Oracle® Communications Session Delivery Manager

Administration Guide

Release 7.3

Formerly Net-Net Central

December 2013

ORACLE

About this Guide

The *Oracle Communications Session Delivery Manager Administration Guide* explains how users who have administration privileges can detect certain types of issues before they can perform administrative functions.

Revision History

This section contains a revision history for this document.

Date	Description
October 2013	• Initial Release
December 2013	• Clarifies the default behavior of the inactivity timer on administrative accounts • Adds note regarding limitation in saving audit logs

Contents

1 Health Monitor

Overview

If you have Administration privileges you can access the Health Monitor console to detect certain types of issues before they can compromise Net-Net Central applications. The Health Monitor provides the administrator with the tools to pro-actively address potential problems in Net-Net Central.

The Health Monitor provides heartbeat indicators and statistics related to Net-Net Central server status and disk utilization for servers configured as members of a Net-Net Central cluster. The Health Monitor displays:

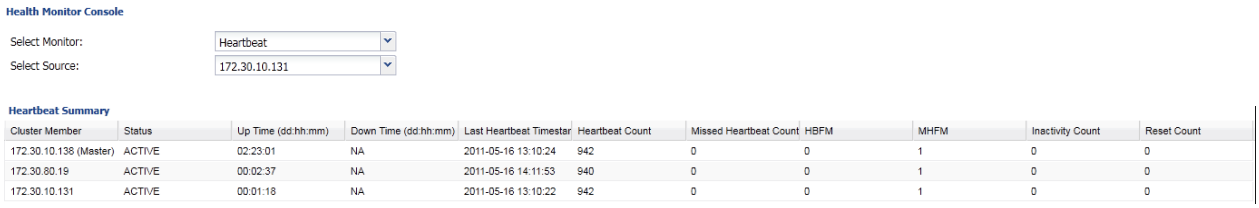
- heartbeat status information and statistics related to members of a NNC server cluster
- server inactive and active count
- disk usage and directory statistics

The Health Monitor includes the Heartbeat Monitor, which detects heartbeat messages and reports on server status and the Disk Usage Monitor, which provides information about disk usage and the size of several NNC directories.

Accessing the Health Monitor Console

To access the Health Monitor Console:

1. From the Net-Net Central Tools menu, choose Health Monitor. The Health Monitor Console appears in the Content area.



Cluster Member	Status	Up Time (dd:hh:mm)	Down Time (dd:hh:mm)	Last Heartbeat Timestar	Heartbeat Count	Missed Heartbeat Count	HBFM	MHFM	Inactivity Count	Reset Count
172.30.10.138 (Master)	ACTIVE	02:23:01	NA	2011-05-16 13:10:24	942	0	0	1	0	0
172.30.80.19	ACTIVE	00:02:37	NA	2011-05-16 14:11:53	940	0	0	1	0	0
172.30.10.131	ACTIVE	00:01:18	NA	2011-05-16 13:10:22	942	0	0	1	0	0

The Heartbeat Monitor display appears by default. From here you can choose to display the statistics for the different members of the cluster or you can choose to access the Disk Usage monitor.

Heartbeat Monitor

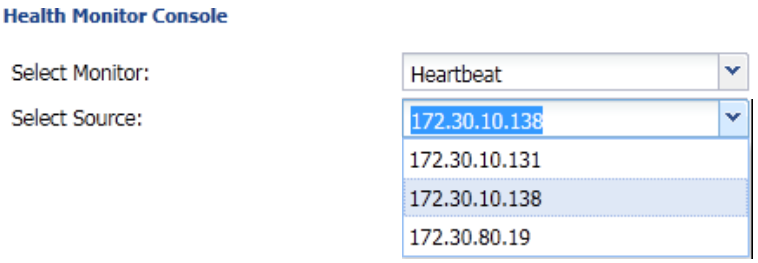
The Heartbeat Monitor maintains the statistics of NNC server heartbeats for all members in a cluster. It also keeps a count of the times a member was considered inactive and the number of times it returned to an active state based on the number of received and missed heartbeats, and a set threshold.

To view heartbeat statistics:

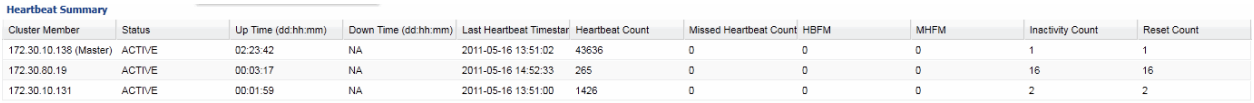
1. In the Health Monitor Console display, ensure Heartbeat is selected in the Select Monitor drop-down list.

   By default the IP address displayed in Select Source is for the server on which Net-Net Central is running and servicing the current client session.

2. Click the down arrow for Select Source to choose from a list of server IP addresses for the other cluster members or retain the default value.



The Heartbeat Summary table displays the cluster gathered statistics as maintained by the selected server. Each server maintains their own separate statistics of each server in the cluster. In the case of failure of one member of the cluster, all other active members can still relate the last known statistical health of the server before it failed.



Heartbeat Summary

Cluster Member	Status	Up Time (dd:hh:mm)	Down Time (dd:hh:mm)	Last Heartbeat Timestar	Heartbeat Count	Missed Heartbeat Count	HBFM	MHFM	Inactivity Count	Reset Count
172.30.10.138 (Master)	ACTIVE	02:23:42	NA	2011-05-16 13:51:02	43636	0	0	0	1	1
172.30.80.19	ACTIVE	00:03:17	NA	2011-05-16 14:52:33	265	0	0	0	16	16
172.30.10.131	ACTIVE	00:01:59	NA	2011-05-16 13:51:00	1426	0	0	0	2	2

The following table list the statistics tracked along with a description.

Statistic	Description
Cluster Member	IP address of the host member of the NNC cluster. If the host IP address has the (Master) label appended, it means this host member is running the master replication database.
Status	Current status of the host member of the cluster. A status of ACTIVE means the member is actively participating in the NNC cluster. A status of DOWN means this host member has failed to send its heartbeats and is considered as either having failed or a network partition exists between the cluster and this member.
Up Time (dd:hh:mm)	Number of days, hours and minutes the NNC server has been up
Down Time (dd:hh:mm)	Number of days, hours and minutes the NNC server has been down
Last Heartbeat Timestamp	Date and time of the last known heartbeat for each host member as recorded by the Select member statistics being viewed.

Statistic	Description
Heartbeat Count	Total count of NNC server heartbeats
Missed Heartbeat Count	Total number of times the monitor on the targeted host member (Selected Source) missed a heartbeat from other members in the cluster. An increase in this statistic might indicate network issues between members in the NNC cluster.
HBFM	Heartbeat Failure Meter statistic indicates the amount of times the required heartbeat counter of a NNC member was not received by the target host member. This number increases when the heartbeats start arriving again. If this statistic reaches a count of 10 (default) this host member is considered by the target host member to be down and its status is set to DOWN.
MHFM	Maximum Heartbeat Failed Meter statistic maintains the high-water mark of the HBFM statistic. This statistic is only reset if a member that left the cluster (status=DOWN) rejoins and starts sending heartbeats again.
Inactivity Count	Number of times the host member was considered to be in the state DOWN by the targeted (Selected Source) member.
Reset Count	Number of times the targeted member (Selected Source) has determined that a host member has gone from a state of DOWN to a state of ACTIVE. If a member rejoins the cluster after being DOWN, the reset counter is incremented by 1 and MHFM is reset to 0.

From here you can choose one of the other members of the cluster from the Select Source drop-down list of choose to view disk usage information.

Disk Usage

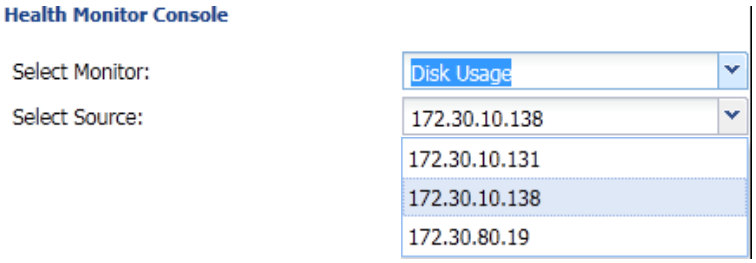
The Disk Usage Monitor maintains the statistics on disk storage usage, and checks if disk usage exceeds two threshold levels, 50% and 90% disk full. The Disk Usage monitor inspects the disk usage for the selected system and gathers statistics for total disk storage, used disk capacity, and free disk capacity. It also provides information about the size of the NNC directories and indicates the partition on which the directory is located. For example, the database directory might be located on a different partition from the other two directories.

