

Administration

This chapter has details about the profiles and users of the Cisco Nexus Dashboard Data Broker.

Beginning with Release 3.10.1, Cisco Nexus Data Broker (NDB) has been renamed to Cisco Nexus Dashboard Data Broker. However, some instances of NDB are present in this document, to correspond with the GUI, and installation folder structure. References of NDB/ Nexus Data Broker/ Nexus Dashboard Data Broker can be used interchangeably.

- AAA , on page 1
- Backup/ Restore, on page 4
- Transport Layer Security , on page 7
- Cluster, on page 8
- Profile, on page 9
- Slices, on page 11
- System Information, on page 13
- User Management, on page 14

AAA

The **AAA** tab displays details of the AAA servers available on the Nexus Dashboard Data Broker. For more details about AAA servers, see About AAA Servers, on page 4.

A table with the following details is displayed:

Column Name	Description
Server Address	The IP address of the AAA server.
Protocol	The protocol running on the server. The options are: • TACACS • RADIUS+ • LDAP

The following actions can be performed from the **AAA** tab:

- **Add Server**—Use this to add a new AAA server. See Adding an AAA Server, on page 2 for the detailed procedure.

- **Delete Server**—Select the server(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete AAA Server**. The selected server(s) is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a server.

Adding an AAA Server

Use this procedure to add an AAA server.

Procedure

Step 1 Navigate to **Administration** > **AAA**.

Step 2 From the **Actions** drop down menu, select **Add AAA Server**.

Step 3 In the **Add AAA Server** dialog box, enter the following details:

Table 1: Add AAA Server

Field	Description
General	
Protocol	Choose a protocol for the AAA server. • Radius • LDAP • TACACS The fields relevant for each option are discussed below.
Protocol: Radius	
Server Address	Server IP address or domain name.
Secret	Secret configured on the AAA server.
Protocol: LDAP	
Server Address	Server IP address or domain name.
Port	Communication port for the AAA server.

Field	Description
User RDN	Enter the Relative Distinguished Name (RDN) , used to authenticate with the LDAP server. User hierarchy defined in the LDAP server. Example: While configuring LDAP in AAA, consider the following hierarchy (defined in LDAP), for user "cn=admin,ou=People,dc=ndb,dc=local", user RDN should be "ou=People,dc=ndb,dc=local". After NDB is configured with LDAP, then to login, only the *cn* value has to be provided for the username. In this case, username is "admin".
Role Attribute	Enter the role attribute which is the LDAP authorization attribute for users. Role Attribute can be any attribute in LDAP for the DN. For example, let *sn* be the defined role-attribute in the local LDAP server. So, for *admin user* in NDB, you can have "network-admin" as a value for the *sn* attribute. When NDB contacts the LDAP sever with the Role Attribute and User RDN and *admin user*, LDAP returns the *sn* value ("network-admin") as authentication.
Role Type Mapping	Click the button to enable Default setting. A list of **Role Mapping** values are displayed. If you have enabled **Default**, then, the following are the existing mapped values: • network-admin—*network-admin* • network-operator—*network-operator* • application-user—*application-user* • slice-user—*slice-user* Disable **Default**, to provide custom mapping of roles with values defined in LDAP. Select a role from the drop down list in the **Role Mapping** column, and enter a value defined in LDAP in the **Role Type Mapping** column. Click **Add Row** to add more Role Type Mapping rows.
Timeout	Enter the wait time by which the LDAP server should respond.
Protocol: TACACS+	
Server Address	TACACS+ server address.
Secret	Secret configured on the TACACS+ server.
Username	Username to login to the server.

Field	Description
Password	Password to login to the server.
Check Server	Click **Check Server** to check if the server is reachable and the authentication credentials are valid.

Note
It is not recommended to change the admin password of the ndb controller when the user management of the ndb controller is performed through TACACS or AAA.

Step 4 Click **Add AAA Server** to add the server.

What to do next

If you chose RADIUS as the protocol for the AAA server, you need to configure user authentication for RADIUS.

