Brocade® SANnav™ Global View User Guide, 2.2.x

User Guide
October 5, 2022

Table of Contents

Introduction

This guide describes how to use SANnav™ Global View to monitor and manage information across multiple SANnav Management Portal instances.

Within this document, SANnav Global View might also be referred to simply as *SANnav*.

Refer to the following guides for additional information:

- *Brocade SANnav Global View Installation and Upgrade Guide* contains detailed steps for installing SANnav Global View and for upgrading from an earlier version.
- *Brocade SANnav Management Portal User Guide* describes how to monitor and manage your storage area network (SAN) using Brocade SANnav Management Portal.
- *Brocade SANnav Management Portal Installation and Upgrade Guide* contains detailed steps for installing SANnav Management Portal and for upgrading from an earlier version. The guide also includes information about installing SANnav Management Portal as an Open Virtual Appliance (OVA).
- *Brocade SANnav Flow Management User Guide* explains how to configure and manage flows using SANnav Management Portal.
- *Brocade SANnav Management Portal REST API and Northbound Streaming Reference Manual* contains definitions of REST APIs that you can use to access SANnav Management Portal, including streaming performance and flow metrics to an external server.
- *Brocade SANnav Global View Release Notes* includes a summary of the new and unsupported features for this release.

Features Affected by Upgrade and Migration

If you upgraded from an earlier SANnav version, some features might behave differently than before.

The following tables list SANnav features and how they are affected by upgrading to SANnav 2.2.x and migrating your data. The first table lists the features that are affected when you migrate from SANnav 2.2.0x to 2.2.x. The next table lists the features that are affected when you migrate from SANnav 2.1.1x to 2.2.x.

Table 1: Features Affected by Migration from SANnav 2.2.0x to 2.2.x

Feature	Effect of Migration
Backup and Restore	In the **SANnav Backup** page, the **Alternate Backup Location** is empty. The **Backup Location** field shows the previously configured location.
Inventory	In the Switch Ports inventory view, the **QSFP** column is replaced with the **Media Form Factor**, **Unit Number**, and **Channel Index** columns. Some of these new columns might be hidden by default.
Licensing	Refer to the "SANnav License Migration" section in the *Brocade SANnav Global View Installation and Upgrade Guide* for details.
User Management	• On the **Users** page, migrated user accounts might not show a value in the **Last Logout Column** until the user logs in and logs out. • The **Session Count** column now displays only the number of sessions per user. Previously, this column would display the number of active sessions per user and the last active interval.

Table 2: Features Affected by Migration from SANnav 2.1.1x to 2.2.x

Feature	Effect of Migration
Backup and Restore	• After migration, any backups that were previously taken are not displayed in the **Outputs** list. The list is empty. • If the schedule name contains space characters, the space characters are removed from the file name of the generated backup file. If you edit the schedule name after migration, you cannot use space characters in the name. • In the **SANnav Backup** page, the **Alternate Backup Location** is empty. The **Backup Location** field shows the previously configured location.
Filters	Filter definition preferences are updated to have an OR condition after migration.
Inventory	In the Switch Ports inventory view, the **Media Form Factor**, **Unit Number**, and **Channel Index** columns are added. Some of these new columns might be hidden by default.
Licensing	Refer to the "SANnav License Migration" section in the *Brocade SANnav Global View Installation and Upgrade Guide* for details.
User Management	• Any accounts with user names **none** or **na** (case insensitive) must be renamed prior to migration. SANnav 2.2 does not support **none** or **na** as a user name. • On the **Users** page, migrated user accounts might not show a value in the **Last Logout Column** until the user logs in and logs out. • The **Session Count** column now displays only the number of sessions per user. Previously, this column would display the number of active sessions per user and the last active interval.

Supported Hardware and Software

SANnav supports Gen 4, Gen 5, Gen 6, and Gen 7 switches and directors

SANnav Global View 2.2.x supports SANnav Management Portal 2.2.x instances that manage fabrics containing the following Fabric OS software versions and hardware platforms.

Fabric OS Software Support

The following Fabric OS software versions are supported by this release of SANnav:

- Fabric OS 9.0 or later
- Fabric OS 8.0 or later
- Fabric OS 7.4 or later

Brocade Gen 7 (64G) Fixed-Port Switches

- Brocade G720 Switch
- Brocade G730 Switch

Brocade Gen 7 (64G) Directors

- Brocade X7-4 Director
- Brocade X7-8 Director

Brocade Gen 6 (32G) Fixed-Port Switches

- Brocade G610 Switch
- Brocade G620 Switch
- Brocade G630 Switch
- Brocade 7810 Extension Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module

Brocade Gen 6 (32G) Directors

- Brocade X6-4 Director
- Brocade X6-8 Director

Brocade Gen 5 (16G) Fixed-Port Switches

- Brocade 6505 Switch
- Brocade 6510 Switch
- Brocade 6520 Switch
- Brocade M6505 Blade Server SAN I/O Module
- Brocade 6542 Blade Server SAN I/O Module
- Brocade 6543 Blade Server SAN I/O Module
- Brocade 6545 Blade Server SAN I/O Module
- Brocade 6546 Blade Server SAN I/O Module
- Brocade 6547 Blade Server SAN I/O Module
- Brocade 6548 Blade Server SAN I/O Module
- Brocade 6558 Blade Server SAN I/O Module
- Brocade 7840 Extension Switch

Brocade Gen 5 (16G) Directors

- Brocade DCX 8510-4 Director
- Brocade DCX 8510-8 Director

Brocade Gen 4 (8G) Fixed-Port Switches

- Brocade 300 Switch
- Brocade 5424 Blade Server SAN I/O Module
- Brocade 5460 Blade Server SAN I/O Module
- Brocade 5480 Blade Server SAN I/O Module
- Brocade NC-5480 Blade Server SAN I/O Module
- Brocade 7800 Extension Switch

Contacting Technical Support for Your Brocade® Product

If you purchased Brocade® product support from a Broadcom® OEM or solution provider, contact your OEM or solution provider for all your product support needs.

- OEM and solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM or solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.
- For questions regarding service levels and response times, contact your OEM or solution provider.

If you purchased Brocade product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7. For product support information and the latest information on contacting the Technical Assistance Center, go to www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: • **Case Management** • **Software Downloads** • **Licensing** • **SAN Reports** • **Brocade Support Link** • **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Document Feedback

Quality is our first concern. We have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission or if you think that a topic needs further development, we want to hear from you. Send your feedback to documentation.pdl@broadcom.com. Provide the publication title; topic heading; publication number and page number (for PDF documents); URL (for HTML documents); and as much detail as possible.

Getting Started

SANnav Global View is a higher-level *global* management application that provides a comprehensive view of a SAN environment that spans multiple SANnav Management Portal instances.

Using SANnav Global View, you can navigate seamlessly across multiple SANnav Management Portal instances and focus on any individual instance to perform detailed monitoring, investigation, and troubleshooting.

> **NOTE**
> SANnav Global View is a separate product from SANnav Management Portal, and it requires separate installation and licensing.

You log in to the SANnav Global View application and add portals to SANnav Global View, which then uses information in the portals to build a global view of the dashboard and inventory.

> **NOTE**
> SANnav Global View is compatible only with SANnav Management Portal instances that are running the same version as Global View.

Browser Requirements for SANnav Global View

Any laptop or machine that launches web applications can be used to launch SANnav Global View. For optimal performance, have at least 16 GB of memory.

The following browsers can be used to access SANnav Global View:

- Chrome (Google)
- Firefox (Mozilla)
- Microsoft Edge

If you access the client from the Remote Desktop, the user interface may have degraded performance.

Logging In to SANnav Global View

To log in to SANnav Global View, perform the following steps:

1. Open your browser and enter the IP address or fully qualified domain name (FQDN) of the SANnav Global View server.

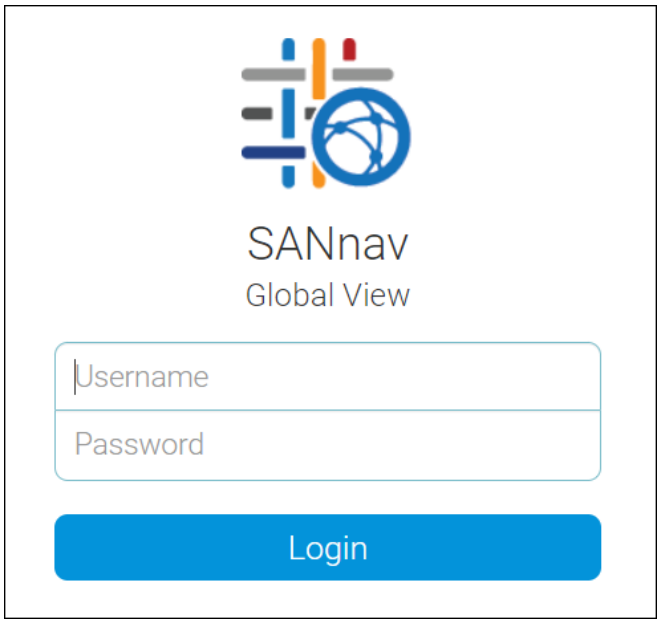
   You can use HTTP or HTTPS, for example:

   ```
   http://192.0.2.0
   ```

   or

   ```
   https://192.0.2.0
   ```

   The SANnav Global View login window appears.



If the login window does not appear, try the following:

- Ping the SANnav server to ensure that it is up.
- Check if SANnav services are running. See Checking the Server Health.
- If you used HTTP, try using HTTPS instead.
- Check the firewall settings.
- Check if your IP address is in the list of allowed browsers, if such a list is created. (See Creating a List of Allowed Browsers to Access SANnav.)

2. Enter your SANnav user name and password, and click **Login**.

   For the first SANnav login, the default user name is "Administrator" and the default password is "password". You are prompted to change the default password.

   SANnav launches with the default dashboard displayed.

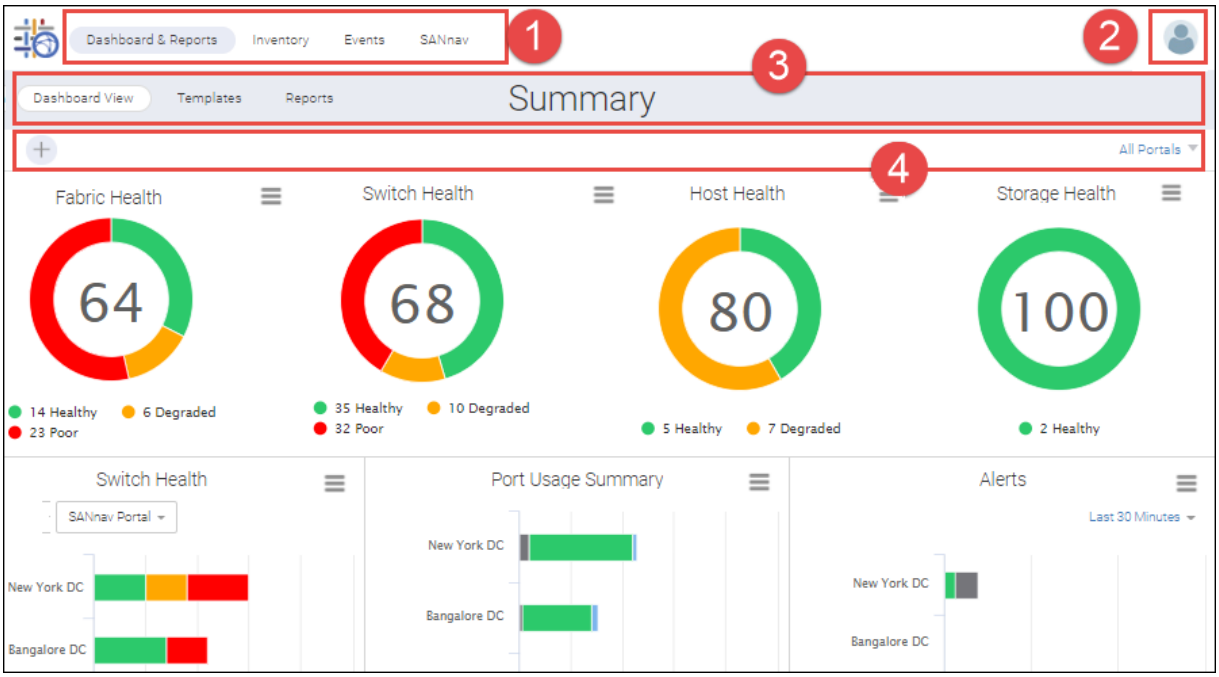
   If SANnav displays the message `Login Failed. Service is not available at this time.` , try the following actions:

   - Wait a few minutes, and try again. SANnav is in the process of starting up.
   - Ensure that you are not using a proxy server URL. SANnav does not support access through a proxy server URL.

Quick Tour of SANnav Global View

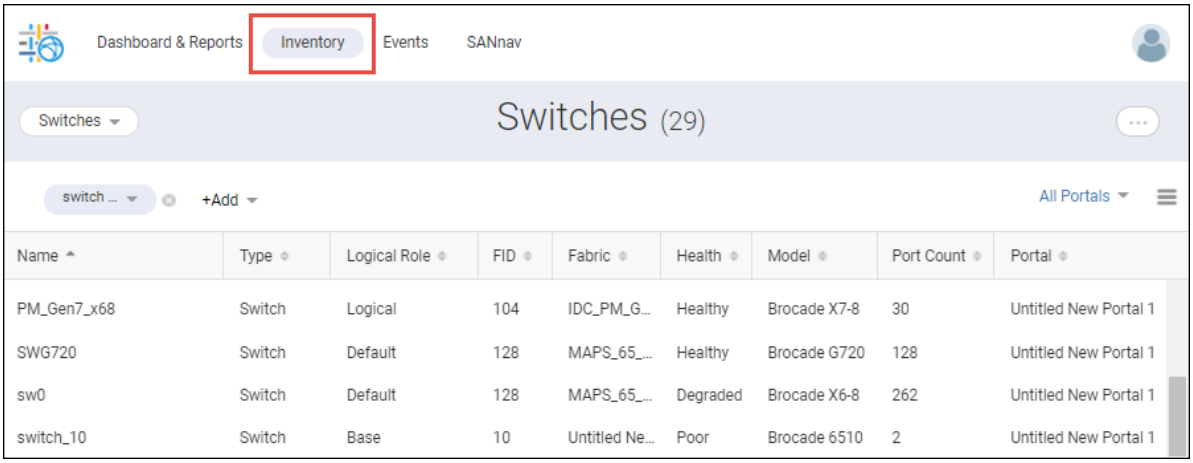
Once familiar with the basic components of SANnav Global View, you can quickly start monitoring SANnav Management Portal instances.

When you first log in to SANnav Global View, you see the **Summary** dashboard, the single dashboard provided with Global View. The following screen capture shows the basic layout of the SANnav Global View user interface.

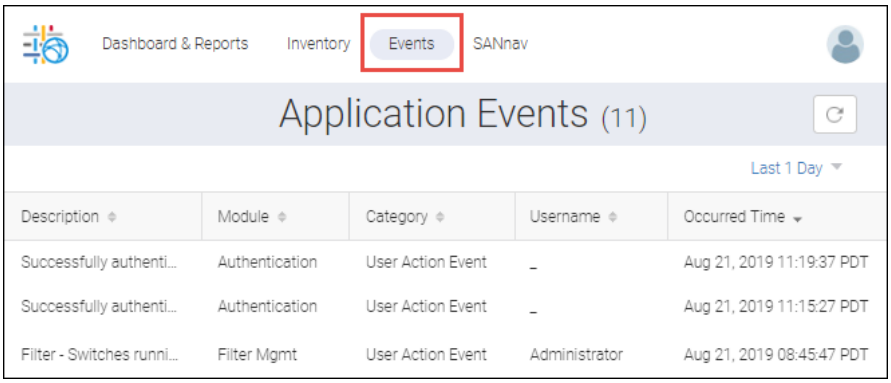


1. Navigation bar. Contains links to feature pages. The **SANnav** link displays the page where various settings and configurations can be performed.
2. Profile menu. Displays links for changing user preferences, viewing system properties, displaying the SANnav version, and logging out.
3. Subnavigation bar. Provides the page title and optional item count within parentheses. Also includes buttons and menus to take actions within the page.
4. Filter bar. Allows you to filter the display based on table columns, portal scope, and customized filters.

Click **Inventory** to display inventory information about fabrics, switches, switch ports, chassis, host and storage devices, and host and storage ports across all Management Portal instances.



Click **Events** to show all application events that stem from a user or system action. A system action is triggered under certain situations like when a portal is disconnected. You can filter the events list by date range. Events from SANnav Management Portal instances are not listed here.

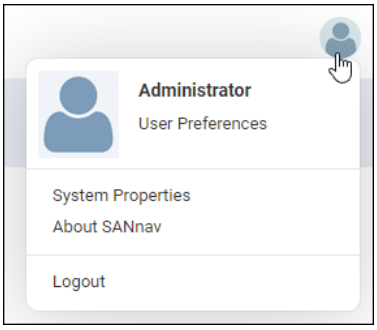


Click **SANnav** to discover Management Portal instances, manage filters, and perform various configuration settings across several feature categories.

The profile menu is where you can add your phone number, change your password, and change the display theme (light or dark). It is also where you can enable **FICON Display**, **Persist Last Filter Selection**, and **Persist Table Column Customization**.

Column customization is the ability to choose what columns you want to see in a tabular view. For example, by default, only a few of the many available columns in inventory are shown, but you can customize the table by adding or removing columns.

When FICON Display is enabled, certain columns in the switch and switch port inventory pages are rearranged for FICON mode.



Customizing and Sorting Tables

SANnav allows you to customize tables by adding and deleting columns, rearranging columns, resizing columns, freezing columns, and sorting columns.

The following tables allow customizations:

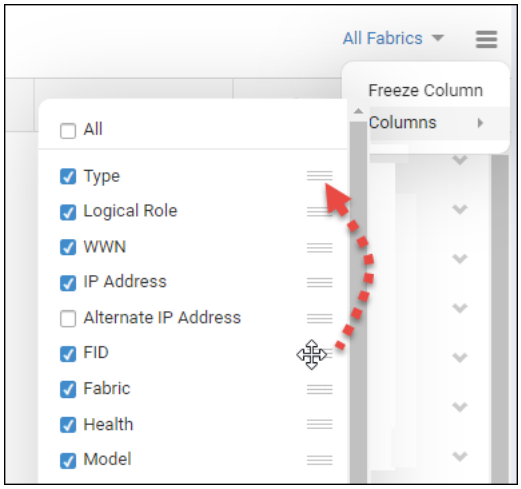
- Inventory
- Report templates

Column customizations persist across page navigation and across logins. If you do not want column customizations to persist across logins, you can update the user preferences.

1. Click the hamburger icon (☰) on the right side of the filter bar, and select **Columns**.
2. To control which columns are shown, select the checkboxes next to the columns that you want to display. Clear the checkboxes next to the columns that you want to hide.

   To display all columns, select the **All** checkbox at the top of the column list.

3. To rearrange columns, hover over the move icon ( ), and drag it up or down.



4. Click anywhere outside the column list window to close it.
5. To resize a table column, hover the mouse over the right-side column boundary and drag the boundary.
6. To freeze columns when you scroll horizontally, perform the following steps:
   a) Rearrange the columns so that the columns that you want to freeze are on the left side of the table.
   b) Click the hamburger icon on the right side of the filter bar, and select **Freeze Column**.
   c) In the **Freeze Columns** dialog, select the number of columns you want to freeze, and click **Save**.

   If the table has more columns than can fit on the page, the number of columns you selected are frozen when you scroll horizontally through the table. You can freeze a maximum of five columns.

   The ability to freeze columns is available for Inventory tables.
7. To sort a table column, click the small arrows next to the column name.

   To perform a multicolumn sort, first sort on one column, and then press **Shift+Click** over the second column. You can sort on a maximum of two columns.

   Multicolumn sorting is not supported in the detail page of a report.
8. To change the user preferences so that column customizations do not persist across logins, perform the following steps:
   a) Click the user icon in the top-right corner of the window, and then click **User Preferences**.
   b) Click the **Edit** button next to **Display Options**.
   c) Clear the **Persist Table Column Customization** option, and then click **Save**.

Filters

Filters are a set of criteria that limit the data that SANnav displays.

You can use filters for inventory items, dashboards, and reports.

For example, you can create the following filters:

- On the **Inventory** page, you can create filters to display only switches in degraded or poor health.
- When viewing a dashboard, you can filter out all healthy switches and focus only on the unhealthy switches.
- When generating a report, you can create a filter to gather report data only from switches that are running a specific Fabric OS version.

Filters can be temporary or permanent:

- Temporary filters exist until you close them or log out of the application. You can assign a name to a temporary filter and save it to make it a permanent filter.
- Permanent filters exist until you specifically delete them. By default, permanent filters persist across logins. You can update user preferences so that permanent filters that you apply will *not* persist across logins. Permanent filters are shared with other SANnav users. Only the user who created the permanent filter can update or delete that filter.

To enable filter settings and conditions (AND, OR, and NOT) to persist across logins, perform the following steps:

1. Click the user icon in the top-right corner of the window, and then click **User Preferences**.
2. Click the **Edit** button next to **Display Options**.
3. Select **Persist Last Filter Selection**, and then click **Save**.

Creating Filters

In SANnav, create filters when you want to view a subset of items or when you want to create report content for a subset of objects.

You can create filters on pages with the add button (**+**) on the left side of the filter bar. If a page does not have a **+** button, that page does not support filters.

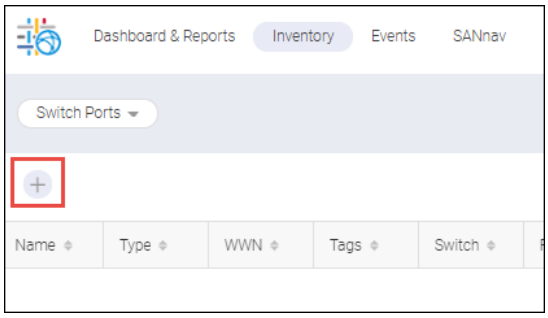
You can create a filter for one-time use, or you can give the filter a name and save it, so you can use it again and make it available for other SANnav users.

The following example shows how you can create a switch port filter to display all U_Ports in Fabric_C.

1. Navigate to the page where you want to create the filter.

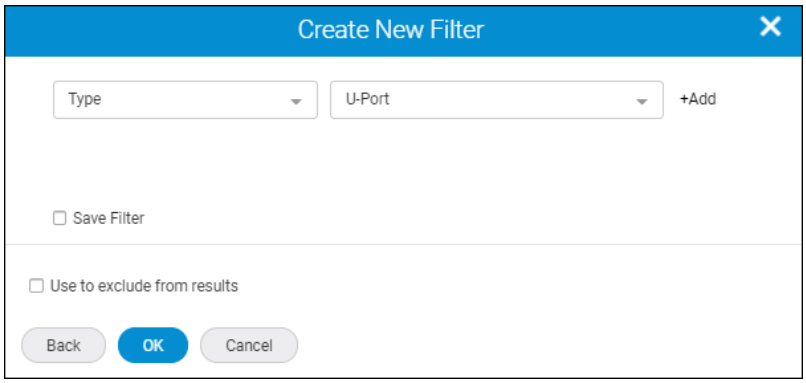
   This example assumes that you are viewing the inventory of switch ports. For this example, select **Inventory** in the navigation bar, and then click **Switch Ports** from the drop-down list.

2. Click the add button (**+**) in the filter bar.



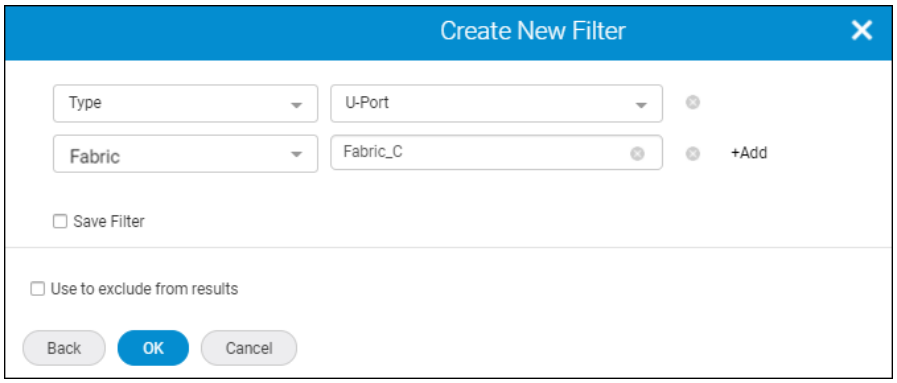
3. In the **Add Filter** dialog, click the **Create New** button.
4. In the **Create New Filter** dialog, select any property from the drop-down list, and enter a value on which to filter.

   For this example, select **Type** as the property and **U-Port** as the value.



5. Click **+Add** to add additional properties and values to the filter.

   For this example, select **Fabric** as the property, and enter **Fabric_C** as the value.



6. Save the filter.

   - Click **OK** to create a temporary filter on the **Inventory** page. This filter is automatically deleted when you log out of the application.

     Or

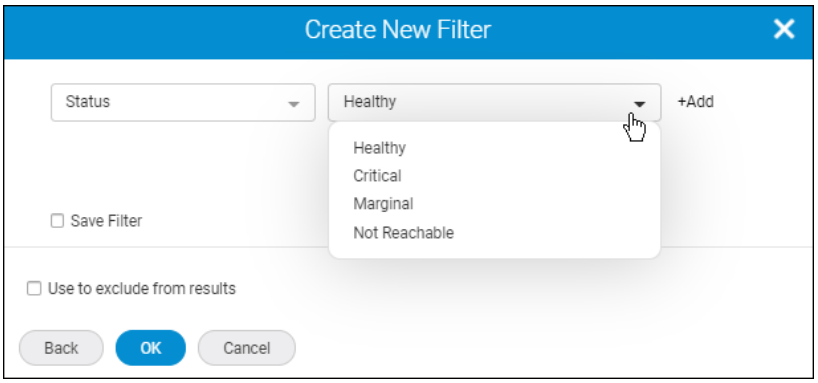
   - Click the **Save Filter** checkbox, provide a name, tags, and description details, and then click **OK**. The filter is available on the **Inventory** page and is also saved as a permanent filter in the **Filter Management** page.

     NOTE
     Although the **Description** field is optional, provide a good description so that you and other users can understand what the filter does.

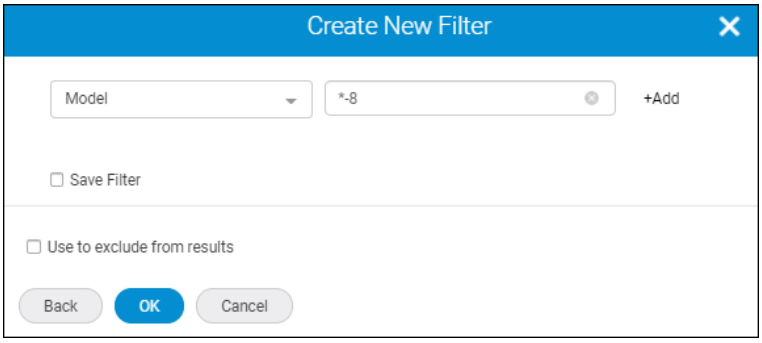
Wildcards in Filters

SANnav supports the asterisk (*) wildcard character in filters. An asterisk represents zero or more characters.

When you create filters, you select properties and values. Some of the properties have fixed values, and you select them from a drop-down list. For example, for a switch filter, the **Status** property has the fixed values **Healthy**, **Critical**, **Marginal**, and **Not Reachable**.



Some of the properties have values that you enter manually. You can enter complete or partial values, and you can use wildcards in the values. The values are not case-sensitive. For example, you can create a switch filter and specify ***-8** for the model to display all Brocade X6-8 and X7-8 directors in the **Inventory** page.



AND, OR, and NOT Filter Conditions

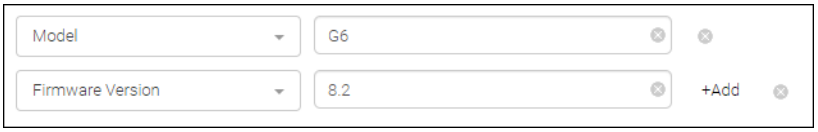
In SANnav, you can create filters with AND, OR, and NOT conditions:

- Create AND conditions by using multiple, dissimilar properties in the filters.
- Create OR conditions by using multiple, similar properties in the filters.
- Create NOT conditions by selecting the **Use to exclude from results** option when creating the filters.

AND and OR Conditions within a Filter

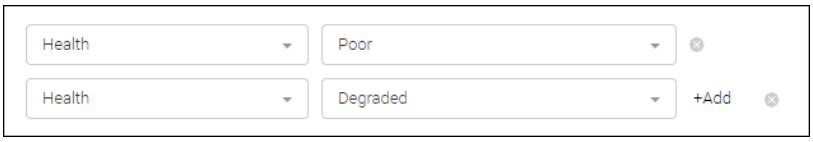
A filter with different properties creates an AND condition. For example, if you want to find all Brocade G610, G620, and G630 switches running Fabric OS 8.2.x, you can create a filter with **Model** = **G6** and **Firmware Version** = **8.2**. The following filter finds all switches with "G6" in the model property AND with "8.2" in the firmware version.

Figure 1: AND Filter



A filter with properties that are the same creates an OR condition. For example, the following filter finds all fabrics with **Health** = **Poor** OR **Health** = **Degraded**. The two **Health** properties create an OR condition.

Figure 2: OR Filter



Adding a combination of properties creates AND and OR conditions within the same filter. For example, the following filter finds all fabrics with "Fabric" in the **Name** property AND with **Health** = **Poor** OR **Health** = **Degraded**. (The **Name** property is not case-sensitive.)

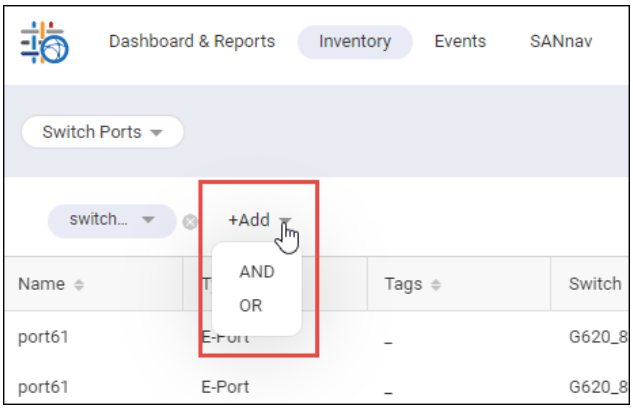
Figure 3: AND and OR Filter

AND and OR Conditions with Multiple Filters

You can use multiple filters for filtering data. When you create multiple filters, you specify whether you want the filters to be AND or OR conditions.

Create the first filter, and then click the **+Add** button to add a second filter. Select **AND** or **OR** from the drop-down.

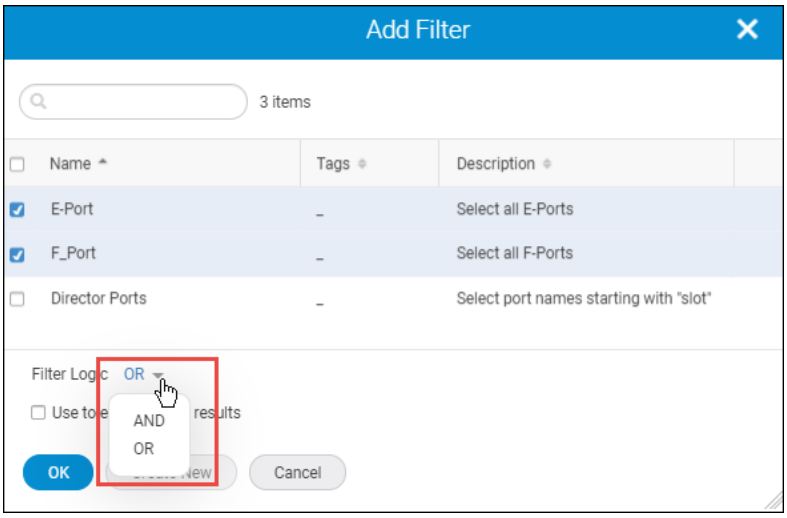
Figure 4: Selecting AND or OR Filters



Note that if you have multiple filters, they must all be either AND conditions or OR conditions. You cannot have a mix of AND and OR conditions. If you want to change from one logical operand to another (for example, to change from AND to OR), you must remove the selected filters and then reselect the filters with the new condition.

