NSP
Network Services Platform
Release 23.8

User Manager Application Help

3HE-18997-AAAB-TQZZA
Issue 1
August 2023

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

About this document

Purpose

The *User Manager Application Help* introduces the User Manager application GUI to operators and administrators by describing application usage and features.

Scope

The help for User Manager covers the full set of application features; however, some feature sets described in the help require the purchase and configuration of additional feature packages.

See the *NSP System Architecture Guide* for more information about feature packages and installation options.

User Manager functions are available for OSS using programmable APIs. For general information about developer support, see the API documentation page on the Network Developer Portal.

For specific documentation about REST APIs for User Manager, click on API Reference in the User Manager row.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to documentation.feedback@nokia.com.

1 User Manager

1.1 What is User Manager?

With the User Manager application, you perform four centralized administrative functions for NSP users:

- User session management: monitor active user sessions in NSP; see 3.1 “What is session management?” (p. 27).
- User activity logging: monitor user events in NSP applications; see 2.1 “What is user activity logging?” (p. 21).
- User Access Control: create NSP user groups and create roles to assign group access to applications, network resources, and Analytics resources.

  A Lawful Intercept user role allows designated LI users to navigate NSP applications without being monitored by user activity logging.

  In CLM deployments, User Access Control applies to CLM users.
- Local user account management: create and modify local NSP user accounts. Import user accounts from NFM-P.

1.2 What is User Access Control?

NSP User Access Control (UAC) is disabled by default in User Manager. While UAC is disabled, users continue with the same access they currently have to applications and resources. For example, users could be managed through an NFM-P user database or a WS-NOC user database. User access to applications and resources are defined at the application level. A user's user group defines what they can access within the application.

When UAC is enabled, access is assigned at the NSP level and applies across multiple applications. Users will see their specified NSP access rights enforced when they login to NSP. The user access configuration specified in User Manager is enforced **in place of** any pre-existing access control setup (from NFM-P or WS-NOC). Local NSP user access to NSP resources is always controlled through User Manager, regardless of whether UAC is enabled or not.

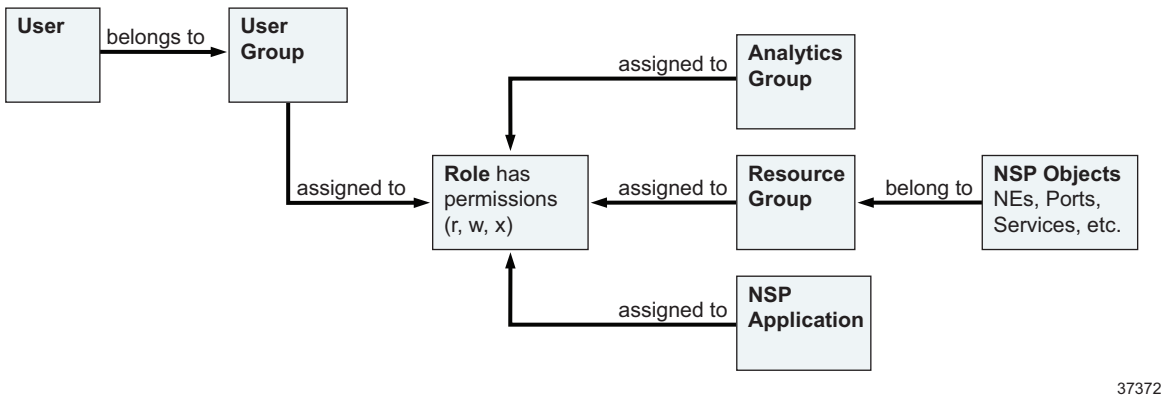
As a network evolves, an NSP administrator must create or modify user groups, roles, and resource groups to provide the required user access. Be aware of application dependencies. For example, Fault Management alarm information is required by other applications such as Network Supervision, and Service Supervision. An operator who requires access to such an application also requires Fault Management access.

When NSP UAC is enabled, it controls user access to NSP applications independently of the user management systems in NFM-P or WS-NOC.

NSP UAC does not apply to WS-NOC or NFM-P (GUI or OSS client sessions), where pre-existing user access control mechanisms in those applications are retained. If you are maintaining your NSP user accounts in an NFM-P user database, all NFM-P functions relating to user lifecycle management, such as password expiry time frame or failed-login lockout, will affect NSP user

access as well. When NSP is deployed with the OAUTH2 module, local NSP user accounts that are created within User Manager are configured for UAC and lifecycle management entirely within User Manager.

Figure 1-1 User Access Control architecture



1.2.1 Roles

A role object specifies which resources and NSP applications its associated user groups can access. Network resource access is assigned to a role through resource groups, while application access and Analytics resource access are specified directly on a role object.

