



Restricting Port Profile Visibility

This chapter contains the following sections:

- [Information About Restricting Port Profile Visibility, on page 1](#)
- [Guidelines and Limitations for Restricting Port Profile Visibility, on page 2](#)
- [Defining DVS Access in vSphere Client, on page 3](#)
- [Enabling the Port Profile Role Feature, on page 7](#)
- [Restricting Port Profile Visibility on the VSM, on page 8](#)
- [Removing a Port Profile Role, on page 10](#)
- [Feature History for Restricting Port Profile Visibility, on page 11](#)

Information About Restricting Port Profile Visibility

Port Profile Visibility

You can restrict which VMware vCenter users or user groups have visibility into specific port groups on the Cisco Nexus 1000V.

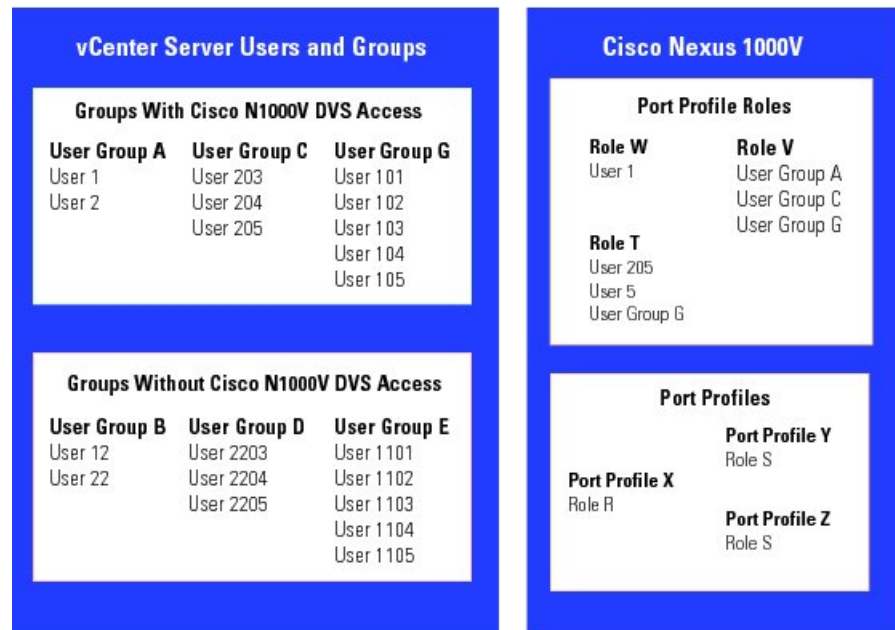
Before you can restrict the visibility of a port group, the server administrator must define which VMware vCenter users and user groups have access to the Cisco Nexus 1000V DVS top level folder in VMware vCenter Server. The network administrator can then further define the visibility of specific port groups on the Virtual Supervisor Module (VSM). This configuration on the VSM is then published to the VMware vCenter Server so that access to specific port groups is restricted.

Group or User Access

You can save the time of defining access on the VSM per user by, instead, adding new users to groups in VMware vCenter where access is already defined. Group members defined in VMware vCenter automatically gain access to the port groups defined for the group.

You can see in the following figure the relationship between users and groups in vCenter Server and port profiles and port profile roles in Cisco Nexus 1000V.

Figure 1: Port Profile Visibility: User, Groups, Roles, and Port Profiles



- Multiple users and groups can be assigned to a role.
- Only one role can be assigned to a port profile at a time.
- A role can be assigned to multiple port profiles.
- Up to 256 port profile roles are allowed per VSM.
- A total of 16 users and groups are allowed per role.

2830133

Guidelines and Limitations for Restricting Port Profile Visibility

- The server administrator does not propagate access from the DVS down to lower folders. Instead, port group access is defined by the network administrator on the VSM and then published to the VMware vCenter Server.
- The Cisco Nexus 1000V VSM must be connected to the VMware vCenter Server before port profile roles are created or assigned. If this connection is not in place when port profile visibility is updated on the VSM, it is not published to VMware vCenter Server and is not affected.
- The following are guidelines for port profile roles on the VSM:
 - You cannot remove a port profile role if a port profile is assigned to it. You must first remove the role from the port profile.
 - Multiple users and groups can be assigned to a role.
 - Only one role can be assigned to a port profile.
 - A role can be assigned to multiple port profiles.
- You can define up to 256 port profile roles per VSM.
- You can define a total of 16 users and groups per role.