When you first add a filter, if you select two or more permanent filters at the same time, you can specify in the **Add Filter** dialog whether the filters are to have AND or OR conditions. In the following screen capture, selecting the OR operand would be appropriate, because the selected filters display E_Ports or F_Ports.

Figure 5: Selecting Filter Logic in the Add Filter Dialog

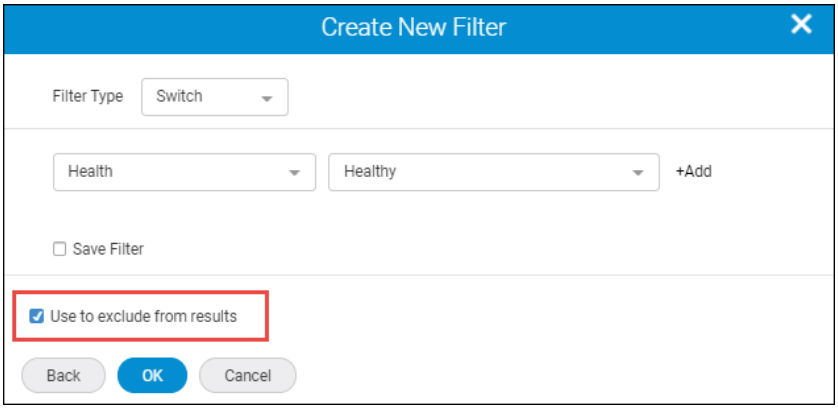


NOT Conditions in Filters

When you create a filter, you can specify whether the filter should include or exclude items that match the filter.

For example, on the **Dashboard** page, you might want to focus on only the unhealthy switches. The following filter is for switches with **Health = Healthy**. Select the **Use to exclude from results** checkbox to create a NOT condition. For this filter, all switches except for healthy switches are displayed. Switches with **Health = Healthy** are not displayed.

Figure 6: Filter with a NOT Condition



When you select permanent filters to add, you can also select the **Use to exclude from results** checkbox in the **Add Filter** dialog.

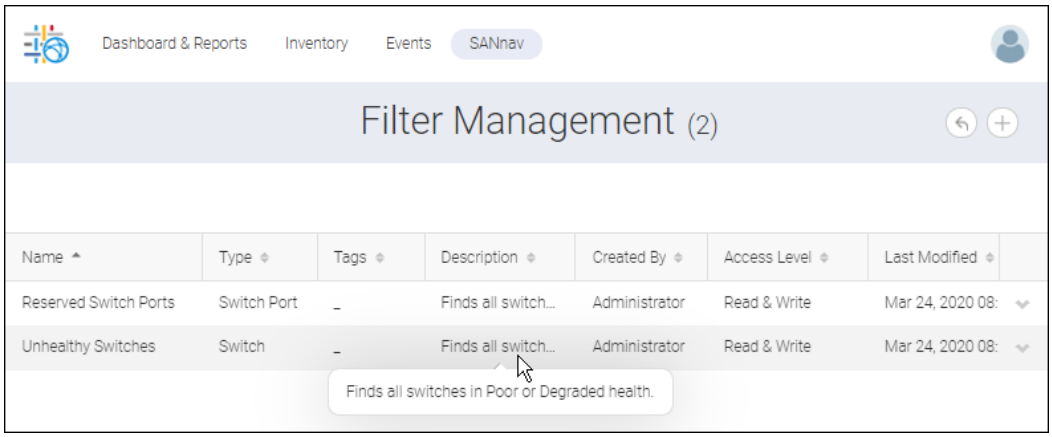
Managing Filters

You can view, modify, create, and delete permanent filters from the SANnav **Filter Management** page. The **Filter Management** page displays all permanent filters, including filters created by other users.

If you create filters in the **Filter Management** page, you can then apply these filters in the **Inventory**, **Dashboard**, and **Reports** pages. Conversely, if you create and save filters in the **Inventory**, **Dashboard**, and **Reports** pages, you can then view and manage these filters in the **Filter Management** page.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** > **Filter Management**.

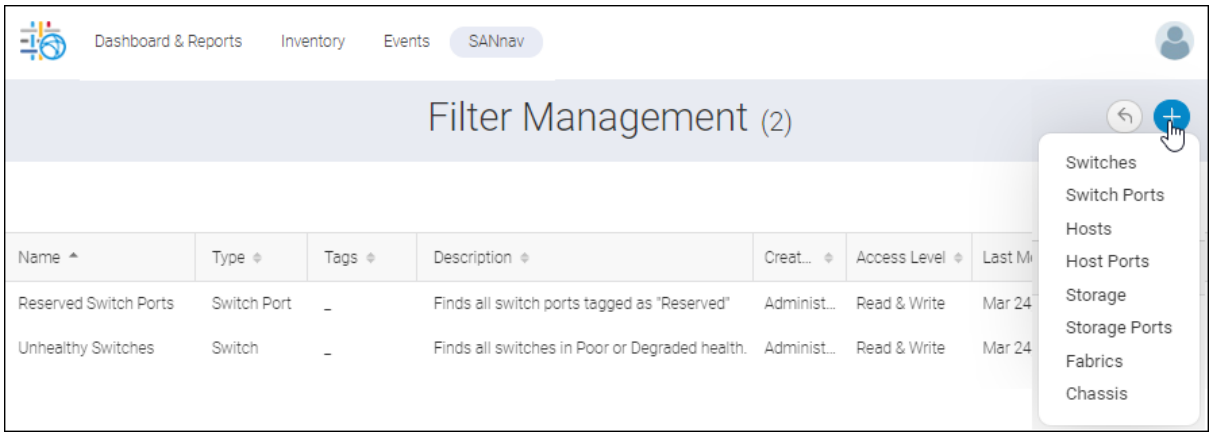
   A list of all permanent filters displays.



2. To modify or delete a filter, click the filter name or click the down arrow in the action menu and select **View**.

   The filter detail page opens, where you can edit the filter, save it as a different filter, or delete it. If you want to modify a filter for which you have only read access, you must first save it as a different filter.

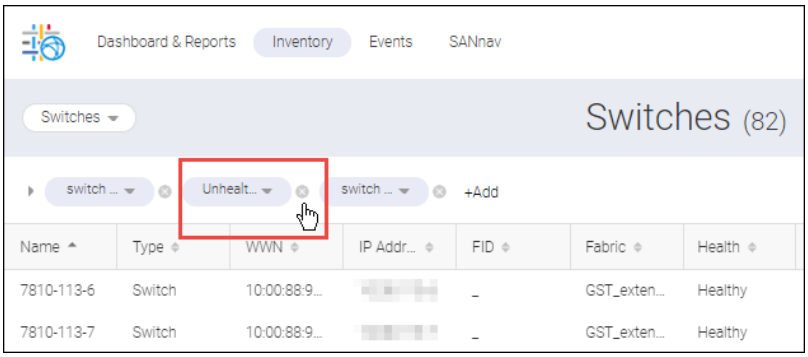
3. To create a filter, click the add button (**+**) in the top-right corner of the page, and then select the type of filter that you want to create from the drop-down list.



Deleting Filters

In SANnav, if you create filters, you can delete the filters. Only the user who created a filter can delete the filter.

If you want to remove a filter from the filter bar, click the small **X** to the right of the filter.



When you click the **X**, the filter is removed from consideration. If the filter is a temporary filter, it is deleted. You must recreate it if you want to use it again. If the filter is a permanent filter, it is removed from the filter bar, but it is not deleted. You can select it again when you add a new filter to the page.

To delete permanent filters, perform the following steps.

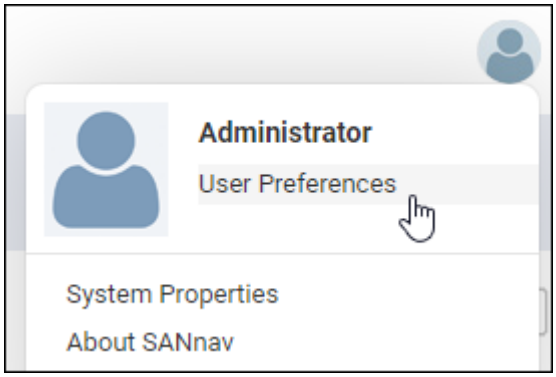
1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** > **Filter Management**.
   The list of permanent filters displays.
2. Click the filter name or click the down arrow to the right of the filter that you want to delete, and select **View**.
3. Click **Delete** in the filter details page.
4. Click **OK** in the confirmation dialog.

Configuring the Theme for the User Interface

By default, SANnav uses a white-background theme for the user interface. You can change to a dark mode theme.

The theme preference is on a per-user basis and is persisted across logins.

1. Click the user icon in the top-right corner of the window, and then click **User Preferences**.



2. In the **Display Theme** section, select either **Light** or **Dark** from the drop-down list.

   Light is the default white background theme. **Dark** is a dark background theme.

   The theme changes to the selected mode. All exported files (PDF and HTML) continue to use the Light theme format, regardless of the selected theme.

Licensing

When you install SANnav, you have a 30-day trial period, during which you can use SANnav for free, without a license. To use SANnav beyond the trial period, you must purchase a software license.

> **NOTE**
> The 30-day trial period is activated automatically and starts from the time you install the SANnav product.

SANnav licenses are subscription-based, which means that they expire at the end of the subscription period. If the license expires, you cannot log in to SANnav unless you provide a new license certificate. Before your license expires, you should renew the license to ensure uninterrupted service. By default, during installation SANnav is configured to automatically retrieve and activate renewed licenses.

SANnav Management Portal and SANnav Global View are two separate products, which require separate license certificates and are independent in terms of licensing.

When you install SANnav, whether on a server or on a virtual machine (VM), a server unique ID (UID) is generated for that SANnav instance. The server UID and the transaction key are used to generate a SANnav license. The license is locked to that server UID and SANnav instance.

> **NOTE**
> SANnav 2.2.0 and higher use a license certificate (XML file). Earlier versions of SANnav use a license key (text string). These license keys are not supported by SANnav 2.2.0 and higher. During migration to SANnav 2.2.1 from 2.1.1, the existing license key is automatically converted to a license certificate.
>
> Refer to the *Brocade SANnav Global View Installation and Upgrade Guide* for more details.

You need one license for every SANnav instance, and each license can be used on only one SANnav instance. For example, if you have multiple VMs on a single server and you install SANnav on every VM, each installation generates a separate server UID and requires a separate license. You cannot clone a VM and use the same license on the cloned VM.

If you must move a license from one SANnav instance to another, such as if you want to move the installation to a different server, you do not need to purchase a new license; you can "rehost" the license on the new SANnav instance.

SANnav Licensing Terminology

The following terms are used in this document:

- **license certificate** – An XML file that enables you to use a particular SANnav instance. A license certificate has an expiration date, after which you can no longer use SANnav unless you renew the license. The license certificate is generated from the Broadcom licensing portal.
- **rehost key** – A key that is used when you want to move the SANnav application from one server or virtual machine (VM) to another or when the MAC address of the server changes. The rehost key is generated by SANnav when you release the current license.
- **server unique ID (UID)** – A unique ID that identifies the physical server or VM on which SANnav is installed. The server UID is used with a transaction key to generate and download a software license from the Broadcom licensing portal. The server UID is generated when you install the SANnav application.

  Note that the server UID is not the same as the VMware UUID.
- **transaction key** – A unique key, along with the server UID, used to generate a SANnav license from the Broadcom licensing portal. You obtain the transaction key from your vendor when you order a SANnav license.

How SANnav Licensing Works

Through a combination of the server unique ID (UID) and the transaction key, you can generate a license certificate to activate the SANnav license.

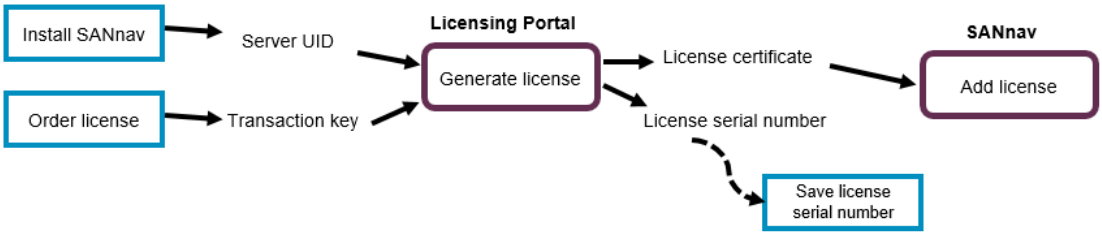
When you install SANnav on a server or virtual machine (VM), a server UID is generated. You can view this server UID and copy it from the **SANnav Licensing** page.

When you order a license, an email message, along with a transaction key, is issued by Broadcom as fulfillment of your license purchase. The transaction key and server UID are used to generate a license certificate and license serial number from the Broadcom licensing portal.

After you obtain the license certificate, add it in SANnav, and activate the license.

This flow is illustrated in the following diagram.

Figure 7: Generating a License



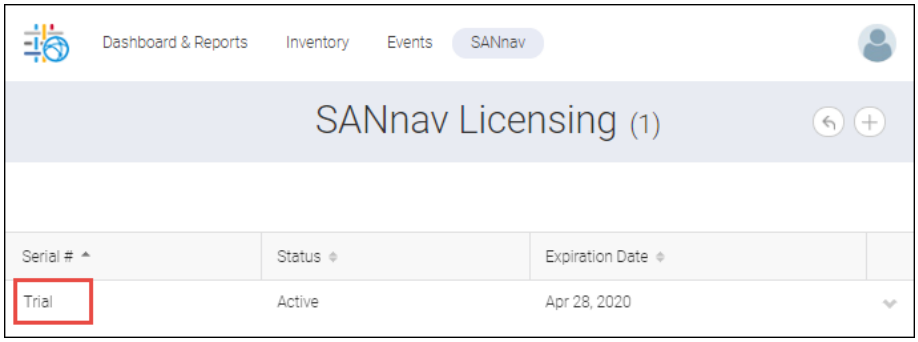
Keep a record of the license serial number. You need the license serial number if you contact support. The license serial number can also be obtained from the **Licensing** page of the SANnav user interface.

Obtaining the Server UID

During installation, SANnav generates a server unique ID (UID), which you need when you generate a license. You can obtain the server UID from the **SANnav Licensing** page.

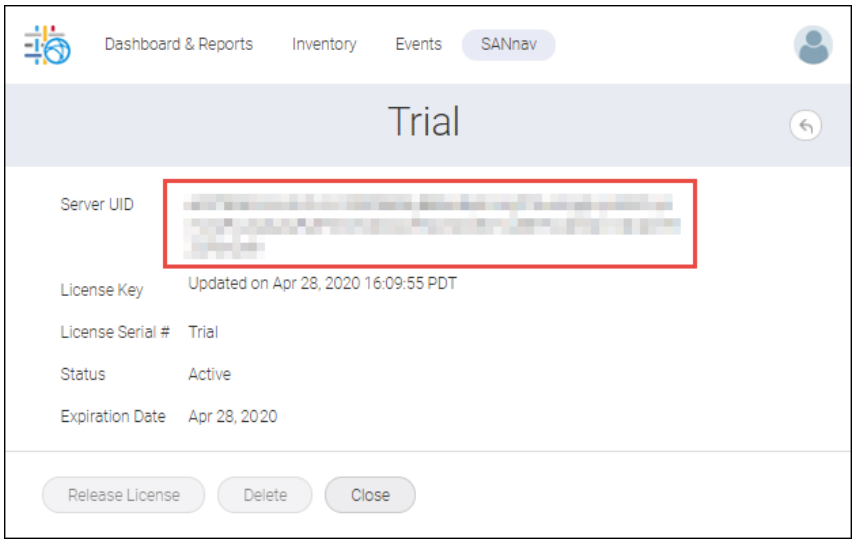
1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Licensing**.
2. Click the license for which you want to obtain the server UID.

   When you first install SANnav, only one license displays, so click **Trial**.



3. Copy the server UID so that you can paste it later.

   NOTE
   Be sure to copy the server UID completely, without missing any characters. An incorrect or partial server UID can lead to an incorrect license being generated from the license portal.



The next step is to access the Broadcom licensing portal, where you use the server UID to generate a license certificate.

Generating a License

Access the Broadcom licensing portal to generate a SANnav license key.

Before you generate the license, make sure that you have a server unique ID (UID). After you install SANnav, you can obtain the server UID from the **SANnav Licensing** page.

Use the following procedure to generate and obtain a SANnav license key.

1. Obtain a transaction key from your SANnav vendor.

   You will receive an email with the license transaction key in the form of an electronic transaction key. Do not discard the email with the electronic key. Keep it in a safe place in case it is needed for technical support or product replacement.

2. Go to https://www.broadcom.com, and then select the **LOGIN** drop-down at the top-right of the web page.
3. Click **LOGIN** or **REGISTER**.

   Once logged in, you are redirected to the Broadcom support portal.

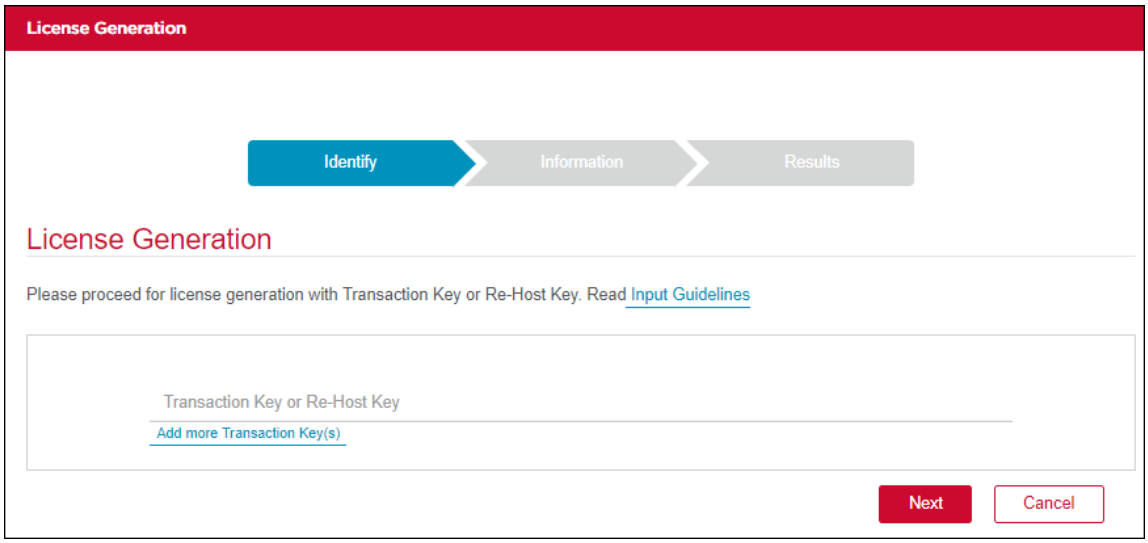
4. Click **Brocade Products**.

   You are redirected to the **Brocade Products** page.

5. Click **Licensing**.

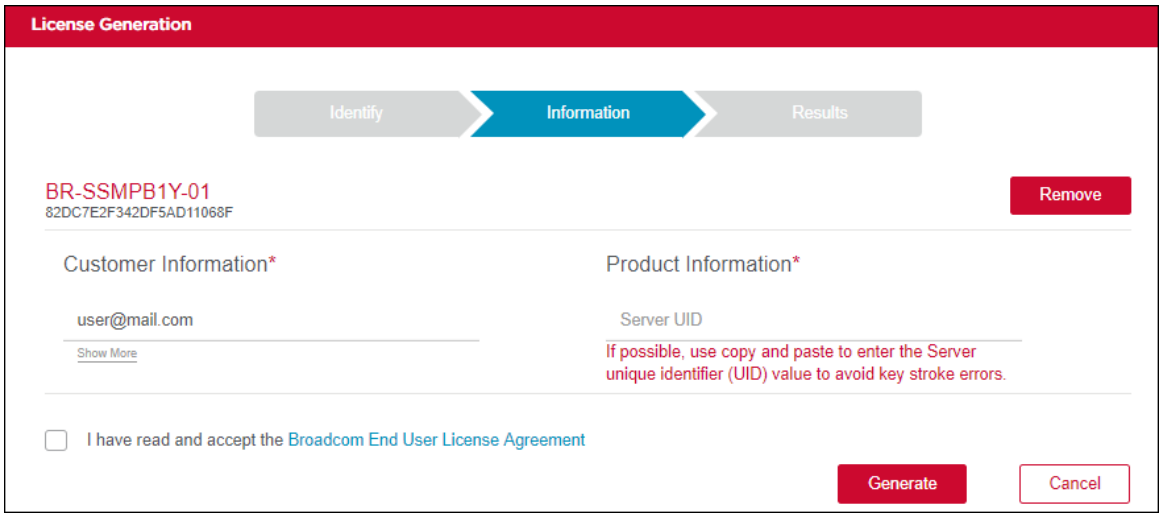
   You are redirected to the **Broadcom Licensing Portal** page.

6. Enter the license transaction key or rehost key in the **License Generation** window, and click **Next**.



7. In the **Product Information** area, enter the server UID that you obtained from SANnav.

   NOTE
   Be sure to enter the server UID completely, without missing any characters. An incorrect or partial server UID can lead to an incorrect license being generated.



8. Read the Broadcom End User License Agreement, and if you agree to the terms, select the **I have read and accept** checkbox.
9. Click **Generate**.

   The **Results** window displays an order summary and the results of the license request.

   - If the license request is successful, the License field contains a hyperlink to the generated license file. The license file is automatically sent by email to the specified customer email address.
   - If the license request fails, the reason for failure and the action to take are displayed on the page.

10. Click the hyperlink in the **License** field to display the license key.

11. Copy the license key to a .txt file and save it.

    You will use this license key when you add the license to SANnav.

12. Click **Export to Excel** to export the results to a Microsoft Excel file, or click **Generate Another License** to generate a new license.

Next, you must add the license to SANnav.

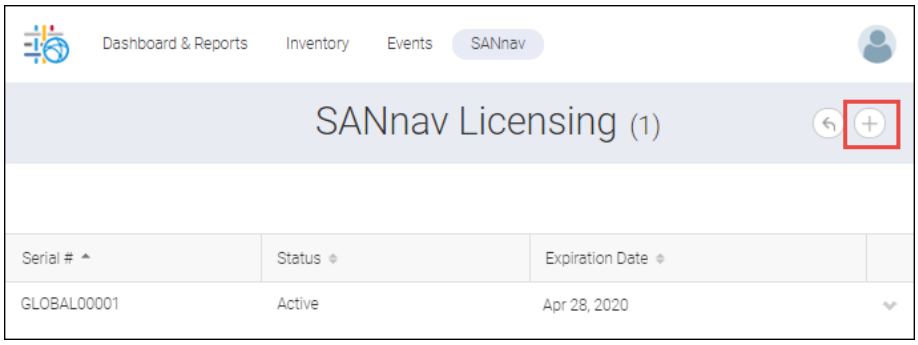
Adding a License to SANnav

After you obtain a license certificate from the Broadcom licensing portal, you must add the license certificate to SANnav to activate the license.

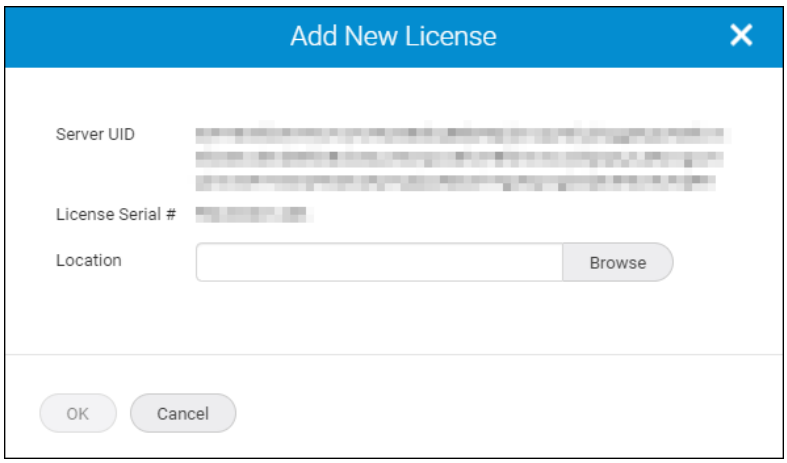
Before you start, make sure that you have the license certificate that was generated from the Broadcom licensing portal. The license certificate must be the XML file that was generated for this instance of SANnav (using the server UID of this instance). The entire XML file must be installed to enable the license.

> **NOTE**
> When you activate a new license, the current license is deactivated, but the expiration date of the current license remains the same. For example, assume you install a 1-year Base license. After 8 months you purchase and activate an Enterprise license on the same SANnav server. The Base license becomes inactive and expires in 4 months (on the original expiration date).

1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Licensing** to view the license list.
2. Click the **+** button at the top-right corner of the **SANnav Licensing** page.



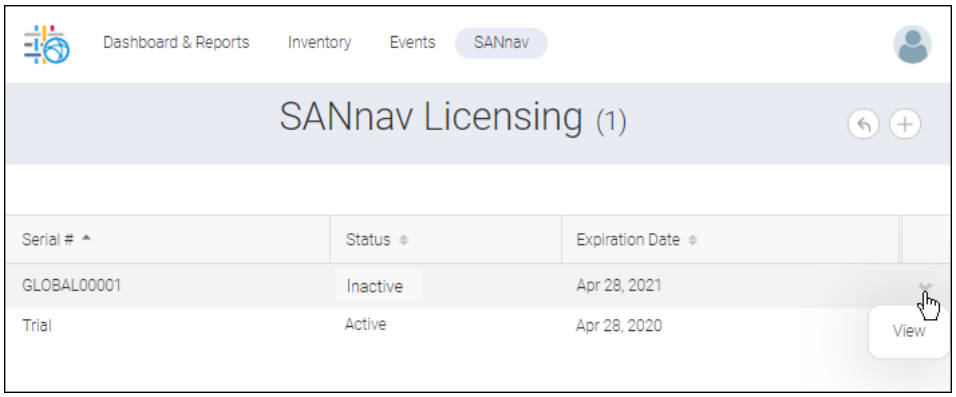
3. Click **Browse**, and navigate to the location of the license certificate file that you obtained from the Broadcom licensing portal. Select this file, and click **OK**.



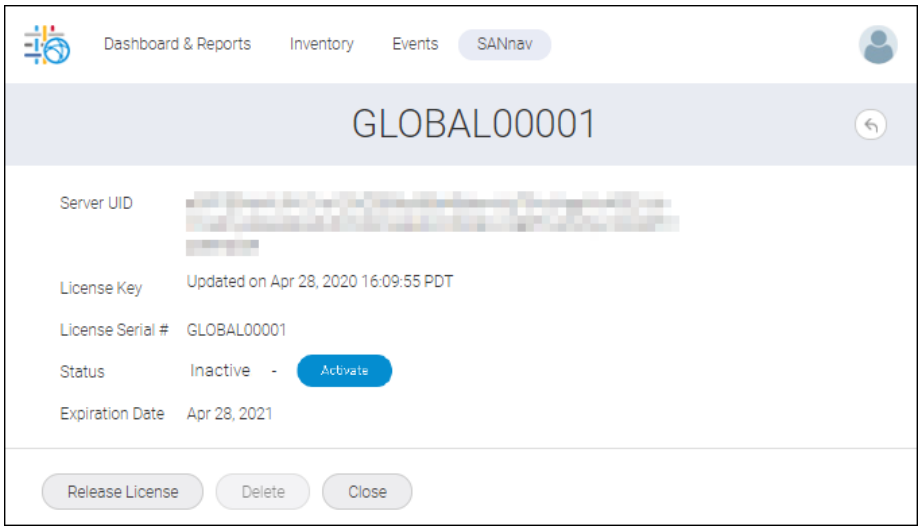
The new license is added to the **SANnav Licensing** page.

- If the new license has the same serial number as the existing license, the new license replaces the existing license and is automatically activated.
- If the new license has a different serial number from the existing license, the new license is added as a separate entity in the **SANnav Licensing** page and is in an inactive state.

4. To activate the license, click the down arrow at the right of the license row, and then click **View** to display the license details page.



5. Click the **Activate** button to activate the license.



Only one license can be active at a time. When you activate any license, any previously active license is deactivated. You cannot activate expired or released licenses.

6. Click **Close** to return to the **SANnav Licensing** page.

Renewing a License

By default, SANnav is configured to automatically retrieve and activate renewal licenses. If SANnav is not configured to automatically retrieve and activate renewal licenses, you must manually apply the license.

The option for SANnav to automatically retrieve and activate renewal licenses is configured during installation. (See the *Brocade SANnav Global View Installation and Upgrade Guide* for more details.)

When you purchase a renewal license, the license certificate is sent in an email, and the Broadcom licensing portal is updated with the new license certificate. The serial number of the new license must match the serial number of the existing license.

Once a month, SANnav checks the licensing portal. If a new license certificate is found, SANnav automatically retrieves it from the licensing portal and activates it.

Starting 90 days before the license expiration date, SANnav checks the licensing portal daily. When you log in to SANnav, a pop-up message alerts you that your license is about to expire and prompts you to renew the license.

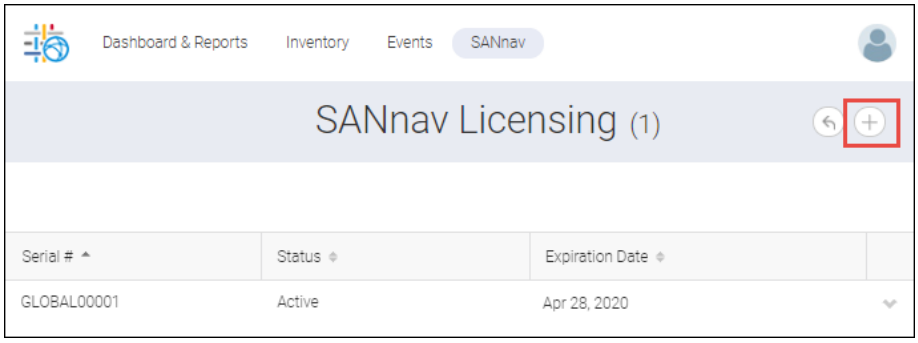
When you renew a license, the new expiration date is the expiration date of the new license.

If SANnav does not automatically apply the license, you must perform the following steps to manually apply the license.

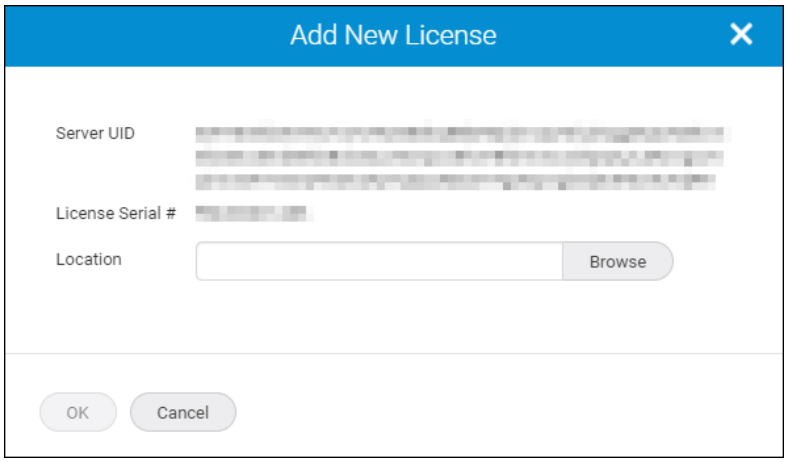
NOTE
When the new license is applied, whether automatically or manually, all logged-in users are logged out and must log in again.

1. Obtain a license certificate from your SANnav vendor.
   The license certificate is sent in an email.

2. Log in to SANnav.
3. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Licensing** to view the license list.
4. Click the **+** button at the top-right corner of the **SANnav Licensing** page.



5. Browse to the location of the license certificate file, and click **OK**.



The license is automatically activated, and your session is logged out. Log in again to use the SANnav application.

Rehosting a License on a Different Server: Planned Migration

If you want to move SANnav from one server or VM to another, you need a new license. Instead of purchasing a new license, you can use a rehost key to generate a license for the new server or VM.