Summary

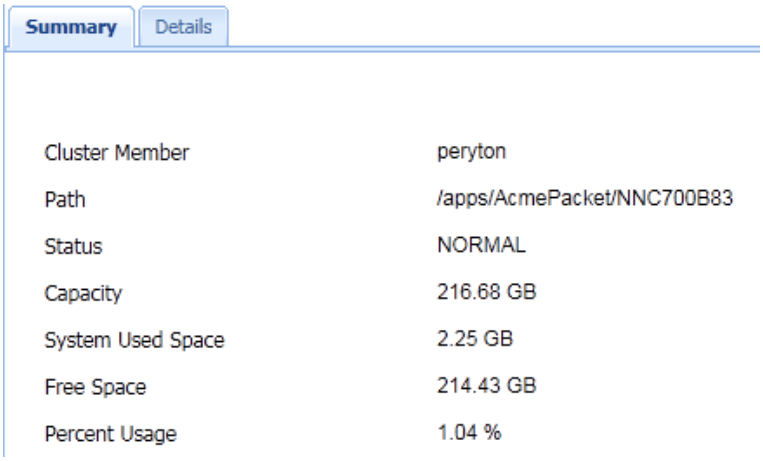
To view summary statistics:

1. Select Disk Usage from the Select Monitor drop-down list.

2. Click the down arrow for Select Source to choose from a list of server IP addresses for the members of the cluster or retain the default value.



The Disk Usage Summary view appears.



Note: The summary tab shows the statistics for the partition that NNC is installed on. If some parts of NNC, for example, the database, are installed on different partitions, the summary tab will display a table with the statistics of the different partitions.

The following table lists the disk summary statistics along with a description.

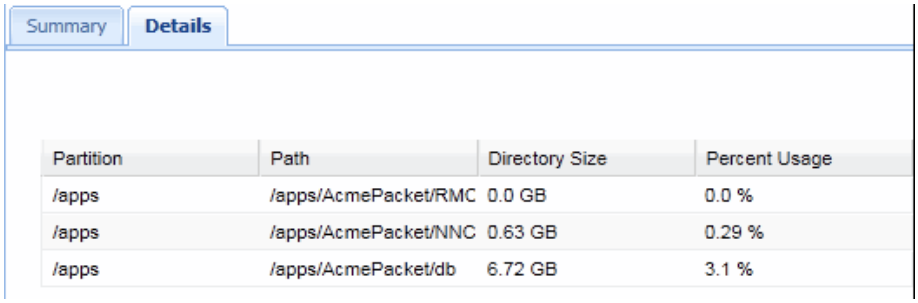
Statistic	Description
Cluster member	Name of the NNC server
Path	Path to where NNC is installed.
Status	Status of partition space use: • Normal: below the minimum threshold value (default is 50%) • Warning: at or above the minimum threshold value but below the maximum threshold value (default is 90%) • Critical: at or above the maximum threshold value (default is 90%)
Capacity	Total partition disk space in GB.
System Used Space	Total amount of disk space being used.
Free Space	Remaining disk space in GB.
Percent Usage	Percent of used space for the entire partition.

Details

The Details tab displays information about the space being taken up by the NNC directories: NNC, RMCArchive, and DB. It also shows the size of each directory and the percentage of space taken up by each directory.

To access details:

1. Click the Details tab. The Details table appears.



There are three directories listed in the example that are all located on the same partition.

The following table lists the information included in the Details view.

Statistic	Description
Partition	Name of the partition where the directory is located
Path	Path indicating the location of the directory
Directory Size	Amount of disk space used in the directory in GB
Percent Usage	Percentage of partition space being used by the specific directory

2 Security Manager

Overview

The Security Manager slider in Net-Net Central contains only those users who belong to the administration group can perform. Those users who have administration privileges are considered security administrators. They can access the different functions to manage users and audit logs.

User Management

User management lets you create new users and new user groups, and set group-based authorization where users are assigned to groups with different levels of authorization.

Setting authorization means you assign privileges to the group to which a user belongs. The privileges for that group are also assigned to all users who are members of the group. When a user logs into Net-Net Central, they can access functionality based on the privileges assigned to them.

The administrator is responsible for creating new user groups and users, and f or controlling the different security levels of Net-Net Central by assigning privileges. Administrators can:

- Create user groups and users
- Assign users to groups that provide specific authorization policies to for all members of that group
- Provide fine-grained access control for specific groups, views, operations
- Limit the access for some users to specific features and functionality

Groups

A group is a logical collection of users grouped together to access common information or perform similar tasks. You assign specific permissions to a group and then assign users to it. Those users in turn, inherit the group-based permissions.

The following groups are created by default when Net-Net Central is installed:

- administrators: Super user group privileged to perform all operations
- LIAdministrators: Privileged to perform most operations including Lawful Intercept (LI) configuration changes. Privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable/disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups
- provisioners: Privileged to configure Net-Net SBCs (if licensed for Element Manager) and save and apply the configuration with the exception of a LI configuration.
- monitors: Privileged to only view data, both configuration and other kinds of data. They cannot configure Net-Net SBCs. This group has the fewest privileges.

Users

A user is an individual who logs into Net-Net Central and performs a set of Net-Net Central- or application-related operations for which they have permission. Before a user

can access Net-Net Central operations, they must be added as a user to the Net-Net Central server database. When you have create users, you add them to user groups and the user privileges for that group will apply to them.

After logging into Net-Net Central, the operations available to a user are based on the group to which the specific user belongs.

The following users are created by default when Net-Net Central is installed:

- admin: inherits the privileges from the administrators group
- LIadmin: inherits the privileges from the LIadmin group

Operations

Operations are all the tasks you can perform using Net-Net Central, such as configuring Net-Net SBCs and performing administrative functions. They are logically arranged in a tree structure with parent and child operations (the Operations Tree) you access when creating group and user accounts. You provide or deny access to these operations by assigning a privilege to them.

Although Net-Net Central displays all the operations it supports, some only pertain to those users licensed for specific applications. For example, configuration operations only apply if the user is licensed for Element Manager.

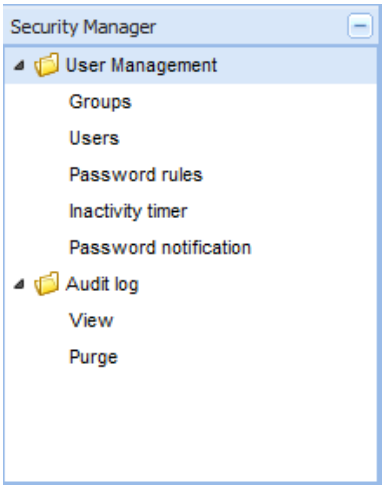
Privileges

Privileges include allowing or disallowing a user from performing operations. Privileges are assigned on the group level and are propagated to all users who belong to the group.

Accessing Security Manager

To access Security Manager:

1. Expand the Security Manager slider:



From here you can create user groups and users, change password rules, set the inactivity timer and password notification. You can also view and audit log that contains information about tasks performed using Net-Net Central.

Operations and Privileges

This section defines the operations and privileges you assign to a user group as the administrator. Net-Net Central displays all the operations it can support when you access the operations, including those intended for use with separately licensed applications.

For example, SBC configuration operations appear on the Configuration tab but do not apply unless you are licensed for Element Manager. Route management configuration operations also appear and do not apply unless you are licensed for Route Manager. Another example are the Fault Management operations that do not apply unless you are licensed for Element Manager. See the *Net-Net Central Core Functionality Guide* for licensing details.

Operations Categories

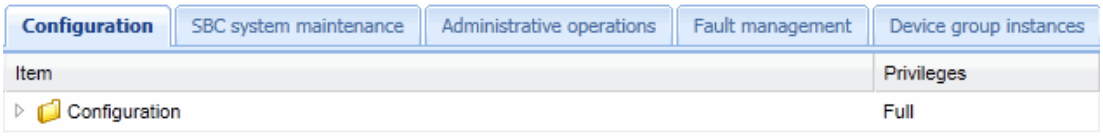
When you create a new user group, you need to indicate which of the operations the group members can or cannot perform by assigning privileges. There are five categories of operations for each group:

- Configuration (applicable if licensed for Element Manager and/or Route Manager)
- SBC system maintenance
- Administrative operations
- Fault management (applicable if licensed for Element Manager)
- Device group instances

Operations Location

You access the operations when you are creating a user group.

1. Create a new user group. See Creating User Groups for details.
2. Click the new group name in the table and click Edit. The operations tabs appear.