NSP administrator role

A predefined NSP administrator role, user group, and admin user account are automatically created during NSP system installation and cannot be modified. The admin user has full access to all applications and resources, and can define the roles and resource groups that are assigned to user groups. The admin user can create additional roles with the Administrator designation, which carries the same unlimited application and resource access.

Lawful Intercept role

The Lawful Intercept (LI) role designation is intended for use with an LI user group. The activities of LI users are not tracked under the User Activity Logging function. The admin user must assign application and resource access to Lawful Intercept-designated roles.

1.2.2 User groups

In User Manager, a user group associates a group of NSP users with one or more roles, thereby enabling user access to applications and resources. Administrators create user groups and assign roles to them, according to the type of network activities the user group is meant to perform. When a role is assigned to a user group, all users within the group have the same access to resources and applications, as specified on the role. A user group can be assigned multiple roles to allow broader access rights for its users.

Individual NSP users can be created by external authentication sources (NFM-P, LDAP, RADIUS, TACACS) where users are assigned to corresponding user groups. In order for the members of a user group to have access to NSP resources and applications, the user group name returned by the authentication source must exactly match a corresponding user group name in the User Manager application.

Local NSP users and user groups can also be created in User Manager when NSP is configured with the OAUTH2 module.

Users requiring WS-NOC access require a user group assignment that maps to a predefined WS-NOC role; for information, see *To map external user groups to predefined WS-NOC roles* in the *NSP Installation and Upgrade Guide*.

1.2.3 Resource groups

A resource group can be a collection of network equipment or services which can be assigned to a role. The role is assigned to a user group, thereby granting the user group access to the network resources in the resource group.

Resource groups are defined in the NSP Group Manager application. The term “Equipment Group” in User Manager includes both NE and port resource groups created in Group Manager.

1.3 Workflow: Configure NSP user access control

This workflow describes the recommended order of tasks to configure user access control across NSP. The sequence of tasks outlined here is especially recommended if you are setting up user access control in NSP for the first time. Once you have user access control deployed in NSP, you can configure your user groups, roles, and resource groups in any order.

Prerequisite: create group directories and resource groups

1

You create group directories and resource groups in the NSP Group Manager application. Resource groups are applied to role objects in User Manager to grant user access rights to network resources.

Optional: configure Analytics reporting

2

If you are using Analytics reporting in NSP, you must fully configure the Analytics application and Analytics server prior to configuring Analytics resource access in your roles. You cannot configure Analytics resource access on a role if Analytics is not running in NSP.

Create roles

3

Create roles according to the type of tasks your user groups will be performing, and the types of resources they will need to access. A role object specifies access rights to specific NSP applications and resources.

See 1.5 “How do I configure a role?” (p. 12)

Import or create user groups

4

Choose one of the following options:

- If you have been working with a user access control configuration from NFM-P, it is strongly recommended that you import your user groups from NFM-P. This ensures that all of your existing users are included in the new access control setup, and helps ensure a seamless transition from the NFM-P setup; see 4.3 “How do I import users and groups from NFM-P?” (p. 30).

  If NSP is deployed with the OAUTH2 module, the import operation imports user groups **and** user accounts from NFM-P.
- If you are configuring user access control to work against an external authentication sources (NFM-P, LDAP, RADIUS, TACACS), create new user groups; see 1.8 “How do I configure a user group?” (p. 18).

Enable User Access Control

5

Note: When you enable User Access Control in NSP, individual users will see their specified access rights enforced when they login to NSP. The user access configuration you specified in User Manager is enforced **in place of** any previously-existing access control setup, except in NFM-P and WS-NOC, where user access continues to be defined within those applications. Local NSP user access to NSP resources is always controlled through User Manager, regardless of whether UAC is enabled or not.

Once you have configured (and reviewed) your user groups and their associated roles, you can enable user access control.

See 1.9 “How do I enable access control?” (p. 19)

1.4 How do I configure alarm access using roles?

Users can only view alarms for objects that are included in the resource groups assigned to their roles. Viewing service-related alarms requires access to the appropriate service-related objects.

Consider the following when configuring service-related alarm access:

- Service Site: the user must have access to the associated NE and service to view alarms for a service site.
- SAPs: the user must have access to the associated service and the (NE | port) to view alarms for a SAP.
- Physical Links: the user must have access to all endpoint objects to view alarms for a physical link.
- LAGs: the user must have access to the associated NE to view alarms for a LAG.
- Tunnel Bindings: the user must have access to the associated NE and service to view alarms for a tunnel binding.
- Top Unhealthy NEs page in Fault Management: the user must have access to any NEs that might appear in the page.

The following workflow describes the high-level steps required to create a role intended for alarm management and assign it to a user group. This workflow applies to all NSP users who need to view object alarms, regardless of which application they use for alarm viewing.

Create resource groups in the Group Manager application

1

Create an NE | port group directory using the Group Manager application.