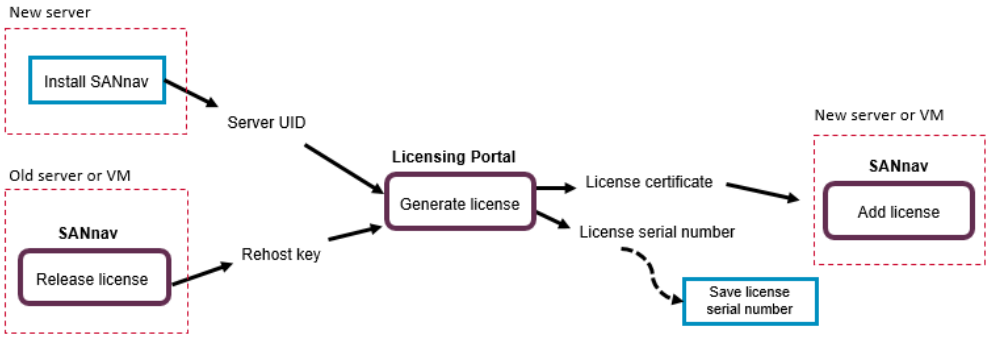
Migrating a license from one SANnav instance to another is called *rehosting*. If you want to move SANnav from the current server or VM to another, you must first release the current license. When you release the license, a rehost key is generated. You must provide the rehost key and the new server UID to get a license for the new SANnav instance.

The license rehosting process is used in the following circumstances:

- If you want to migrate SANnav from one server or VM to another
- If the MAC address of the server in which SANnav is installed changes for any reason

The following diagram illustrates the rehosting flow.

Figure 8: Rehosting a License



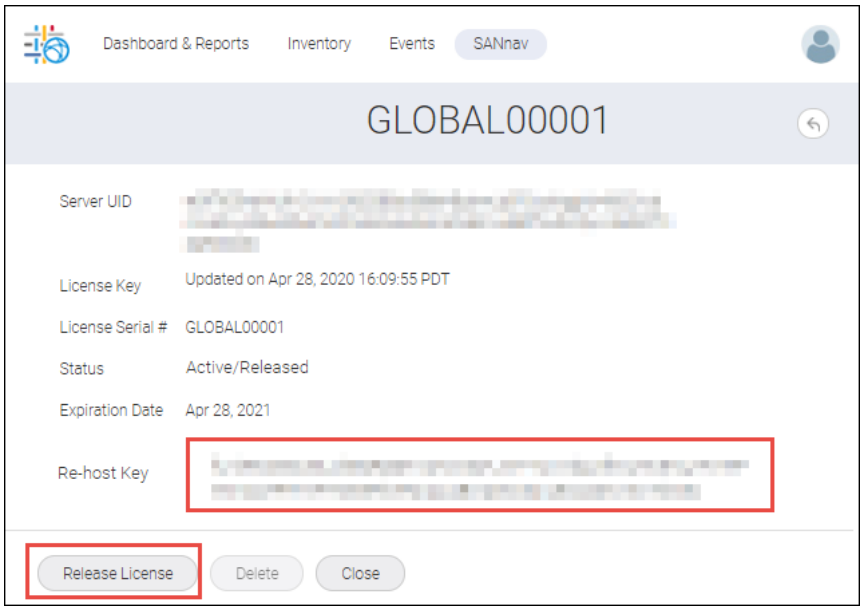
The released license remains active (that is, you can continue to use the SANnav instance) for 30 days from the time of release or until the original expiration date, whichever comes first. This 30-day period gives you time to install SANnav on the new server or VM and to validate that the new server or VM is working.

> **NOTE**
> Before you move SANnav, you should take a full backup. After the migration, you can restore the backup on the new server or VM.

To rehost the license, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Licensing** to view the license list.
2. Click the down arrow at the right of the license row, and then click **View** to display the license details page.
3. Click the **Release License** button to release the license on the current server or VM.
   You can release both active licenses and inactive licenses (licenses not yet active).

   SANnav displays a rehost key.



4. Copy the rehost key for later use when generating the new SANnav license on the Broadcom licensing portal.
5. Install SANnav on the new server or VM and obtain the server UID.
6. Using the rehost key and the server UID from the new server or VM, generate a new license on the Broadcom licensing portal.
7. Add the license to SANnav.

See Obtaining the Server UID, Generating a License, and Adding a License to SANnav for instructions.

Moving a License to a Different Server: Unplanned Migration

If the server on which SANnav is installed experiences a permanent hardware failure and can no longer be used, you can install SANnav on a new server with a replacement license.

Unlike a planned license migration, in this unplanned migration you cannot access SANnav and so cannot get a rehost key. Instead, you must contact Technical Support to get a replacement license certificate.

1. Locate the license serial number for the original license.
2. Install SANnav on a new server and obtain the server unique ID (UID).
3. Contact Technical Support and provide the license serial number and server UID to request a replacement license certificate.

After you install SANnav on the new server, if you have taken a SANnav backup, you can restore the backup on the new server.

Deleting a License

You can delete inactive, expired, and released SANnav licenses.

1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Licensing** to view the license list.
2. Click the down arrow at the right of a license row, and then click **View** to display the license details page.
3. Click the **Delete** button to delete the license.

Security

SANnav provides several security features that allow you to manage user accounts, the login banner, and user authentication.

From the SANnav user interface, you can manage user accounts and passwords. You can also configure an external server for user authentication.

You can use provided scripts to perform the following tasks:

- Replace the SANnav self-signed certificate with a trusted CA signed certificate.
- Create a list of IP addresses that are allowed to access SANnav.

User Management

Access to SANnav is controlled by authentication and authorization of users. *Authentication* is the process of validating user names and passwords. *Authorization* is the process of validating the roles, privileges, and areas of responsibility (AORs) for each user.

> **NOTE**
> SANnav Global View supports only one role (SAN System Administrator) and one AOR (All Fabrics) for all users.

You can configure SANnav to perform authentication and authorization locally or by using an external server (such as AD LDAP Server or CA LDAP Server, AD Global Catalog, RADIUS, or TACACS+).

User management involves the following general steps:

1. Configuring password policies.
   You should configure password policies first, because when you create user accounts, you assign a password to the account, and you must assign passwords that conform to the password policies. The password policies are applicable for SANnav users only when you select primary authentication as the local database.
2. Setting up user accounts.
   User accounts contain the identification of the SANnav user. At least one user account with the User Management read-write privilege must always be defined on the SANnav server. You cannot delete this user account. This user account can be the default Administrator account or a custom user-created local account.

   > **NOTE**
   > The user accounts described here are for users to log in to SANnav Global View. They are not the same user accounts that the SANnav Global View server uses to log in to each SANnav Management Portal server instance.

Global View Password and Lockout Policy

Having a strong password policy is a key component for secure access to SANnav.

When you set up password policies in SANnav Global View, these policies apply only to the local database. If you are using an external server for authentication, these policies do not apply, and you must set up password policies on the external server. If primary authentication on the external server fails, and you fall back to secondary authentication on the local database, then the password policies that are defined in SANnav apply.

If you change the password policy so that the passwords of logged-in users are now in violation of the new policy, the users remain logged in, but the next time they try to log in, they get a password violation message and are prompted to change their password.

The following steps provide a guideline for creating a strong password policy. Your policy may vary.

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav Password and Lockout Policy**.
2. Configure the password strength policy, as follows.

Option	Description
Minimum Length	The minimum length is 8 to 40 characters. Longer passwords increase security dramatically.
Uppercase Letters **Lowercase Letters** **Digits** **Special Characters**	This is the minimum number of upper- and lowercase letters, digits, and special characters required in the password. The default value for each of these options is 0. For strong passwords, you should set each of these options to at least 1.
Maximum Repeat	Maximum Repeat specifies the maximum number of repeated characters that are allowed. For example, if Maximum Repeat is 2, then "password" is valid, but "passsword" is not. Select a value or use the default value (2).
Maximum Sequence	Maximum Sequence specifies the maximum number of sequential characters that are allowed. The sequence is based on the ASCII value of the characters. For example, if Maximum Sequence is 1, then "password1" is valid, but "password12" is not, and "passworda" is valid, but "passworde" is not (sequence "de" violates the policy). Select a value or use the default value (1). Note that if you use the default value, some common two-letter sequences (such as "hi", "st", and "no") will be disallowed in passwords.

3. Configure the password expiration and password history policies.

Option	Description
Password never expires	By default, passwords never expire. If your password policy enforces strong passwords, you might not want the passwords to expire unless security is compromised. Uncheck this box if you want passwords to automatically expire after a specific time period.
Password Age	The amount of time after which a password automatically expires. This value is between 15 days (default) and 12 months. For the most security, choose shorter values. A good value is between 45 days and 6 months.
Warning Period	The number of days prior to password expiration that a user starts getting warning messages. Select a value from 1 (default) to 15 days.
Password History	The number of previous passwords that cannot be reused. For example, if Password History is 5, users cannot reuse their most recent 5 passwords. Select a value between 1 (default) and 10. For the most security, select 10.

4. Configure the account lockout and session policy.

Option	Description
Lockout After	By default, a user account is locked after three failed login attempts. You can change this to 4 or 5 failed login attempts. For the most security, keep the default (3).
Lockout Duration	A locked account automatically unlocks after the amount of time specified by **Lockout Duration**. Lockout duration is between 15 (default) and 60 minutes. Keep in mind that when setting the lockout duration, the higher settings might result in increased support calls, whereas lower settings might make SANnav more vulnerable to brute force attacks. For higher levels of security, select the higher settings.

Option	Description
Inactive Duration	By default, you are logged out after 30 minutes of inactivity. You set this value to between 15 minutes and 12 hours. If you select **Keep Dashboard active after session expires**, then if you are on the dashboard page and the session expires, you are not logged out. You can continue to view the dashboard, which is dynamically updated. If you move off the dashboard page, however, you are logged out and must log in again.

5. Click **Save**.

Creating a New User Account

Creating user accounts in SANnav Global View is similar to creating user accounts in SANnav Management Portal. In SANnav Global View, however, users do not need to be mapped to roles and areas of responsibility (AORs). All users who are created in SANnav Global View have all privileges in the product and can do all operations and functions that are provided by the Global View.

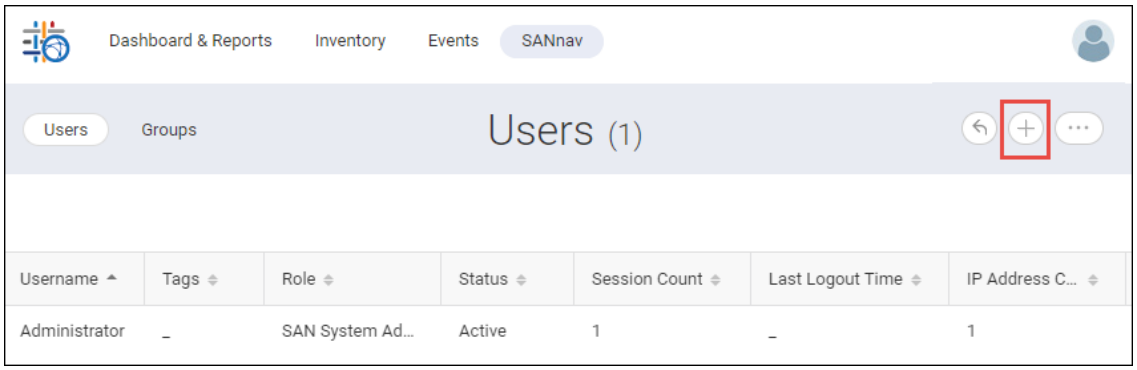
A SANnav Global View user does not have privileges to modify a SANnav Management Portal instance. An attempt to do this triggers a request to log in to the Management Portal. The SANnav Management Portal login credentials determine what a user can perform in that portal.

A SANnav Global View user can see summarized information regarding all fabrics as managed by various portals (though this information is limited to what SANnav Global View presents).

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.

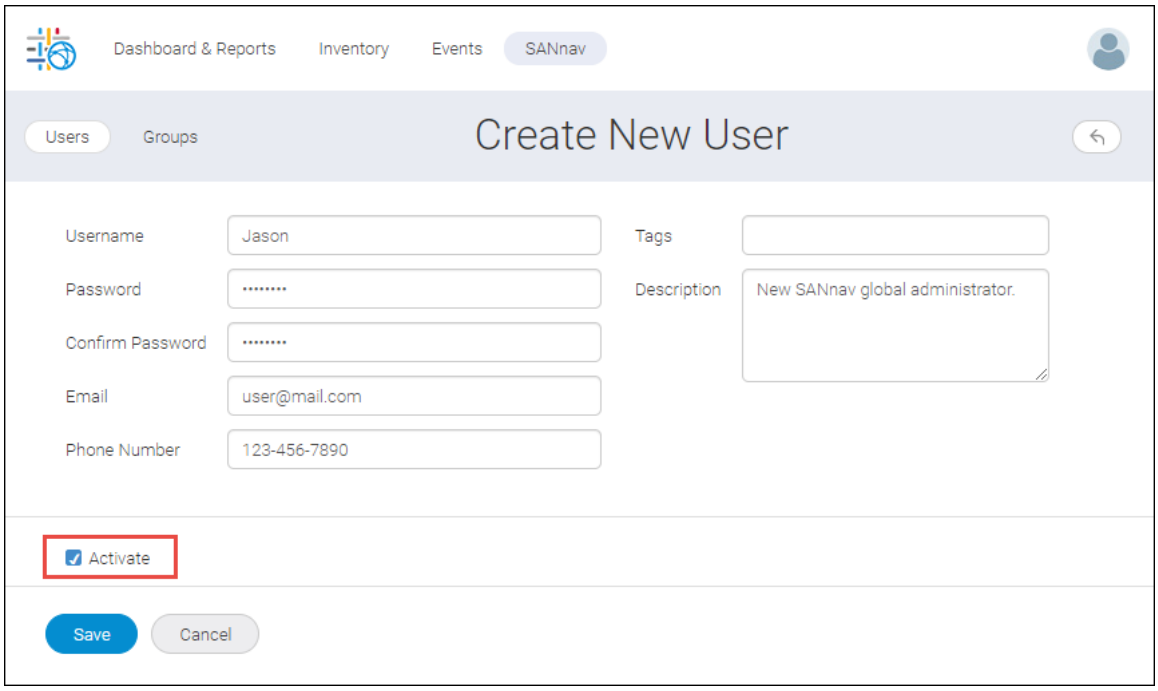
   A list of users displays.

2. Click the **+** icon in the top-right corner of the page.



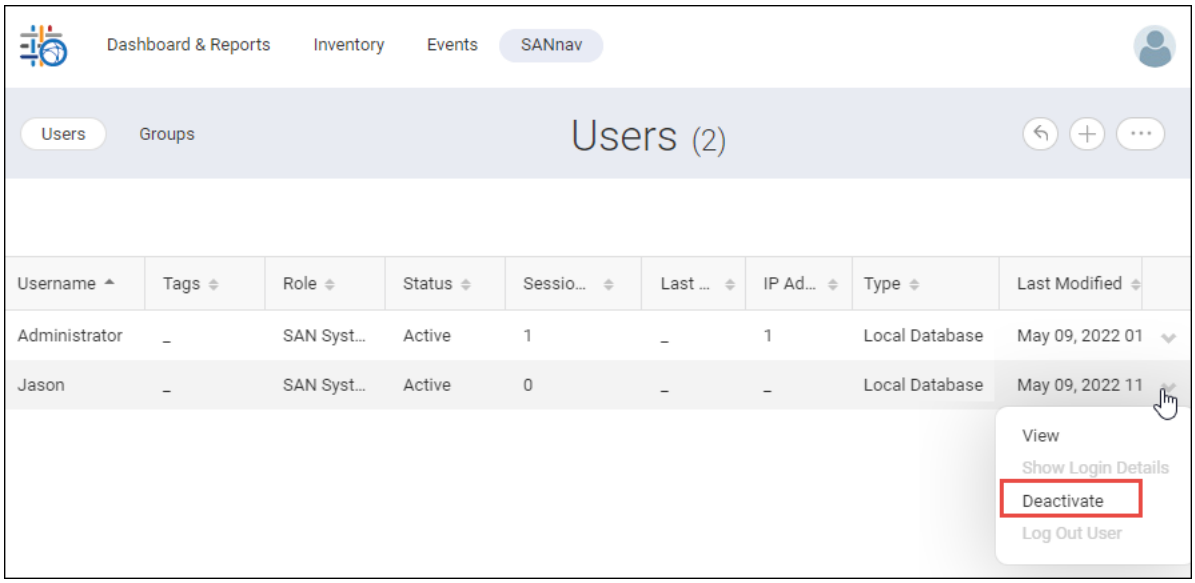
3. Fill out the **Create New User** form, and click **Save**.

   By default, saving the form activates the account.



The new user is added to the list of Global View users.

4. If you want to deactivate a user account, click the down arrow in the rightmost column and select **Deactivate**.



Viewing a List of Users

To view a list of SANnav users, complete the following steps.:

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Click **Users**, if necessary.
   The user session details include the following information:

- **Username** – The name of the user.
- **Tags** – Any tags included for the user.
- **Role** – The role of the user (such as, Operator).
- **Status** – The status of the user (such as, Active).
- **Session Count** – The number of sessions opened by the user.
- **Last Logout Time** – The date and time when a user logged out of the SANnav client. For the server, active sessions are polled every 5 minutes; therefore, there may be a delay up to 5 minutes. A dash (-) in the **Last Logout Time** column indicates that the user is active.
- **IP Address Count**– The number of unique IP addresses in use by the user.
- **Type** – The authentication type (such as, AD LDAP Server).
- **Last Modified** – The last time the user account was modified.

Exporting User Session Details

To export the user session details for all users, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Click **Users**, if necessary.
3. Click the more button ( ) in the top-right corner of the page, and click **Export All Session Details**.
   A `.csv` file is downloaded to your local machine.

The user session details include the following information:

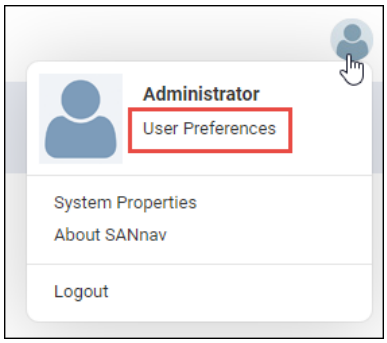
- **Username** – The name of the user.
- **Role** – The role of the user (such as, Operator).
- **Status** – The status of the user (such as, Active).
- **Type** – The authentication type (such as, AD LDAP Server).
- **Client** IP – The IP address of the client.
- **Login Time** – The login time of the user (date and time).
- **Last Logout Time** – The date and time when the user logged out of the SANnav client. For the server, active sessions are polled every 5 minutes; therefore, there may be a delay up to 5 minutes. A dash (-) in the **Last Logout Time** column indicates that the user is active.

Changing Your Password

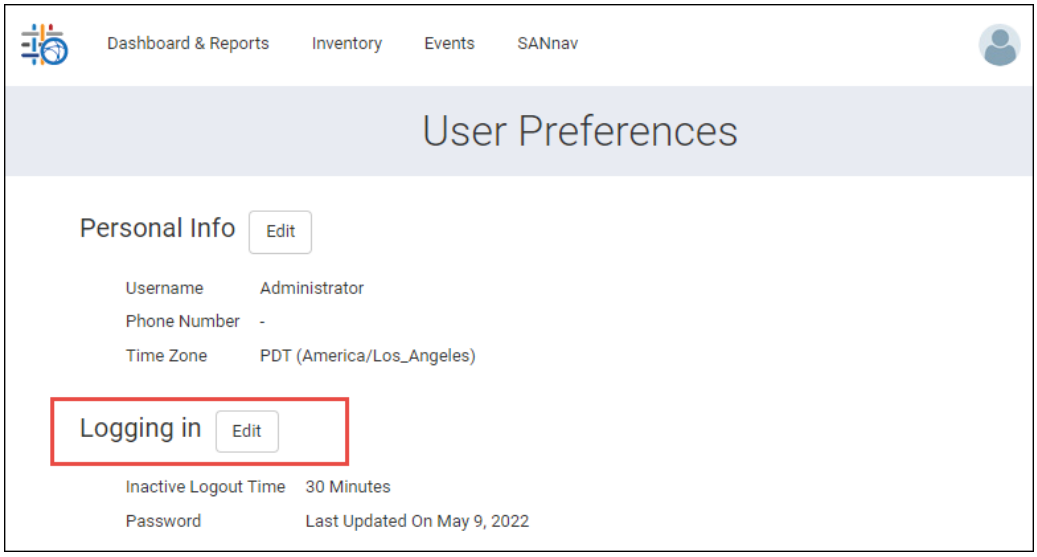
NOTE
The first time a new user logs in successfully, a change password warning displays. You must change your password immediately before you can access SANnav.

After you change your password, you are automatically logged out, and you must log in again using the new password.

1. Click the user icon in the top-right corner of the window, and then click **User Preferences**.



2. Click the **Edit** button next to **Logging in**.

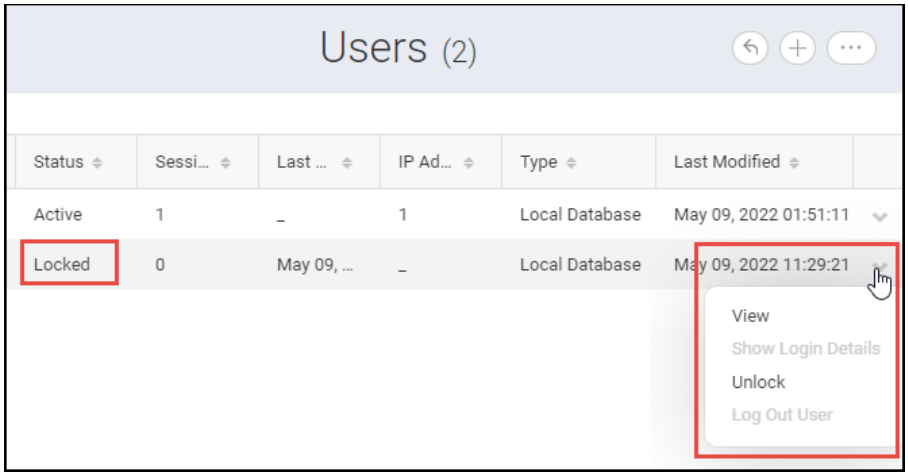


3. Click **Change** on the **Logging in** page.
4. Fill out the **Change Password** fields, and click **OK**.
   You are automatically logged out of SANnav.
5. Log in to SANnav again using your new password.
   When you change your password, a password change application event displays on the **Events** page.

Unlocking a User Account

If a user account is locked due to excessive failed login attempts, you can manually unlock the account for the user. If the account is not manually unlocked, the user must wait until the lockout duration expires.

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Locate the locked user (Status = Locked), click the down arrow at the right of the row, and select **Unlock**.



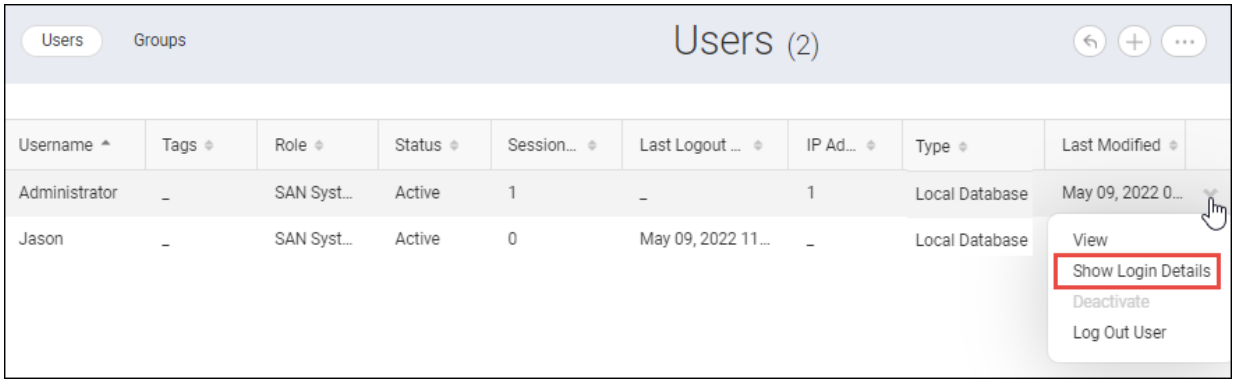
The status changes to Active, and the user can now try to log in again.

Viewing User Sessions

The **User Login Details** dialog displays all open sessions for a selected user.

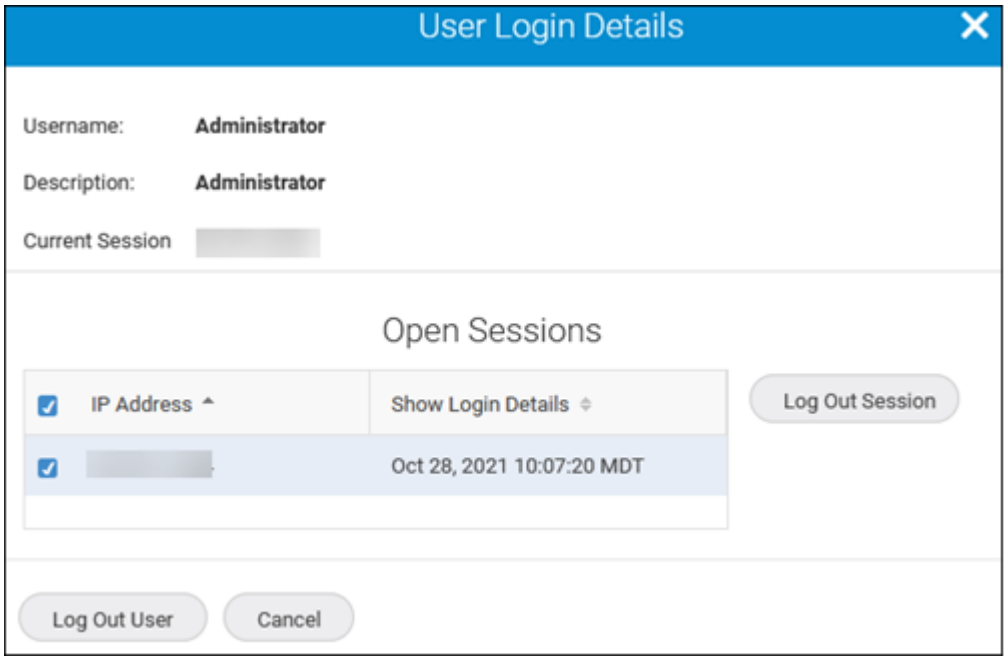
The maximum number of open sessions per user is 25.

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Click **Users**.



3. Click **Show Login Details** from the action menu for a specific user.

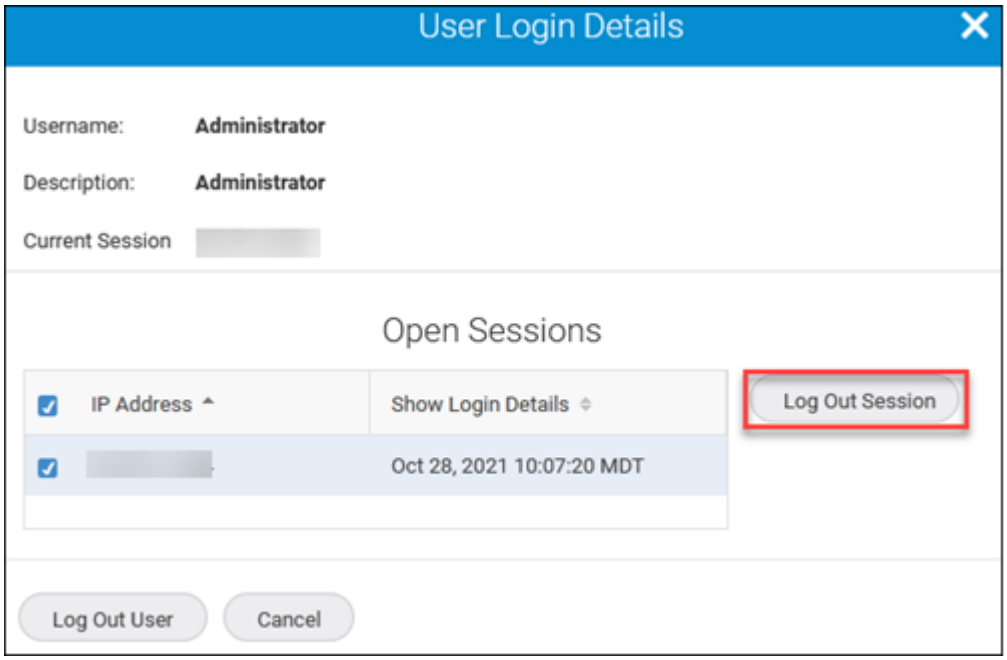
   The **User Login Details** dialog displays with a list of all open sessions for the selected user.



Logging Out a User from a Specific Session

To log out a user from a specific session, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Click **Users**.
3. Click **Show Login Details** from the action menu for a specific user.
   The **User Login Details** dialog displays with a list of all open sessions for the selected user.

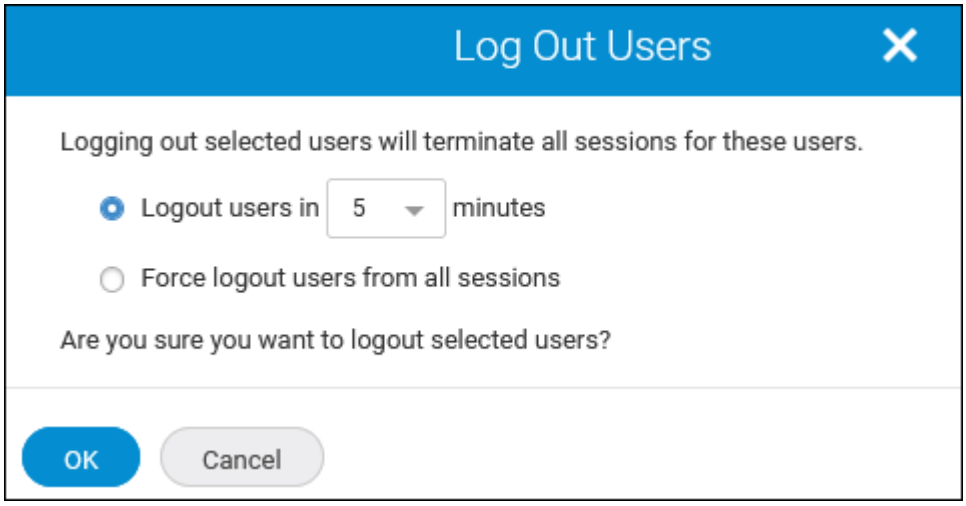


4. Select the checkbox for the session from which you want to log out the user, and click **Log Out Session**.
5. Click **OK** in the confirmation dialog.

Logging Out One or More Active Users

You can log out a user immediately or after a specified time (5, 10, or 15 minutes).

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Click **Users**.
3. Choose one of the following options:
   - For a single user, select **Log Out User** from the action menu for the user that you want to log out.
   - For multiple users, click the more button (···) in the top-right corner of the page, and click **Bulk Select**.
     a. Select the checkboxes for the users that you want to log out.
     b. Select **Actions** > **Log Out Users**.
4. Choose one of the following options:



   - Select **Logout users in 5 minutes**, and select the time (5, 10, or 15 minutes) to log out the users after the specified time.
   - Select **Force logout users from all sessions** to log out the users immediately.
5. Click **OK** in the **Log Out Users** dialog.

   If you selected to force logout, the users are immediately logged out. If you selected to delay logout, a message displays for the users telling them how long they have until they are logged out.

Activating or Deactivating Users

When you deactivate a user, that user can no longer access SANnav.

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Click **Users**.
3. Choose one of the following options:
   - For a single user, select **Activate/Deactivate** from the action menu for the user that you want to activate or deactivate.
   - For multiple users, click the more button and select **Bulk Select**.

A column of checkboxes displays on the left-most side of the table.

a. Select the checkboxes for the users that you want to activate or deactivate.
b. Select **Actions** > **Activate/Deactivate**.
c. Click **OK** on the 'confirmation' and 'sucessful' messages.

Deleting Users

Administrators can delete users from the local SANnav system. You cannot delete the last active user with the User Management read+write privileges.