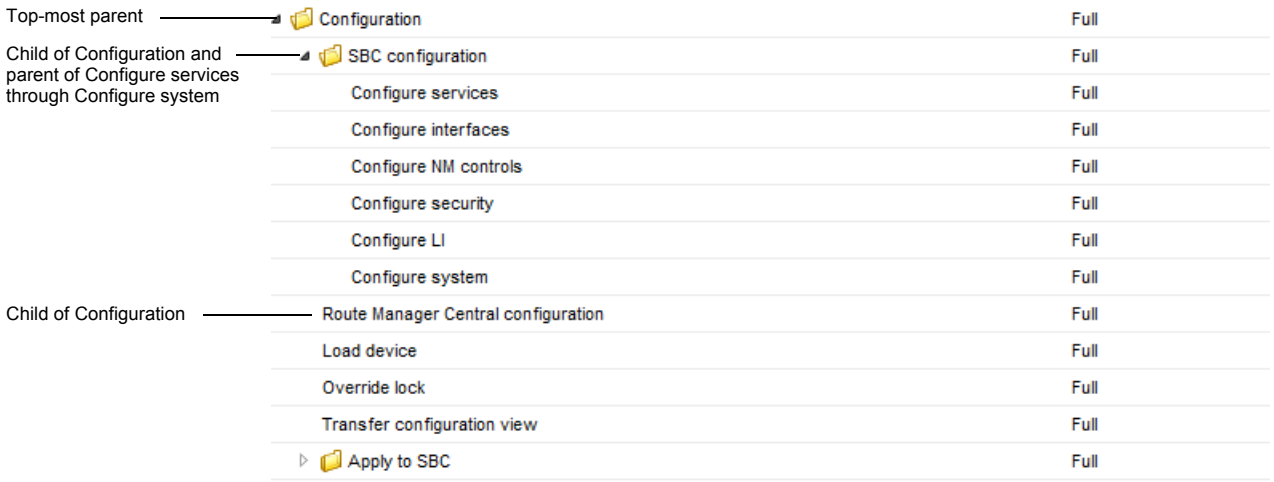


3. Click a category tab to access the list of operations for which you assign privileges. The Configuration operations appear by default.

Operations Tree

Operations are presented in a tree structure with the top of the tree being the operation tree root. Beneath the root there can be one or more operation categories that serve as

parents for individual operations (children). The following example shows the Configuration operations.



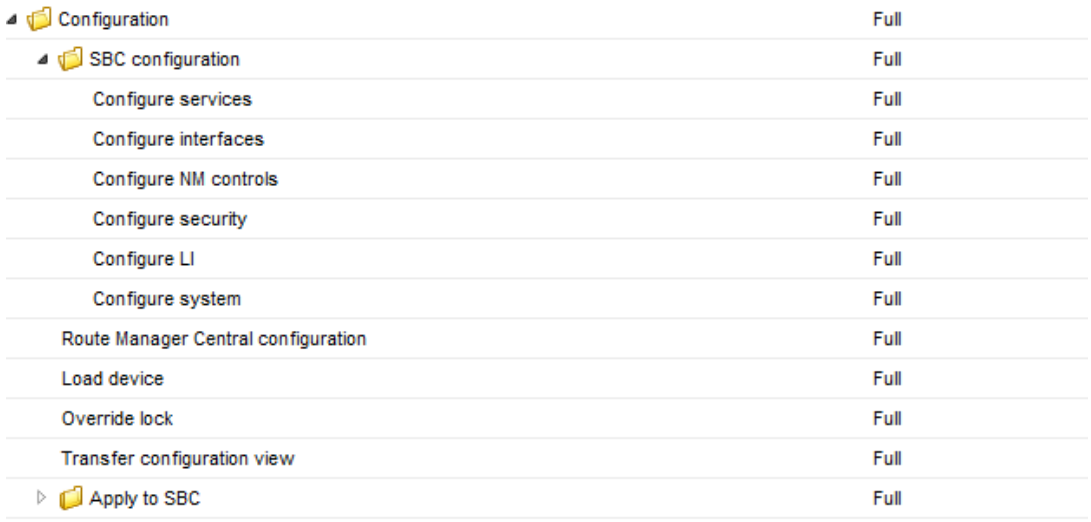
The types of privileges available for operations that are children of higher-level (or parent) operations are equal to or less than those for their parent. When you change the parent's privilege type you may or may not change the type for the children depending on the level of the privilege.

For example, the default type for SBC configuration and its child operations is Full as shown in the example above. If you change SBC configuration's type to View, which is a lesser privilege than Full, the type for all the child operations changes to View.

However, if you set the parent (SBCconfiguration) back to Full, the child operations remain at View. Full is considered a greater privilege than View. This greater privilege is not automatically reinstated for the child operations. You need to set each child operation back to Full one-by-one.

Configuration Operations

Configuration operations include those you perform to configure a Net-Net SBC, to configure Route Manager (if licensed for these applications), and to configure those operations Net-Net Central uses to facilitate the configuration process.



You can assign the following privileges:

- Full: View and modify configuration
- View: View but not modify configuration
- None: Operation does not appear in the Net-Net Central GUI

When you assign permission for SBC configuration operations, you assign it to all actions involved with that operation. For example, if you assign the Full privilege to the Configure service operation, the user can configure SIP realm, SIP interface, SIP options, SIP header manipulation and so on if configuring SIP service.

Element Manager and Route Manager Licensing

If you do not have licenses for the Element Manager or the Route Manager applications, the Configuration operations will not pertain to you. You can set the top-most operation (Configuration) to None to prevent the Configuration Manager and/or Route Manager sliders from appearing in the Net-Net Central GUI.

You can also select just those operations that belong to the applications you are licensed for to display the associated sliders in the Net-Net Central GUI. For example, you can set all configuration operations to None except for Route Manager Central configuration if you are licensed only for Route Manager. The Route Manager slider appears in the Net-Net Central GUI.

Operation Descriptions

The following table lists the operations along with a brief description.

Permission	Description
SBC configuration	**Set permission level for all the following configuration operations.**
Configure services	**Configure the signaling services for a Net-Net SBC. Includes SIP, DNS ALG, H.323, MGC{P, H248**
Configure interfaces	**Configure a physical and network interfaces for a Net-Net SBC.**

Permission	Description
Configure NM controls	Configure network management controls for multimedia traffic.
Configure security	Configure the following Net-Net SBC security features: • TLS • IPSec • RADIUS accounting and server authentication • packet tracing • password policy
Configure LI	Configure lawful intercept for the Net-Net SBC if licensed.
Configure system	Configure Net-Net SBC system
Route Management Central configuration	Allows Route Manager to be enabled, if licensed.
Load device	Allow user to manage SBC devices.
Override lock	Override a lock set by user on a managed device configuration.
Transfer configuration ownership	Transfer ownership of records in the local configuration view.
Apply to SBC	
Save configuration	Save the Net-Net SBC configuration edits made using Net-Net Central.
Save and activate configuration	Save and activate Net-Net SBC configuration edits made using Net-Net Central.
Activate configuration	Activate saved Net-Net SBC configuration edits made using Net-Net Central.

SBC System Maintenance

SBC system maintenance operations apply to Net-Net SBC system maintenance.

You can assign the following privileges:

- Full: Allowed to reboot Net-Net SBC
- None: Not allowed to reboot Net-Net SBC

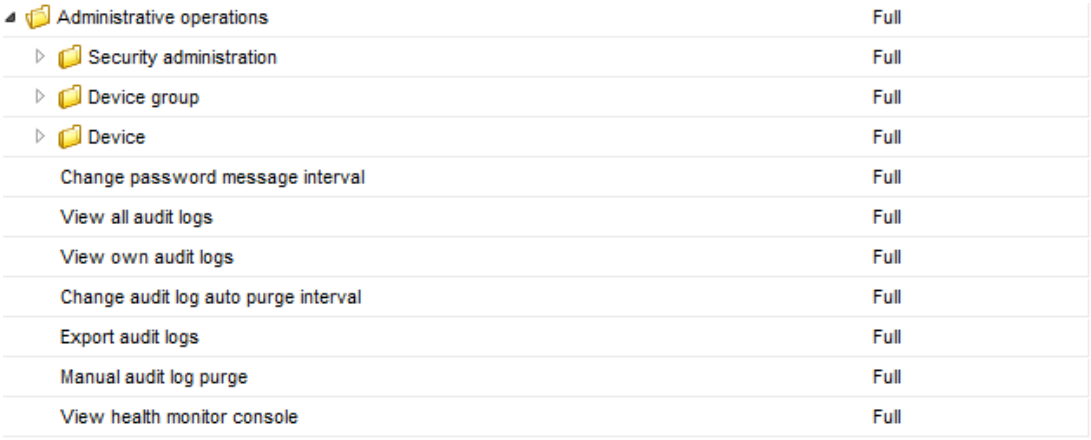
Operation Descriptions

The following table lists the Net-Net SBC system maintenance operations along with a brief description

Permission	Description
Reboot	Reboot the Net-Net SBC.

