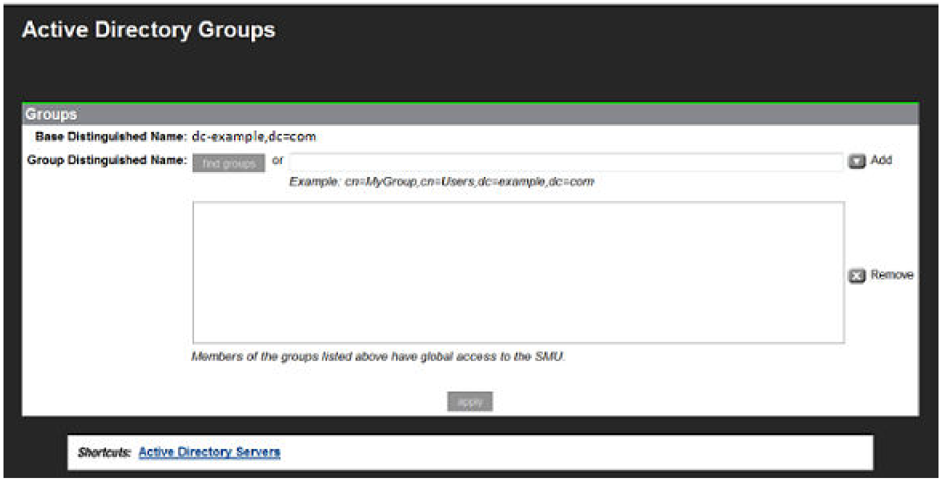
In order to allow Active Directory users to log into the SMU, it is necessary to configure one or more groups. Once an group has been added and saved, all users who are members of that group will be able to log into the SMU using their Active Directory name and password. Configuring a group gives SMU access to members of any sub-groups of that group.

Prerequisites

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** to display the **Active Directory Groups** page.



Active Directory Groups

Groups

Base Distinguished Name: dc-example,dc=com

Group Distinguished Name: find groups or

Example: cn=MyGroup,cn=Users,dc=example,dc=com

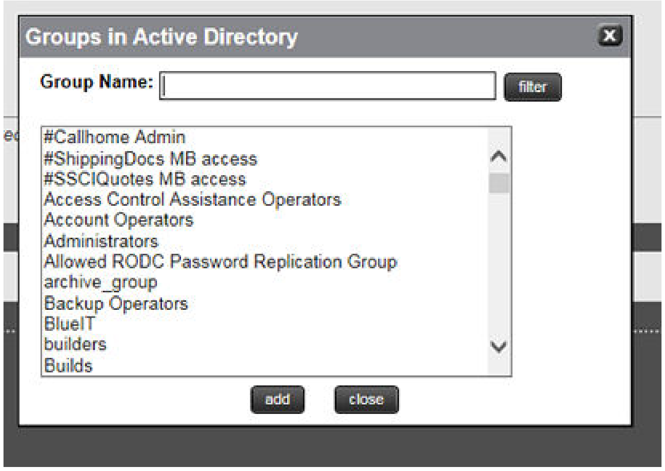
Members of the groups listed above have global access to the SMU.

The following table describes the fields on this page:

Field/Item	Description
Groups	
Group Distinguished Name	Groups can be added manually by entering their distinguished name and then pressing the **Add** button. A maximum of 100 groups can be added. Alternatively, groups can be added by using the **find groups** button.
find groups	Queries the Active Directory to show the list of available groups. The list can be filtered by entering a partial group name. A maximum of 1000 group names is displayed.
Add	Use to add a group.
Remove	Use to remove a group.
apply	Saves the list of groups and closes the page. The SMU checks that the groups exist in Active Directory.

2. 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.
   - Click the **find groups** button.
     - Groups that that exist under this Base DN are displayed in a dialog window. The list can be filtered by entering a partial group name. A maximum of 1000 group names is displayed. Select one or more groups from the list.
     - Click **Add** to add the group or groups to the list on the **Active Directory Groups** page.

- ○ When you are finished, click **close** to return to the **Active Directory Groups** page.



3. Click **apply** to save the list of groups.

   The SMU will perform a test to check that all the groups exist in Active Directory and display a warning if they do not, giving the user the opportunity to modify the groups or to 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`

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

User authentication through RADIUS servers

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.

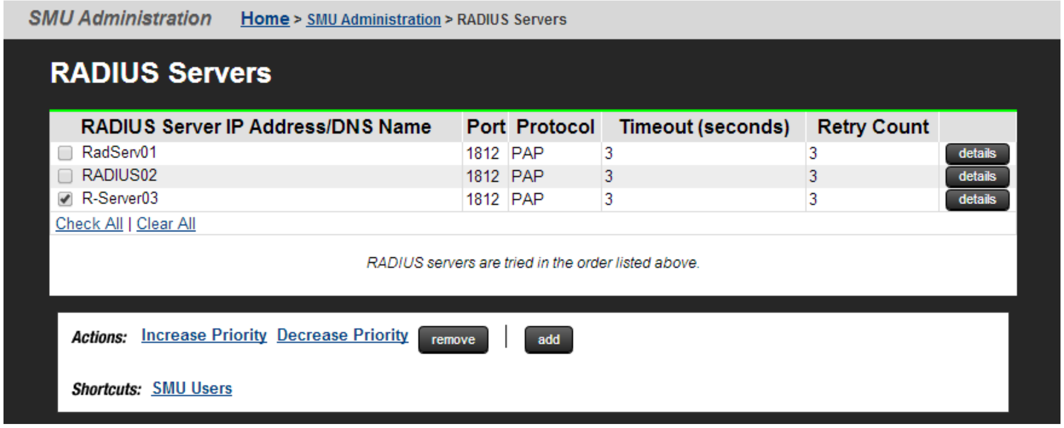
You can specify and prioritize multiple RADIUS servers for authentication.