NOTE
Deleting users is disruptive to the active sessions.

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Click **Users**.
3. Click the more button and select **Bulk Select**.
   A column of checkboxes displays on the left-most side of the table.
4. Select the checkboxes for the users that you want to delete.
   If you select a currently logged in user, that user is skipped during the bulk delete.
5. Select **Actions** > **Delete**.
6. Click **OK** on the 'confirmation' and 'successful' messages.

SANnav Login Banner

SANnav provides a login banner to display messages related to company security policy.

Configuring the Login Banner

To configure the login banner, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Security** > **Login Banner**.
2. Enter a security policy message for your company in the **Banner Message** text field.
   You can enter up to 2048 characters in the field.
3. Select the **Display login banner upon client login** checkbox.
4. Click **Save**.

Disabling the Login Banner

To disable the login banner, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Security** > **Login Banner**.
2. Clear the **Display login banner upon client login** checkbox.
3. Click **Save**.

Configuring SANnav to Use an External Server for Authentication

You can configure SANnav to use an external server for authentication of user names and passwords. You can also optionally use this server for user authorization.

NOTE

- User names on the external authentication server that are the same (such as, Administrator) in the local database are blocked from logging in to SANnav when the authorization preference is not set to Local Database.
- If you are configuring an external server for authentication and authorization, this guide assumes that you understand how external authentication works, that the external servers are already set up, and that the user names and passwords are already configured on the external server.

SANnav supports the following types of external servers for authentication and authorization:

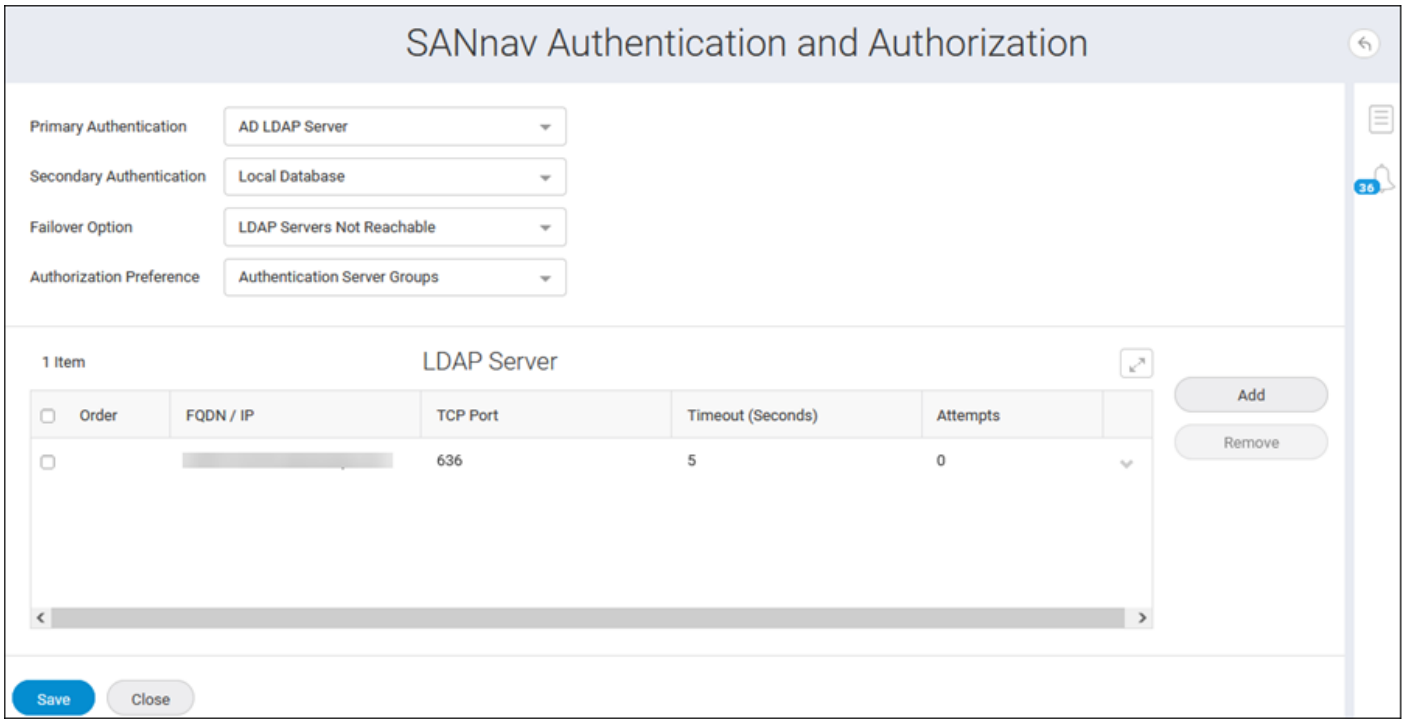
- AD LDAP Server
- CA LDAP Server
- AD Global Catalog (AD GC)
- RADIUS
- TACACS+

When you select AD LDAP Server, CA LDAP Server, RADIUS, or TACACS+ as the primary authentication method, you must provide SANnav with a list of up to three LDAP, RADIUS, or TACACS+ servers. If you provide more than one server, then if the first server is not reachable or if authentication fails, SANnav attempts to access the next server on the list.

When you select AD Global Catalog as the primary authentication method, you can provide SANnav with one AD GC server only. For AD GC as primary authentication, you can configure secondary authentication to local database only.

If all external servers are unreachable or if authentication fails, you can specify whether to use the local SANnav database as a secondary authentication method.

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav Authentication and Authorization**.



2. Select the type of primary authentication (AD LDAP Server, CA LDAP Server, AD Global Catalog, RADIUS, or TACACS+).
3. Optional: Set up secondary authentication in case the primary authentication method fails.

   The default is **None**.

   a) Select **Local Database** in the **Secondary Authentication** drop-down list.

      If the primary authentication fails, SANnav uses the local database to try to authenticate the user.

   b) From the **Failover Option** drop-down list, select the condition under which you want to fail over to the local database.
4. Select the authorization preference.
5. Add the list of external servers to use for authentication.

   You must add at least one server and can add a maximum of three servers. Best practice is to add more than one server.

   NOTE

   - If you select AD Global Catalog as the primary authentication, you can add only one server.
   - If you have multiple LDAP servers that resolve to a common DNS name, you can use the DNS name instead of adding multiple server entries.

   If you add more than one server, make sure that the list is in the correct order. The first server in the list is used first. If that server is not reachable, SANnav tries to reach the next server on the list, and then the next, until either a server is reached or the list is exhausted. Click the arrows in the **Order** column to rearrange the order of the servers.
6. Click **Save** to save the configuration and exit the page.

The user names and passwords must be configured on the external servers.

AD LDAP Server, CA LDAP Server, and AD Global Catalog Configuration

If you use an AD LDAP Server or CA LDAP Server or AD Global Catalog (GC) for authentication, when users log in to SANnav, they are authenticated using the user name and password list on the AD LDAP Server or CA LDAP Server or AD GC.

You can use an AD LDAP Server or CA LDAP Server or AD GC for authentication only or for both authentication and authorization.

- If you are using an AD LDAP Server or CA LDAP Server for authentication, the user accounts must be created on the AD LDAP Server or CA LDAP Server.
- If you are using an AD LDAP Server for authentication, use one of the following formats for the SANnav Username field:
  - If the AD LDAP Server is configured to use SSL/TLS, use the LDAP format: `userPrincipalName` . For example, user_logon_name@domainName.
  - If the AD LDAP Server is configured to not use SSL/TLS, use the LDAP format: `samAccountName` . For example, user_logon_name.

Check with your company IT team or the AD Administrator to make sure that you are using the correct user name.

- If you are using an AD GC for authentication, the user accounts must be created on the AD GC. The user name for AD GC must use the format: `username@domainName` for SANnav login.
- If you are using an AD LDAP Server or CA LDAP Server for authentication and Local Database for authorization, you must create a user in SANnav with a user name present in the AD LDAP Server or CA LDAP Server.
- If you are using AD GC for authentication and Local Database for authorization, you must create a user in SANnav using the format: `username@domainName` for SANnav login.
- If you are also using LDAP for authorization, you should use LDAP groups for authorization.

NOTE

- This guide assumes that the AD LDAP Server or CA LDAP Server or AD GC are already configured with the list of user accounts. If you are using LDAP groups for authorization, this guide assumes that the AD LDAP Server or CA LDAP Server or AD GC is already configured with groups and that users are assigned to the groups.
- When an LDAP user belongs to more than one group with different privileges, SANnav uses the group with the highest privileges.

The following tables outline the steps that you must perform on SANnav and on the external AD LDAP Server or CA LDAP Server or AD GC for various scenarios.

Table 3: Tasks Required for Setting Up Authentication and Authorization on an External AD LDAP Server or CA LDAP Server

Scenario	Tasks Performed in SANnav	Tasks Performed on the LDAP Server
Primary authentication = AD LDAP Server or CA LDAP Server Secondary authentication = None Authorization = Local database	1. Configure SANnav to use an external AD LDAP Server or CA LDAP Server. 2. Create user accounts. If you are using an AD LDAP Server for authentication, use one of the following formats for the SANnav Username field: • If the AD LDAP Server is configured to use SSL/ TLS, use the LDAP format: `userPrincipalName` . For example, user_logon_name@domainName. • If the AD LDAP Server is configured to not use SSL/ TLS, use the LDAP format: `samAccountName` . For example, user_logon_name. Check with your company IT team or the AD Administrator to make sure that you are using the correct user name.	User accounts must already be created on the AD LDAP Server or CA LDAP Server. No additional tasks are needed.
Primary authentication = AD LDAP Server Secondary authentication = None Authorization = External server	1. Configure SANnav to use an external AD LDAP Server.	User accounts must already be created on the AD LDAP Server. Create role and AOR custom attributes in the LDAP Active Directory.
Primary authentication = AD LDAP Server or CA LDAP Server Secondary authentication = None Authorization = LDAP groups	1. Configure SANnav to use an external AD LDAP Server or CA LDAP Server. 2. Upload LDAP groups into the local database for authorization. For CA LDAP Server, you must manually create the LDAP group in SANnav.	User accounts and groups must already be created on the AD LDAP Server or CA LDAP Server, and the users must be assigned to groups. No additional tasks are needed.

Scenario	Tasks Performed in SANnav	Tasks Performed on the LDAP Server
Primary authentication = AD LDAP Server or CA LDAP Server Secondary authentication = Local database Authorization = Local database	1. Configure SANnav to use an external AD LDAP Server or CA LDAP Server. 2. Create user accounts. If you are using an AD LDAP Server for authentication, use one of the following formats for the SANnav Username field: • If the AD LDAP Server is configured to use SSL/ TLS, use the LDAP format: `userPrincipalName` . For example, user_logon_name@domainName. • If the AD LDAP Server is configured to not use SSL/ TLS, use the LDAP format: `samAccountName` . For example, user_logon_name. Check with your company IT team or the AD Administrator to make sure that you are using the correct user name.	User accounts must already be created on the AD LDAP Server or CA LDAP Server. No additional tasks are needed.
Primary authentication = AD LDAP Server Secondary authentication = Local database Authorization = External server	1. Configure SANnav to use an external AD LDAP Server. 2. Create user accounts.	User accounts must already be created on the AD LDAP Server.
Primary authentication = AD LDAP Server or CA LDAP Server Secondary authentication = Local database Authorization = LDAP groups	1. Configure SANnav to use an external AD LDAP Server or CA LDAP Server. 2. Create user accounts in case primary authentication fails. 3. Upload LDAP groups into the local database for authorization. For CA LDAP Server, you must manually create the LDAP group in SANnav.	User accounts and groups must already be created on the AD LDAP Server or CA LDAP Server, and the users must be assigned to groups. No additional tasks are needed.

Table 4: Tasks Required for Setting Up Authentication and Authorization on an External AD GC

Scenario	Tasks Performed in SANnav	Tasks Performed on the LDAP GC
Primary authentication = AD Global Catalog Secondary authentication = None Authorization = Local database	1. Configure SANnav to use an external AD GC. You must use port 3269 for AD GC. 2. Create user accounts. You must create a user account using the format username@domainName for SANnav login.	User accounts must already be created on the AD GC. The “rootdomainnamingcontext” attribute must already be created on the AD GC for validation. No additional tasks are needed.
Primary authentication = AD Global Catalog Secondary authentication = None Authorization = LDAP groups	1. Configure SANnav to use an external AD GC. You must use port 3269 for AD GC. 2. Upload LDAP groups into the local database for authorization.	User accounts and groups must already be created on the AD GC, and the users must be assigned to groups. Note that SANnav supports universal groups only. The “rootdomainnamingcontext” attribute must already be created on the AD GC for validation. No additional tasks are needed.
Primary authentication = AD Global Catalog Secondary authentication = Local database Authorization = Local database	1. Configure SANnav to use an external AD GC. You must use port 3269 for AD GC. 2. Create user accounts. You must create a user account using the format username@domainName for SANnav login.	User accounts must already be created on the AD GC. The “rootdomainnamingcontext” attribute must already be created on the AD GC for validation. No additional tasks are needed.
Primary authentication = AD Global Catalog Secondary authentication = Local database Authorization = LDAP groups	1. Configure SANnav to use an external AD GC. You must use port 3269 for AD GC. 2. Create user accounts in case primary authentication fails. You must create a user account using the format username@domainName for SANnav login. 3. Upload LDAP groups into the local database for authorization.	User accounts and groups must already be created on the AD GC, and the users must be assigned to groups. Note that SANnav supports universal groups only. The “rootdomainnamingcontext” attribute must already be created on the AD GC for validation. No additional tasks are needed.

Creating Role and AOR Custom Attributes in the LDAP Active Directory

If you use the LDAP server for authorization without groups, you must update the Microsoft Active Directory (AD) to add the custom attributes NmRoles and NmAors for roles and AORs.

This procedure assumes that you are familiar with Microsoft Management Console (MMC) and Microsoft Active Directory (AD).

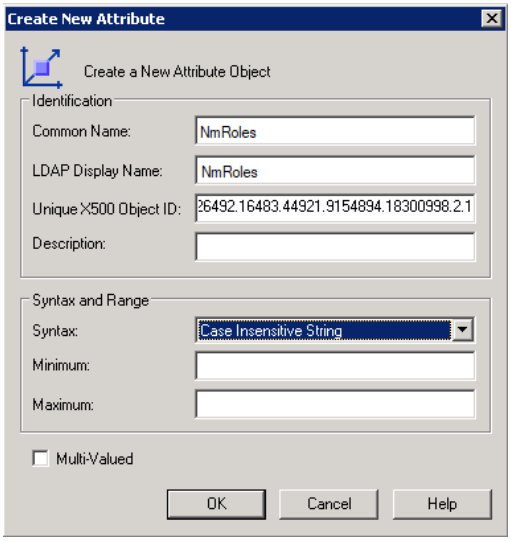
Before performing this task, you must obtain two unique object identifiers: one for the roles attribute and another one for the AOR attribute.

NOTE
If you have more than just a few users, it is recommended that you perform authorization using LDAP groups. If you use groups, you do not need to perform this task, but you do need to have the groups created on the LDAP server. On SANnav, you must upload the groups and assign roles and AORs to the groups.

Perform the following steps on the LDAP server to add two new custom attributes to the AD: NmRoles and NmAors. Note that this procedure is an example only.

NOTE
Depending on your Windows environment, the actual steps and windows might be different.

1. On the LDAP server, install the Active Directory Schema.
   a) Select **Start** > **Run**.
   b) Type **regsvr schmmgmt.dll** and press **Enter**.
2. Open the MMC, and add the Active Directory Schema into the MMC console.
3. Expand the Active Directory Schema tree in the MMC console, right-click the **Attributes** folder, and select **Create Attribute**.
4. Enter values for the NmRoles attribute in the **Create New Attribute** dialog, and click **OK**.
   - **Common Name** = NmRoles
   - **LDAP Display Name** = NmRoles
   - **Unique X500 Object ID** = The unique OID you obtained previously
   - **Syntax** = Case Insensitive String



5. Repeat Step 4 to add the NmAors attribute.
   - **Common Name** = NmAors
   - **LDAP Display Name** = NmAors
   - **Unique X500 Object ID** = The unique OID you obtained previously
   - **Syntax** = Case Insensitive String

6. Add the new attributes to the user class.
   a) Expand the **Classes** folder, right-click **user**, and select **Properties**.
   b) Click the **Attributes** tab, and then click **Add**.
   c) Select the **NmRoles** attribute, and click **OK**.
   d) Click **Add** again, select the **NmAors** attribute, and click **OK**.
   e) Click **OK** to close the dialog.
7. Close the MMC, and restart the Active Directory service.

Adding an AD LDAP Server, CA LDAP Server, or AD Global Catalog to the Docker Container

NOTE
Use this procedure only when no LDAP server DNS is present in the environment and name resolution fails.

1. Obtain the Docker container ID for the authentication service.

```
$ docker ps | grep authentication
Output: de4103a2454e     localhost:5000/mw-authentication-rbac:latest     "/bin/sh /dcm1.0.0/w…"     2
 days ago     Up 23 hours     0.0.0.0:7089->7089/tcp, 0.0.0.0:18095->18095/tcp, 0.0.0.0:28095->28095/tcp
```

   The Docker container ID is shown in bold text.

2. Use the Docker container ID to open a bash shell session in the container.

```
$ docker exec -it container_id bash
```

   For example:

```
$ docker exec -it de4103a2454e bash
```

3. Add the AD LDAP Server, CA LDAP Server, or AD Global Catalog, using the format *IP_address hostname,* to the `/etc/hosts` file.

   For example: `10.122.15.11 WIN-REYU4.devldap.com`

Uploading AD LDAP Groups to SANnav

If you are using LDAP for authentication, the recommended method is to use LDAP groups. You must upload these groups to SANnav Global View. Unlike in SANnav Management Portal, in SANnav Global View you do not assign roles and areas of responsibility (AORs) to the groups. All groups are automatically assigned the SAN Administrator role. SANnav Global View does not use AORs.

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Import the groups from the LDAP server.
   a) Click **Groups**.
   b) Click the **+** button, and select **Fetch**.
   c) Enter the LDAP server information in the **Fetch Groups** dialog, and click **OK**.

      For SSL ports, SANnav supports channel binding for a simple bind on AD LDAP servers. To use an SSL port, you must enable channel binding on the AD LDAP server (see Enabling Channel Binding for AD LDAP Servers).

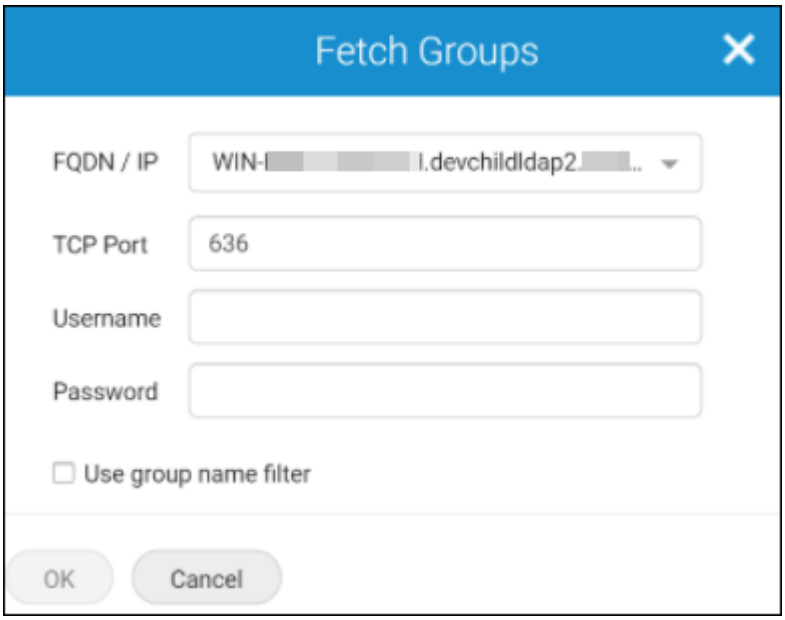
      Non-SSL ports use MD5 encryption for authentication. For non-SSL ports, you must disable channel binding on the LDAP server (see Disabling Channel Binding for AD LDAP Servers).

      If you are using an AD LDAP Server for authentication, use one of the following formats for the SANnav Username field:

- If the AD LDAP Server is configured to use SSL/TLS, use the LDAP format: `userPrincipalName` . For example, user_logon_name@domainName.
- If the AD LDAP Server is configured to not use SSL/TLS, use the LDAP format: `samAccountName` . For example, user_logon_name.

Check with your company IT team or the AD Administrator to make sure that you are using the correct user name.

If you select the **Use group name filter** checkbox and enter a text string, you are presented with a filtered list of groups; otherwise, you are presented with all groups in the LDAP server. The user name for AD GC must use the format username@domainName for the SANnav login.



d) Select the groups that you want to upload, and click **OK**.

NOTE
This process might take several minutes, depending on the number of groups present in the LDAP server.

Enabling Channel Binding for AD LDAP Servers

To enable but not enforce channel binding for AD LDAP servers, complete the following steps:

1. Configure the `LdapEnforceChannelBinding` setting to enforce channel binding.

```
Reg Add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v
 "LdapEnforceChannelBinding" /t REG_DWORD /d 1
```

2. Configure the `ldapserverintegrity` setting to enforce the use of signing by the client.

```
Reg Add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v "ldapserverintegrity" /t
 REG_DWORD /d 1
```

Disabling Channel Binding for AD LDAP Servers

To disable channel binding for AD LDAP servers, complete the following steps:

1. Configure the `LdapEnforceChannelBinding` setting to not enforce channel binding.

```
Reg Add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v
 "LdapEnforceChannelBinding" /t REG_DWORD /d 0
```

2. Configure the `ldapserverintegrity` setting to not enforce the use of signing by the client.

```
Reg Add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v "ldapserverintegrity" /t
REG_DWORD /d 0
```

Creating a CA LDAP Group

Perform the following steps to create a CA LDAP group:

1. Click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.
2. Click **Groups**.
3. Click the **+** button, and select **Create New**.
4. Enter a name for the group.

   CA LDAP group names are case insensitive.
5. Optionally add a description to help you identify the group, and add one or more tags to help you find the group in a search.
6. Click **Save**.

RADIUS Server Configuration

If you use a RADIUS server for authentication, when users log in to SANnav, they are authenticated using the user name and password list on the RADIUS server.

If you select **RADIUS Server** as your primary authentication method, it is assumed that the user names and passwords are already configured on the RADIUS server. You must now configure the following on the RADIUS server:

- Configure SANnav credentials, including the default authentication type.

Depending on whether secondary authentication is enabled, you must also configure user names and passwords on the local database (the SANnav server). The following table outlines the steps you must perform on SANnav and on the external RADIUS servers for various scenarios.

Table 5: Tasks Required for Setting Up Authentication and Authorization on an External RADIUS Server

Scenario	Tasks Performed in SANnav	Tasks Performed on the RADIUS Servers
Primary authentication = RADIUS server Secondary authentication = None Authorization = Local database	1. Configure SANnav to use an external RADIUS server. 2. Create user accounts.	User accounts must already be created on the RADIUS servers. You must perform the following additional task: 1. Configure SANnav credentials.
Primary authentication = RADIUS server Secondary authentication = None Authorization = External server	1. Configure SANnav to use an external RADIUS server.	User accounts must already be created on the RADIUS servers. You must perform the following additional tasks: 1. Configure SANnav credentials. 2. Assign roles and AORs to users. 3. Configure a dictionary file to include the role and AOR attributes.
Primary authentication = RADIUS server Secondary authentication = Local database Authorization = Local database	1. Configure SANnav to use an external RADIUS server. 2. Create user accounts.	User accounts must already be created on the RADIUS servers. You must perform the following additional task: 1. Configure SANnav credentials.
Primary authentication = RADIUS server Secondary authentication = Local database Authorization = External server	1. Configure SANnav to use an external RADIUS server. 2. Create user accounts.	User accounts must already be created on the RADIUS servers. You must perform the following additional tasks: 1. Configure SANnav credentials. 2. Assign roles and AORs to users. 3. Configure a dictionary file to include the role and AOR attributes.

Configuring SANnav Credentials on the RADIUS Server

Perform this task if you are using a RADIUS server for authentication. You must provide the server with the SANnav configuration information so that the RADIUS server can communicate with the SANnav server.

For this task, you update two files on the RADIUS server:

- Update the `clients.conf` file with the SANnav information.
- Update the `users.conf` file to specify the default authentication type.

Depending on the RADIUS server that you install, the configuration files may have different names.

1. On the RADIUS server, open the client configuration file (`clients.conf`) in a text editor (such as Notepad).
   The client configuration file contains definitions of the RADIUS clients.
2. Enter the SANnav data.

```
client ip_address
{
secret     = user_defined_secret
shortname  = localhost_name
}
```

   Where *`ip_address`* is the address of the SANnav server, *`user-defined-secret`* is the shared secret that you configured on the SANnav server when you added the RADIUS server for authentication, and *`localhost_name`* is the host name of the SANnav server.

   For example:

```
client 192.0.2.0 {
```

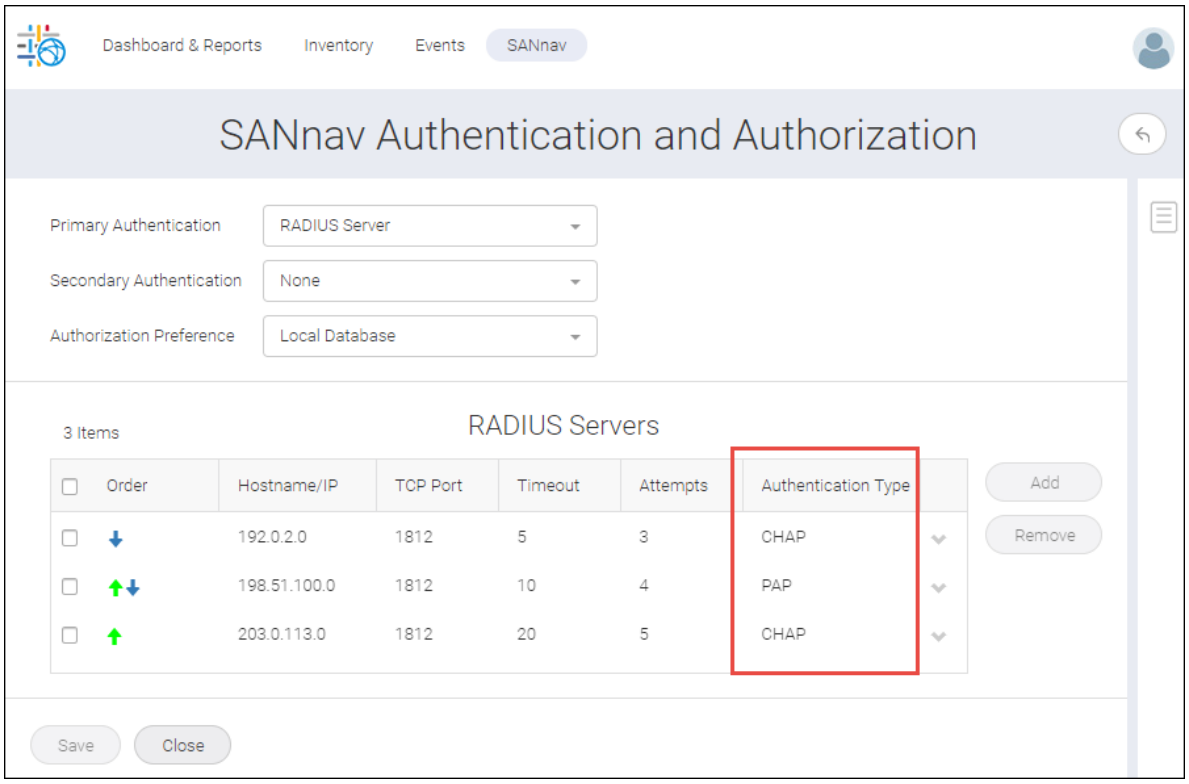
```
        secret      = password
        shortname   = GVM1server
}
```

3. Save and close the `clients.conf` file.
4. Open the user configuration file (`users.conf`) in a text editor (such as Notepad).
5. Enter the following line to set the default authentication type.

```
DEFAULT          Auth-Type = authtype
```

   Where *`authtype`* is CHAP or PAP. The default authentication type should match what you configured in SANnav when you added the RADIUS server for authentication.

   If you are not sure of the authentication type, in SANnav, click **SANnav** in the navigation bar, and then click **Security** > **SANnav Authentication and Authorization**.



6. Save and close the `users.conf` file.

TACACS+ Server Configuration

If you use a TACACS+ server for authentication, when users log in to SANnav, they are authenticated using the user name and password list on the TACACS+ server.

> **NOTE**
> If your TACACS+ server is configured as a RADIUS server, follow the instructions for RADIUS server configuration.

If TACACS+ is your primary authentication method, it is assumed that the user accounts are already configured on the TACACS+ server.

Depending on whether secondary authentication is enabled, you must also configure user names and passwords on the local database (the SANnav server). The following table outlines the steps that you must perform on SANnav and on the external TACACS+ server for various scenarios.

Table 6: Tasks Required for Setting Up Authentication and Authorization on an External TACACS+ Server

Scenario	Tasks Performed in SANnav	Tasks Performed on the TACACS+ Servers
Primary authentication = TACACS+ Server Secondary authentication = None Authorization = Local database	1. Configure SANnav to use an external TACACS+ server. 2. Create user accounts.	User accounts must already be created on the TACACS+ server. No additional tasks are needed.
Primary authentication = TACACS+ Server Secondary authentication = None Authorization = External server	1. Configure SANnav to use an external TACACS+ server.	User accounts must already be created on the TACACS+ server. You must perform the following additional tasks: 1. Configure SANnav credentials.
Primary authentication = TACACS+ Server Secondary authentication = Local database Authorization = Local database	1. Configure SANnav to use an external TACACS+ server. 2. Create user accounts.	User accounts must already be created on the TACACS+ server. No additional tasks are needed.
Primary authentication = TACACS+ Server Secondary authentication = Local database Authorization = External server	1. Configure SANnav to use an external TACACS+ server. 2. Create user accounts.	User accounts must already be created on the TACACS+ servers. You must perform the following additional tasks: 1. Configure SANnav credentials.

Transport Layer Security Protocol Version

SANnav enables you to quickly view the Transport Layer Security (TLS) protocol version for the SANnav server and client.

NOTE
SANnav 2.2.x supports TLS 1.3 and TLS 1.2. If TLS 1.3 is not available, then TLS 1.2 is used.

Viewing the TLS Protocol Version for SANnav

You can view the TLS protocol versions supported on the SANnav server and the TLS version used in the client connection.

1. Click the user icon in the top-right corner of the window, and then click **System Properties**.
   The **System Properties** dialog displays with the following details:
   - SANnav server (v2.2.1) supported TLS versions 1.2, 1.3
   - SANnav client connected TLS version 1.3
2. Click **Close** to close the **System Properties** dialog.

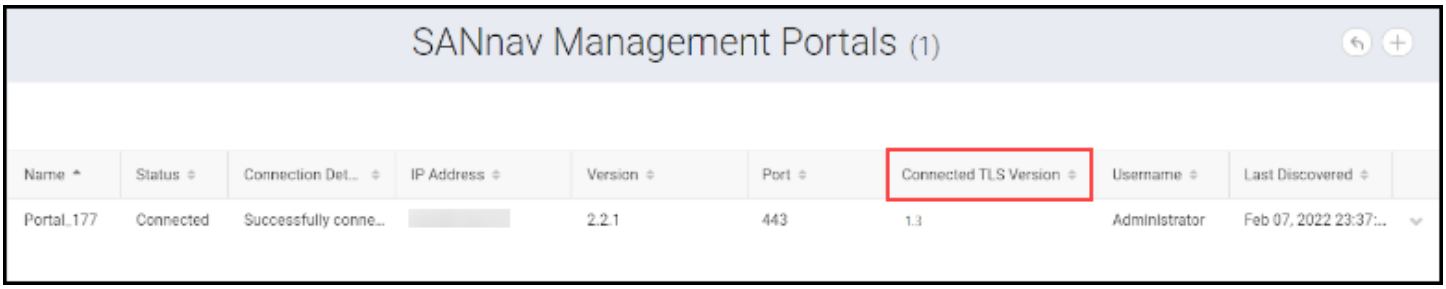
Viewing the TLS Version for a SANnav Management Portal Instance

You can view the negotiated TLS version between SANnav Global View and SANnav Management Portal on the **SANnav Management Portals** page.