Administrative Privileges

Administrative privileges are for Net-Net Central administrative operations that include user management and device management. The following example shows default Administrative privileges for the administrator group. The default privilege setting might differ for a different type of user group.



You can assign the following privileges:

- Full: Allowed to perform administrative operation
- None: Not allowed to perform administrative operation

Operation Descriptions

The following table lists the administrative operations along with a brief description.

Operation	Description
Administrative operations	Set the privilege levels for all of the following administrative operations
Security administration	Set the privilege levels for all of the following user management operations accessible on the Security Manager slider
Group operations	Set privilege levels for all the following group operations.
Add group	Add a new group.
Update group	Modify groups.
Delete group	Delete existing groups.
User operations	Set privilege levels for all the following user operations accessible on the Security Manager slider
Add users	Create new users.
Update users	Modify user information.
Delete users	Delete existing users.
Reset password	Reset your password used to login to Net-Net RM.
Change password	Change another user's password used to login to Net-Net RM.
Change inactivity timer	Change the inactivity timer, which logs off the user if the client is no longer being used.

Operation	Description
Change Password Rule	Configure the password rules used when creating a new user.
Password notification	Change notification interval
Device group	Assign privilege to all of the following device group operations accessible through the Device Manager slider
Add device group	Add a new device group
Delete device group	Delete a device group
Move device group	Move a device group
Rename device group	Rename a device group
Device	Assign privilege to all of the following device operations accessible through the Device Manager slider
Add device	Add a new device
Remove device	Remove an existing device
Move device	Move a device
Change password message interval	Send alert that prompts user to change their password a certain number of days before their password expires
View all audit logs	View all audit logs
View own audit log	View only personal audit log
Change audit log auto purge interval	Configure the number of days of audit logs to keep
Export audit logs	Export all or part of an audit log to a file
Manual audit log purge	Manually purge audit logs
View health monitor console	Access health monitor console to detect issues

Fault Management

Fault management operations apply to the events and alarms that appear on the Fault Manager slider.

You can assign the following privileges:

- Full: Allowed to perform event or alarm operation
- None: Not allowed to perform event or alarm operation

Element Manager Licensing

If users are not licensed for the Element Manager, the Fault Management operations will not pertain to them. You can set the top-most operation (Events and Alarms) to None to prevent the Fault Manager slider from appearing in the Net-Net Central GUI.

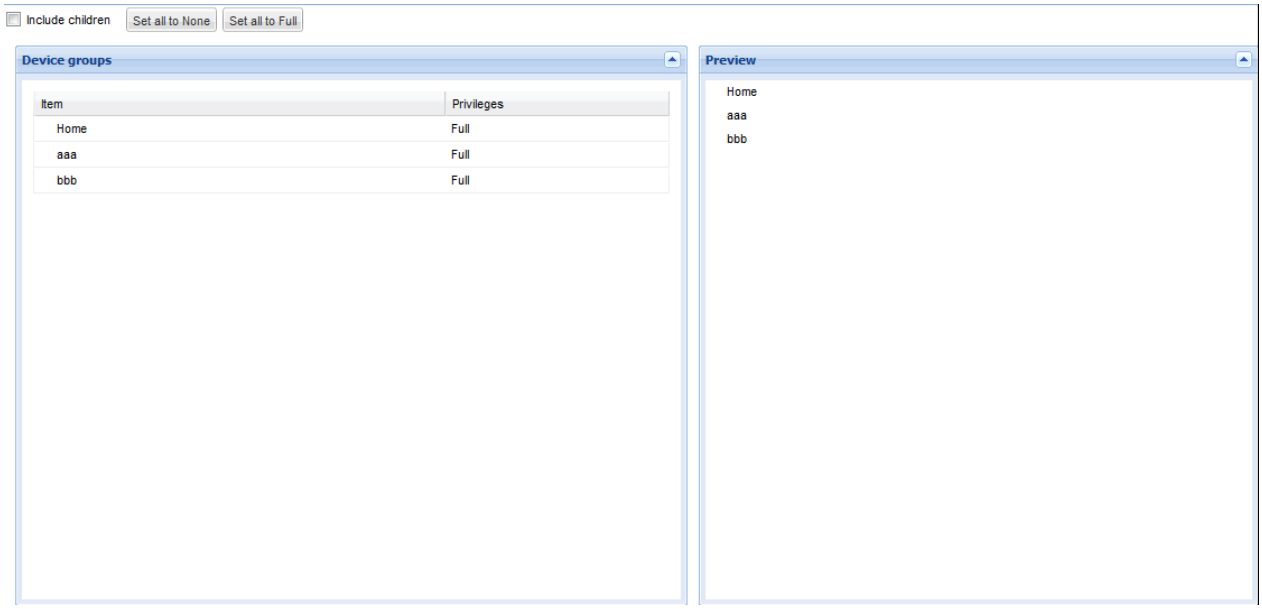
Operation Descriptions

The following table lists the fault management operations along with a brief description

Permission	Description
Events and Alarms	Assign the privileges for all of the following event and alarm operations accessible on the Fault Manager slider.
Alarms	Assign the privileges for all of the following alarm operations accessible on the Fault Manager slider.
Set email notification	Create an email list for alarms.
Delete alarm	Delete alarms.
Remap severities	Edit the alarm severity levels.
Events	Assign the privileges for all of the following event operations accessible on the Fault Manager slider.
Delete events	Delete events.

Device Group Instances

Device group instance privileges apply to device groups displayed on the Device Manager slider. The Device group instances tab lets you assign privileges and preview the device group hierarchy based on the privileges selected. That hierarchy will be reflected on the Device Manager slider.



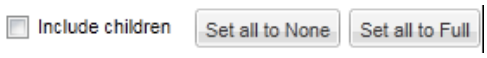
The Device groups column displays the device groups contained on the Device Manager slider. The Preview column displays the device group hierarchy based on the privileges assigned. Device groups with the privilege set to None do not appear in the Preview column.

You can assign the following privileges:

- None: Users do not have authorization to that device group. The group will not be displayed on the Device Manager slider. The device group also does not appear in the Preview column.
- View: Users can view the group on the Device Manager slider but cannot perform any operations such as adding or deleting a child group.
- Full: Users can view the groups on the Device Manager slider and perform all operations. If the user adds a new device group, the default privilege for that new group is Full.

Operation Descriptions

The following checkbox and buttons appear when you access.Device Group Instances operations



The following table describes the

Permission	Description
Include children	If selected, changing privilege type for a device group changes the privilege for any child group to the same value
Set all to None	Set the privilege for all groups to None
Set all to Full	Set the privilege for all groups to Full

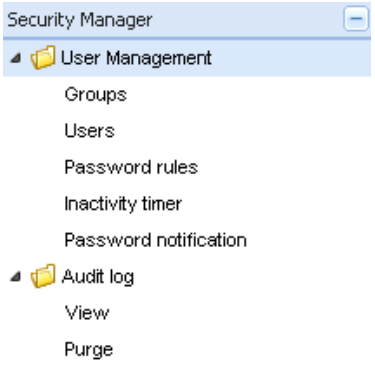
Managing User Groups and Users

Managing users means you have administrator access and can create new user groups and assign the group operational privileges, can create and assign new users to these groups, and can edit existing user groups and users.

Accessing User Management

To access user management:

1. While logged into Net-Net Central, expand the Security slider in the Navigation bar.
2. Expand the User Management directory.



From here you can access all user management functionality.