Configuring User Authentication for RADIUS Server

User authorization on a RADIUS server must conform to the Cisco Attribute-Value (av-pair) format. In the RADIUS server, configure the Cisco av-pair attribute for a user as follows:

```
shell:roles="Network-Admin Slice-Admin"
```

About AAA Servers

AAA enables the security appliance to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting). Cisco Nexus Dashboard Data Broker uses Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to communicate with an AAA server.

AAA server supports remote authentication and authorization. To authenticate each user, Cisco Nexus Dashboard Data Broker uses both the login credentials and an attribute-value (AV) pair. An AV pair assigns the authorized role for the user as part of the user administration. After successful authentication, the Cisco AV pair is returned to Cisco Nexus Dashboard Data Broker for resource access authorization.

Backup/ Restore

The **Backup/ Restore** tab has two subtabs:

- **Scheduled Backups**—for details of the schedule of backup(s) on the Nexus Dashboard Data Broker controller, see Schedule of Backups, on page 5.
- **Backups** —for details of completed backups on the Nexus Dashboard Data Broker controller, see Backups, on page 6.

Schedule of Backups

The **Schedule of Backups** tab displays details of the scheduled backups for the Nexus Dashboard Data Broker controller.

A table with the following details is displayed:

Table 2: Backup

Column Name	Description
Start Date	The start date for the backup.
Start Time	The start time for the backup.
End Date	The end date for the backup.
Pattern	The backup pattern. Options are: • Daily • Weekly • Monthly
Occurences	Number of occurrences based on the selected pattern.

The following actions can be performed from the **Backup** tab:

- **Schedule Backup**—Use this to schedule a backup. See Scheduling Backup, on page 5 .
- **Backup Locally**—Configuration is backed up on your local machine.
- **Restore Locally**—In the **Restore Locally** window that appears, choose a file from your local machine to restore the configuration.

  Select the **Restore** check-box if you want Nexus Dashboard Data Broker to re-configure the configurations of the device, from the uploaded backup after Nexus Dashboard Data Broker is restarted. The following configurations are reconfigured:

  - Global Configurations
  - Port Configurations
  - UDF
  - Connections

  The **Restore** check-box is applicable only for configuration downloaded from NDB Release 3.8 and above.

Scheduling Backup

Use this procedure to schedule a backup.

It is always recommended to take a backup before upgrading to the next Nexus Dashboard Data Broker version.

Procedure

Step 1 Navigate to **Administration** > **Backup / Restore**.

Step 2 From the **Actions** drop-down list, select **Schedule Backup**.

Step 3 In the **Schedule Backup** dialog box, enter the following details:

Table 3: Schedule Backup

Field	Description
Schedule	
Start Date	Enter the start date for the backup.
Start Time	Enter the start time for the backup.
Repeat	Select one of the options: • **Daily**—the backup operation occurs daily. • **Weekly**—the backup operation occurs on the selected day of the week, every week. • **Monthly**—the backup operation starts on the selected date every month. **Note** Check the **Last Day** check-box for the backup to be perfomed till the end of the selected month.
End	Select one of the options to stop the backup process: • **No End Date**—continue taking back up. • **End Date** —continue taking backup till the specified end date. • **Occurences** —takes backup based on the number selected in the **Number of Occurrences** field.
Enable	The **Enable** check box is selected by default. Leave the check box checked, to enable the backup per the schedule.

Step 4 Click **Schedule**.

Backups

The **Backups** tab displays the backup information.

The information displayed here is based on the schedule generated using Scheduling Backup. A table with the following details is displayed:

Column Name	Description
Item	Time of backup.
Cluster Backup Status	Cluster backup status of the Nexus Dashboard Data Broker controller. Options are: • Success • Failure
Description	Description of the backup.
Restore Triggers	Timestamp when the restore backup was triggered.

The following actions can be performed from the **Backups** tab:

- **Backup to NDB Server**—Backup is created at the specified time in the NDB server. After you select this option, the backup details appear in the **Backups** tab.
- **Restore Backup**—The selected backup is restored on the Nexus Dashboard Data Broker controller. It is recommended to always choose the latest backup for restoration. If you choose an old backup, there could be connection failures based on recent topology changes.