Defining DVS Access in vSphere Client

The server administrator can use this procedure to allow access to the top level Cisco Nexus 1000V DVS folder in vSphere client.

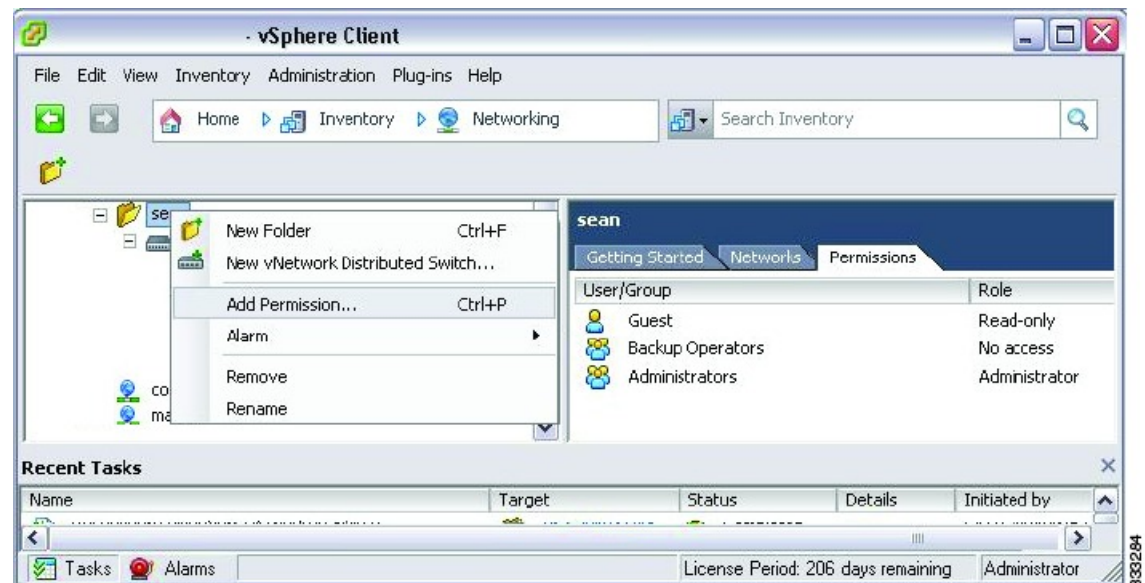
Before you begin

- You are logged in to the vSphere Client.
- You know which users or groups need access to the DVS.
- This procedure defines who can access the Cisco Nexus 1000V DVS. Access to individual port groups is done on the VSM; see [Restricting Port Profile Visibility on the VSM, on page 8](#).