Click **SANnav** in the navigation bar, and then select **SAN Monitoring** > **Portals**.

The **SANnav Management Portals** page displays.

The negotiated TLS version displays in the **SANnav Management Portals** list. A dash (-) in the **Connected TLS Version** column indicates that the SANnav instance is disconnected.



Managing Signed Certificates

It is recommended that you use a trusted certificate authority (CA) signed certificate once the SANnav application is up and running. Using a trusted CA signed certificate assures client users that the server is the correct, approved server.

By default, SANnav uses a self-signed certificate that is created with a unique key at installation time. This self-signed certificate is valid for 13 months.

NOTE
Starting in SANnav 2.2.0, certificates are valid for 13 months. In SANnav 2.1.1, certificates were valid for 27 months and in earlier versions of SANnav, certificates were valid for 5 years. If you migrate to SANnav 2.2.1 from an earlier version, the following behavior applies:

- If you replaced the self-signed certificate with a third-party signed certificate, the third-party certificate is migrated and is valid for the remainder of its original duration.
- If you were running SANnav with a self-signed certificate, the certificate is not migrated. Instead, a new self-signed certificate is generated with a 13-month validity.

After the application is installed and running, it is recommended that you replace the self-signed certificate with a trusted CA signed certificate.

NOTE
SANnav 2.2.x supports TLS 1.3 and TLS 1.2. If TLS 1.3 is not available, then TLS 1.2 is used.

Perform the following steps to replace the SSL certificates in SANnav for client-server communication. OpenSSL is used in this example.

1. Generate a private key and certificate signing request (CSR) using the following command.
   ```
   openssl req -newkey rsa:2048 -nodes -keyout sannav.key -out sannav.csr
   ```
   Where *sannav.key* is the file where the private key is saved, and *sannav.csr* is the file where the CSR is saved.
   Provide all input for the certificate. Ensure that the common name matches the host name of the SANnav server.
2. If you are replacing the certificate with a signed certificate, submit the CSR to your CA with proper credentials to identify you as authorized to create certificates and receive the signed certificate from the CA.
   Now you have both the key and the signed certificate.
3. If you are replacing the certificate with a self-signed certificate, generate the self-signed certificate using the key and the following command.
   ```
   openssl req -key sannav.key -new -x509 -days 365 -out sannav.crt
   ```
   Where *sannav.key* is the existing key file, and *sannav.crt* is the file where the certificate is stored.
   Provide all required input for the certificate.
   Now you have both the key and the self-signed certificate.

4. Copy both the key and the certificate to a location on the SANnav server, for example, `/root/certificates`.
5. If you have CA root and intermediate CA certificates, chain them into one before replacing the certificates.

   Use the following command:

   ```
   cat my_intermediate.crt [intermediate2.crt] ... my_root.crt > ca-cert-chain.pem
   ```

6. Run the following script to replace the public certificate and private key and restart the services.

   ```
   /<install_home>/bin/replace-sannav-certificates.sh
   ```

   Provide the full paths for both the key and the certificate.

   After the script starts the services, wait a few more minutes.
7. Launch the SANnav client in a browser window, and check if the new certificate information is shown.

Creating a List of Allowed Browsers to Access SANnav

By default, all IP addresses can access SANnav. However, you can limit SANnav access to specific client IP addresses by creating a list of allowed IP addresses.

Before you start, make sure that you have a list of the IPv4 addresses that you want to allow.

> **NOTE**
> For dual NIC machines with two IP addresses, both IP addresses must be added to the allowed list.

You can use only IPv4 addresses. You cannot use IPv6 addresses, host names, loopback addresses, or localhost IP addresses.

Note the following considerations if you are using both SANnav Management Portal and SANnav Global View:

- If you create an allowed list for a SANnav Management Portal instance, be sure to add the IP address of SANnav Global View to the allowed list to allow Global View to discover the Management Portal instance.
- If you add an IP address to the SANnav Global View allowed list, you should add the same IP address to the SANnav Management Portal allowed list. Otherwise, the "Show in Portal" feature of SANnav Global View will not work.

To create and manage an allowed list, use the script that is provided during SANnav installation. Use the script only after SANnav installation completes successfully.

1. Go to the `<install_home>/bin` folder, and run the following script:

   ```
   ./manage-sannav-whitelisting.sh
   ```

2. At the prompt, enter one of the following options:
   - 1: Display the current allowed list.
   - 2: Provide a comma-separated list of IP addresses to be added to the allowed list.
   - 3: Provide a comma-separated list of IP addresses to be removed from the allowed list.
   - 4: Remove all IP addresses from the allowed list and allow access to all.

   If you modified the allowed list (options 2, 3, or 4), the proxy service is restarted and then the updated allowed list is in effect.

To run another option, for example if you want to add some IP addresses and then remove some, you must run the script again. You can select only one option with each iteration of the script.

Monitoring

SANnav Global View provides several features for monitoring and troubleshooting your storage area networks.

After you add SANnav Management Portal instances, the following features are available:

- The SANnav Global View **Summary** dashboard provides comprehensive "global" visibility across multiple SANnav Management Portal instances.
- The **Reports** page contains summary data that is gathered from all SANnav Management Portal instances.
- The **Inventory** page is a central location where you can view the inventory of all discovered fabrics, switches, switch ports, hosts, host ports, storage, storage ports, and physical chassis across all SANnav Management Portal instances.
- SANnav Global View Investigation mode displays graphs of historic performance metrics for one or more switch ports.

Adding a SANnav Management Portal Instance

After you add SANnav Management Portal instances to SANnav Global View, you can monitor them.

When adding the SANnav Management Portal instance to SANnav Global View, you must provide the Management Portal IP address/host name, port number, user name, and password. The login credentials are used for authentication of SANnav Global View when communicating with the SANnav Management Portal instance for retrieving data.

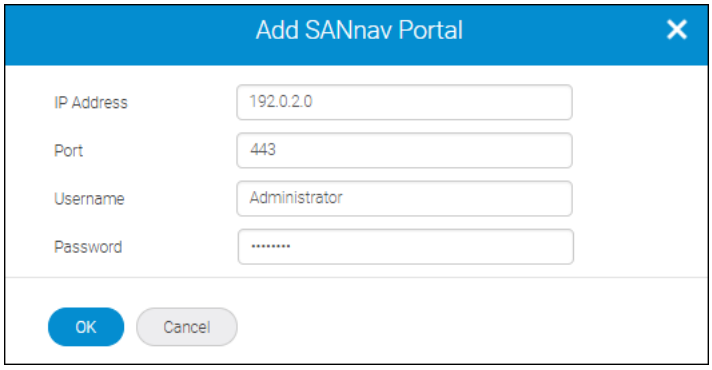
When you add portal instances to SANnav Global View, the portal credentials must have SAN System Administrator or equivalent privilege and full areas of responsibility (AORs) to all fabrics in that portal instance. If not, the addition and discovery of that portal instance fails.

A maximum of 20 SANnav Management Portal instances can be connected to one SANnav Global View. The total port count must not exceed 120,000 ports. The total port count is the sum of ports that are managed by all Management Portal instances.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** > **Portals**.

   The **SANnav Management Portals** list displays.

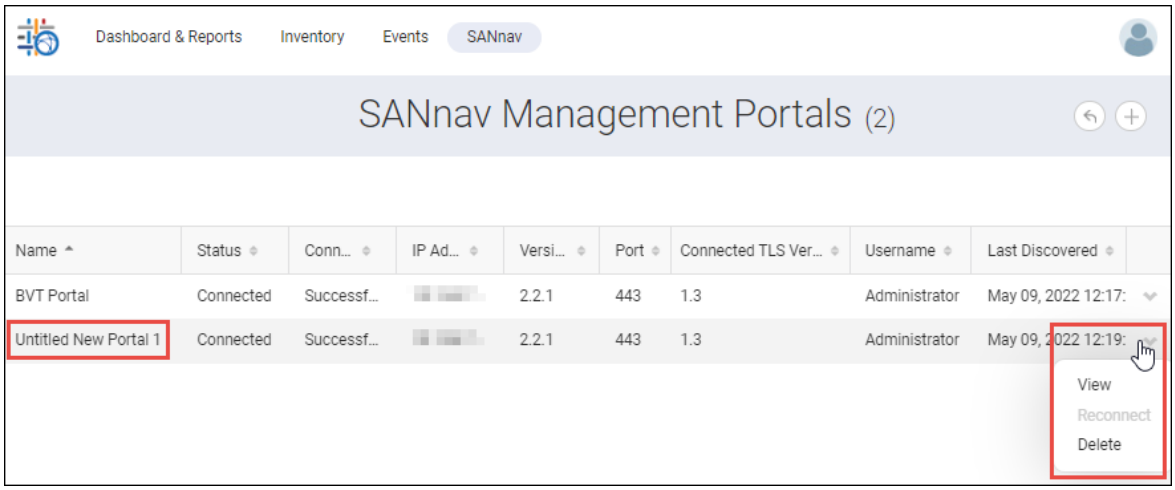
2. Click the **+** icon in the upper-right corner, and specify the IP address and login credentials of the SANnav Management Portal server.



3. Click **OK**.

   The new portal appears in the list. The default name of the portal is "Untitled New Portal #".

4. If you want to change the name of the portal, either click the name or select **View** from its action menu.



Notice that the action menu also has options to reconnect a disconnected portal and to delete a portal.

5. Edit the name field, and then click **Save**.

The new name appears on the portals list.

SANnav Global View automatically pings the SANnav Management Portal instances every 5 minutes. If a portal does not respond, its status changes to "Disconnected". The actions that happen next depend on the reason for the disconnect, which is described in the **Connection Details** column:

- **Portal is not reachable**: The portal is not reachable because of network issues. SANnav Global View keeps pinging the portal. When the portal comes up, it is automatically reconnected. If SANnav Management Portal is configured with Disaster Recovery and the primary node fails, you must remove the primary node from SANnav Global View and add the backup node.
- **Portal login failed due to invalid credentials**: The portal is not reachable because of a password change. SANnav Global View does not keep pinging the portal. If the portal password is restored to the previous password, you must select **Reconnect** from the action menu to reconnect to the portal. Reconnection does not happen automatically.

Global Dashboard Overview

The SANnav Global View **Summary** dashboard provides comprehensive "global" visibility across multiple SANnav Management Portal instances.

The **Summary** dashboard is automatically refreshed every 15 minutes.

The **Summary** dashboard provides the following widgets: health summary, **Switch Health**, **Port Usage Summary**, and **Alerts**. These widgets indicate the status of the fabric, switch, host, and storage entities that are managed by the portal instances that are currently added in SANnav Global View.

The health summary widgets are categorized by health state: **Healthy**, **Degraded**, or **Poor**. Listed below each widget are the exact number of entities in each health state.

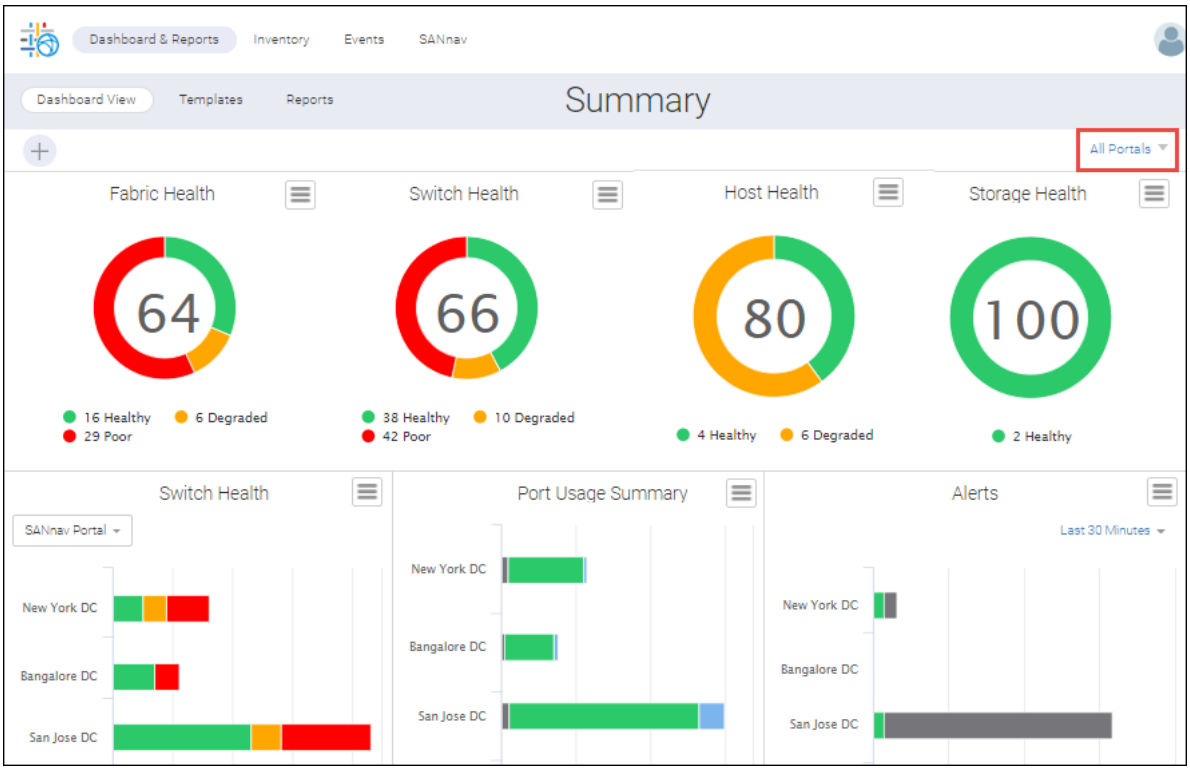
The health state for each type of object is determined by its health score, which is determined by a set of predefined factors. For example, a health score for fabrics is influenced by whether a link is down or redundant paths are missing. For more details on how the health score is computed, see Factors Contributing to the Overall Health Score.

Health State	Health Score
Healthy	Greater than 90
Degraded	Between 71 and 90
Poor	70 or less

The health information is retrieved from each of the SANnav Management Portal instances, and an aggregate global view is presented. Health calculations for various entities are done at the SANnav Management Portal level.

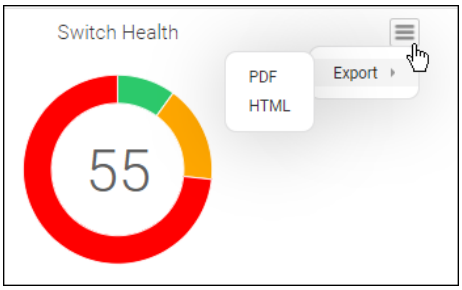
The **Summary** dashboard allows you to gather additional information from the dashboard widgets.

By default, the scope of the dashboard is set to **All Portals** (that is, all SANnav Management Portal instances). You can choose one or more SANnav Management Portal instances to change the scope.



Clicking the **+** icon on the left side of the filter bar allows you to create dashboard filters based on fabric, switch, switch port, host, and storage properties. Setting a filter impacts what is displayed in the dashboard widgets. Note that the **Alerts** widget is not affected by filters.

You can export the individual widgets in the dashboard by clicking the hamburger icon next to the widget and selecting **Export**. Export options are PDF and HTML.



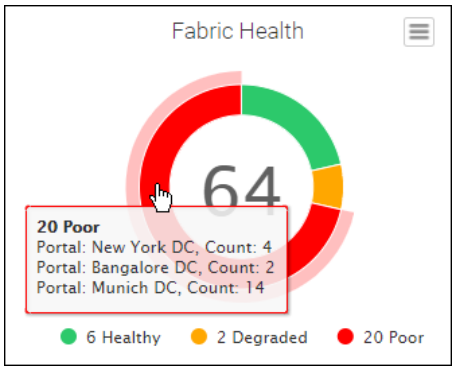
Monitoring Fabric Health

The **Fabric Health** widget of SANnav Global View shows the number of fabrics in Healthy, Degraded, and Poor state. The least overall score across all objects in this group of fabrics is shown in the center of the circular widget.

The following procedure shows how to use the Global View dashboard to investigate the health state of fabrics across all SANnav Management Portal instances. You can similarly investigate the health state of switches, hosts, and storage using the respective circular widgets.

1. Click **Dashboard & Reports** in the navigation bar.
2. Hover over a colored portion of the **Fabric Health** widget to display details of the fabrics with that state.

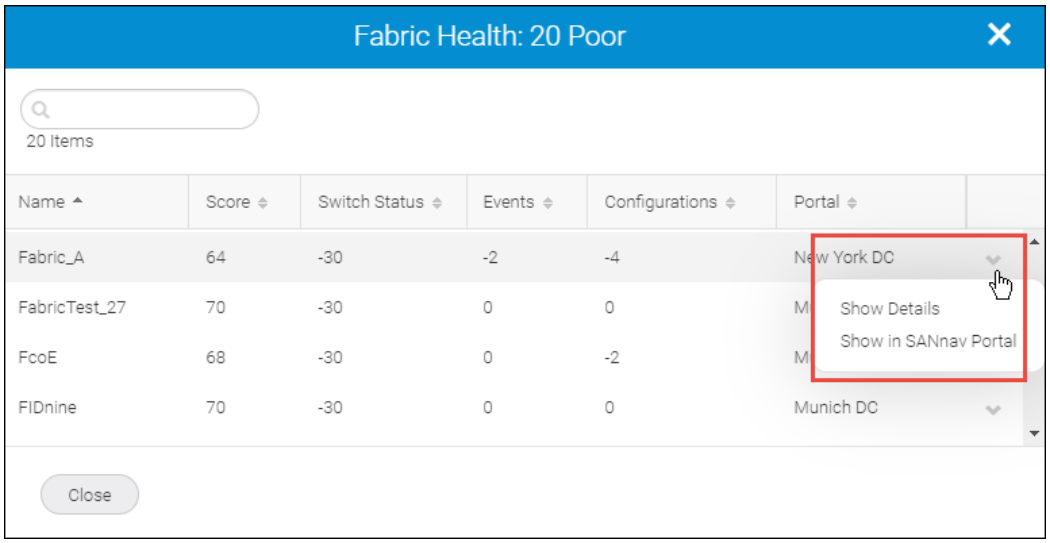
   For example, hover over the red portion to display a list of SANnav Management Portal instances and the number of fabrics in each portal having a poor state.



3. To view further details on the fabrics, click the colored segment of the widget.

   For example, clicking the red segment displays a table showing the health scores for the fabrics in poor health.
4. Click **Show Details** on the action menu of the fabric list to see details associated with that health score.

   The **Show Details** option is available only if the score is less than 100.



A pop-up window displays the factors that cause deductions in the health score for this fabric.

5. Click **Back** to return to the list of portal instances.
6. Select **Show in SANnav Portal** from the action menu to launch the SANnav Management Portal instance responsible for the data that you are viewing.

   You might need to make sure that pop-ups are not blocked in your browser.

   If you are not logged in to this portal, credentials (for this portal) are required.

Monitoring Switch Health across Management Portal Instances

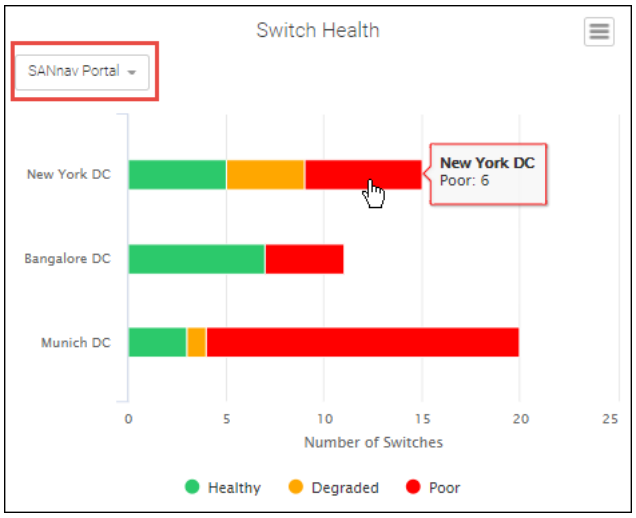
The Switch Health widget displays details of switch health across Management Portal instances. You can get a summarized view as well as details of switches based on firmware version, Management Portal instance, switch model, and product category.

The following procedure shows how to use the Global View dashboard to display switch health across multiple Management Portal instances.

1. Click **Dashboard & Reports** in the navigation bar.

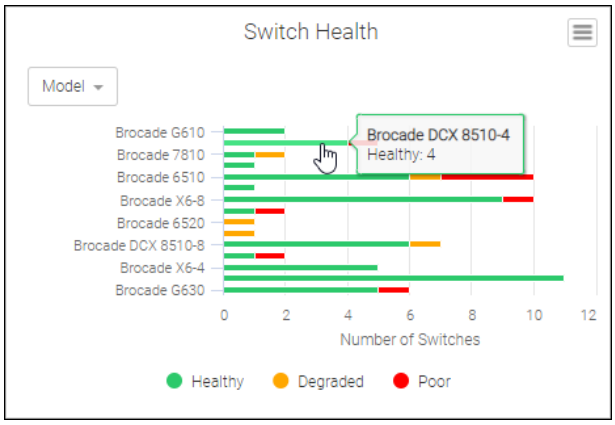
   On the bottom row of the dashboard, the **Switch Health** widget displays.

   In this screen you see switches grouped by **SANnav Portal** instances. You can select a different grouping from the drop-down list.



2. Hover over the graph to display details.

   Note that for the **Firmware Version** and **Model** categories, more bars may be displayed in the graph than are listed in the row names on the left. In this case, hover over an intermediate bar in the graph to display the details.



3. To see the details on all switches in a particular category, click the bar chart of the widget, and then select **Show Details**.

4. Click **Close** to return to the dashboard.
5. Select **SANnav Portal** from the drop-down list in the widget, click the bar graph, and select **Show in Portal** to display the switch inventory in the selected SANnav Management Portal instance.

   If you are not logged in to this portal, credentials (for this portal) are required.

   A separate window opens for the Management Portal instance.

Factors Contributing to the Overall Health Score

For the **Health Summary** dashboard in SANnav, various factors are considered when determining the overall health score for fabrics, switches, hosts, and storage.

Health scores start at 100, and points are deducted for various predefined factors.

The following tables list the factors for computing the health score for fabrics, switches, hosts, and storage, and the default number of points deducted from the score.

In SANnav Management Portal, you can customize which factors are considered and the number of points that are deducted for each violation.

Table 7: Fabric Health Score Factors and Default Points Deducted

General Category	Factor	Default Points Deducted
Member Switch Health (Maximum 30 points deducted)	Any switch in the fabric having a status of Degraded.	10
	Any switch in the fabric having a status of Poor.	30
Important Incidents (Maximum 50 points deducted)	A link went down without coming back up. You can define how many links should be down before points are deducted.	2 per link
	Fabric Performance Impact (FPI) violations.	2 per violation
SAN Best Practices (Maximum 20 points deducted)	Missing redundant ISLs or ICLs between switches.	2 per ISL
	For FCR backbone fabrics, no redundant IFL connections from each backbone switch to the edge fabrics.	2 per IFL
	Edge Hold Time (EHT) > 220 ms for an edge switch and > 500 ms for core switches. This check is performed only for switches running Fabric OS 8.2.1 and higher.	2
	Default zoning set to All Access.	2
	Zoning database size > 90% of the maximum allowed size. You can change the percentage.	2

Table 8: Switch Health Score Factors and Default Points Deducted

General Category	Factor	Default Points Deducted
Switch Status (Maximum 30 points deducted)	Switch status Marginal.	10
	Switch status Down.	30

General Category	Factor	Default Points Deducted
	Switch status unknown.	10
Important Incidents (Maximum 60 points deducted)	Call Home events originated from the switch.	5
	MAPS violations: • Port health • Fabric state change • FRU health • Security health • Switch resource monitoring measures • FCIP Extension tunnel measures • Traffic measures • Backend port measures	2 for each category. The score is reduced one time per category, even if multiple violations for that category occur.
	Events, traps, or syslogs that have been marked as a **SANnav Tagged Event** in the event policy and have not been acknowledged.	2 per event/trap
	Port data collection failure, which may be caused by SNMP connection failures.	5, if SNMP connection failures have occurred in the last 15 minutes.
Configuration (Maximum 10 points deducted)	Configuration policy drifts.	5
	HTTPS is not enabled.	2
	The default MAPS base policy is the active policy on the switch. This policy provides limited monitoring support.	10

Table 9: Host and Storage Health Score Factors and Default Points Deducted

General Category	Factor	Default Points Deducted
Device Status (Maximum 30 points deducted)	One or more device ports are offline.	30
Threshold Events (Maximum 60 points deducted)	MAPS violations on F_Ports.	5 per violation
	FPI violations or error events on connected F_Ports.	10 per violation
	Congestion state of Medium for F_Ports.	2 per port
	Virtual machine (VM) alarms for servers (when vCenter integration is available).	2 per VM
Best Practices (Maximum 10 points deducted)	Missing redundant paths between host and zoned storage.	10 per host
	Host not zoned following best practices: • A zone should have at most one host. • A peer zone should have the single host as a principle member.	1 per host
	Fan-in ratio to storage exceeds 10:1. You can change the ratio.	2 per host

Displaying Port Usage Details

The Port Usage Summary widget displays data for each SANnav Management Portal instance categorized by the number of device ports, unused ports, and ISL/IFL ports.

Note the following:

- Device ports include F_Ports, L_Ports, and N_Ports.
- Unused ports include G_Ports and U_Ports.
- ISL/IFL ports include E_Ports and EX_Ports.

This widget covers only the FC ports. FCIP and ETH ports are not covered as part of the widget.

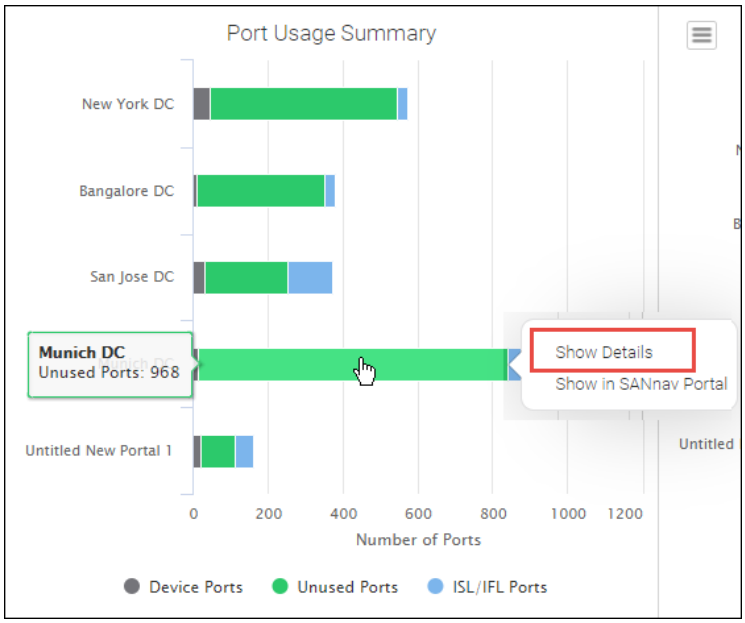
Tooltips provide the count and Management Portal name. You can see port details that are related to a particular section of the bar chart, and you can navigate to a web page in SANnav Management Portal for ports that are related to that section.

The following procedure shows how to use the Global View dashboard to display details on port usage across Management Portal instances:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Dashboard View** in the subnavigation bar.

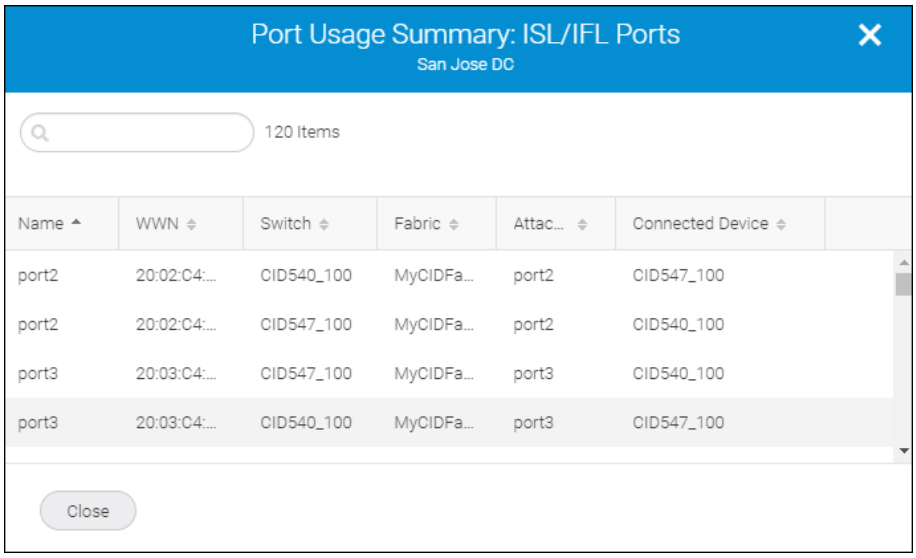
   On the bottom row of the dashboard, the **Port Usage Summary** widget displays.

2. Hover over a segment of the **Port Usage Summary** widget to see details on that segment of the bar graph.



3. To view more details on the ports, click the port usage summary bar graph, and then select **Show Details**.

   You see a table that details the ports for that segment of the fabric.



4. Click **Close** to return to the dashboard.
5. To see the Management Portal instance responsible for the data that you are viewing, click the port usage summary bar graph, and then select **Show in SANnav Portal**.

   If you are not logged in to this portal, credentials (for this portal) are required.

Viewing Alerts

For each SANnav Management Portal instance, the **Alerts** widget displays the count of alerts, including alerts generated by configuration drifts.

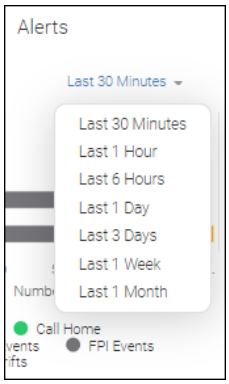
The alerts shown are based on the chosen date range.

The following procedure shows how to use the Global View **Summary** dashboard to investigate details behind Global View alerts:

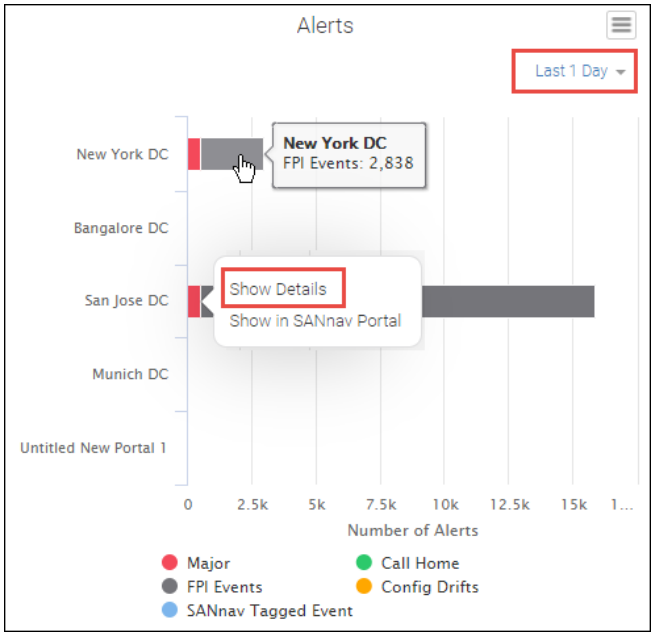
1. Click **Dashboard & Reports** in the navigation bar, and then click **Dashboard View** in the subnavigation bar.

   On the bottom row of the dashboard, the **Alerts** widget displays.

   The Alerts widget contains a date range, which is set to **Last 30 Minutes** by default. You can select a different date range, up to 1 month.