Creating User Groups

To create user groups:

1. Click Groups in the Navigation bar. A table of user groups appears in the content body.

User Groups

Group name	# users	Configuration access	System maintenance ac	Administrative operation	Fault management acce
LIAdministrators	1	Full	Full	Full	Full
administrators	2	Full	Full	Full	Full
provisioners	1	Partial	Full	Partial	Partial
monitors	1	None	None	None	Partial
grp_adm	1	None	Full	Full	Full
grp_pro	1	None	Full	Full	Full
grp_mon	1	None	None	None	Full

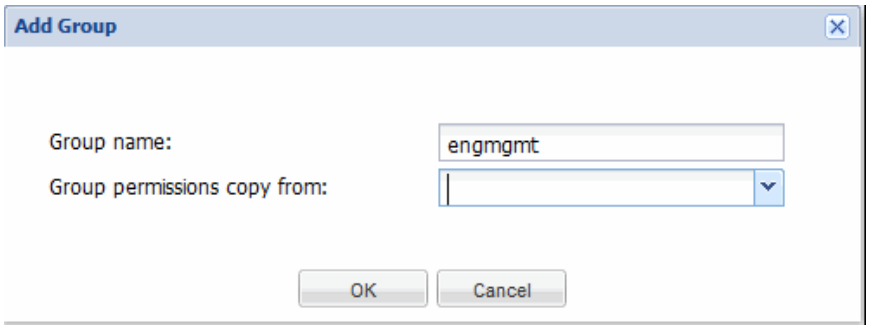
The table displays all of the operations categories with the current privilege levels for each user group. Each group can have one of three types of authorization access:

- Full: Full authorization for all operations in this category
- Partial: Limited authorization for the operations in this category
- None: No authorization for the operations in this category

Setting authorization means you assign permissions to the group to which a user belongs. The permissions for that group are also assigned to the user. When a user logs into Net-Net Central, they can access features and functionality based on the

permissions assigned to them. You can review the specifics for each category to see what operations are allowed or disallowed.

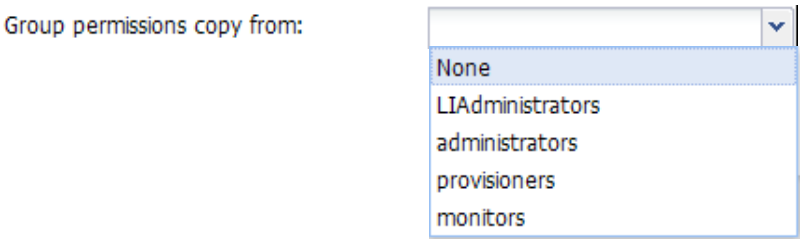
2. Click **Add**. The Add Group dialog box appears.
3. **Group name**—Enter a name for this group.



Guidelines for the group name include the following:

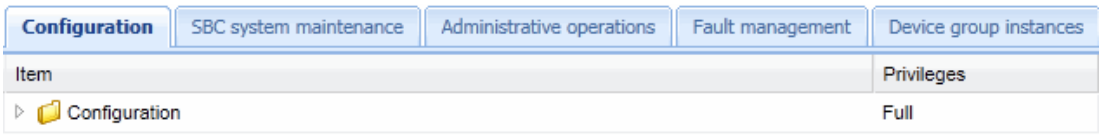
- minimum of 3 characters and maximum of 50
- name must start with an alphabetical character
- alphanumeric characters, hyphens, and underscores are allowed
- case insensitive
- must be unique, cannot be the same as an existing group name

4. **Group permissions copy from**—Choose an existing group from the drop-down list or choose None to manually configure the permissions.



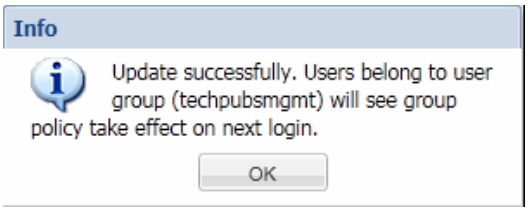
5. Click **OK**. A message appears indicating success.
6. Click **OK** to clear the message.

   If you did not choose to inherit permissions from an existing group, you need to configure them.
7. Click the new group name in the table and click Edit. The operations tabs appear.



8. Assign privileges. See Operations and Privileges for details.

9. Click Apply to assign the privileges. A confirmation message appears.



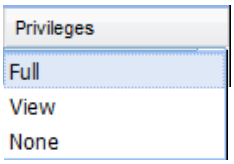
10. Click OK to clear the message.
11. Click Back to return to the User Groups table.

Setting Privilege Type

Within each category, you set the type of privilege for the operations contained in that category. For most of the categories you set it to one of two types, Full or None. For the Configuration and Device instances categories, you also have the View type.

To set privilege type:

1. Click the operation row in the table under Privilege. The drop-down list is activated.



2. Choose the appropriate privilege type.
3. Press Enter to accept the selected type.
4. Click Apply.

   Refer to the following sections for more details about the operations you sent privileges for and the types of privileges that apply to each category of operations.

Creating Users

To create users:

1. Click Users in the Navigation bar. A table of users appears in the content body.

Users

User name	Group	Status	Operation status
Lladmin	LlAdministrators	enabled	active
admin	administrators	enabled	active
usr_adm	administrators	enabled	active
san_adm	grp_adm	enabled	active
san_mon	grp_mon	enabled	active
san_pro	grp_pro	enabled	active
usr_pro	monitors	enabled	active
usr_mon	provisioners	enabled	active

The following table describes the information that appears.

Column	Description
User name	Name of the user
Group	Name of the group to which the user belongs
Status	Status of the user's account either enabled or disabled
Operation status	State of the user's account with respect to expiration dates: • Active: Account is valid and the user can log in. Neither the account nor password expiration dates have been exceeded. • Account expired: Account expiration date has expired. • Password expired: Password expiration date has expired. • Password deactivated: User's failed logins exceeded the allowed number of tries as specified by the value set for Password reuse count parameter in Password rules. • Locked out: User has exceeded the login failures and the account is disabled until the lockout duration has passed.

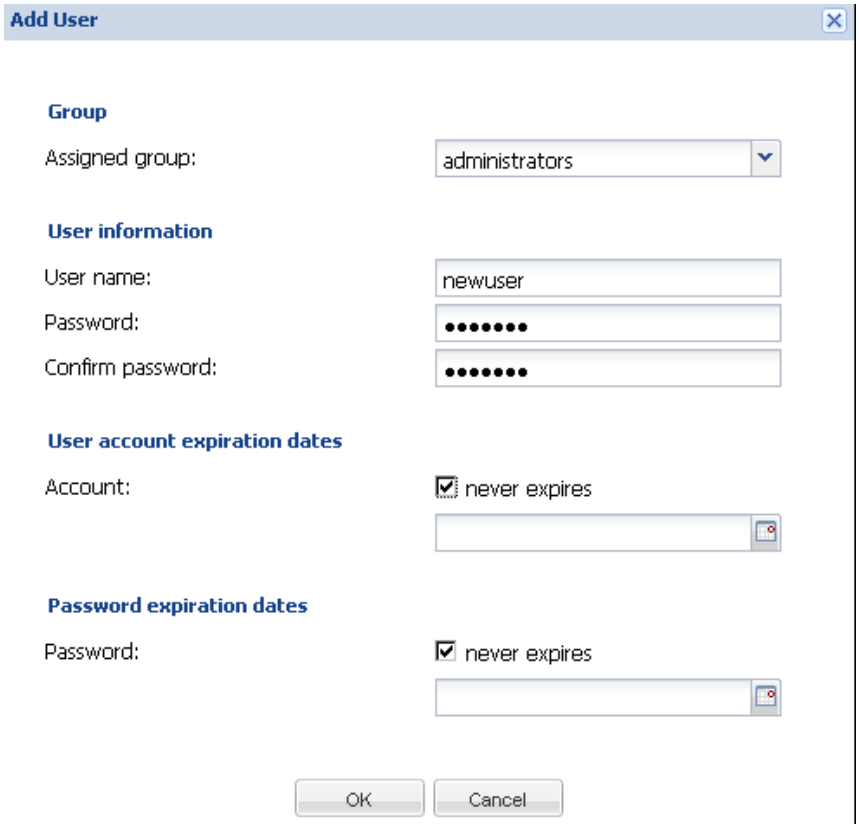
2. Click **Add**. The Add User dialog box appears.
3. **Assigned group**—Choose the group to which you want to add the user. The permissions for that group apply to this user.

4. **User name**—Enter the user's name using the following guidelines:
   - minimum of 3 characters and maximum of 50
   - name must start with an alphabetical character
   - alphanumeric characters, hyphens, and underscores are allowed
   - case insensitive
   - cannot be the same as an existing group name
5. **Password**—Enter the password for this user using the following guidelines.
   - **Numeric:** Use of at least one numeric character from 0 to 9 in the password
   - **Alphabetic character**: Use at least one character from the English language alphabet in the password.
   - Special characters include {, |, }, ~, [, \,], ^, _, ‘, :, ;, <, =, >, ?, !, “, #, $, %, &, `, (,), *, +, ,, -, ., and /
6. **Confirm password**—Enter the password for this user again to confirm it.
7. **Expiration Date: Account**—Click the calendar icon to open a calendar to choose the date after which the user's account expires and blank out the checkbox.