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**.



SMU Administration Home > SMU Administration > RADIUS Servers

RADIUS Servers

	RADIUS Server IP Address/DNS Name	Port	Protocol	Timeout (seconds)	Retry Count	
☐	RadServ01	1812	PAP	3	3	details
☐	RADIUS02	1812	PAP	3	3	details
☑	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

Field/Item	Description
RADIUS server IP address/DNS name	Specifies the RADIUS server IP address or DNS name. To connect with the RADIUS server, you must enter either an IP address or a DNS name. An IP address is preferred, both because it eliminates the dependency on the network DNS severs, and to improve login performance.
Port	The port number on which each server listens. **Note:** 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 RADIUS server protocol. PAP is the default.
Timeout	Specifies the timeout count. The timeout is the number of seconds the SMU waits before retrying (retying 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	Specifies the 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.

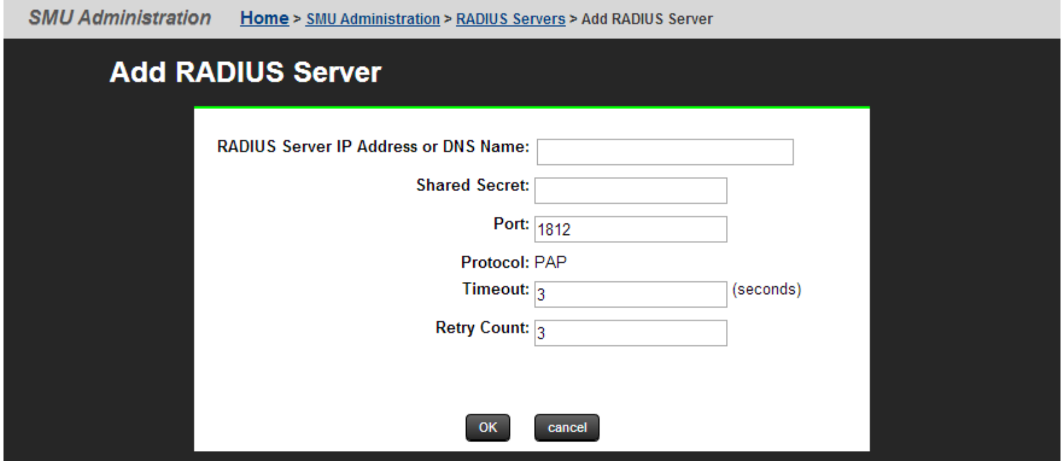
Field/Item	Description
details	Displays the **RADIUS Server Details** page in which you can view the details of the selected RADIUS server.
Check All	Selects all of the RADIUS servers in the server list.
Clear All	Unselects any selected RADIUS servers in the server list.
Increase Priority and **Decrease Priority**	Click **Increase Priority** to increase the server priority. Click **Decrease Priority** to decrease the server priority. 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.
remove	Removes the selected RADIUS server.
add	Opens the **Add Server RADIUS** page where the properties of the new server account are defined.
SMU Users	Opens the **SMU Users** page where you can view and add new 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: 1812

Protocol: PAP

Timeout: 3 (seconds)

Retry Count: 3

Field/Item	Description
RADIUS server IP address or DNS name	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. 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 *Network Administration Guide*.
Shared Secret	Specify the shared secret. 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. 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. • 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.

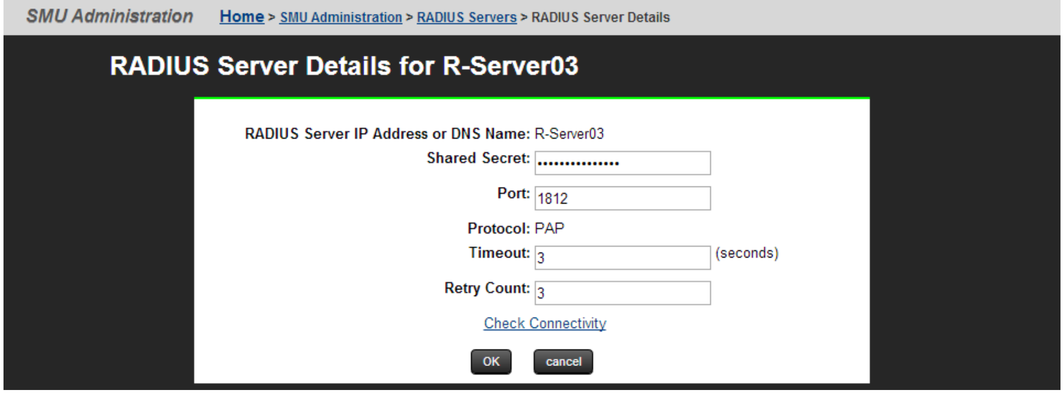
Field/Item	Description
Timeout	Specify the timeout, which is the number of seconds the SMU waits before retrying (retying is re-transmitting the authentication request to the same RADIUS server). If the timeout is reached and there is no response from the first RADIUS server in the list, the SMU attempts another retry.
Retry Count	Specify the 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 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: 1812
Protocol: PAP
Timeout: 3 (seconds)
Retry Count: 3

Check Connectivity
OK
cancel

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 (retying 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.
OK	Saves configuration changes, and closes the page.
cancel	Closes the page without saving configuration changes.

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-92HNAS013-04