2

Create an NE | port resource group in the group directory, and define a filter that includes the network elements the user needs to view.

You can create multiple resource groups within a group directory.

3

Create a service group directory.

4

Create a Service resource group in the service group directory, and define a filter that includes the services the user needs to view. You can create multiple service resource groups within a group directory.

You can create the service resource group based on a Site ID (NE system address) to include all services for the associated NE.

Assign resource groups to roles in the User Management application

5

Add the resource groups to a role in the User Management application. See 1.5 “How do I configure a role?” (p. 11).

6

Assign the role to the appropriate user group. See 1.8 “How do I configure a user group?” (p. 18).

1.5 How do I configure a role?

A role object specifies access rights to specific NSP applications and network resources. Roles are assigned to user groups, bringing all access rights defined on the role to all members of the user group.

Consider the following before configuring a role:

- If you intend to assign resource group access to a role, you must configure your resource groups in the Group Manager application before completing this procedure.
- If you intend to assign Analytics resource access in this role, you must fully configure the Analytics application and Analytics server, and you must assign Read/Write/Execute permission to either the Analyze/Assure application category, or to the Analytics application.

Note: Do not confuse the Application Access settings in User Manager with the Application Deployment Control settings that are configured on the NSP Launchpad. (The Application Deployment Control settings determine which applications are activated and available on the NSP Launchpad.)

1

Click on the ACCESS CONTROL tab.

2

Select **Roles** from the drop-down list on the toolbar.

3

Click + **Create Role**. The Create Role form opens.

4

In the Identification panel, specify a role name and description.

Do not use the following reserved characters in the Role Name and Description fields: **% + , . / ; = ? **.

5

In the Characteristics panel, you can enable special designations for the role:

- To create an administrative role with access to all resource groups and applications, enable the **Administrator** check box.

  If you enable this option, no further steps are necessary. Click **Create** to save the role.
- If the role is intended specifically for Lawful Intercept users, enable the **Lawful Intercept** check box.

  LI users are exempt from the User Activity Logging function.

6

To assign application access to the role, go to the Application Access panel and select an access level from the drop-down menu for each application you want to include in the role.

If you intend to assign Analytics resource access in this role, you must assign Read/Write/Execute permission to the Analytics application.

The available access permissions may vary, depending on the application you are looking at; see 1.7 “NSP application user access levels” (p. 15).

7

To assign network resource access to the role, go to the Network Resource Access panel. (For a detailed explanation of the Network Resource Access panel, see 1.6 “Setting network resource access levels” (p. 14).)

You can assign resource access globally, to resource group categories, to individual resource groups, or a combination of these.

a. You can assign network resource access globally by resource type. Enable either or both options:
   - **Access To All Equipment** assigns full permissions on all NE resource groups and port resource groups to the role.
   - **Access To All Services** assigns full permissions on all service resource groups to the role.

b. Expand the resource group category for resource groups you want to include in the role. (For a detailed explanation of the Network Resource Access panel, see 1.6 “Setting network resource access levels” (p. 14).)
   - Select an access level from the drop-down menu for each resource type you want to include in the role.
   - If you specify an access level to a resource group category, all resource groups within the category are included in the role at the same access level.

   If the Group Category list is empty or the resource group you are looking for does not appear, you can create resource groups in the Group Manager application.

8

To assign Analytics resource access to the role, go to the Analytics Resource Access panel.

In order for the Analytics Resource Access panel to appear, Analytics reporting must be fully configured and running in NSP and you must assign Read/Write/Execute access to the Analytics application in this role.

Assign access to Analytics categories or individual Analytics resources in the Analytics Repository list:

- To obfuscate specific Analytics report data for user groups associated with the role, enable the **Data Anonymization** check box.
- Assign access to an entire Analytics category from by enabling its corresponding **Permissions** check box ☑.
- Assign access to individual Analytics resource items by expanding an Analytics category, selecting an Analytics resource, enabling its corresponding **Permissions** check box ☑.
  Some Analytics categories have nested subcategories, each containing individual Analytics resources. An Analytics category or subcategory with access granted on all of its contained resources is displayed as fully-enabled ☑. If access is granted on only some of its contained resources, it is displayed as partially-enabled ▣.

Note: The View/Execute permissions for a report in an Analytics report repository do not apply to drill-downs.
For example, a user group has View/Execute permission for report A but no permission for report B. If report B is a drill-down from report A, users will be able to execute report A via report B, although this might not seem obvious.

9

Click **Create** to save your changes and return to the Roles list.