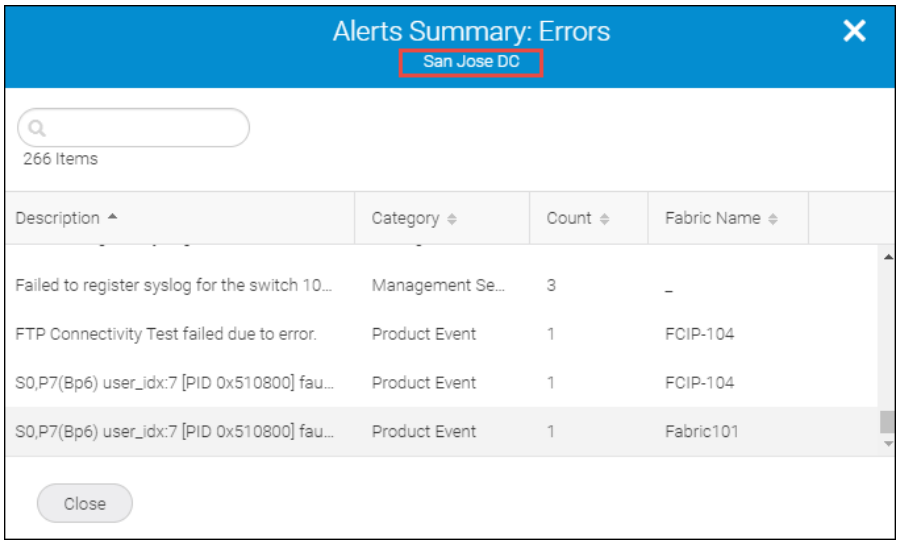


2. Hover over a segment of a bar to see the number of alerts (associated with a particular alert category) that have been received for that Management Portal instance.



3. To see more details, click the alerts bar graph, and then select **Show Details**.

   The alerts are listed in a table along with their category, occurrence count, and fabric. The heading indicates the particular SANnav Management Portal instance involved. A maximum of 5000 alerts are displayed.



   Click **Close** to return to the Global View **Summary** dashboard.

4. Click the alerts bar graph in the dashboard and then select **Show in SANnav Portal** to see the actual events on the Management Portal responsible for the data that you are viewing.

   If you are not logged in to this portal, credentials (for this portal) are required.

Creating a Global Report Template

You can create summary reports from data gathered from all SANnav Management Portal instances.

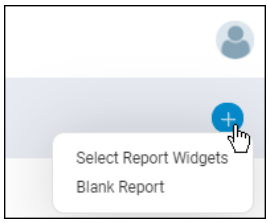
To generate reports, first you create report templates, which define the widgets that comprise the report as well as the Management Portal scope and other filters.

You can create several types of report templates, such as one template for daily reports and another one for weekly reports. Or, you can create separate templates for individual data centers and one template for all the data centers together.

The process for creating report templates is similar to the process for SANnav Management Portal, except that with SANnav Global View, the scope of the reports is based on Management Portal instances. Report scheduling, generation, and exporting are the same as in SANnav Management Portal.

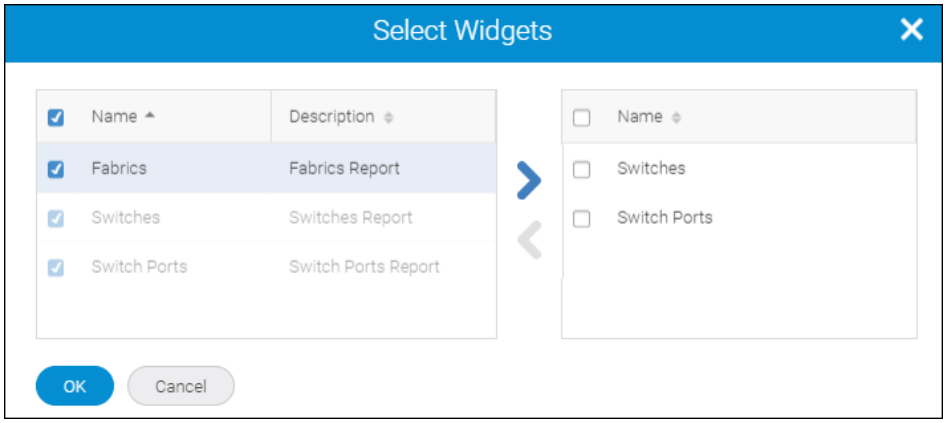
Perform the following procedure to create a report template in SANnav Global View.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Click the **+** icon in the upper-right corner, and then select **Select Report Widgets**.



3. Select the widgets that you want in your report, and click the right arrow to move them to the right side of the dialog.

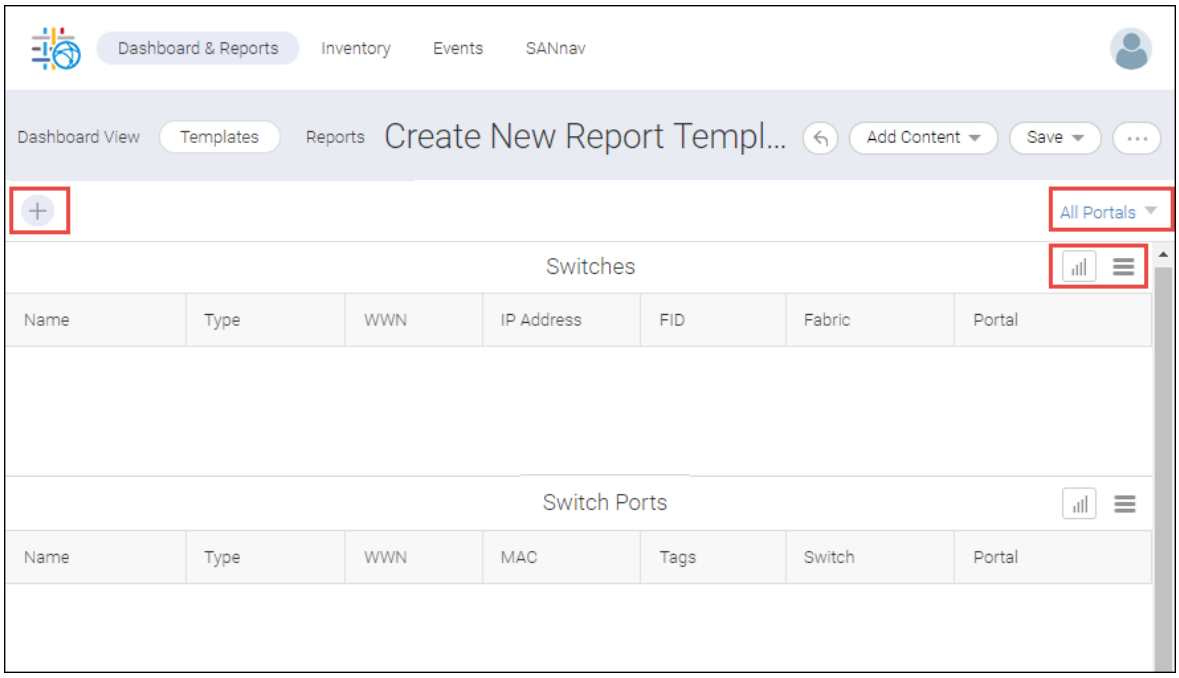
   If you want the widgets in a particular order, select each widget separately and then click the right arrow before selecting the next widget.



4. Click **OK**.

   The template displays with placeholders for each widget.

   A report layout is created with a default name and default columns, which you can now customize.



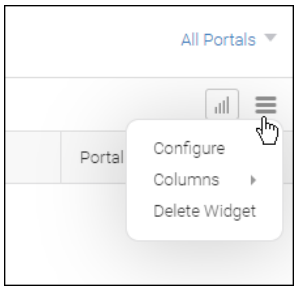
5. Add filters to the report template.

   You can customize the report by changing the Management Portal scope using the drop-down list on the right side of the filter bar. Click the **+** button on the left side of the filter bar to add specific filters for fabrics, switches, and switch ports. The filters apply to all widgets in the template.

   The generated report contains data for only those objects that meet the filter requirements.

   NOTE
   Although there is no restriction on the number of filters that can be added or applied as part of the report template, it is recommended that you follow this guideline: two parameter conditions within a filter and two filters within a report.

6. Customize the widgets.

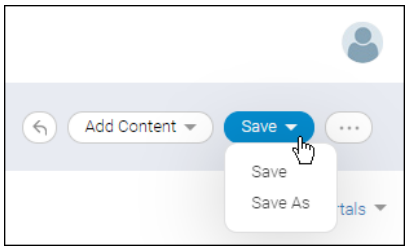


   Click the hamburger icon for each widget to do the following:

   - Change the name of the widget in the report (**Configure** option).
   - Add or delete columns and change the order of the columns.
   - Delete the widget from the report.

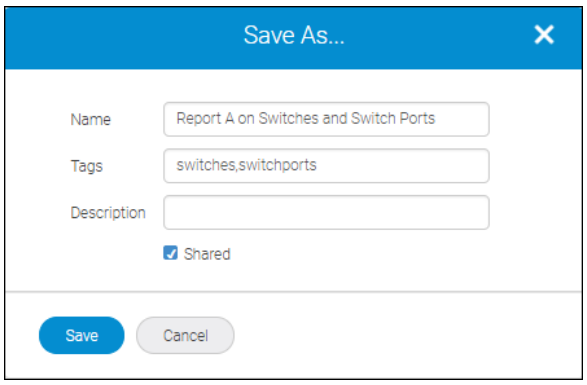
   You cannot rearrange the widgets in the report, but you can add widgets to the top and bottom of the report by clicking **Add Content** > **Add Widgets**.

7. Click either **Save** > **Save** or **Save** > **Save As** to save the report template.



8. Enter a name for the template, along with optional tags and a description, and select the **Shared** box if you want other SANnav Global View users to view the content.

   The template name can contain only alphanumeric characters, as well as the hyphen (-), underscore (_), and period (.).



9. Click **Save**.

To generate your report, go to the **Templates** page and select **Generate** from the action menu. To schedule report generation to run at a future time, select **Schedule**. For detailed instructions, see Scheduling a Report and Generating and Exporting Reports.

Scheduling a Report

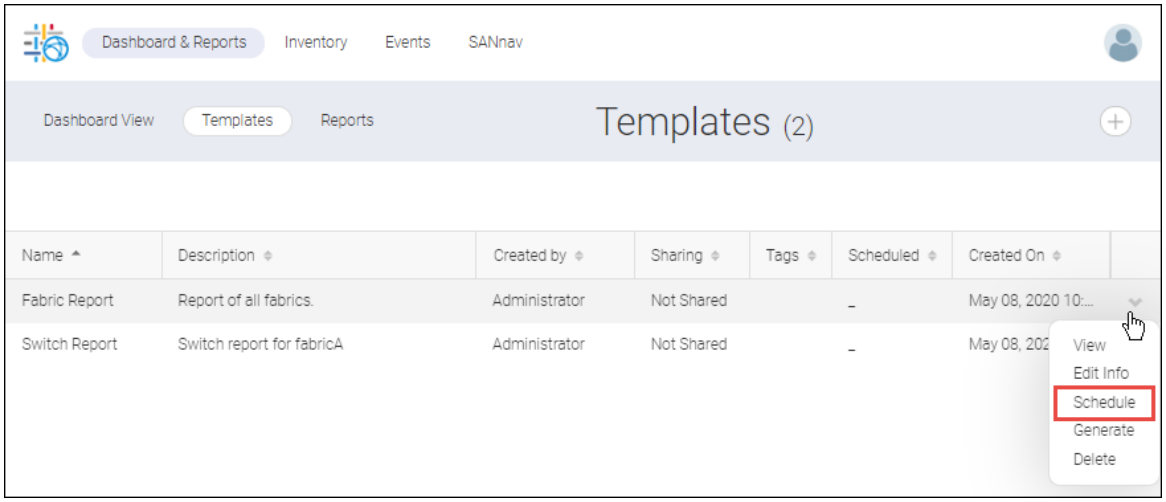
In SANnav, you can schedule a report to run later.

If you want to specify an email address to which the generated report will be sent, the email server must be configured and enabled in SANnav. See Setting Up Global View Email.

NOTE
A maximum of four schedules can be associated with one report template.

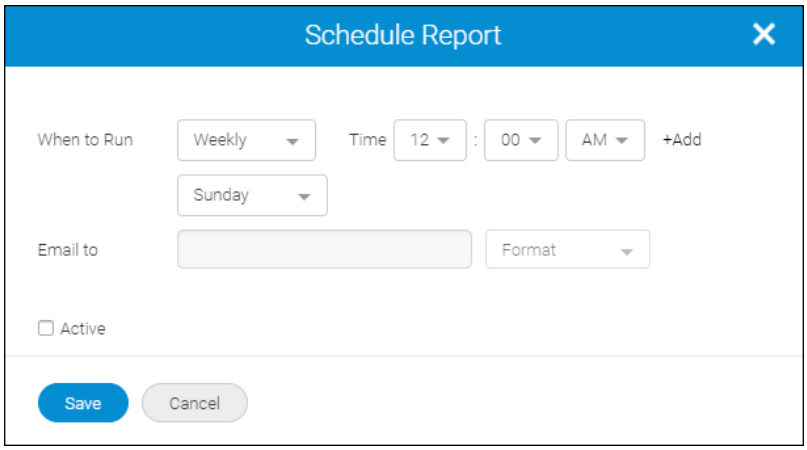
To schedule a report, perform the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Locate the report template and click **Schedule** on the down arrow to the right of the table entry.



3. Select a time interval and a time to run the report.

   For example, the following screen capture schedules a report to run every Sunday at 12:00 a.m.

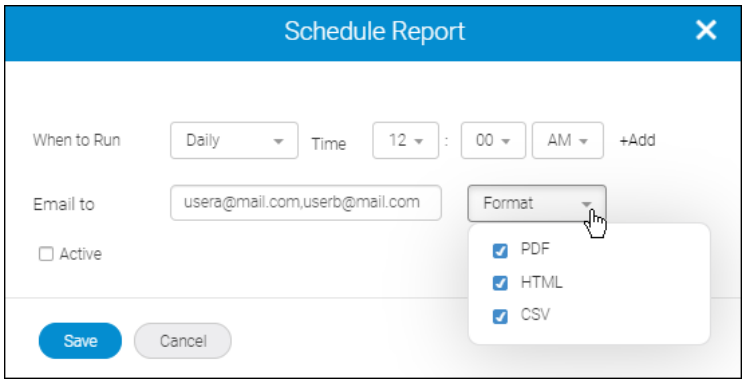


4. Specify the email address of the receiver and the formats in which the report will be sent.

   You can enter multiple email addresses separated by commas.

   If the **Email to** field is disabled, an email server is not configured or is not enabled in SANnav.

   If you select multiple formats for the report output, they are zipped into one file.

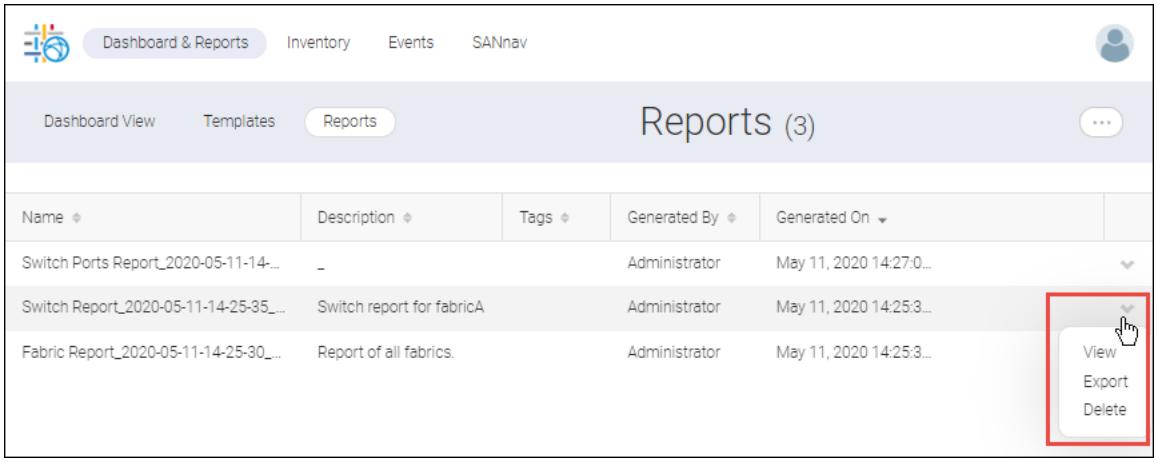


5. Select **Active** to activate the report schedule.
6. Click **+ Add** to add another schedule.
   You can add up to four schedules.
7. Click **Save**.
   On the **Templates** page, the **Scheduled** column now shows the schedule for when the report will be run.

Generating and Exporting Reports

In SANnav, in addition to scheduling reports, you can generate and view a report at any time. You can also export the generated output to PDF, HTML, and CSV files.

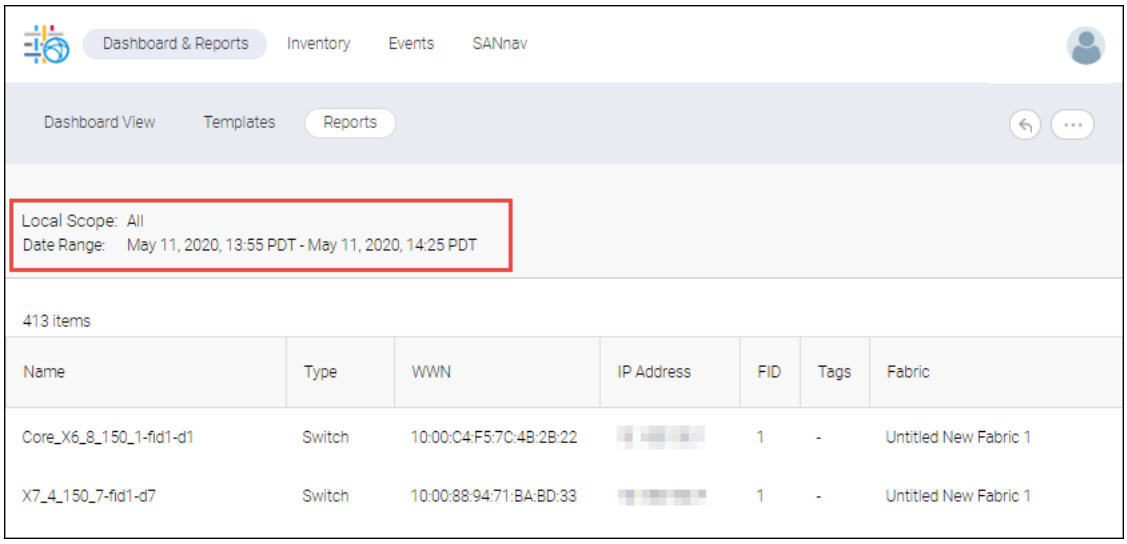
1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
   The **Templates** page lists all report templates.
2. Locate the report template that you want, and select **Generate Report** from the action menu.
   The report starts generating. This process might take some time depending on the contents of the template.
3. Click **Reports** in the subnavigation bar.
   The **Reports** page lists all reports that were generated by logged-in users in the past 30 days. Reports older than 30 days are automatically deleted.
4. Locate the report that you want to see, and select **View** from the action menu.



The report is displayed in HTML format.

On the top left, the context of the reports (applied filters, and so on) is displayed.

The generated output data and date range have the time zone of the browser that is used to schedule or generate the report.



5. Click the more button (···), and then select **Export** to download and export the report.

   The report is downloaded as a ZIP file containing HTML, PDF, and CSV files.

Setting Up Global View Email

Similar to SANnav Management Portal, SANnav Global View enables you to configure the email server, which the system can then use to send an email notification during report generation if you elect to do so.

1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Email Setup**.

   The **SANnav Email Setup** dialog displays.

2. Enter the email server in the **Email Server** field.

3. Select an option from the **Security** list.

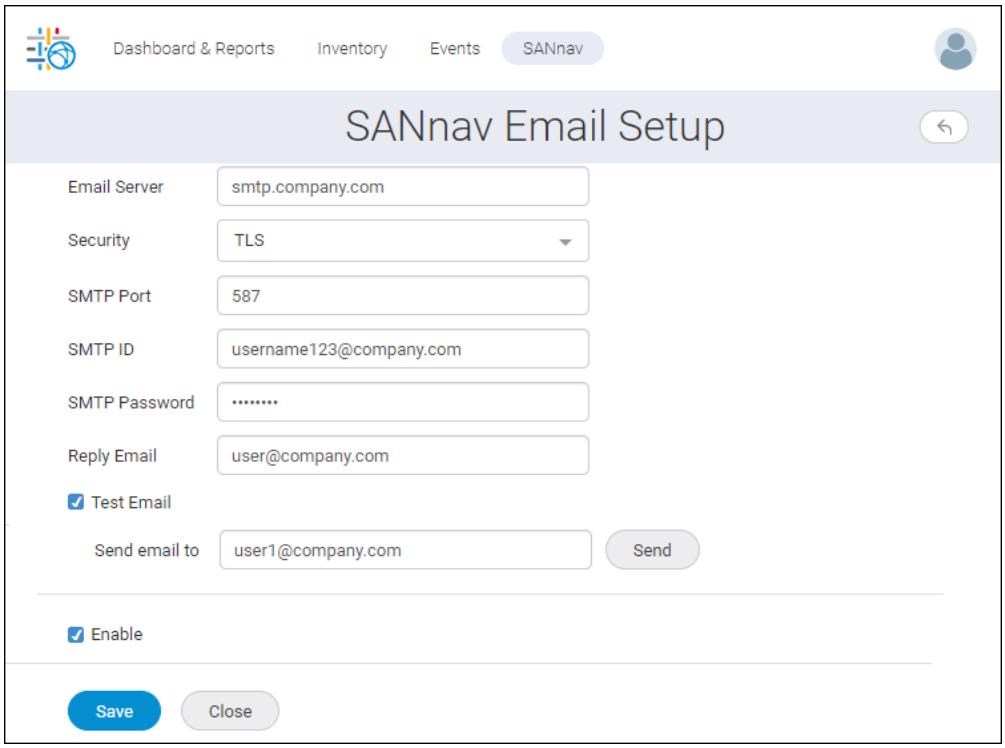
   If you select **SSL** or **TLS**, you must also provide the SMTP ID and password.

4. Enter the email address in the **Reply Email** field.

   The **Reply Email** is the email address to which reply notifications are sent.

5. To send a test email, select the **Test Email** checkbox, enter an email address, and click **Send**.

   If you have more than one email ID to set up, separate the email IDs with a comma (and no space).



6. Select the **Enable** checkbox to activate the email configuration.
7. Click **Save** to save the email setup.

Global View Inventory Management

The SANnav Global View **Inventory** page is a central location where you can view and manage the inventory of all discovered fabrics, switches, switch ports, hosts, host ports, storage, storage ports, and physical chassis across all SANnav Management Portal instances.

When you first view the **Inventory** page, it is empty. You must add filters to display data. The exception to this is that when you view chassis objects, all of the chassis display.

In addition to viewing inventory, you can export the data to a CSV file.

For switch ports, you can launch investigation mode to view performance measures.

Viewing Inventory Using Filters

Inventory can contain thousands of components. In searching for inventory items, use filters to narrow the inventory and display only the items that you are interested in from among all SANnav Management Portal instances.

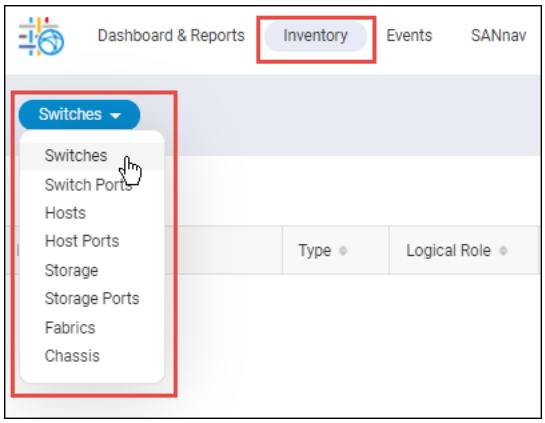
The **Inventory** page displays a maximum of 500 entries per portal.

> **NOTE**
> When creating filters, type-ahead is not supported in SANnav Global View.

The following procedure shows how to use filters to display a list of switches in degraded or poor health across all Management Portal instances.

1. Click **Inventory** in the navigation bar, and then select the type of inventory object.

   For this example, select **Switches**.

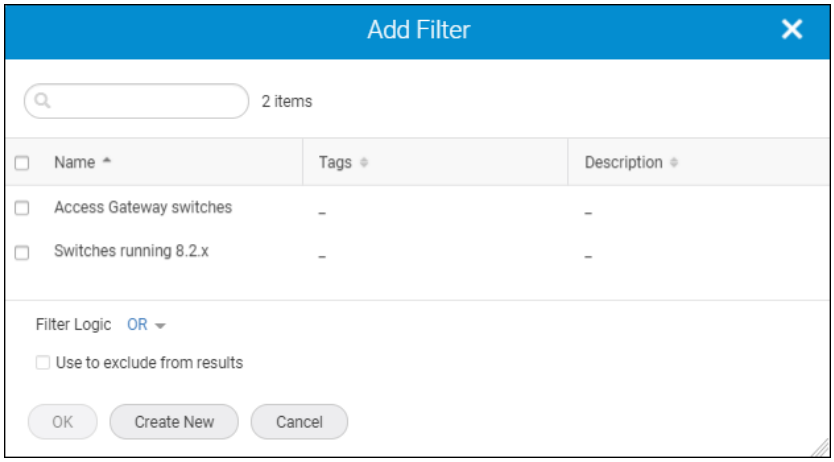


For all inventory objects other than **Chassis**, the page is empty. You must add filters to determine which objects in inventory are displayed.

2. Click the **+** on the upper left to add a filter.

   You can select from existing filters, or you can create a filter.

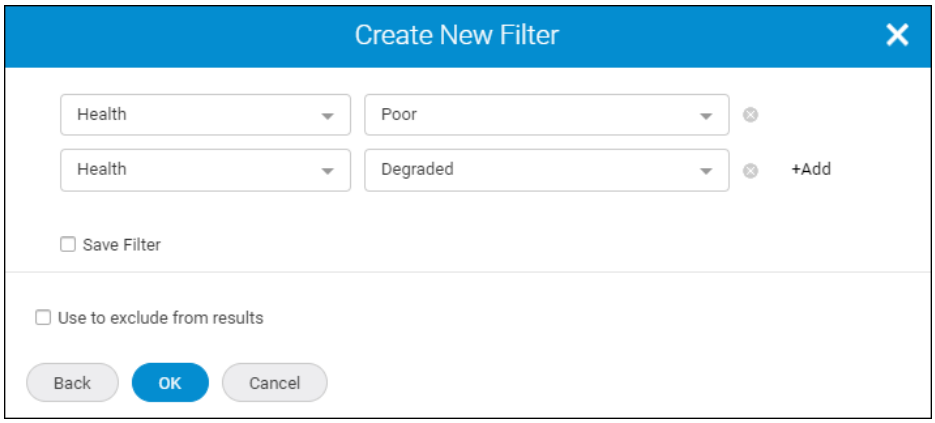
   In the following example, two switch filters have already been created and saved; however, for this example, a new filter is created.



3. Click **Create New**.
4. Select the filter attribute and value.

   Click **+Add** if you want to add additional attribute-value pairs.

   The following filter displays all switches with poor or degraded health.



For a complete description of filters and filtering rules, see Filters.

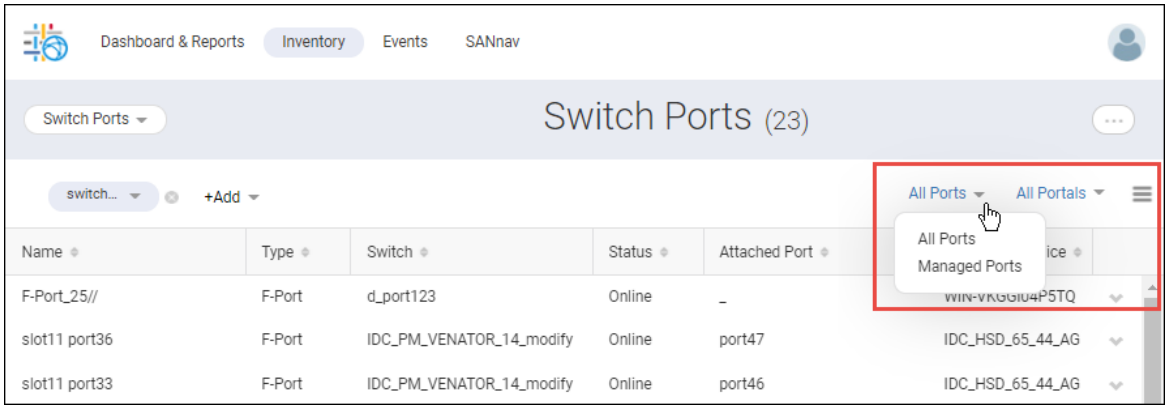
5. Select the **Save Filter** checkbox if you want to name this filter and save it for use later.
6. Select the **Use to exclude from results** checkbox if you want this filter to be a NOT filter.
7. Click **OK**.

   The **Inventory** page displays all switches that meet the filter criteria.

   You can perform additional filtering by limiting the display to specific Management Portal instances. You can filter the columns that are displayed by clicking the hamburger icon (≡).

   For switch ports, you can also filter the display to show all ports or only managed ports. Selecting **Managed Ports** displays only licensed switch ports and AG ports. The following ports are not displayed:

   - Unlicensed ports (ports that are not licensed under a Ports on Demand license)
   - ICL ports
   - Logical ports
   - Unmonitored ports (ports on unmonitored fabrics or switches)
   - Unmanaged or unreachable ports
   - Ports on switches that are missing from the fabric

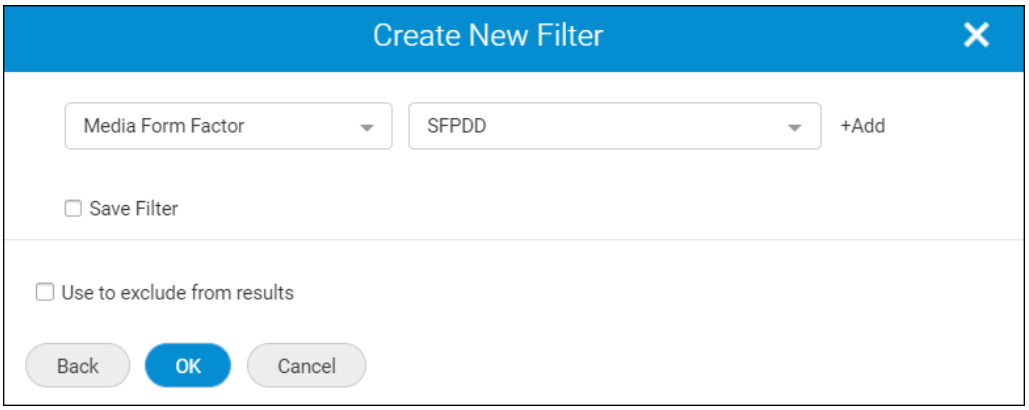


Media Form Factor

The **Media Form Factor** column, together with the **Unit Number** and **Channel Index** columns, display information for switches running Fabric OS 9.1.1 or higher. For example, for QSFP ports, the **Media Form Factor** column displays **QSFP**, **QSFP+**, **QSFP28**, or **QSFP_CMIS**, and the **Unit Number** column displays the

QSFP number. For SFPDD ports, the **Media Form Factor** column displays SFPDD and the **Channel Index** column displays the SFPDD channel (1 or 2). The **Unit Number** and **Channel Index** columns are hidden by default. You can create a filter to display only ports of a specific media form factor, as shown in the following screenshot.

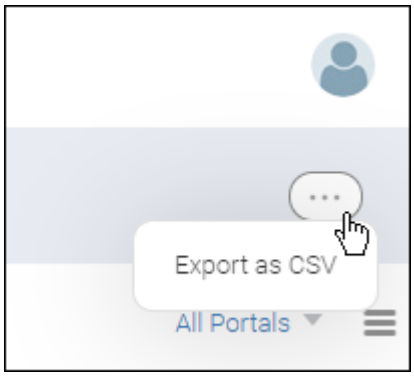
Figure 9: Creating a Media Form Factor Filter



Exporting Inventory Views

In SANnav Global View, you can export the inventory tables to a CSV file.

1. Click **Inventory** in the navigation bar, and select the type of inventory that you want to view.
2. Add filters to display the inventory.
3. Click the More button in the upper-right corner, and select **Export as CSV**.