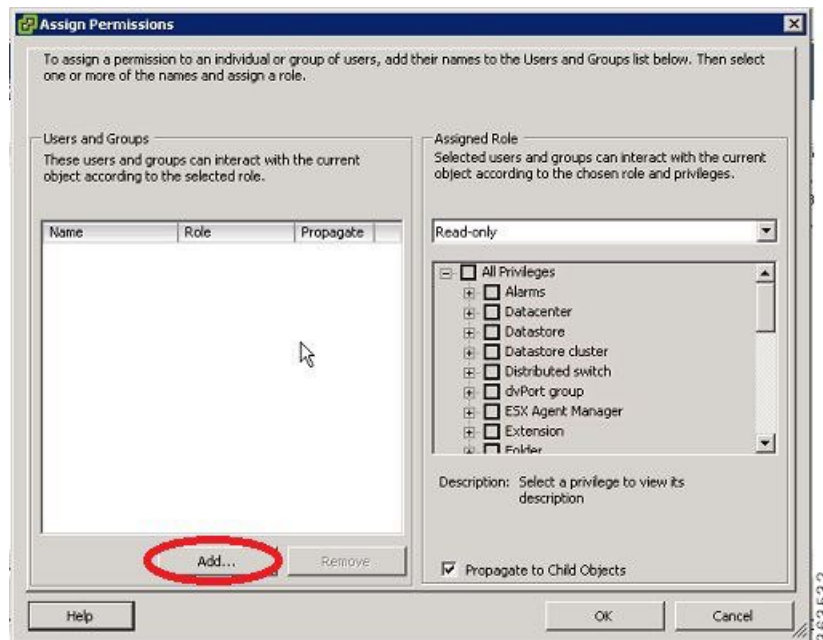
Procedure

Step 1 In the **vSphere Client** window, do the following:

- Choose **Inventory > Networking**.
- Right-click a DVS folder object and choose **Add Permission**.

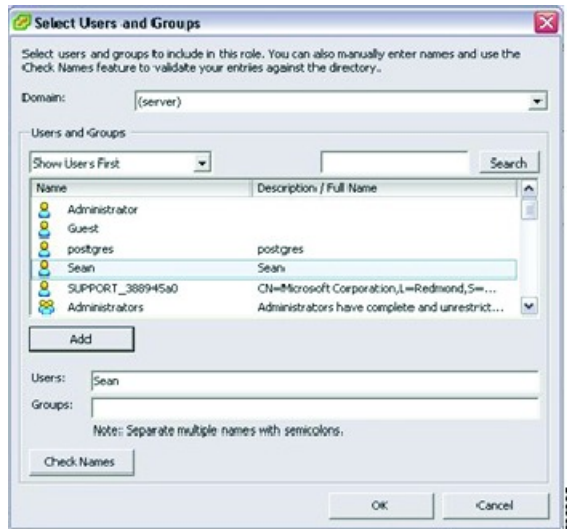


Step 2 In the **Assign Permissions** window, click **Add**.



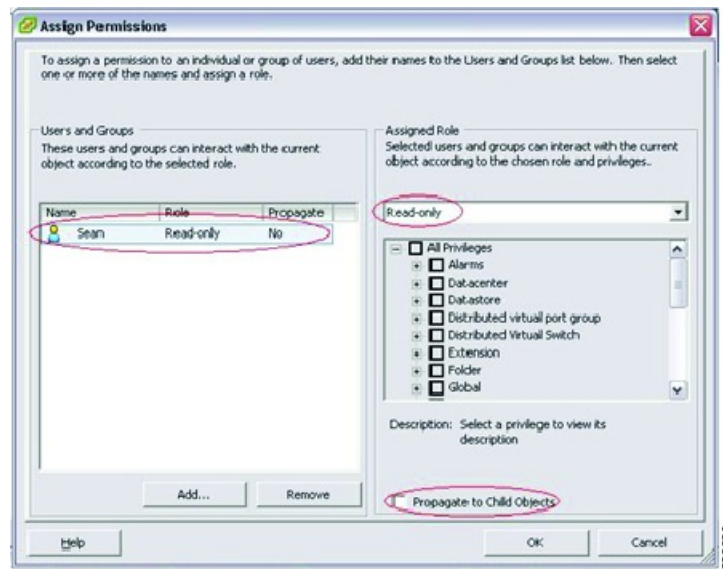
Step 3 In the **Select Users and Groups** window, do the following:

- Choose the name from the list of users and groups.
- Click **Add**.
- Click **OK**.



Step 4 In the **Assign Permissions** window, do the following:

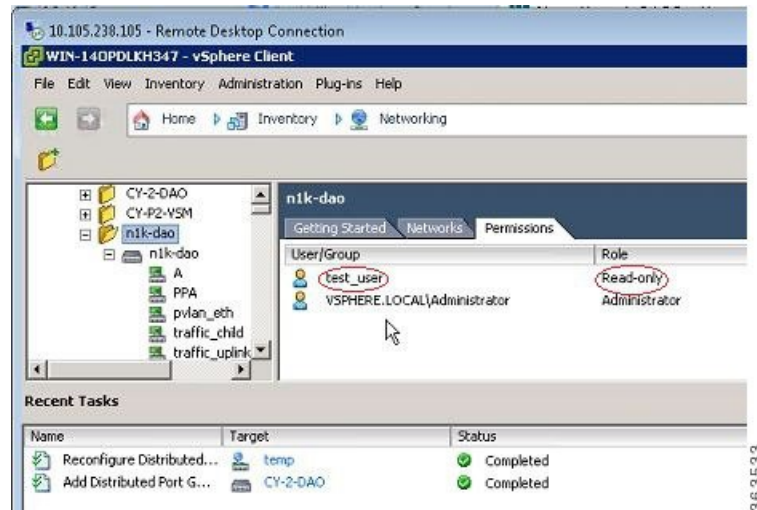
- From the **Assigned Role** selection list, choose a role for this user or group.
- Make sure that the **Propagate to Child Objects** check box is unchecked.
- Click **OK**.



The user is granted the same access to the DVS object.

Note Do not propagate the role definition here. Specific port group access is configured on the VSM, which is then pushed to vSphere Client.

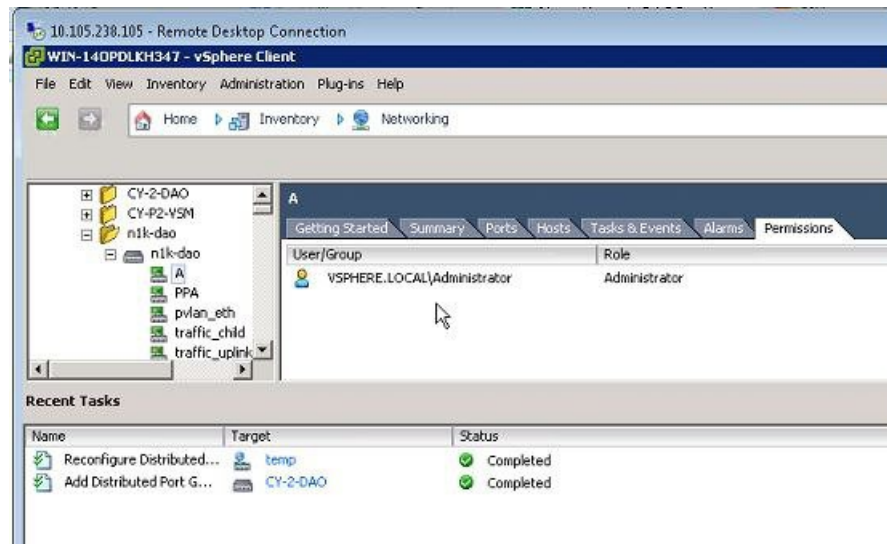
Step 5 (Optional) In the **vSphere Client** window, click the **Permissions** tab.



In the example shown, the user is granted read-only access to the DVS folder object and eventually the DVS object.

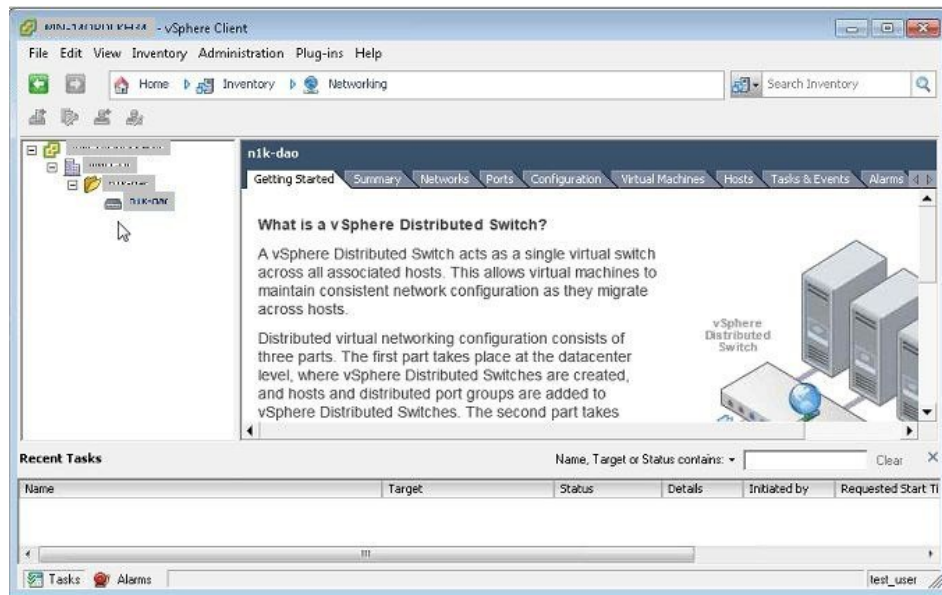
Step 6 (Optional) In the **vSphere Client** window, under the same DVS object, do the following:

- Click any port profile.
- Click the **Permissions** tab.



In the example shown, note that the new user is not listed under the **Permissions** tab for port profiles. Access to individual port profile groups is given on the VSM; see [Restricting Port Profile Visibility on the VSM, on page 8](#).

- Step 7** (Optional) Log in to vSphere Client using the new user login credentials. vSphere client shows the list of port profiles the user has access to for any DVS object.



In the example shown, note that no port profiles are listed under the DVS object for the new user.

You can now access the top-level Cisco Nexus 1000V DVS folder according to the assigned role.



Note To restrict access to specific port groups, go to [Restricting Port Profile Visibility on the VSM, on page 8](#).

Enabling the Port Profile Role Feature

Before you begin

You are logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# feature port-profile-role	Enables the port profile roles feature to restrict user and group access.
Step 3	(Optional) switch(config)# show feature	Displays the configuration for verification.
Step 4	(Optional) switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable the port profile role feature:

```
switch# configure terminal
switch(config)# feature port-profile-role adminUser
switch(config)# show feature
Feature Name      Instance  State
-----
dhcp-snooping    1         enabled
http-server      1         enabled
ippool           1         enabled
lACP              1         enabled
lisp             1         enabled
lisphelper       1         enabled
netflow          1         disabled
port-profile-roles 1         enabled
private-vlan     1         disabled
sshServer        1         enabled
tacacs           1         enabled
telnetServer     1         enabled
switch(config)# copy running-config startup-config
```

Restricting Port Profile Visibility on the VSM

The network administrator can use this procedure to create a role for restricting port profile visibility on the VSM, which is then pushed to vCenter Server.

Before you begin

- You are logged in to the CLI in EXEC mode.
- You know which users or groups should have access to the role that you are creating.
- You have already created the users and groups to be assigned to this role in vCenter and have access to the Cisco Nexus 1000V DVS folder where the VSM resides. See [Defining DVS Access in vSphere Client, on page 3](#).
- You have enabled the port profile role feature. See [Enabling the Port Profile Role Feature, on page 7](#).
- You have identified the characteristics needed for this role:
 - Role name
 - Role description
 - Users to assign
 - Groups to assign
 - Port profile to assign

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# port-profile-role <i>role-name</i>	Enters port profile role configuration mode for the named role. If the role does not already exist, it is created with the following characteristic: <ul style="list-style-type: none"> • <i>role-name</i>—The role name can contain up to 32 alphanumeric characters and must be unique for each role on the Cisco Nexus 1000V.
Step 3	(Optional) switch(config-port-prof-role)# description <i>role-description</i>	Adds a description of up to 32 characters to the role. This description is automatically pushed to vCenter Server.
Step 4	(Optional) switch(config-port-prof-role)# show port-profile-role users	Displays all the users on vCenter Server who have access to the DVS parent folder and who can be assigned to the role.