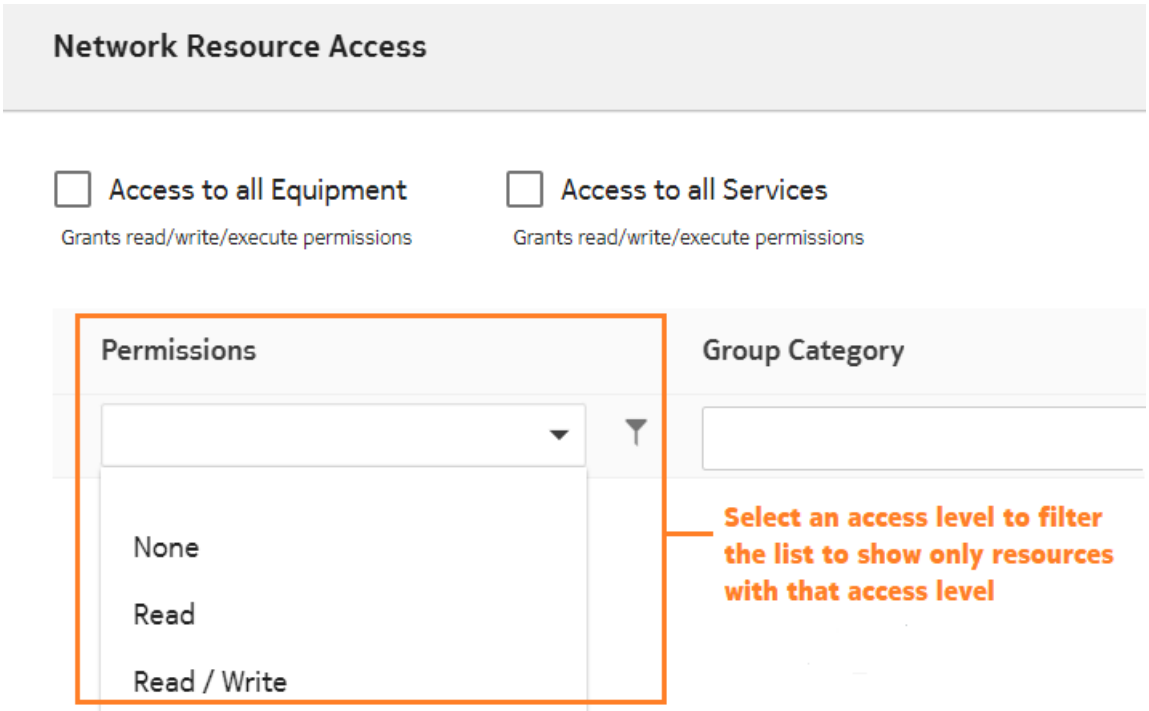
END OF STEPS

1.6 Setting network resource access levels

This topic describes the features of the Network Resource Access panel in the Create Role form. You can search for specific resources and you can search for resources with a common access level. Use this topic as a reference when performing the 1.5 “How do I configure a role?” (p. 12) procedure.

1.6.1 Filter the list

You can filter the network resource list to a specific access level by selecting an access level from the drop-down menu at the top of the Permissions column. The list is reduced to show only resources that have the same access level. The filter is set to a null value (no access level selected) by default so that all available resources are displayed in the list.



1.6.2 Search the list

You can search the resource list by typing a string in the Search field at the top of the Group Category column. The list updates dynamically with matching entries as you type.

1.6.3 Set access permissions on a category

You can set global access permissions on an entire category of resources. Select an access level from the drop-down menu next to a resource group category. The access permissions are set to the same level for all resources in the category.

1.6.4 Set access permissions on an individual item

You can set access permissions on a single resource group. Expand the resource group and then select an access level from the drop-down menu next to a resource group.

1.7 NSP application user access levels

The following table lists NSP applications and the user access levels that can be assigned for each.

Table 1-1 NSP application user access levels

Applications	Access levels
Analytics	None Read / Write / Execute
Cross Domain Coordinator	None Read / Write / Execute
Device Administrator	None Read / Write / Execute
Fault Management	None Read / Write / Execute
Group Manager	Read / Write / Execute access permanently enabled for Administrative user. Application not visible to other users.
Insights Administrator	None Read / Write / Execute
Intent Administrator	None Read The following application scopes can be enabled • Manage Intent Types • Manage Intents • Manage Mediators • Import • Operate Intents • Manage Policies • Write Intent Types
Intent Manager	None Read
IP/MPLS Optimization	None Read / Write / Execute
IP/MPLS Simulation	None Read / Write / Execute
Modeled Device Configurator	None Read / Write / Execute
Network Functions Manager - Packet	None Read / Write / Execute

Table 1-1 NSP application user access levels (continued)

Applications	Access levels
Network Supervision	None Read / Write / Execute
NFV Server	None Read
Original Service Fulfillment	None Read Read / Write Read / Write / Execute
Policy Management	None Read Read / Write Read / Write / Execute
Service Fulfillment	None Read Read / Write Read / Execute Read / Write / Execute
Service Supervision	None Read / Write / Execute
User Manager	Read / Write / Execute access permanently enabled for Administrative user. Application not visible to other users.
Wireless NE Views	None Read / Write / Execute
Wireless Supervision	None Read / Write / Execute

Table 1-1 NSP application user access levels (continued)

Applications	Access levels
Workflow Manager	None Read The following application scopes can be enabled • Import • Write Workflow Artifacts • Publish Workflow Artifacts • Manage Executions • Manage Environments • Manage Triggers • Debug • Execute Workflow Artifacts

1.8 How do I configure a user group?

A user group is a definition of user roles and associated access rights. You assign application and resource access rights to a user group through role objects. When a role is assigned to a user group, all access rights defined on the role are assigned to the user group.