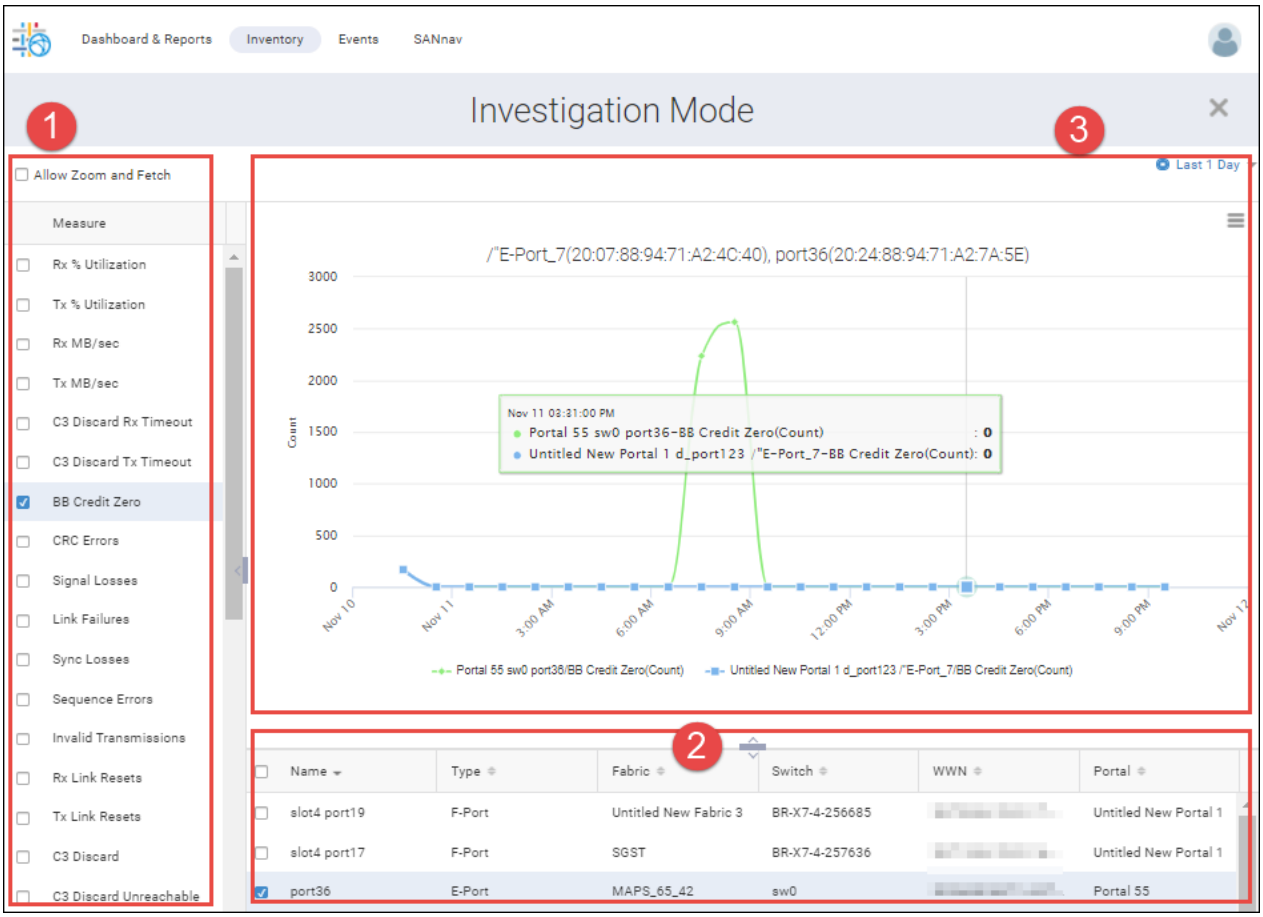
A CSV file is downloaded to your local machine. The file name is `export_data.csv`.

Using Investigation Mode

SANnav Global View Investigation mode displays graphs of historic performance metrics for one or more switch ports. Investigation mode launches when you click **Investigate** from the **Inventory** page.

The **Investigation Mode** page consists of three parts: a **Measures** panel, a details table for the selected ports, and a graph area. Select measures and ports to investigate, and the resultant graph displays in the graph area.

Figure 10: Investigation Mode Page Overview



1. Measures panel. Contains a list of measures available for the selected ports.
2. Details table. Displays the ports that are selected for investigation.
3. Graph area. Displays a different colored line for each selected measure-port pair.

Measures Panel

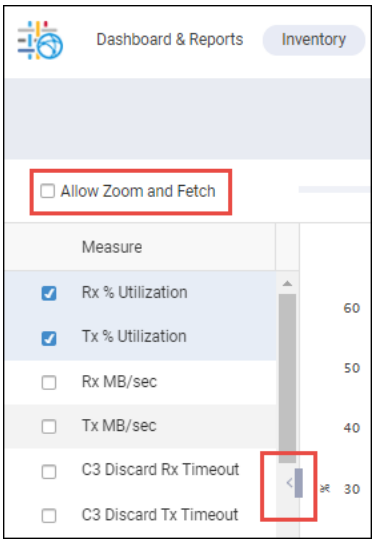
The list of available measures depends on the type of entity selected. For example, GigE ports have different measures than F_Ports and E_Ports.

Select the measures that you want to monitor. You can select up to eight measures to monitor up to four ports or four measures to monitor up to eight ports.

Select **Allow Zoom and Fetch** to be able to view data points at a higher level of granularity. If this checkbox is selected, you can select only a single measure.

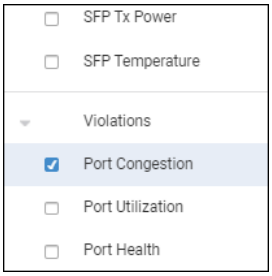
After you select the measures, you can click the hide arrow to hide the **Measures** panel and allow more space for the graph.

Figure 11: Measures Panel Options



For FC ports, the **Measures** panel includes port congestion, port utilization, and port health violations. Scroll to the bottom of the **Measures** panel to select these violations.

Figure 12: Measures Panel: Violations Measures



Details Table

The details table displays the ports that are chosen for investigation.

Select ports in the table to display in the graph area. You can select up to eight ports for up to four measures. If more than four measures are selected, you can select up to four ports.

Graph Area

The graph plot depends on the ports and measures selected. The graph area displays one line for each port/measure pair.

> **NOTE**
> If the graph area is empty, either measures are not selected or data might not exist for this combination of measure and port.

By default, the graphs display historic data from the last 30 minutes. You can change this value by selecting the date range drop-down in the upper-right corner of the graph area.

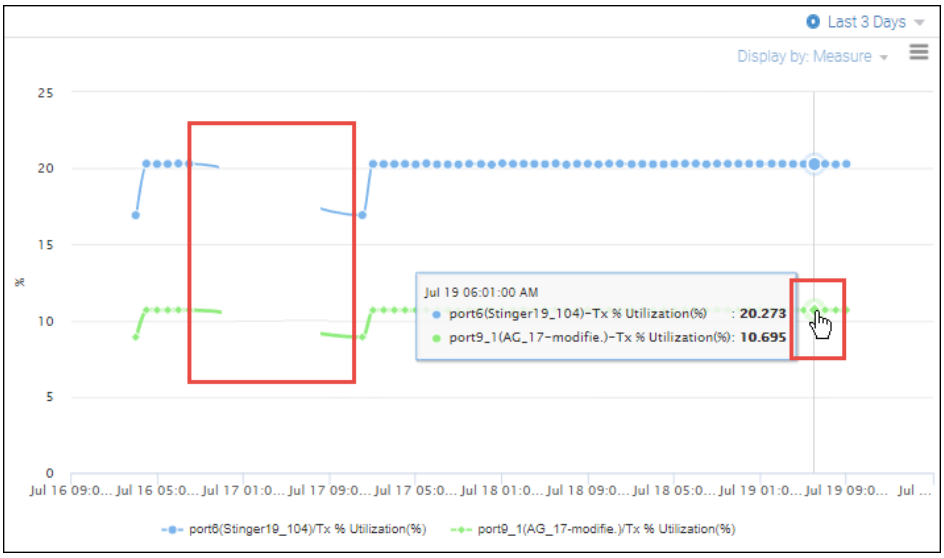
Data Points

Hover the mouse over a data point in the graph to see additional details in a tool-tip box.

Some data points might be missing, which could be due to an SNMP timeout or to performance data collection being disabled. If this happens, there is a gap in the graph.

The following graph plots TX % utilization on two ports. Hovering over a data point in one line gives details for all data points for that same time period. Note the missing data points, indicated by a gap in the graph.

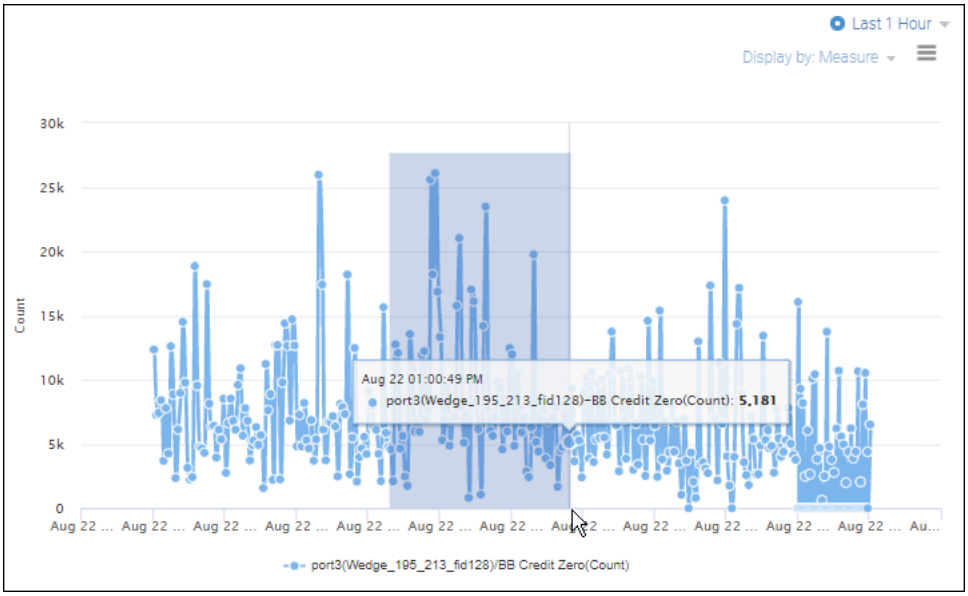
Figure 13: Performance Graph Data Points and Missing Data Points



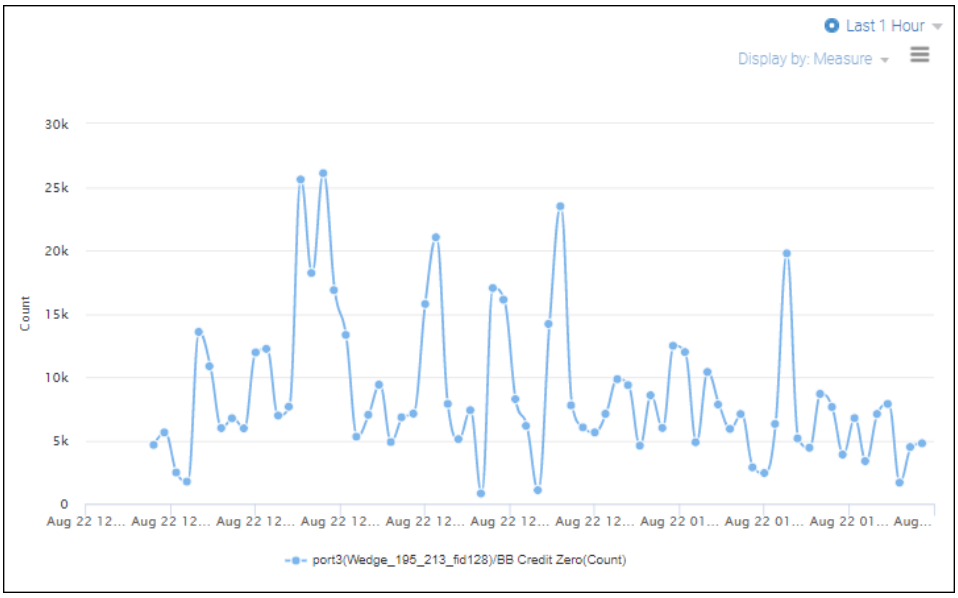
Zooming In on Data

To zoom in on an area of the graph, drag out a rectangular area in the graph with your mouse pointer.

Figure 14: Highlighting Part of a Graph to Zoom In



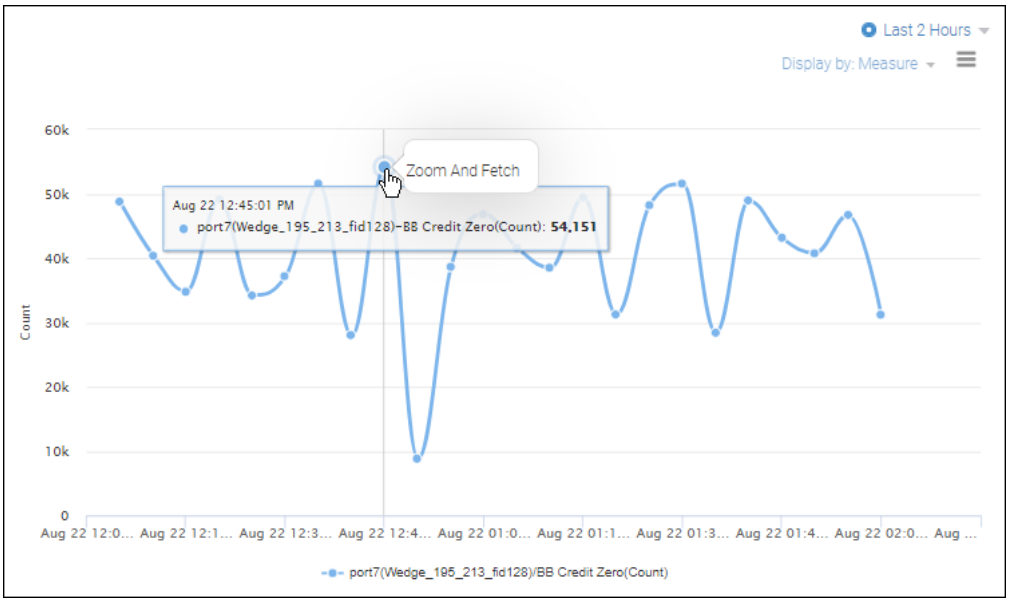
The graph is redrawn with the selected area magnified.



Zoom and Fetch for Higher Granularity

You can obtain ("fetch") a higher level of granularity for a particular data point with **Zoom And Fetch**. Click a data point in the graph, and then click **Zoom And Fetch**.

NOTE
You must select **Allow Zoom and Fetch** in the measures panel to enable this capability.



The graph displays at a higher granularity. Each successive application of **Zoom And Fetch** displays a greater level of granularity. For example, **Zoom And Fetch** applied to 1-day granularity displays data at 1-hour granularity. Applying **Zoom And Fetch** to 1-hour granularity displays data at 5-minute granularity.

NOTE

Zoom And Fetch is applicable only to FC switch ports of type E, F, EX, N, and SIM, and only in a graph with one port and one measure. **Zoom And Fetch** is not available if multiple ports or multiple measures are selected.

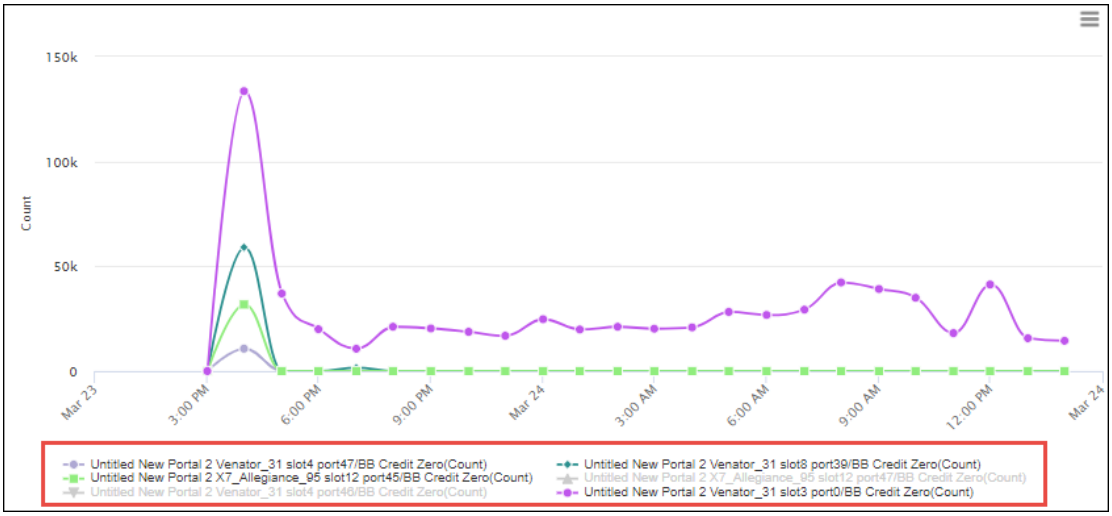
Zoom And Fetch is not applicable for port violations measures.

Graph Legend

Below each graph is a legend, which lists the entity, measure, and unit of measurement for each line in the graph. You can click items in the legend to hide or display the corresponding lines in the graph.

The following graph plots measures for six switch ports. Note that two of the switch ports have been deselected in the legend, so only four lines display in the graph.

Figure 15: Performance Graph Legend



Types of Graphs

The graph area can display single or multiple graphs.

The following combinations are displayed in a single graph:

- One port and up to eight measures (1x8)
- Up to eight ports and one measure (8x1)

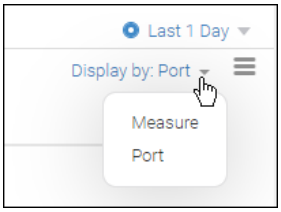
The following combinations are displayed in multiple graphs:

- Up to eight ports and up to four measures (8x4)
- Up to four ports and up to eight measures (4x8)

For example, if you select six measures, you can select up to four ports. If you select one port, you can select up to eight measures.

SANnav displays up to eight graphs. Each graph is limited to one measure and eight ports or eight measures and one port. The graphs can be displayed by port or by measure, depending on the value in the **Display by** drop-down.

Figure 16: Displaying Performance Graphs by Measure or by Entity



When multiple graphs are displayed, you can move the slider bar at the top left of the graph area to compress the graphs so that you can view more on a single page. Note that when you compress the graphs, the legend below them disappears.

Figure 17: Multiple Graphs, Compressed

Exporting the Graph

To export a static copy of the graph, click the hamburger icon in the top right of the graph and select **Export**. Select whether to download the graph as an HTML or CSV file.

If you download as a CSV file, one file is generated for each port or measure that is selected. For example, if you select **Display by Measure** and you selected eight measures, then eight CSV files are generated.

Investigating Switch Ports in SANnav Global View

SANnav Global View enables you to search for and investigate switch ports. The switch ports span all SANnav Management Portal instances that have been added to SANnav Global View.

Investigation mode is available for all FC protocol switch ports. For FCIP, it is available for GigE-Port type switch ports, and for Ethernet, it is available for ETH type switch ports.

Note the following about Investigation mode in SANnav Global View:

- Global View monitoring is historical only. Real-time monitoring is unavailable.
- The maximum date range is the last 30 days.
- You can display the following types of graphs:
  - Up to four ports and eight measures
  - Up to eight ports and four measures

The following procedure shows you how to launch Investigation mode for switch ports. For additional information, see Using Investigation Mode.

1. Click **Inventory** in the navigation bar, and select **Switch Ports** from the context drop-down.
2. Add a filter to display switch ports.
3. Select the ports that you want to investigate.
   - To investigate a single port, select **Investigate** from the action menu for that port.
   - To investigate multiple ports, click the More button (···), and click **Bulk Select**. Select the switch ports that you want to investigate, and click **Actions** > **Investigate**. Using the **Bulk Select** option allows you to select and investigate ports from different portal instances.

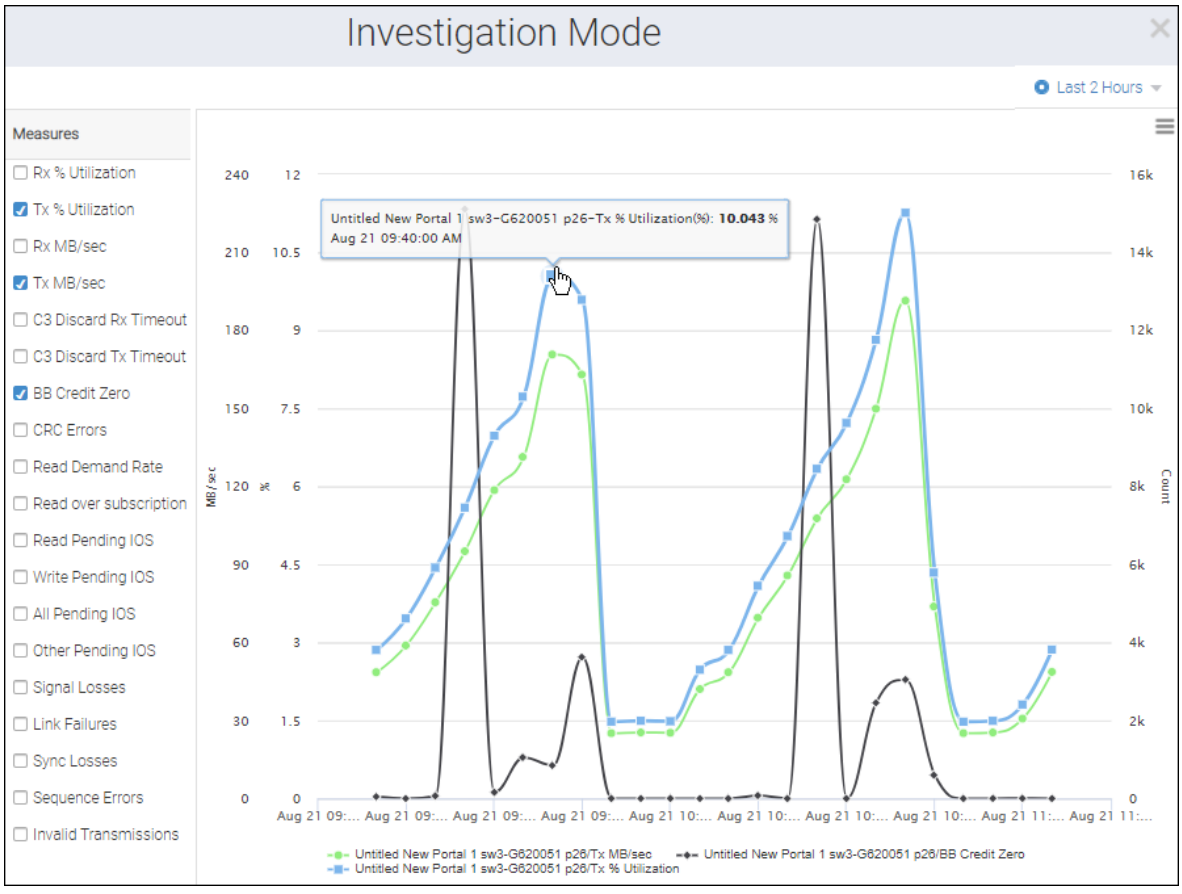
   The **Investigation Mode** page displays.

   By default, this page is blank. You must select ports and measures to obtain the related details.
4. Select the ports from the table at the bottom of the page, and select the measures from the panel on the left.

   You can select up to four ports and eight measures or up to eight ports and four measures.

   The list of available measures depends on the selected port type. Note that for switch ports, in addition to performance measures, you can view switch port (FC port) violations, such as port health, congestion, and port utilization violations.

   A graph displays for the selected ports and measures. If you hover over a point of the graph, you see the details that are associated with that data point.



The date/time of the graph is shown in the upper-right drop-down. By default, **Last 30 Minutes** is selected.

5. To change the scale of the graph, click the drop-down to display the **Select Date Range** dialog.

   You can either select a predefined time interval or manually specify a date range, up to the last 30 days.

Configuration Policy Management

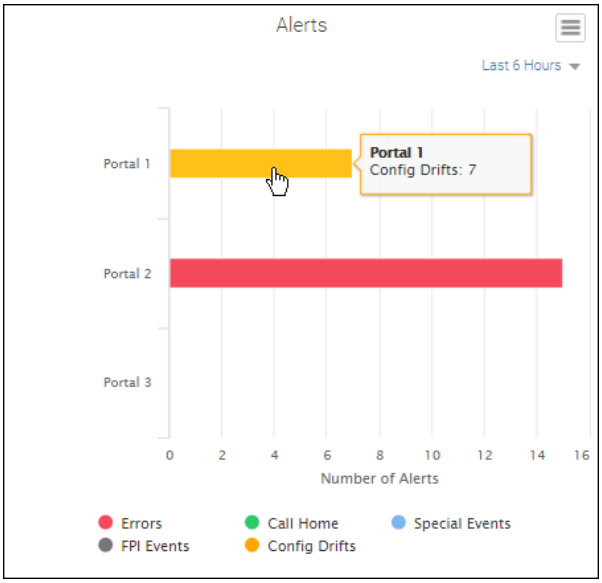
Maintain consistent settings on all switches in the same fabric, because inconsistent parameters, such as inconsistent PID formats, can cause fabric segmentation.

In SANnav Management Portal, you can create a configuration policy, and then push the policy to multiple switches and fabrics. In SANnav Global View, you cannot create a configuration policy, but you can import a configuration policy from a SANnav Management Portal instance. This imported policy becomes a global policy. You can then synchronize the global policy to multiple portal instances, so that all portal instances are using the same policy.

When you import a configuration policy, you cannot modify it, other than changing the name, tags, and description. Make sure that you make any changes to the policy before importing it.

> **NOTE**
> When synchronized to a portal, the global policy cannot be modified by the SANnav Management Portal administrator. However, the administrator can clone the policy if changes are needed.

The **Alerts** widget in the dashboard displays the number of switches with configuration drifts; that is, switches with a configuration that does not match the SANnav Management Portal monitored configuration.

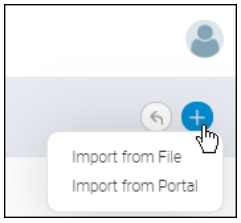


Importing Configuration Policies

You can import a configuration policy from a SANnav Management Portal to create a global policy, which can then be pushed to one or more portal instances.

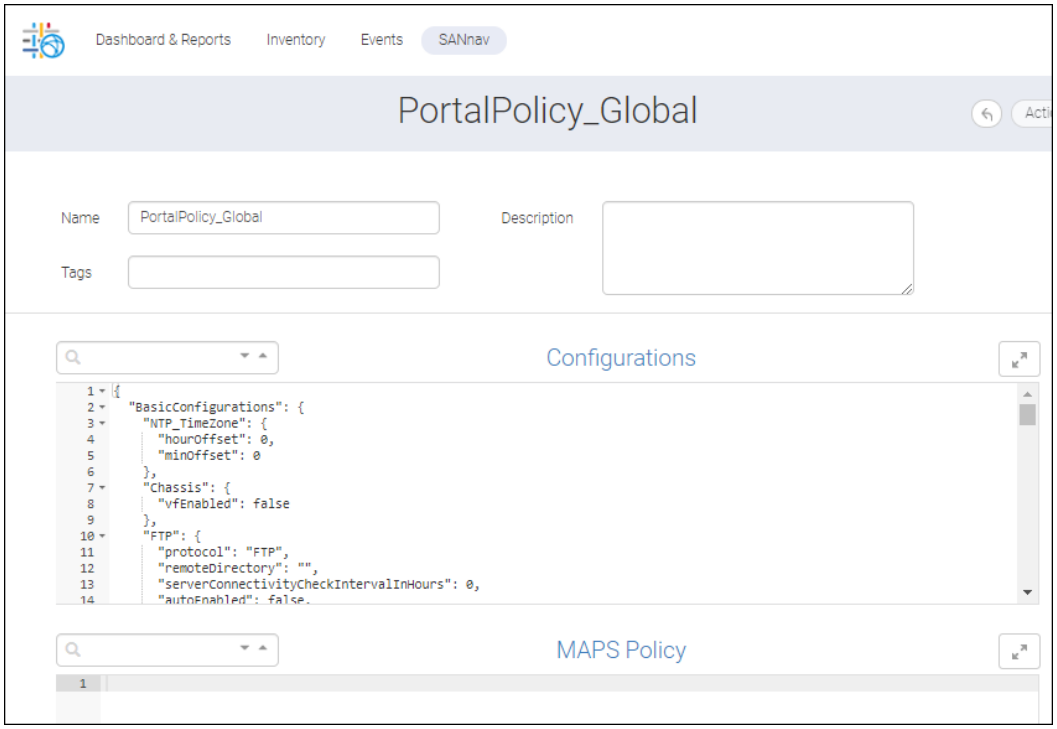
Perform the following steps to import a configuration policy from a portal instance:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** > **Policy Management**.
2. Click the **+** icon in the upper-right corner, and then select **Import from Portal**.



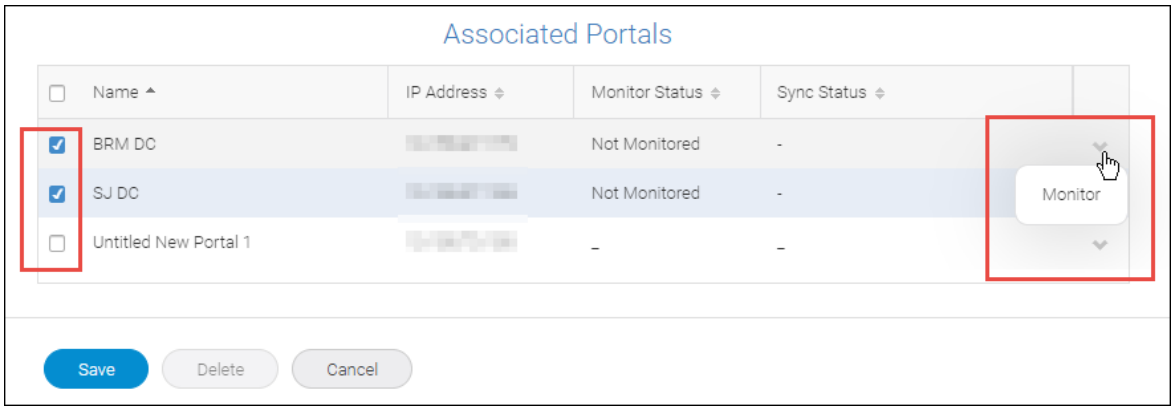
   You can also select **Import from File** to import a policy from a file. This example imports a policy from a portal instance.
3. Select the portal instance, and click **Next**.
4. Select the configuration policy, and click **OK**.

   The policy displays in the window. The policy name is the same as the original name, but with "_Global" appended. You can change the name of the policy, but cannot modify the configuration blocks.



5. Scroll down the window to the **Associated Portals** table, and select the portal instances that you want to associate with the policy.

   If you want to monitor the policies in the portal instances, select **Monitor** from the action menu for each selected portal instance.

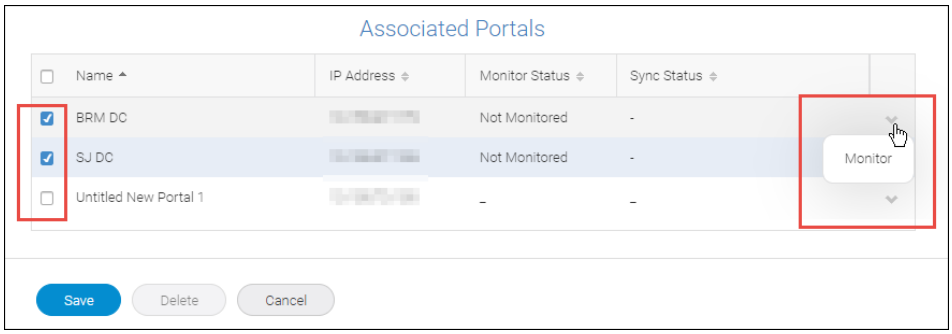


6. Click **Save** to save the policy and push it to the selected portal instances.

Pushing Configuration Policies to SANnav Management Portal Instances

Policies that have been imported to SANnav Global View are called global policies. You can push these global policies to one or more SANnav Management Portal instances, so that all portal instances use the same policies.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** > **Policy Management**.
   A list of imported configuration policies displays.
2. Click the name of the policy you want to push.
3. Scroll to the bottom of the policy details page, and select the portal instances to which the policy is to be pushed.