   Leave the checkbox checked (default) if you want the account to not expire.

8. **Expiration Date: Password**—Click the calendar icon to open a calendar to choose the date after which the user's password expires and blank out the checkbox.

   Leave the checkbox checked (default) if you want the password to not expire.



9. Click **OK**.

Adding Administrative Users

When adding a device in the NNC GUI, you are asked to input a User name for the device. It is possible that the user name you supply does not have administrative privilieges, and therefore, certain operations are restricted. In this event, a warning message is sent:

```
Warning: the user XXX is not known by NNC to be an administrator
on the device. Would you like to proceed? (Yes/No):
```

By default, each device has one administrative user to begin: admin. In order to add more user names to this admin list, you must modify the sbcAdmins.conf file. The file is located in the following directory within NNC installation:

```
<NNC folder>/conf/device/sbcAdmins.conf
```

Once you modify this file by adding an Administrative user, you must restart NNC in order for the changes to be applied.

To add users to the administrative user list:

1. In Superuser mode, navigate to the file <NNC folder>/conf/device/sbcAdmins.conf.
2. Edit the sbcAdmins.conf file using any text editor.
3. Type the name to append to the admins list.
4. Save the file.

For example:

```
# This file contains a listing of all SBC usernames NNC will
consider as "admins".

# By default, this file contains just the "admin" username.

# To add a new username, simply append a new line containing just
the username.

admin

Robert
```

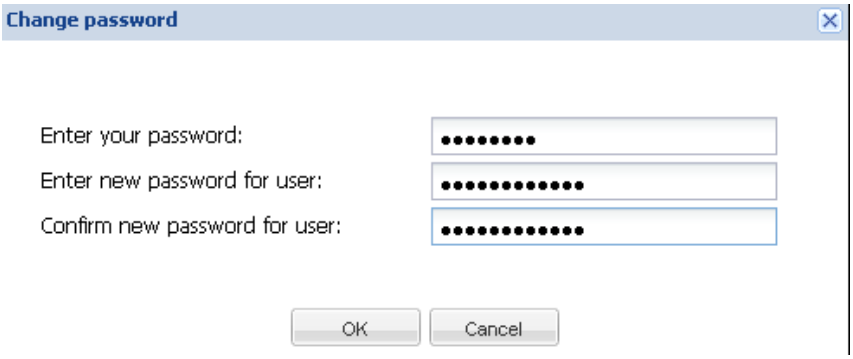
5.

Changing Passwords

If you have administrative operations permission, you can change a user's password.

To change a user password:

1. Click a user from the table and click **Change Password**. The Change Password dialog box appears.
2. **Enter your password**—Enter your password to be able to change the user password.
3. **Enter new password for user**—Enter the new password for this user.
4. **Confirm new password for user**—Enter the new password for this user again to confirm it.



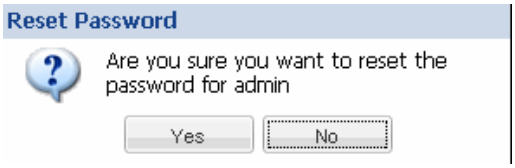
5. Click **OK**.

Resetting Passwords

If you have permission to reset passwords, you can reset user passwords.

To reset user passwords:

1. Click a user from the table and click **Reset Password**. The Reset Password window appears prompting for confirmation you want to reset the password.



2. Click **Yes** to reset it or **No** to exit the window and quit the reset process.

Editing User Groups and Users

This section contains information about editing existing user groups and users.

Editing Groups

You can edit operations and privilege levels assigned to user groups, with the exception of the default groups provided by Net-Net Central.

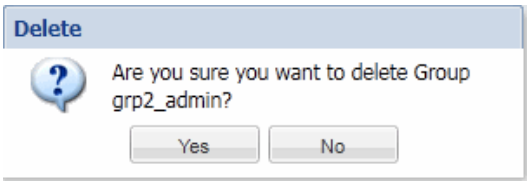
To edit groups:

1. On the Security Manager slider, choose Groups under User Management.
2. Click the row in the table for the group you want to edit and click Edit. The operations tabs appear.
3. Make your edits to the group privileges. See Creating User Groups for details.

Deleting Groups

To delete a group:

1. On the Security Manager slider, choose Groups under User Management.
2. Click the row in the table for the group you want to delete and click Delete. A confirmation message appears.



3. Click No to cancel the deletion or Yes to continue. A confirmation message appears.
4. Click Yes to clear the message. The user group is removed from the User Groups table.

Editing Users

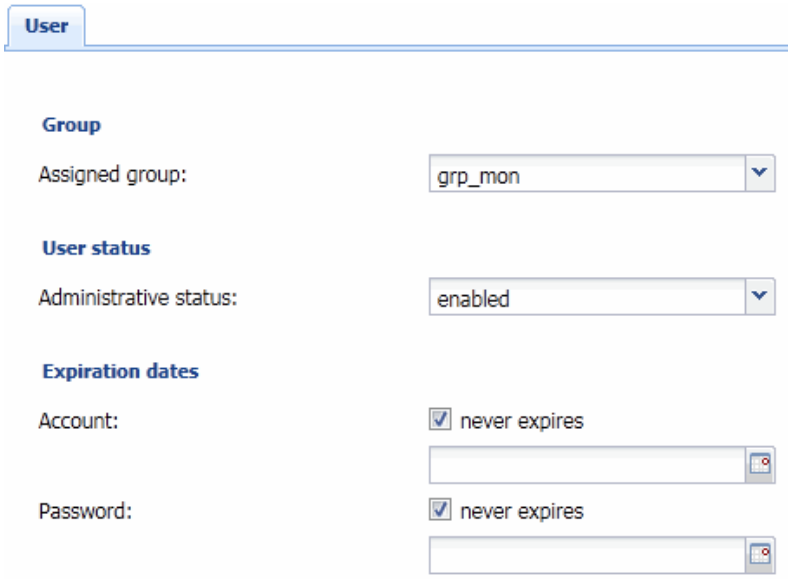
You can edit users and change the following user information:

- group association
- status
- account expiration
- password expiration

To edit users:

1. On the Security Manager slider, choose Users under User Management.

2. Click the row in the table for the user you want to edit and click Edit. The User information appears in the Content pane.



3. Assigned group—Click the down arrow to display all user groups and choose a new group.
4. Administrative status—Click the down arrow and choose a new status, either enabled or disabled. When their account is enabled, a user can login as long as their account and password expiration dates are valid. When their account is disabled, a user is denied access to Net-Net Central. They cannot login even if their account and password expiration dates are valid.
5. **Expiration Date: Account**— Leave the checkbox checked (default) if you want the account to not expire. Click the calendar icon to open a calendar to choose the date after which the user's account expires and blank out the checkbox.
6. **Expiration Date: Password**—Leave the checkbox checked (default) if you want the password to not expire. Click the calendar icon to open a calendar to choose the date after which the user's password expires and blank out the checkbox.
7. Click Apply.

Reactivating User Accounts

A user can be denied access to Net-Net Central if their account is disabled, expired, the password expired or failed to login more than is allowed by the Password reuse count value.

You can reactivate a user's account by to editing the user profile to reset the status to enable, then reset the expiration in days for account and password. Or you can delete the expired account and recreate it by adding a new account for the same user.

The following table lists the possible causes for user account deactivation and how to reactivate it.

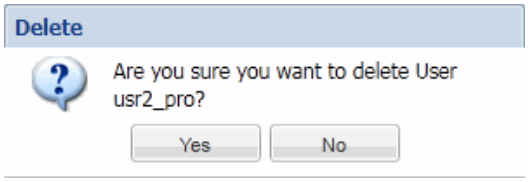
Cause	Action
Account expired	Reset the account calendar to a new date
Password expired	Reset the password calendar to a new date

Cause	Action
Password deactivated	Reactivate the user's account by: • Changing the user password if all expiration dates are still valid • Extending the account expiration date • Extend the password expiration date
Account disabled	Reset the user account to enabled.

Deleting Users

To delete users:

1. On the Security Manager slider, choose Users under User Management. The Users table appears in the Content pane.
2. Click the row in the table for the user you want to delete and click Delete. A confirmation message appears.



3. Click No to cancel to deletion or Yes to continue. A message indicates the deletion was successful.
4. Click OK to clear the message. The user name is removed from the Users table.

Changing Password Rules

This section explains how you can change the password rules. The password rules determine the format of the passwords administrators enter when creating new users. You can specify the length of the password, how many times it can be reused, and whether specific characters, such as a numeric value, can be used.