To configure a complete user group, you should have appropriate roles configured before starting this procedure. 1.5 “How do I configure a role?” (p. 12)

1

Click on the ACCESS CONTROL tab.

2

Select **User Groups** from the drop-down list on the toolbar.

3

Click **+ Create User Group**.The Create User Group form opens.

To make changes to an existing user group, select the group in the list and click **Edit User Group**. The Edit User Group form opens.

4

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

Do not use the following reserved characters in the User Group Name and Description fields: **% + , . / ; = ? **.

5

To assign user roles to the group, click **Add Roles** on the Roles panel. The Add Roles form opens.

6

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

7

Click **Create** to save your changes and return to the User Groups list.

END OF STEPS

1.9 How do I enable access control?

Note: When you enable user access control in User Manager, individual users will see their NSP access rights enforced when they login to NSP.

The user groups and roles you create in User Manager are enforced **in place of** any previously-existing access control setup, except in NFM-P and WS-NOC, where user access continues to be defined within those applications.

1

Click on the ACCESS CONTROL tab.

2

Click **More**, **Settings**.

3

In the Access Control Settings form, enable the **User Access Control** option.

4

Click **Save** to enable access control.

END OF STEPS

1.10 NSP operator roles and responsibilities

Operator responsibilities determine whether you assign Read or Write privileges to the resource groups of an associated role. For example, the administrator role has Write privileges to all resources. A user with an assigned network operator role, however, may have Read access to the NEs in multiple resource groups for troubleshooting purposes, but be granted Write access only to the resource group for the NEs that they maintain.

Note: When only application access is configured in a role that has no assigned resource groups, the role has full access to all resource groups.

The following table lists and describes typical network operator roles and responsibilities as examples for NSP role creation.

Role	Responsibilities
Administrator	User access control, network monitoring, system administration
Network operator	Network fault detection and troubleshooting, equipment health and service infrastructure monitoring
Service operator	Multi-layer service provisioning
Network engineer, traffic path	Routing management, optimization, and planning
Network engineer, cross-domain	IP/optical network connectivity, optimization, and planning
Network engineer, provisioning	Device configuration, NE software and script management

2 Activity logging

2.1 What is user activity logging?

Administrators can use the NSP activity logging function to centralize user activity logging across all NSP applications. NSP user actions are logged in the User Manager application, including actions invoked through application REST APIs or application GUIs.

Application user event logs contain the following types of information:

- identity of user associated with event
- event type (configuration change, file access, etc.)
- executed operations and their results
- event time

You can retain activity logs for up to 365 days, with up to 10000000 log events, as configured in the application settings. You can also export activity logs to an external file for archival purposes.

Note: The NFM-P and WS-NOC activity logging functions run separately from NSP activity logging.

2.2 How do I view application events?

This procedure describes basic event viewing options. To learn how to create advanced log filters, see 2.3 “How do I reduce the log contents to what I want to see?” (p. 22).

1

Click on the LOGS tab. The Activity Logs list displays a list of application events over a specified time period (All Available, by default).

2

Use any of the following viewing options to control what you see in the log:

- Change the log event time period by clicking the Time Period:Past 30 days **Time Period** menu and selecting a new time period.
- **Filter the Log under a specific column:** Type a text string in the text field at the top of a column and press Enter, or use the date picker (where available). Click **Refresh** to update the list.

  When typing a search string for the User Name column, you must type a complete, case-sensitive, user name. For other columns, you can type a partial search string.
- **Sort the Log under a specific column:** Click on a column header to sort the list under that column. Click the column header a second time to toggle the sort order (ascending/descending), as indicated by the Up/Down arrow. Click the column header a third time to clear sorting under that column.

- **Clear all filters:** Click **Clear Filter** to clear column filters.

3

To view details about a specific log event, click on the event item in the log.

The Info panel displays expanded information about the event, including the name of the user who executed the event, affected objects, and affected parameters.

END OF STEPS

2.3 How do I reduce the log contents to what I want to see?

Create advanced filters to reduce the log to specific events that you want to investigate. Using boolean filter expressions, you can create and combine filters to narrow log events to very specific parameters.

1

On the LOGS tab, click **Add Filter** and select **Add New Filter**. The New Filter form opens.