   Select all portal instances to which the policy is to be pushed, including portal instances that were previously selected.

   If you want to monitor the policies in the portal instances, select **Monitor** from the action menu for each selected portal. Note that the SANnav Management Portal administrator cannot change this option.
4. Click **Save** to push the policy to the selected portal instances.

Deleting Configuration Policies

You can delete a configuration policy from one or more associated SANnav Management Portal instances. You can also delete a configuration policy from SANnav Global View, in which case the policy is also removed from the portal instances.

1. Click SANnav in the navigation bar, and then select **SAN Monitoring** > **Policy Management**.
   A list of imported configuration policies displays.

2. Click the name of the policy you want to delete.
3. To delete the policy from one or more portal instances, scroll down to the **Associated Portals** table, unselect the portal instances, and click **Save**.

   The policy is removed from the unselected portal instances, but remains applied to the selected portal instances.
4. To delete the policy from SANnav Global View, scroll to the bottom of the policy details page, and click **Delete**.

   The policy is deleted from SANnav Global View and is also deleted from all associated portal instances, if the portal instances are accessible from Global View.

Event Management

SANnav Global View displays application events, including those events generated by user action.

SANnav Global View does not display events from the SANnav Management Portal instances.

The following procedure describes how to view the events and filter them based on a date range.

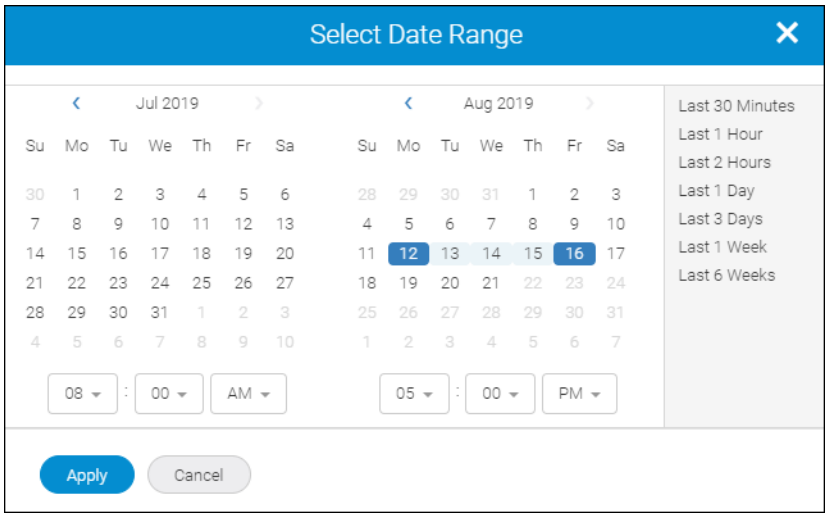
1. Click **Events** in the navigation bar.

   By default, events that are recorded in the **Last 30 Minutes** are displayed, as indicated by the Date Range drop-down in the upper-right corner.

2. Click the date range drop-down, and then select the range for which you want to display events.

   You can select from fixed ranges on the right side of the dialog, or select custom start and end dates using the calendar.

   For example, the following screen capture selects a date range from 8:00 a.m. on August 12 to 5:00 p.m. on August 16.

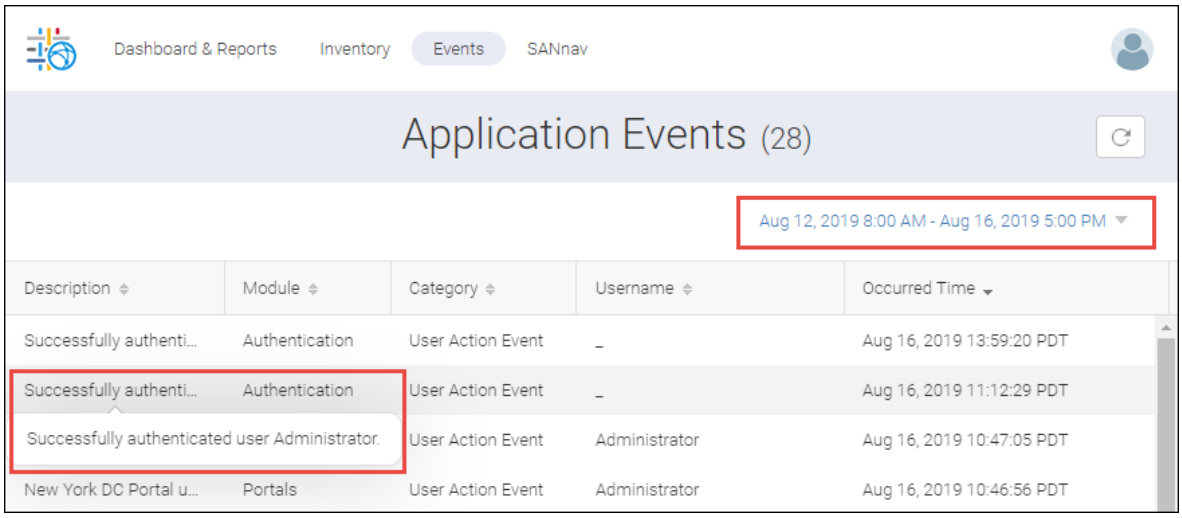


3. Click **Apply**.

   Events for the given date range are displayed. For this example, 28 events are displayed, as indicated by the page title.

   Note that if you want to see the full event message, you can widen the **Description** column, or you can hover over the truncated message to see the complete description.

   To update the page, click the refresh icon on the right side of the subnavigation bar.


Dashboard & Reports
Inventory
Events
SANnav
Application Events (28)
Aug 12, 2019 8:00 AM - Aug 16, 2019 5:00 PM
Description
Module
Category
Username
Occurred Time
Successfully authenti...
Authentication
User Action Event
_
Aug 16, 2019 13:59:20 PDT
Successfully authenti...
Authentication
User Action Event
_
Aug 16, 2019 11:12:29 PDT
Successfully authenticated user Administrator.
User Action Event
Administrator
Aug 16, 2019 10:47:05 PDT
New York DC Portal u...
Portals
User Action Event
Administrator
Aug 16, 2019 10:46:56 PDT

SANnav Maintenance and Support

This section contains procedures for performing several SANnav maintenance tasks:

- Shutting down SANnav gracefully to perform maintenance or move the server.
- Configuring regular and on-demand backups of SANnav data.
- Checking the SANnav status.

Instructions are also included for generating a support data collection file, which you can send to your switch service provider if you encounter any issues with SANnav.

Global View Backup and Restore

SANnav Global View allows you to back up the SANnav server data and restore it as required, such as in scenarios where the data is deleted or corrupted. Also, you can use the backup when you want to bring up a new SANnav server.

Creating a backup helps to protect the server's data and configuration in the event of a disaster, such as server failure.

A backup includes all data on the Global View database, system configuration, and (optionally) reports generated in the system. You can perform an on-demand backup with or without reports, as well as schedule daily and weekly backups.

NOTE
The backup option is not supported with the trial license.

To access backup, click **SANnav** in the navigation bar, and then select **Services** > **SANnav Backup**.

Recommendations for backup are given below:

- Make sure that your backup locations have enough disk space before you back up your data.
- Make sure that your backup locations are different from the location where SANnav is installed.
- For scheduled backups, occasionally check if the backup data size has any abnormal pattern, such as some files being too large or too small.

Configuring a Backup File Location

Before you can back up SANnav, you must configure a location where the backup files are to be saved. You can configure up to two locations, but you must configure at least one.

The following rules apply to both locations:

- The backup locations must be accessible from the SANnav server.
- The backup locations must have enough disk space to accommodate the backup files.

Also note the following best practices for backup locations:

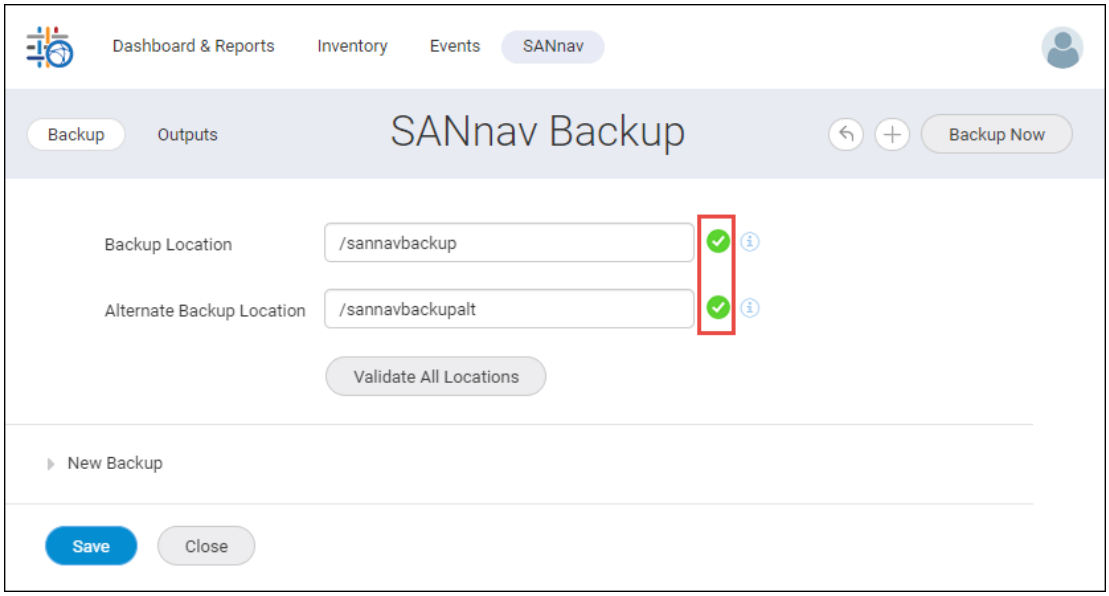
- The backup location should be an accessible path on the server on which SANnav is installed, but it should be different from the actual installation folder.
- You can specify a location on your local machine or on external storage. If the location is on external storage, the external storage should be mounted locally.
- Make sure that you check the disk space periodically so that your backups are successful.

Perform the following steps to configure one or two backup locations:

1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Backup**.
2. In the **Backup Location** field, enter the Linux location where you want to save the backup file.
3. In the **Alternate Backup Location** field, enter another Linux location where backup files can be saved.
4. Click **Validate All Locations**.

   A green checkmark indicates that the location is valid.

   If both locations are invalid, you must provide a valid location before continuing.



5. Click **Save**.

   These locations can now be selected when you perform SANnav backups.

Configuring a Scheduled Backup

You can schedule up to two backups of the SANnav server data. For example, you can schedule a daily backup and a weekly backup.

Required privilege: Server Backup with read/write permission.

When scheduling a backup, you select a location for the backup file to be saved and the time for the backup to start. If a backup location has not already been configured, see Configuring a Backup File Location. Make sure that you check the disk space periodically so that your scheduled backups are successful.

The following steps create two backup schedules: a daily backup that includes database and configuration files and a weekly backup that also includes reports.

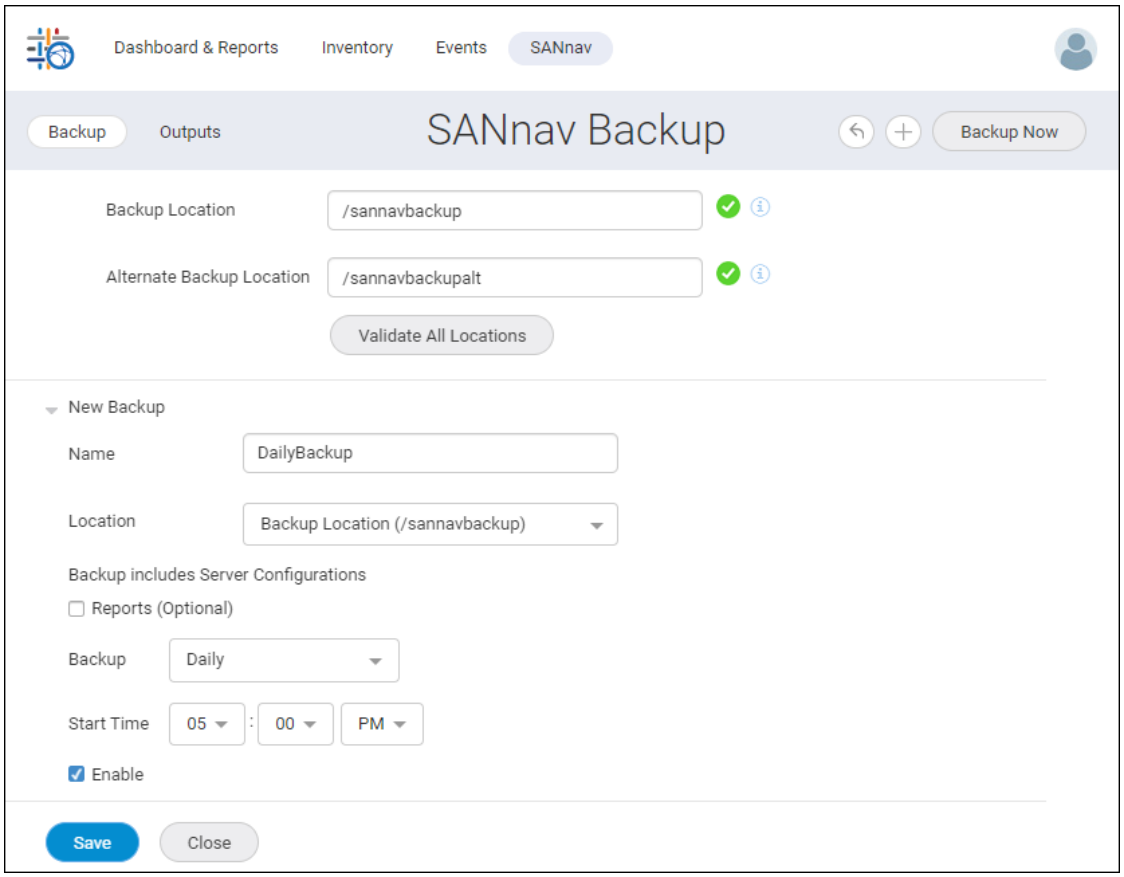
1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Backup**.
2. Select the **New Backup** drop-down, and enter a name for the backup.
3. Select the backup location from the **Location** drop-down.
4. Select **Daily** from the **Backup** drop-down, and enter the start time for the daily backup.

   By default, the backup includes database and configuration files.

   For this scenario, do not select the optional **Reports** checkbox.

5. Select **Enable** to activate the backup, and click **Save**.

   If the **Save** button is not active, check that you specified a name and selected a location for the backup.



6. Click the **+** icon on the top-right corner of the window to add an additional backup.

   NOTE
   You can create a maximum of two scheduled backups. You can schedule one weekly backup and one daily backup, or you can schedule two weekly backups. You cannot schedule two daily backups.

7. Enter the name for the second backup in the **Name** field.
8. Select the backup location from the **Location** drop-down.

   The location can be different from the location of the first backup.

9. For this example, select the optional **Reports** checkbox.
10. Select **Weekly** from the **Backup** drop-down, and then select the day and start time.

    There must be more than three hours difference between the start times of the two backups. For example, if the daily start time is 12:00 AM, the weekly start time must be set to more than three hours before or after the daily start time; for example, 8:45 PM or 3:15 AM.

    If you create two weekly backups, in addition to the three-hour time difference, the weekly backups must start on two different days.

11. Select **Enable** to activate the second scheduled backup, and click **Save**.

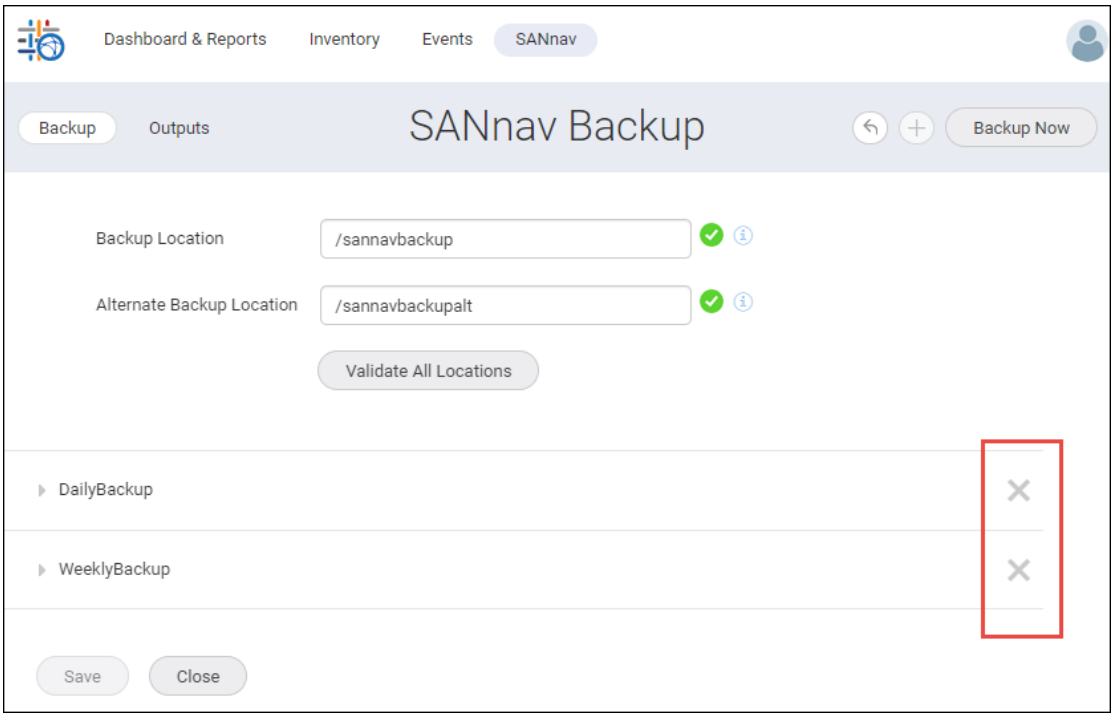
    If the **Save** button is not active, check that you specified a name and selected a location for the backup.

NOTE
You must enable each scheduled backup to generate that backup.

System Behavior

SANnav verifies the storage location and starts the backup as per the schedule. The backup files are saved as a `.tar.gz` file in the specified location. The **Outputs** tab lists all the completed backups that are present in the backup and alternate backup locations.

If you want to delete a scheduled backup, click the **X** that is on the right side of the schedule name. You cannot delete the last backup, but you can clear the **Enable** checkbox to disable it.



Backing Up On Demand

You can back up the SANnav server data at any given moment to save the latest configurations.

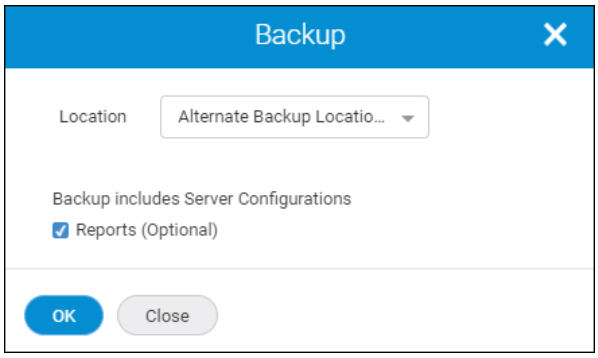
Required privilege: Server Backup with read/write permission.

For example, you can back up the application before you update the SANnav version. If the upgrade does not complete successfully or if the existing data is corrupted or deleted, you can use the backup file to restore your data.

When backing up on demand, you select a location for the backup file to be saved. If a backup location has not already been configured, see Configuring a Backup File Location. Make sure that you check the disk space periodically so that your backups are successful.

1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Backup**.
2. Click **Backup Now** on the top-right corner of the window.
   The **Backup** dialog displays.

3. Select the backup location from the **Location** drop-down.
4. Select the optional **Reports** checkbox if you also want to back up reports.



5. Click **OK**.

   The backup starts immediately. The **Backup Now** button is deactivated while the backup is in progress. The backup files are saved as a `.tar.gz` file in the selected location. You can view the list of on-demand backup files in the **Outputs** tab.

   Application events are generated when the backup completes or if the backup fails.

Managing and Deleting SANnav Backup Files

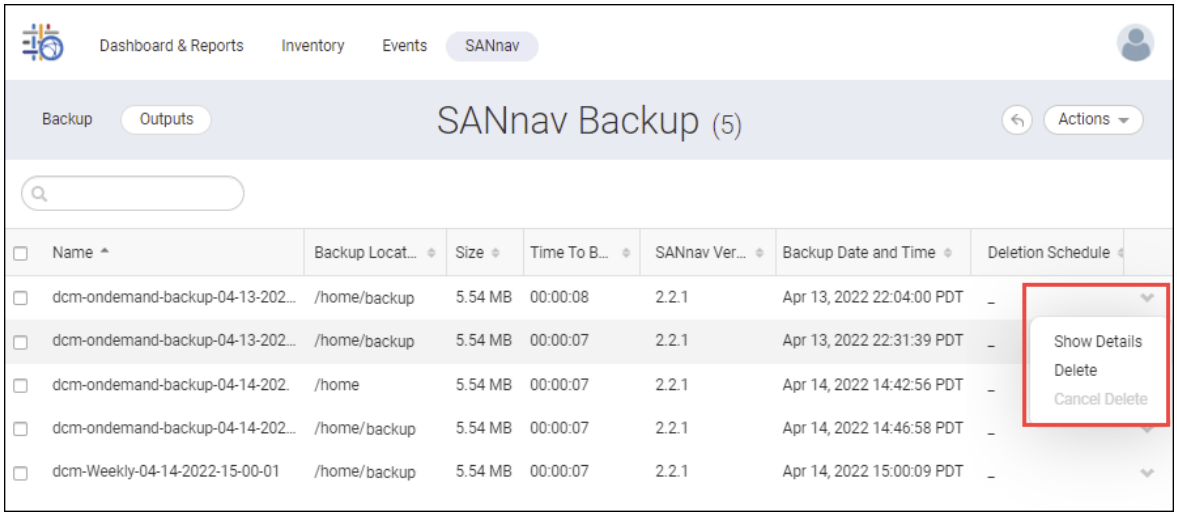
Backup files can use a lot of disk space. Periodically check the list of saved backups, and delete the ones that you do not need.

Required privilege: Server Backup with read/write permission.

You can delete backup files on-demand, or you can schedule a backup file to be deleted at a future time.

1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Backup**.
2. Click the **Outputs** tab.

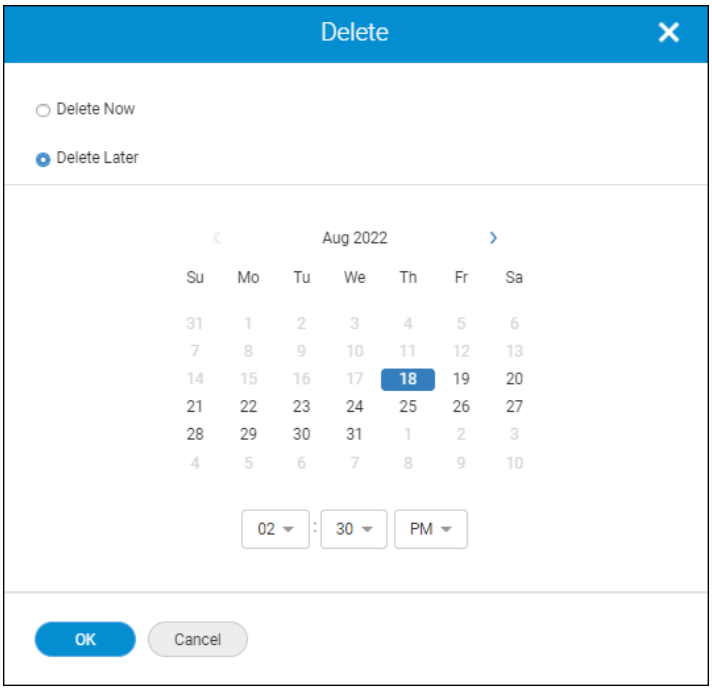
   The **Outputs** page displays a list of all the backup files that are present in the configured backup locations. If backup files are moved from the configured locations, they are not displayed in the **Outputs** page.



3. To see the list of items included in the backup, click the down arrow to the right of a table entry and select **Show Details**.
4. To delete a backup file that is not already scheduled for deletion, perform the following steps:
   a) Click the down arrow and select **Delete**.

      You can also select multiple backup files and select **Delete** from the **Actions** menu in the top-right corner.
   b) Select either **Delete Now** or **Delete Later** in the **Delete** dialog.

      If you select **Delete Later**, you must also select the date and time when the backup files will be deleted.



   c) Click **OK** in the confirmation dialog.

      Deleted backup files are removed from the **SANnav Backup** page. For backup files that are scheduled for deletion later, the **Deletion Schedule** column indicates the date and time when the files will be deleted. This column is empty if the backup files are not scheduled for deletion.
5. To cancel a future backup file deletion, click the down arrow and select **Cancel Delete**.

   The **Cancel Delete** option is available only when a deletion is scheduled.

Application events are raised if you delete a backup file, schedule a backup file for deletion later, or cancel a backup file deletion.

Restoring SANnav Backup Files

Restoration is done using a command line interface (CLI) script. You cannot use the SANnav user interface to restore the backup files.

Required privilege: Server Backup with read/write permission.

The restoration process stops all SANnav services, restores the data from the backup files, and then restarts the SANnav services.

NOTE

- During a restore process, the ports that are configured in the backup server are carried over to the restore server. SANnav provides custom port input if the existing ports are unoccupied.
- SANnav does not restore the license nor any license-related attributes, such as port count and expiration date. The license on the restore server remains the same after the restore process completes.

The restoration time depends on the size of the backup file.

NOTE
Before you start the restore process, ensure that all users log out from SANnav.

Restrictions for Restoration

- Both the backup server and the restore server must have the same main SANnav version and build.
- Patch versions can be different on the backup server and the restore server, as long as the main version is the same. The patch version of the backup must be higher than or the same as the patch version of the restore server. For example, you can restore a 2.2.xb backup on a 2.2.xa server.
- Both the backup server and the restore server must have the same IP configuration type (IPv4 or IPv6).

To restore the backup file using a CLI script, perform the following steps:

1. Log in to the SANnav server, and go to `<install_home>/bin/backuprestore`.
   Log in using an account with administrator privilege.
2. Run the `./restore.sh` script, and provide the full path to the backup file, including the file name.
   The backup file must be a `.tar.gz` file and must have been previously generated from the SANnav user interface. The backup file contains a checksum file, which ensures that the file is not corrupted and is a valid backup file.

   ```
   ./restore.sh <backup_file_path> true
   ```

3. If you also want to restore self-signed and third-party certificates, respond **Yes** when prompted.
   The default is to not restore certificates.
4. When the restore is complete, wait a few minutes for the SANnav services to start.
   See Checking the Server Health to check the status of the services.

If the backup server uses LDAP as the primary authentication method and you do not have a DNS server, contact Technical Support for assistance in adding the LDAP server to the restore server after the restore is complete.

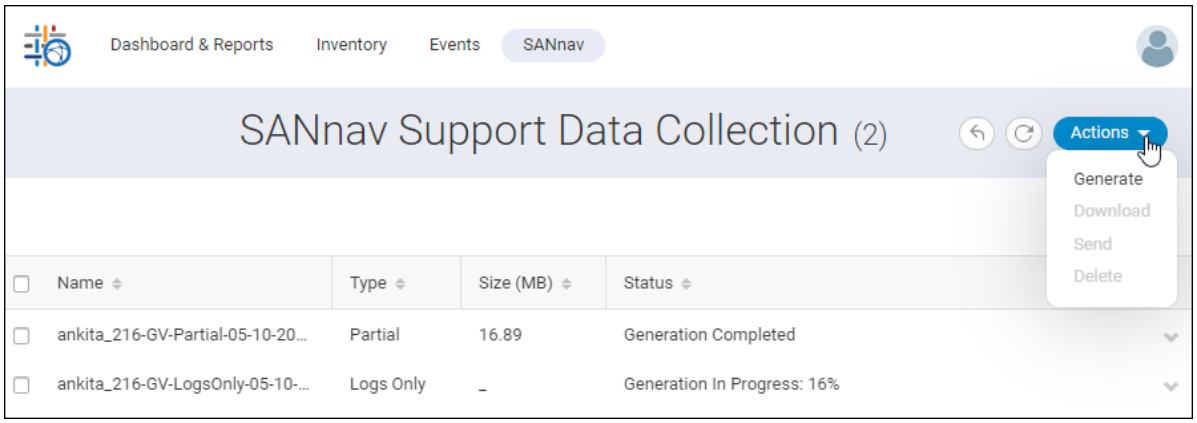
Global View Support Data Collection

Similar to SANnav Management Portal, SANnav Global View enables you to collect support data from the SANnav Global View server for offline analysis. You can collect only logs or both logs and the database. Generated files are saved for 30 days.

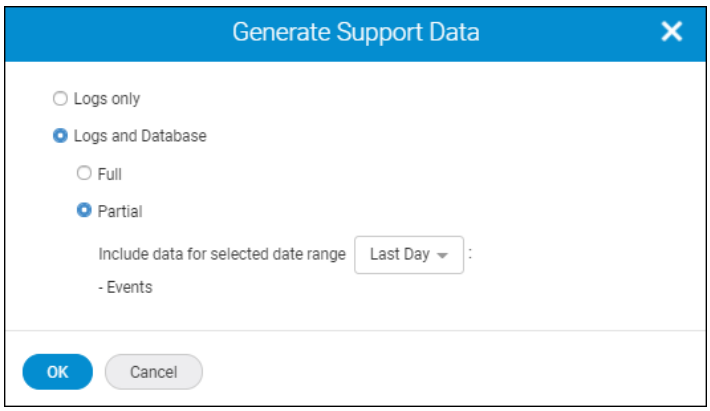
The following steps show how to perform SANnav Global View support data collection:

1. Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Support Data Collection**.
   From the **SANnav Support Data Collection** page, you can collect data, download data collection files to offline storage, and send them to an external FTP server.

2. To generate support data, click the **Actions** menu, and then select **Generate**.



3. Select whether to generate logs only or both logs and the database, and click **OK**.



After some time, the generated support data collection file appears in the list. You may need to refresh your browser.

The **Status** column indicates the progression of the collection. The status does not update dynamically. You must click the refresh button in the upper-right corner of the page to see the updated status.

4. To download a data collection file to offline storage, select the file and click **Download** from the **Actions** menu.

5. To forward a data collection file to an external server, select the file and click **Send** from the **Actions** menu.
   The FTP, SFTP, and SCP protocols are supported for sending the file.

Checking the Server Health

After the installation is complete, you can check the health of the SANnav server using the `check-sannav-status.sh` script. If any of the services is down, it is listed in the script output.

To check the health of the server, go to the `<install_home>/bin` folder, and run the following script:

```
./check-sannav-status.sh
```

The following sample output is from a healthy server:

```
-bash-4.2# sh ./check-sannav-status.sh
SANnav server is healthy. All the services are currently in running state.
```

The following sample output is from an unhealthy server:

```
-bash-4.2# sh ./check-sannav-status.sh
Following services are currently down
authentication-rbac-middleware
dashboard-middleware
license-mw
asyncjobscheduler-worker
dashboard-summaryprovider
```

NOTE

If any service is found down while checking the server health status, it is automatically started by the system monitor within 20 minutes.

Revision History

The revision history provides a list of the significant changes in each version of the document.

SANnav-22x-GV-UG101; October 5, 2022

- Added the section Features Affected by Upgrade and Migration.
- Moved the "Installation and Upgrade" chapter to a separate document, the *Brocade SANnav Global View Installation and Upgrade Guide*.

SANnav-22x-GV-UG100; June 22, 2022

Initial document version.

Documentation Legal Notice

This notice provides copyright and trademark information as well as legal disclaimers.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, to view the licensing terms applicable to the open source software, and to obtain a copy of the programming source code, please download the open source disclosure documents in the Broadcom Customer Support Portal (CSP). If you do not have a CSP account or are unable to log in, please contact your support provider for this information.


BROADCOM®