Note Restart the Nexus Dashboard Data Broker controller after restoring a backup.

- **Delete Backup**—Select the backup(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Backup(s)**.

Transport Layer Security

From release 3.10.5, you can enable Transport Layer Security (TLS) using the GUI. If you already have the KeyStore and TrustStore which have the certificates, then, see the Upload TLS files, on page 7 procedure.

Upload TLS files

Use this procedure to sync your existing KeyStore and TrustStore files with the data broker controller.

Before you begin

Keep the KeyStore and TrustStore files ready.

Procedure

Step 1 Navigate to **Administration** > **TLS** > **Actions** > **Upload TLS Files**.

Step 2 On the **Enable Transport Layer Security** screen that is displayed, enter the following:

- Enable method: you can upload from a server or from a local path.
- KeyStore: drag and drop the KeyStore file.
- Password: enter the password for the KeyStore file.
- TrustStore: drag and drop the TrustStore file.
- Password: enter the password for the TrustStore file.

Step 3 Click **Save**.

Cluster

The **Cluster** tab displays details of the clusters available on the Nexus Dashboard Data Broker controller. Nexus Dashboard Data Broker supports high availability clustering in active/active mode with up to five controllers in a cluster.

A table with the following details is displayed:

Column Name	Description
Controller	The IP address of the controller.
Type	Displayed options are either **Primary** or **Member**.

Note For the backup and upload features to work properly, all the servers in the cluster should be stopped and then they should be restarted. You should not configure any functionality during this time. Once the upload configuration is done, you should not configure anything from any other nodes in the cluster as it might lead to inconsistencies in the data.

Note After a backup is uploaded, all the instances of the cluster should be shut down and the server on which the backup is uploaded should be started first.

Profile

The **Profiles** tab displays details of the profiles available on the Nexus Dashboard Data Broker controller. A profile allows you to manage multiple devices associated to an Nexus Dashboard Data Broker controller. You can attach multiple devices to a profile.

The profile configuration is applied to all the member switches.

A table with the following details is displayed:

Column Name	Description
Profile Name	Name of the profile.
User Name	User name that created the profile.

Use the *Filter by attributes* bar to filter the table based on displayed filter details. Choose the attribute, operator and filter-value.

The following actions can be performed from the **Profiles** tab:

- **Add Profile**—Use this to add a new profile. See *Add Profile* for details about this task.
- **Delete Profile**—Select the required profile(s) by checking the check box which is at the beginning of the row and then click **Delete Profile**. The selected profile(s) are deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a profile.

Note A profile which is in use cannot be deleted.

Adding a Profile

Use this procedure to add a new profile.

Procedure

Step 1 Navigate to **Administration** > **Profile**.

Step 2 From the **Actions** drop down menu, select **Add Profile**.

Step 3 In the **Add Profile** dialog box, enter the following details:

Table 4: Add Profile

Field	Description
Profile Name	Enter a profile name.
Username	Enter a user name to login to the device.

Field	Description
Password	Enter a password for the username. Passwords must be between 8 and 256 characters long, contain uppercase and lowercase characters, have at least one numeric character, and have at least one non-alphanumeric character.

Step 4 Click **Add Profile** to create the profile.

Editing a Profile

Use ths procedure to edit a profile.



Note When you edit a profile, devices that are using the profile will be reconnected.

Before you begin

Create one or more profiles.

Procedure

Step 1 Navigate to **Administration** > **Profiles**.

Step 2 In the displayed table, click a **Profile Name**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Profile**.

Step 4 In the **Edit Profile** dialog box, the current profile information is displayed. Modify these fields, as required:

Table 5: Edit Profile

Field	Description
Profile Name	Profile name is displayed and can not be changed.
Username	Enter a username to login to the device.
Password	Enter a password for the username. Passwords must be between 8 and 256 characters long, contain uppercase and lowercase characters, have at least one numeric character, and have at least one non-alphanumeric character.