2

Type a filter name and description.

3

Type a boolean filter expression in the Filter Expression field, starting with a log information attribute type, followed by a boolean operator and an attribute value. The application suggests possible attributes, operators, and attribute values as you type, and displays error messages in red when an expression is invalid. You can combine attribute-value expressions using either **AND** or **OR** operators, but do not combine both operators in the same filter expression.

For example, the following filter expression filters on the **App Name** and **Action Name** attributes...

```
'App Name' = 'session-manager' and 'Action Name' = 'EXPIRY'
```

...and returns only log entries with the respective attribute values of **session-manager** and **EXPIRY**.

Note: When using the **=** filter operator, attribute names and attribute values are case-sensitive.

4

Do one of the following:

- Click **Save Filter** to save the filter to the Filter menu for future use.
- Click **Apply** to apply the filter to the log immediately. The filter expression is not saved.

END OF STEPS

2.4 How do I apply or clear my advanced filters?

Advanced filters that you saved to the Filter menu can be applied to the event log or cleared as needed.

1

On the LOGS tab, click **Add Filter** and select an advanced filter from the menu.

The event log is reduced to display only events that match the filter. You can repeat this step to apply a different filter.

2

Click **Clear Filter** to clear the advanced filter.

END OF STEPS

2.5 How do I modify my advanced filters?

1

On the LOGS tab, click **Add Filter**, **Manage Saved Filter**. The Saved Filters form opens.

2

To modify a filter, hover over the filter item in the list and click **Edit**. The filter opens in the Edit Filter form.

3

Edit the filter expression as required and do one of the following:

- Click **Update Filter** to save the filter changes for future use.
- Click **Apply** to apply the modified filter to the event log immediately. The changes to the filter expression are not saved.

4

If you want to delete a filter, hover over the filter item in the list and click **Delete**. Click **Ok** to confirm the deletion.

5

Click **Ok** to close the Saved Filters form.

END OF STEPS

2.6 How does Auto Refresh work?

The Auto Refresh function continually updates the Activity Log GUI with the most recent system events. Auto Refresh is disabled by default in the Activity Logging application.

Consider the following when enabling Auto Refresh:

- **Auto Refresh On:** If you select an event item in the activity log when Auto Refresh is enabled, the event selection and associated information in the Info panel is cleared at the next auto-refresh. You must select the event again to re-display its information in the Info panel.

  If you want an item selection to remain static while you view it, disable Auto Refresh.
- **Auto Refresh Off:** With Auto Refresh disabled, the event selection and Info panel is cleared when you manually click **Refresh**.

2.7 How do I set limits for log retention?

Use the Settings form to set the maximum retention period for log events, the maximum number of log events to be retained, and overflow settings for log events that exceed the maximum.

1

On the LOGS tab, click **More**, **Settings**.

2

Set the maximum number of days that log events will be retained in the **Log Retention Period** field (minimum 30 days, maximum 365 days).

3

Set the maximum number of individual log events that can be retained during the retention period in the **Maximum Number of Logs** field (minimum 100000 events, maximum 10000000 events).

4

When either of the **Log Retention Period** or **Maximum Number of Logs** settings is approached or reached, a certain percentage of the stored log events are purged from the database.

Configure overflow settings for log events that approach or exceed the maximum settings:

- **Warning Threshold:** percentage of maximum settings at which a warning message is sent.
- **Warning Purge Amount:** percentage of total log events purged from the database when warning threshold is reached.
- **Critical Threshold:** percentage of maximum settings at which a critical warning message is sent.
- **Critical Purge Amount:** percentage of total log events purged from the database when critical threshold is reached.

5

Save your changes and close the form.

END OF STEPS

2.8 How do I export activity log events?

You can export activity logs to an external file for archival purposes. You can export the entire log contents, or only selected events.

1

On the LOGS tab, do one of the following:

- To export the entire activity log contents, click ⋮ **More**, **Export All** on the application banner.
- To export only selected log events, use Ctrl+click or Shift+click to select the events you want to export and then click ⋮ **More**, **Export Selected** at the top of the list.

2

Specify a location to save the export file and click **Save**.

The exported log is saved as a .csv file in a .zip archive.

END OF STEPS

3 Session Management

3.1 What is session management?

The session management function lets administrative users monitor active user sessions in NSP. The Sessions GUI lists all active NSP user sessions and REST API sessions.

Administrative users can manually terminate one or more user sessions and send messages to one or more active NSP users. Messages would typically be sent to forewarn users of an upcoming session termination, or for other operational events in the NSP system. Messages are displayed in any NSP application views the recipient users have open. Messages are flagged as Information, Warning, or Urgent. Recipient users must have NSP open on their desktop to receive messages.

Note: You cannot send messages to REST API sessions because they do not involve actual users. Exercise caution in terminating REST API sessions, as they often involve critical network functions.