	Command or Action	Purpose
Step 5	(Optional) switch(config-port-prof-role)# {user group} {user-name group-name}	Assigns multiple users and groups to a role. Note The users and groups must exist on vCenter Server and must have access to the top-level Cisco Nexus 1000V DVS folder in vSphere Client. For more information, see Defining DVS Access in vSphere Client, on page 3 .
Step 6	switch(config-port-prof-role)# exit	Exits port-profile-role configuration mode and returns you to global configuration mode.
Step 7	switch(config)# port-profile <i>profile-name</i>	Enters port profile configuration mode for the named port profile.
Step 8	switch(config-port-prof)# assign port-profile-role <i>role-name</i>	Assigns the role to a port profile. The port group is updated in vCenter Server and the user or group assigned to this role is granted access. The user or group can assign the port group to a vNIC in a virtual machine or vSWIF or vMKNIC on a host. Note Only one role can be assigned to a port profile. A role can be assigned to multiple port profiles.
Step 9	(Optional) switch(config-port-prof)# show port-profile-role [<i>name role-name</i>]	Displays the configuration for verification.
Step 10	(Optional) switch(config-port-prof)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
Step 11	(Optional) Perform Step 7, on page 6 for the user assigned port profile access in this procedure.	vSphere client shows the list of port profiles that the user has access to for any DVS object.

Example

This example shows how to define access for the allaccess2 port profile by creating and assigning the adminUser port profile role:

```
switch# configure terminal
switch(config)# port-profile-role adminUser
switch(config-port-prof-role)# description adminOnly
switch(config-port-prof-role)# user hdbaar
switch(config-port-prof-role)# exit
switch(config)# port-profile allaccess2
switch(config-port-prof)# assign port-profile-role adminUser
switch(config-port-prof)# show port-profile-role name adminUser
```

```
Name: adminUser
Description: adminOnly
```

```

Users:
    hdbaar (user)
Assigned port-profiles:
    allaccess2
switch(config-port-prof)# copy running-config startup-config

```

Removing a Port Profile Role

You can remove a role that was used for restricting port profile visibility on vCenter Server.

Before you begin

- You are logged in to the CLI in EXEC mode.
- Know that you cannot remove a port profile role if a port profile is assigned to it. You must first remove the role from the port profile. This procedure includes a step for doing this action.

Procedure

	Command or Action	Purpose
Step 1	(Optional) switch# show port-profile-role [<i>name role-name</i>]	Displays the port profile role including any port profiles assigned to it. If there are port profiles assigned to the role, you must remove them before you can remove the role.
Step 2	switch# configure terminal	Enters global configuration mode.
Step 3	switch(config)# port-profile [type { ethernet vethernet }] <i>name</i>	<p>Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:</p> <ul style="list-style-type: none"> • name—The port profile name can be up to 80 alphanumeric characters and must be unique for each port profile on the Cisco Nexus 1000V. • type—(Optional) The port profile type can be Ethernet or vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. <p>Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs).</p>

	Command or Action	Purpose
		Note If a port profile is configured as an Ethernet type, it cannot be used to configure VMware virtual ports.
Step 4	<code>switch(config-port-prof)# no assign port-profile-role role-name</code>	Removes the role from the port profile. The port group is updated in vCenter Server.
Step 5	<code>switch(config-port-prof)# exit</code>	Exits port-profile configuration mode and returns you to global configuration mode.
Step 6	<code>switch(config)# no port-profile-role role-name</code>	Removes the role from the VSM.
Step 7	(Optional) <code>switch# show port-profile-role [name role-name]</code>	Displays the port profile role including any port profiles assigned to it. If there are port profiles assigned to the role, you must remove them before you can remove the role.
Step 8	(Optional) <code>switch(config)# copy running-config startup-config</code>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to remove a port profile role:

```
switch# show port-profile-role name adminUser
Name: adminUser
Description: adminOnly
Users:
  hdbaar (user)
Assigned port-profiles:
  allaccess2
switch# configure terminal
switch(config)# port-profile allaccess2
switch(config-port-prof)# no assign port-profile-role adminUser
switch(config-port-prof)# exit
switch(config)# no port-profile-role adminUser
switch(config)# show port-profile-role name adminUser
switch(config)# copy running-config startup-config
switch(config)#
```

Feature History for Restricting Port Profile Visibility

This section provides the feature history for restricting port profile visibility.

Feature Name	Release	Feature Information
Restricting port profile visibility	4.2(1)SV1(4)	This feature was introduced.