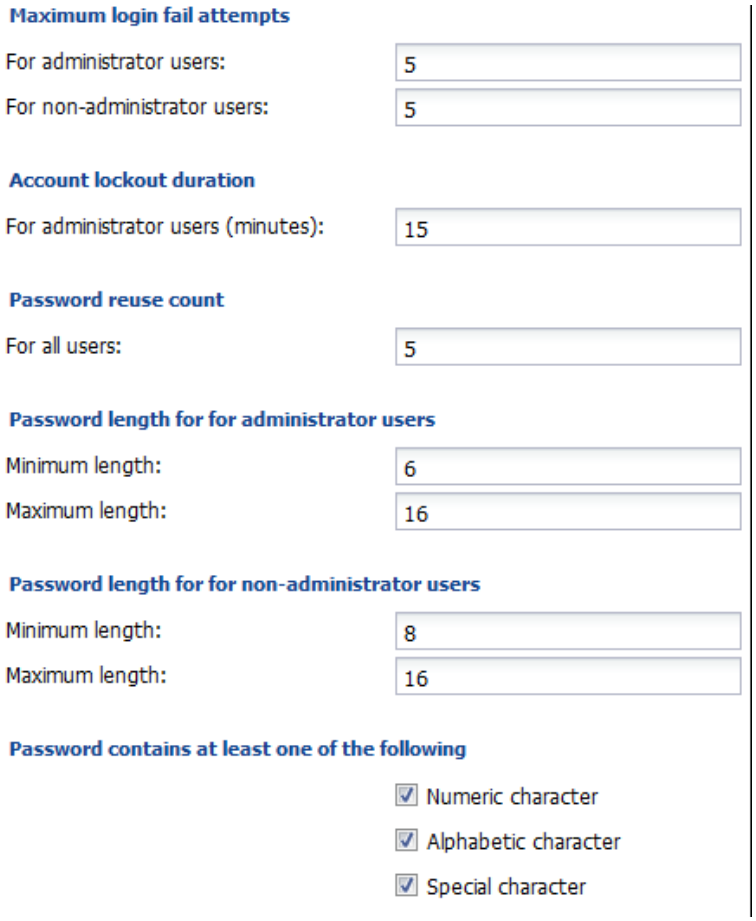
To change the password rules:

1. Click Password Rules under User Management.
2. **Maximum login fail attempts**—Enter a value that indicates the maximum login attempts allowed before the user is locked out of the system. You can set a different value for both Administrator users and Non-administrator users. The default value is 5 attempts.
3. **Account lockout duration**—Enter the number of minutes that an administrator user will be locked out after the **Maximum login fail attempts** value has been reached. The default value is 15 minutes. For example, if you set the **Account lockout duration** value to **8**, and the **Maximum login fail attempts** value is set to **5,** an administrator user would be locked out for 8 minutes after 5 failed attempts to login.

   Note: This parameter applies to Administrator users only. Non-administrator users remain locked out until their login is reset.

4. **Password reuse count**—Enter a value that indicates the number of counts to use to prevent the reuse of a password. The reuse count restricts the user from reusing the password entered in the last *x* number of counts. For example, if you enter 2 here the user cannot reuse the same password used on the previous two occasions.
5. **Password length for administrator users**—Enter the values for the minimum and maximum length of a password for a user who has Administrator privileges.
   - Minimum length: no less than 8 characters
   - Maximum length: up to 16 characters
6. **Password length for non-administrator users**—Enter the values for the minimum and maximum length of a password for a user who does not have Administrator privileges. Maximum value for this field is 16 characters.
   - Minimum length: no less than 8 characters
   - Maximum length: up to 16 characters
7. **Password contains at least one of the following**—Click the checkbox for each rule you want to enforce.
   - **Numeric:** Use of at least one numeric character from 0 to 9 in the password
   - **Alphabetic character**: Use at least one character from the English language alphabet in the password.

- **Special**: Use at least one special or punctuation character in the password. Special characters include {, |, }, ~, [, \,], ^, _, ‘, :, ;, <, =, >, ?, !, “, #, $, %, &, `, (,), *, +, ,, -, ., and /.



8. Click **Apply**. The password rules are saved and the window closes.

Modifying the Inactivity Timer

This section explains how to modify the inactivity timer. The inactivity timer logs off the user from the Net-Net Central session when it's value is exceeded. The user must re-enter their password to continue. You can set different values for a user with administrative permissions and users who do not have administrative permissions.

> **Note:** The default value for an administrator account's inactivity timer is set to 0 (never expire). You must set a different value in order to terminate the user's session after a specefied period of time.

To modify the inactivity timer:

1. From the Navigation bar, click Inactivity timer. The inactivity timer information appears in the content area.
2. **Admin**—Enter the number of minutes of inactivity after which the user with administrative permissions is logged off. The range is zero (0) to 65535. Zero (0) disables the inactivity timer.
3. **Non-Admin**—Enter the number of minutes of inactivity after which the non-administrator user is logged off. The range is one (1) to 65535.

4. Click **Apply**.

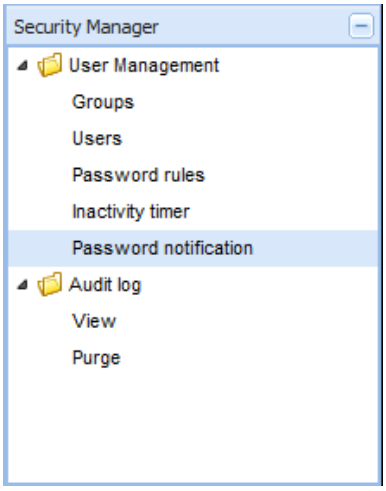
Configuring Password Notification Interval

You can configure the length of the interval after which you want to prompt the user logging in to change their password. When the user logs into Net-Net Central, the system checks their credentials and their password expiry time. If the password is due to expire, Net-Net Central displays a warning and prompts the user to change their password.

> **Note:** The value set here is applicable to all users, you cannot set it on a per-user basis.

To configure password notification interval:

1. Click `Password Notification Interval` under User Management



2. Enter the number of days, after which the user is prompted to change their password. Range is 1 to 31 days.

3. Click **Apply**.

Audit Logs

The audit log provides information about the changes made using Net-Net Central. The audit log contains audit trails. Audit trails enable you to view all operations that have been performed, the time they were performed, whether they were successful, and who performed them.

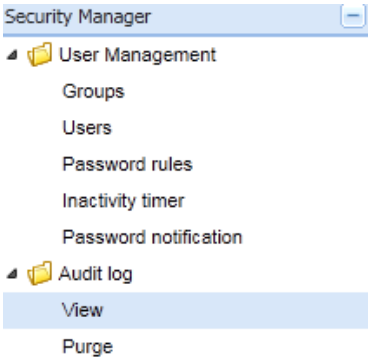
> **Note:** The downloaded CSV file is limited 250 entries. Only the active page's entries are saved.

Viewing and Saving Audit Logs

To view or save an audit log:

1. While logged into Net-Net Central, expand the Security slider in the Navigation bar.
2. Expand the User Management directory.

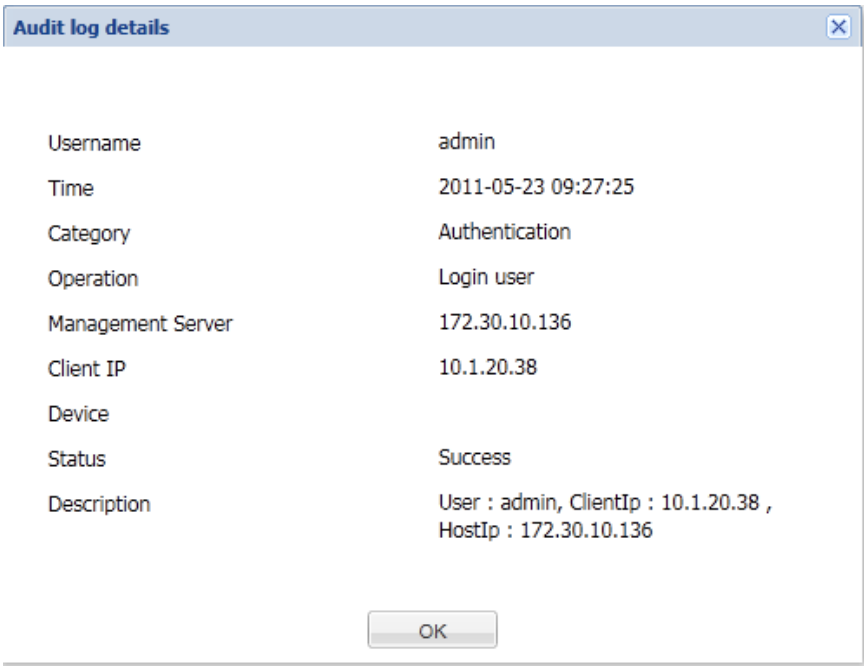
3. Choose View under Audit Log



The audit log table appears in the content area.