Step 5 Click **Save** to edit the profile.

Slices

The **Slices** tab displays details of the slices available on the Nexus Dashboard Data Broker.

Slicing enables you to partition a network into many logical networks. For more information, see About Slices, on page 13.

To view a different network partition, switch the slice using the **Slice** button in the header. As part of the initial Nexus Dashboard Data Broker build, one slice is available and is called the **Default** slice. The following configurations can be performed only on the default slice of the Nexus Dashboard Data Broker controller:

- Adding a new device
- Editing global configurations for devices
- Changing profiles for users
- Changing the parameters for users and associated roles
- Fixing inconsistent device and connection flows

A table with the following details is displayed:

Column Name	Description
Slice	Name of the slice. This field is a hyperlink. Click the **Slice** name and a new pane is displayed on the right. Additional actions that can be performed from here: • Editing a Slice
Configured Port(s)	Ports of a device (or different devices) that are currently part of the slice.
Available Port(s)	Ports of a device (or different devices) that are currently not part of the slice, but can be added to the slice.

You can perform the following actions from the **Slices** tab:

- **Add Slice**—For details about this action, see Adding a Slice.
- **Delete Slice**—Select the slices to be deleted and click **Actions** > **Delete Slice(s)**. If you choose the delete action, without selecting a check box, an error is displayed and you will be prompted to select a slice.

Adding a Slice

Use this procedure to add a slice.

Note A device can be a part of multiple slices; a port can be a part of only one slice at any given time.

Before you begin

Clear all port configurations and connections of a device which is already a part of the default slice, before adding the ports of a device to a new slice.

Procedure

Step 1 Navigate to **Administration** > **Slices**.

Step 2 From the **Actions** drop down menu, select **Add Slice**.

Step 3 In the **Add Slice** dialog box, enter the following details:

Table 6: Add Slice

Field	Description
General	
Slice Name	Enter a name for the slice.
Port	Click **Select Ports** and in the **Select Ports** window, select the device and required ports. **Note** Ensure to have all the ports of a device on the same slice.

Step 4 Click **Add Slice** to create the slice.

Note
After a new slice is added, the default slice is in *read-only* mode. If an active port configuration and/or connection is present on the default slice, then, it is rendered unavailable.

The devices added to a slice are displayed in the slice. For example, if device D1 is added to slice S1, and if the device goes into maintenance mode (or failed state or not ready state), the device is no longer displayed on S1, but is displayed on the default slice.

Editing a Slice

Use this procedure to edit a slice.

Before you begin

Delete the port configurations for a port before deleting the port from a slice.

Procedure

Step 1 Navigate to **Administration** > **Slices**.

Step 2 Click a **Slice** name. A new window opens on the right.

Step 3 Click **Action** > **Edit Slice**.

The **Edit Slice** window is displayed.

Step 4 Make required changes in the **Edit Slice** window. The following details are displayed:

Table 7: Edit Slice

Field	Description
General	
Slice Name	Name for the slice. This field cannot be changed.
Port	The ports that are part of the slice are listed. You can delete / add as required.

Step 5 Click **Save**.

About Slices

Slices enables you to partition networks into many logical networks. This feature allows you to create multiple disjoint networks and assign different roles and access levels to each one. Each logical network can be assigned to departments, groups of individuals, or applications.Multiple disjoint networks can be managed using the Cisco Nexus Dashboard Data Broker application.

Slices are created based on the following criteria:

- Network devices—The devices that can be used in the slice. Network devices can be shared between slices.
- Network device interfaces—The device interfaces that can be used in the slice. Network device interfaces can be shared between slices.

Slices must be created by a Cisco Nexus Dashboard Data Broker user with the Network Administrator role. After creation,the slices can be managed by a user with the Slice Administrator role.