3.2 How do I terminate user sessions?

1

Click on the SESSIONS tab.

2

To terminate a single session, select a user session in the list and click **Terminate Session** on the right side of the item.

3

To terminate multiple sessions, press the Ctrl key and click on the session items you want to terminate, or select all of the sessions by clicking **Select All** on the toolbar, and then clicking **Terminate Session** on the toolbar.

You can cancel a **Select All** command by clicking **Deselect All** on the toolbar.

4

At the prompt, confirm the session termination.

END OF STEPS

3.3 How do I send a message to active users?

1

Click on the SESSIONS tab.

2

To send a message to one user, select a user session in the list and click **Send Message** on the right side of the item.

3

To send a message to all active users, click **Send Broadcast Message** on the toolbar.

4

In the message form that opens, select a message type and then type your message text in the box.

5

Click **Send**.

A confirmation message appears.

Note: Although a message may be confirmed as Sent, this does not guarantee that the message is received by all users. Under some circumstances (user logged out, browser window closed, etc.) some users may not receive the message.

END OF STEPS

4 User management

4.1 What is user management?

NSP supports locally defined users for access to NSP applications. When NSP is deployed with the CAS authentication module and integrated with NFM-P, NFM-P provides local user management. When NSP is deployed with the OAUTH2 authentication module (with or without NFM-P integration), local users are maintained in the User Manager application.

The NSP authentication module (CAS or OAUTH2) is specified at the time of NSP software installation or upgrade.

When migrating from an NSP + NFM-P deployment with CAS authentication to an integrated deployment with OAUTH2 authentication, the NFM-P users must be imported into NSP. NSP with OAUTH2 authentication will not defer authentication to NFM-P.

Local user accounts can be used for machine-to-machine interaction, rather than creating user accounts in your corporate user database. They also provide a backup mechanism for cases where NSP cannot communicate with the corporate user database.

4.2 How do I create an NSP local user?

This procedure describes how to create a local NSP user account using the OAUTH2 authentication module. It does not apply to users managed through external databases.

1

On the Users tab, click **+ Create User**.

2

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

Use all lowercase letters in the username. Uppercase letters will be saved as lowercase.

3

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the **Show Password** option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

4

Click **Save**.

END OF STEPS

4.3 How do I import users and groups from NFM-P?

NFM-P users must be imported into NSP when NSP is deployed with OAUTH2 authentication module. The Import feature migrates all user accounts and user groups from your NFM-P user database into User Manager. The imported users become local NSP users, authenticated through the OAUTH2 module, which must be enabled at NSP installation or upgrade. The imported user groups can be assigned roles that provide the users in the groups with access to NSP applications and resources.

NFM-P users that are imported to NSP must be created with new passwords. Users that have an email address will have a random password emailed to them. Users that do not have an email address will be assigned a global default password, set by the administrator. All imported users will be required to change their password at their first login after import. It is recommended that the NFM-P system administrator assign email addresses to users before the import to NSP to ensure maximum user security.

Before importing users from NFM-P, be aware of the following requirements and limitations:

- If you intend to use email notification of new user passwords, you must ensure that the NSP email server is configured in NSP system settings, and that E-mail Notifications option is enabled in the NSP system settings.
- If NFM-P is configured with remote identity providers, those identity providers must be configured in nsp.sso section of nsp-config.yml.
- The NFM-P user parameters imported to NSP are: user name, description, user group, account state, and email address.
- All NFM-P user IDs are converted to lower case upon import since OAUTH2 authentication is case-insensitive. If two NFM-P user IDs are identical except for case, only one of them is imported. You must clean up any duplicate user IDs in NFM-P prior to import to ensure that all users are imported.
- NSP user groups are case sensitive, as are NFM-P user groups. When NFM-P user groups are imported to NSP, they keep uppercase and lowercase characters. For example, if NFM-P has user groups GROUP1, Group1 and group1, all three are imported into NSP.
- Any NFM-P user names that conflict with existing NSP local users are not imported and do not cause any change to local users.
- The User Manager application supports a maximum of 1000 local NSP users. To ensure that only necessary users are included in the migration, clean up your NFM-P user database before importing to NSP.
- NFM-P remote users are not imported into NSP (remote users include NSP, LDAP, RADIUS, and TACACS users that have access to the NFM-P GUI.)
- OAUTH2 authentication does not support both local and remote user authentication (LDAP, RADIUS, TACACS) with the same user ID. To preserve the use of a remote user ID, the local user ID should be changed to a unique value.

1

On the Users tab, click ⋮ **More**, **Import NFM-P Users and Groups**.

2

In the Temporary Password for Imported Users form, specify and confirm a global temporary password for all imported users.

The global temporary password is only applied to imported users with no email address.

3

Click OK.