Username	Time	Category	Operation	Status	Device
admin	2011-05-23 09:27:25	Authentication	Login user	Success	
admin	2011-05-23 10:22:08	Device	Add device group	Success	
admin	2011-05-23 10:22:13	Device	Add device group	Success	
admin	2011-05-23 10:22:46	Device	Add device	Success	172.30.10.116
admin	2011-05-23 10:23:09	Device	Add device	Failed	172.30.10.113
admin	2011-05-23 10:23:21	Device	Add device	Success	172.30.10.117
admin	2011-05-23 10:23:49	Device	Add device	Success	172.30.10.114-172.30.1
admin	2011-05-23 10:24:08	Device	Move device to device g	Success	172.30.10.116
admin	2011-05-23 10:24:14	Device	Move device to device g	Success	172.30.10.116
admin	2011-05-23 10:24:20	Device	Move device to device g	Success	172.30.10.116
admin	2011-05-23 10:24:25	Device	Move device to device g	Failed	
admin	2011-05-23 10:24:48	Device	Move device to device g	Success	172.30.10.117
admin	2011-05-23 10:24:54	Device	Move device to device g	Success	172.30.10.117
admin	2011-05-23 10:25:00	Device	Move device to device g	Success	172.30.10.114-172.30.1
admin	2011-05-23 10:25:33	Device	Device license associati	Success	
admin	2011-05-23 10:39:54	Authentication	Logout user	Success	
admin	2011-05-23 10:40:35	Authentication	Login user	Success	
admin	2011-05-23 10:40:41	Authentication	Login user	Success	
admin	2011-05-23 12:28:27	Authentication	Login user	Success	
admin	2011-05-23 13:36:38	Device	Reboot device	Success	172.30.10.116
admin	2011-05-23 13:41:02	Authentication	Logout user	Success	
admin	2011-05-23 14:06:03	Authentication	Login user	Success	
admin	2011-05-23 14:06:04	Authentication	Login user	Success	
admin	2011-05-23 14:22:56	Configuration	Load Configuration	Success	172.30.10.117
admin	2011-05-23 15:38:03	Authentication	Login user	Success	
admin	2011-05-23 16:15:04	Configuration	Add element	Failed	172.30.10.117
admin	2011-05-23 16:15:19	Authentication	Logout user	Success	

4. Click a row in the table and click Details. The Audit log details window appears.



Audit trails include the following information:

- Name of the user who performed the operation
- Time the operation was performed by the user
- Category of operation performed by the user
- Specific operation performed by the user
- Address of the management server accessed
- IP address of the client that was used
- Device the user performed operation upon
- Status of the operation performed by the user, whether it was successful or failed
- Description of the operation

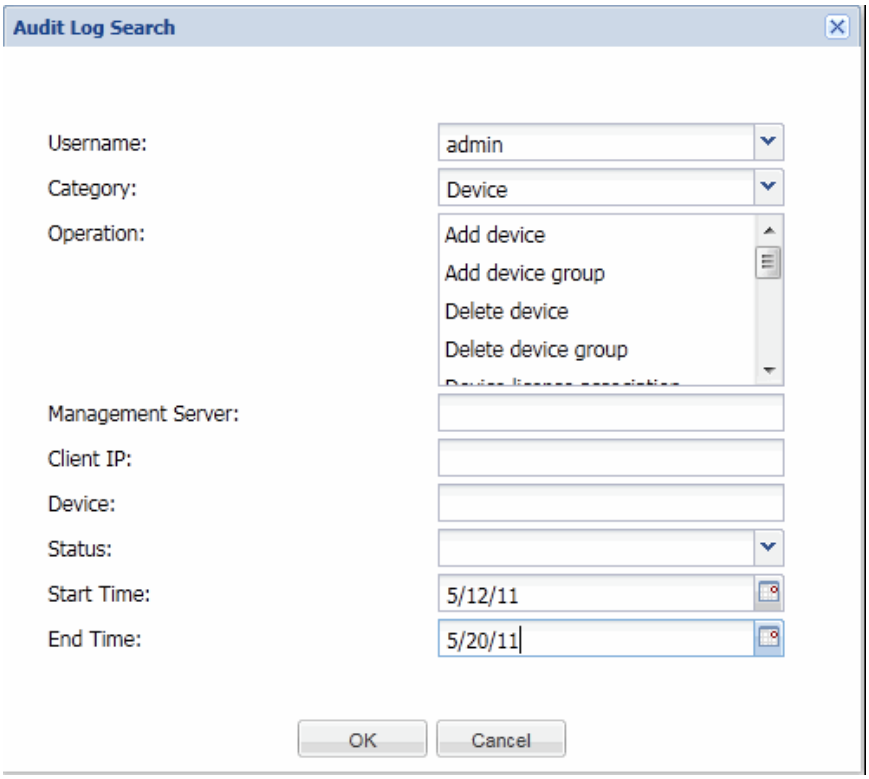
5. Click OK to exit the window.
6. Click Save to file to open the audit log file or save it to a file.

Searching the Audit Log

You can search the audit log using one or more criteria.

To search the audit log:

1. Click Search. The Audit Log Search dialog box appears.
2. **Username:**—Choose a user name from the drop-down list.
3. **Category:**—Choose a category from the drop-down list.
4. **Operation:**—Choose an operation from the drop-down list.
5. **Management Server:**—Enter the IP address of a management server.
6. **Client IP:**—Enter the IP address of a client.
7. **Device:**—Enter a device IP address.
8. **Status:**—Choose a operation status from the drop-down list.
9. **Start Time:**—Choose a start time from the calendar.
10. **End Time:**—Choose an end time from the calendar.



11. Click **OK** to search using the configured criteria and close the dialog box.
12. Click **Cancel** to cancel your configured criteria and close the dialog box.

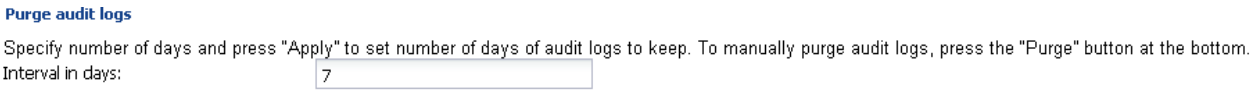
Purging Audit Log Files

If you have the permission assigned, you can configure the number of days of audit logs to keep. You can also manually purge audit logs.

To purge audit log files:

1. While logged into Net-Net Central, expand the Security slider in the Navigation bar.
2. Expand the User Management directory.
3. Choose Purge under Audit Log

4. **Interval in days:**—Enter the number of days for which you want to keep audit logs.



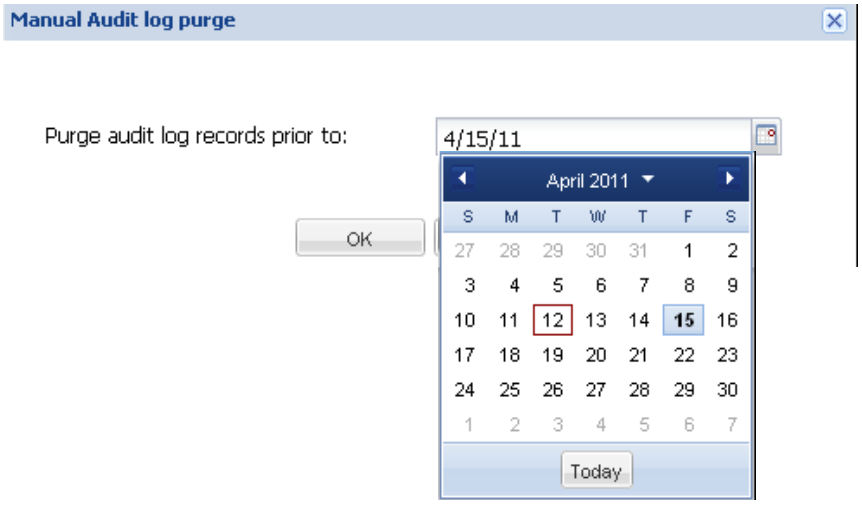
5. Click **Apply**.

Manually Purging

To manually purge audit logs:

1. With the purge audit log information displayed in the content area, click **Purge**. The Manual Audit log purge dialog box appears.

2. **Purge audit log records prior to**—Choose the date from the calendar prior to which you want audit logs purged.



3. Click **OK**.