System Information

The **System Information** tab displays all the information about the Nexus Dashboard Data Broker controller and the Nexus Dashboard Data Broker controller host. The information is available under two headings:

- **NDB Information** —includes information such as Installation Type, Current Build Number, Previous Build number, etc.
- **System Information**—includes information such as Total Memory, Physical Memory, Used Memory, Free Memory of the Nexus Dashboard Data Broker controller host.

User Management

The **User Management** tab has the following subtabs:

- **Users**—users of Nexus Dashboard Data Broker controller. See Users for more details.
- **Roles**—roles that the users are assigned to. See Roles for more details.
- **Groups**—device groups that the ports are assigned to. See Groups for more details.

Users

The **Users** tab displays the details of the users of the Nexus Dashboard Data Broker controller.

A table with the following details is displayed:

Column Name	Description
User	The login name of the user. This field is a hyperlink. Click **User** and a new pane is displayed on the right. The following additional actions can be performed from here: • Change Password • Change Role • **Delete User** **Note** If you are logged in as the default *admin* user, the **Delete User** and **Change Role**options are not available. If you have logged in using TACACS, the **Change Password** option is not available.
Role	The role of the user that was assigned while creating the user.

The following actions can be performed from the **Users** tab:

- **Add User**—Use this to add a new user. See Adding a User for details about this task.
- **Delete User**—Select the user(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Delete User**. The selected user(s) are deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a user.

Adding a User

Use this procedure to add a new user.

Before you begin

Create role(s) that the new user can be assigned to.

Procedure

Step 1 Navigate to **Administration** > **User Management** > **Users**.

Step 2 From the **Actions** drop down menu, select **Add User**.

Step 3 In the **Add User** dialog box, enter the following details:

Table 8: Add User

Field	Description
Username	Enter the user name.
Password	Enter a password for the user. Passwords must be between 8 and 256 characters long, contain uppercase and lowercase characters, have at least one numeric character, and have at least one non-alphanumeric character.
Verify Password	Verify the password by re-entering it.
Choose User Type	Select one of the options: • **Regular User**—can login to the NDB controller without a slice (default slice). • **Slice User**—has access only to a specific slice.
Select Slice This field is applicable only when the User Type is **Slice User**.	Select a slice from the drop-down list. The created user has access only to the selected slice.
Set Role This field is applicable only when the User Type is **Regular User**.	Click **Select Role**. In the **Select Role** dialog box that opens, check the check box for the role(s) you want to assign to the user. The role details are displayed on the right side. Click **Select** to assign the role. You can assign more than one role to a user. The available role options are: • Network Admin—Provides full administrative privileges to all applications. • Network Operator—Provides read-only privileges to all applications.

Step 4 Click **Add User** to add the user.

Note
After creating a user, you can change the password, but you cannot change the roles assigned to the user.

Changing Password for a User

Use this procedure to change the password for a user.

Before you begin

Create one or more users.

Procedure

Step 1 Navigate to **Administration** > **User Management** > **Users**.

Step 2 Click a **User** name. A new window opens on the right.

Step 3 Click **Action** > **Change Password**.

The **Change Password** window is displayed.

Step 4 Make required changes in the **Change Password** window. The following details are displayed:

Table 9: Change Password

Field	Description
General	
User Name	Name of the user. This field cannot be changed.
Current Password	Enter the current password for the username. **Note** This field is displayed only for *admin* user.
Password	Enter the new password.
Verify Password	Enter the new password again.

Step 5 Click **Change Password**.

Changing Role for a User

Use this procedure to change the role of a user.

Before you begin

Create one or more users.

Procedure

Step 1 Navigate to **Administration** > **User Management** > **Users**.

Step 2 Click a **User** name. A new window opens on the right.

Step 3 Click **Action** > **Change Role**.

The **Change Role** window is displayed.

Step 4 Make required changes in the **Change Role** window. The following details are displayed:

Table 10: Change Role

Field	Description
General	
User Name	Name of the user. This field cannot be changed.
Choose User Type	Select either **Regular User** or **Slice User**.
Select Slice	Select an option from the drop down list. This option is displayed only if your User Type selection was **Slice User**.
Select Role	Click **Select Role** and the **Select Role** window is displayed. Choose a role using the radio button and click **Select** . This option is displayed only if your User Type selection was **Regular User**.