The imported users are listed on the Users tab. The imported user groups are listed on the Access Control tab under User Groups.

4

The NFM-P imported users can now login to the NSP Launchpad. All imported users will be required to change their password during first login. NFM-P users with an email address should check their email for their random login password.

Note: In the event that the import fails for certain users or user groups, you can investigate problems in the nspos-tomcat pod logfile at: **`/opt/nsp/os/tomcat/logs/AccessControlApi.log`**

END OF STEPS

4.3.1 Post-import considerations

After importing users from NFM-P, be aware of the following requirements and limitations:

- An imported NFM-P user group that had Administrator scope of command in NFM-P must be assigned to a role with administrative privileges in the NSP User Manager.
- Lawful Intercept (LI) users are imported to NSP with LI privilege. NFM-P LI users cannot be deleted and must remain in NFM-P after import to NSP
- NFM-P XML SOAP OSS users must remain in NFM-P after import to perform XML SOAP OSS transactions with NFM-P.
- Non-NFM-P XML SOAP OSS users that are imported to NSP can be deleted from NFM-P after import to NSP.
- NFM-P user groups must exist in NFM-P to define user access permissions through span and scope of control profiles.
- New NFM-P XML SOAP OSS users need to be created in the NFM-P User Security application.

4.4 How do I set global user password requirements?

The password policy defines global password requirements for local NSP user accounts, including password contents and length, and expiry and reuse limits. The password policy settings apply only

to local NSP user accounts authenticated through the OAUTH2 module. The password policy does not apply to users managed through external databases.

1

On the Users tab, click ⋮ **More**, **Password Policy**.

2

In the Password Policy form, configure user password requirements in any of the following ways:

Not Recently Used	Specifies the number of unique password that must be used before the current password can be used again.
Password Expiry	Specifies the number of days a password can be used before it expires.
Special Characters	Specifies the minimum number of special characters that must be used in the password. Allowable special characters are: `()@#$%&!*_+~`
Uppercase Characters	Specifies the minimum number of uppercase characters that must be used in the password.
Lowercase Characters	Specifies the minimum number of lowercase characters that must be used in the password.
Digits	Specifies the minimum number of numerical characters that must be used in the password.
Minimum Length	Specifies the minimum number of characters that must be used in the password.
Must Not Be Username	Enable this option to prevent the account username from being used as a password.
Must Not Be Email Address	Enable this option to prevent the account email address from being used as a password.

3

Click **SAVE**.

END OF STEPS

4.5 How do I set global user session limits?

You can set global limits for local NSP user sessions and the maximum allowable login time. These settings apply only to local NSP user accounts authenticated through the OAUTH2 module. They do not apply to users managed through external databases.

1

On the Users tab, click ⋮ **More**, **Session Settings**.

2

In the Session Settings form, configure user session limits in any of the following ways:

Access Token Lifespan	The number of minutes before an access token expires.
Session Inactivity Timeout	The number of minutes of user session inactivity before the user is automatically logged out of NSP [1].
Maximum Session Time	The absolute maximum length of a user session (in minutes) before the user is automatically logged out of NSP.
Maximum Time to Complete Login	The maximum time allowed (in minutes) for a user to complete an NSP login.
Maximum Time to Complete Login Steps	The maximum time allowed (in minutes) for an NSP login sequence that involves multiple steps; for example, if the user must change their password during login.
Maximum Sessions Per User	The maximum number of simultaneous GUI and OSS sessions per user account. When this parameter is set to zero, the number of sessions per user is unlimited.

Notes:

1. Some applications continuously communicate with the NSP while in use, and a user session does not become idle as long as the user has that application open. For example, viewing a fault management alarm list.

3

Click **SAVE**.

END OF STEPS

4.6 How do I modify a user account?

You can modify all aspects of a user account, except for the username. You can also change a user's password or compel the user to change their password.

1

In the Users list, select the user account you want to modify.

2

On the user account item, click ⋮ **More**, **Edit User**.

3

On the Update User form, make any of the following changes:

- Change the user's **First Name**, **Last Name**, or their **Description** text.
- Set the **Account State** parameter to **Active|Suspended**.
- Assign the user to a different **User Group**.
- Change the user **Email Address**.
- Enable the **Force User To Change Password** option to compel the user to set a new password at their next NSP login.
- To change the user's password yourself, turn on the **Change Password** toggle to make the user account **Password** fields editable. Specify and confirm a new password.

4

Click **UPDATE**.

END OF STEPS

4.7 How do I suspend a user account?

You can temporarily suspend an NSP user account. After suspension, the user will lose access to the NSP system after they logout and login again.

1

In the Users list, select the user account you want to suspend.

2

On the user account item, click ⋮ **More**, **Edit User**.

3

On the Update User form, set the **Account State** parameter to **Suspended**.

4

Click **UPDATE**.

END OF STEPS