Step 5 Click **Save**.

Roles

The **Roles** tab displays details of the roles available on the Nexus Dashboard Data Broker controller. The default roles are:

- Network-Admin
- Network-Operator

A table is displayed with the following details:

Column Name	Description
Role	The name of the role. The displayed name is a hyperlink. Click the **Role** name, a new pane is displayed on the right. Additional actions that can be performed from here are: • Assigning a Group
Level	The level assigned to the role. The following levels are available: • App-Administrator— Has full access to all data broker resources but the App-Administrator cannot add NXAPI or production devices into Nexus Dashboard Data Broker because Administration tab is not available in Nexus Dashboard Data Broker for App-Administrator role . • App-User—Has access to create, edit, clone, or delete connections and redirections that are assigned to his resource group and resources that are created by another user with similar permissions. An App-User can only view Edge-SPAN, Tap, Monitoring device, and Production ports. An App-User can view resources that are created by another user with similar permissions in Toplogy page of Nexus Dashboard Data Broker. But, you can not configure Edge-SPAN or Connections created by another App-User. • App-Operator—Has access for read-only operations.
Group	The group assigned to the role.

The following actions can be performed from the **Roles** tab:

- **Add Role**—Use this to add a new role. See Add Role for details about this task.
- **Delete Role**—Select the roles to be deleted by checking the check box which is available at the beginning of the row and then click **Delete Role** from the **Actions** menu. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a role.

Note Default roles cannot be deleted.

Adding a Role

Use this procedure to add a role and associate the role to a group.

Before you begin

Create one or more groups to associate a role.

Procedure

Step 1 Navigate to **Administration** > **User Management** > **Roles**.

Step 2 From the **Actions** drop down menu, select **Add Role**.

Step 3 In the **Add Role** dialog box, enter the following details:

Table 11: Add Role

Field	Description
Role Name	Enter the role name.
Select Level	Select a level from the drop-down list.

Step 4 Click **Add** to add the role.

Assigning a Group to a Role

Use this procedure to assign a group to a role. This enables the role to access only the ports in the assigned group.

Before you begin

Add one or more groups.

Procedure

Step 1 Navigate to **Administration** > **User Management** > **Roles**.

Step 2 Click a **Role** name in the displayed table.

A new pane is displayed on the right.

Step 3 Click **Action** > **Assign Group**.

Enter the following details:

Table 12: Assign Group

Field	Description
Role Name	Role name. This field cannot be edited.
Select Level	Level of the role. This field cannot be edited.
Set Group	Click **Select Group** and select a group in the **Select Group** window that is displayed.

Step 4 Click **Assign**.

Groups

The **Groups** tab displays details of the port groups. The default group is:

- allPorts

A group can be a group of ports of one device or across many devices.

A table with the following details is displayed:

Column Name	Description
Group	The name of the group. The displayed name is a hyperlink. Click the name to see more details of the group.
Ports	The number of ports assigned to the group.

The following actions can be performed from the **Groups** tab:

- **Add Group**—Use this to add a new group. See Add Group for details.
- **Delete Group**—Select the groups to be deleted by checking the check box which is available at the beginning of the row and then click **Delete Group** from the **Actions** menu. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a group.

Note Default group(s) cannot be deleted.

Adding a Group

Use this procedure to create a new group.

A group is created for defining access to port(s) for a user. A group is assigned to a role; a user is associated to a role.

Procedure

Step 1 Navigate to **Administration** > **User Management** > **Groups**.

Step 2 From the **Actions** drop down menu, select **Add Group**.

Step 3 In the **Add Group** dialog box, enter the following details:

Table 13: Add Group

Field	Description
Group Name	Enter the group name.
Selected Port(s)	Click **Select Ports**. In the **Select Ports** dialog box that opens, check the check box to assign port(s) to the group. The port details are displayed on the right side. Click **Select** to assign the port.

Step 4 Click **Add Group** to add the group.