User Accounts and RBAC for Smart Switches

User accounts and RBAC for Smart Switches

The N9300 Smart Switches operate in network mode and DPU security mode. Both the network and security features are available in the DPU security mode. This section captures the role and user information for Smart Switches, especially for the DPU security mode which is activated by enabling the service-acceleration feature. For more information, refer to the Onboarding and Security Enablement chapter.

The switch includes several in-built or predefined user roles that control access permissions. For more information about the users and roles for the N9000 Series Switches and N9300 Smart Switches in the network mode, refer to the Configuring User Accounts and RBAC chapter in the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Additional predefined role for DPU security mode

Beginning with NX-OS Release 10.6(3s)F, the N9300 Smart Switches come with an additional user role for the DPU security mode.

netsecops-admin - A specialized role available only on the N9300 Smart Switches that has the privileges to execute the commands within DPU and the Hypershield agent.

To verify the privileges of the netsecops-admin role, use the **show role name netsecops-admin** command.

Example

```
switch(config)# show role name netsecops-admin
Role: netsecops-admin
  Description: Predefined netsecops admin role for service-acceleration feature commands
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  command
switch(config)#
```

Users

The default and predefined users have roles assigned to them, and you cannot change the user roles. The users on a Smart Switch are similar to that of the N9000 Series Switches except for the netsecops-admin user. However, there is a slight change in privileges for a few users on the N9300 Smart Switches unlike rest of the N9000 Series Switches which are captured in this section.

- **admin** – The default user available on the switch with a role that provides complete read-and-write access to the entire N9000 Series Sitch. On N9300 Smart Switches, the admin user is the only user who has read-and-write access to the entire switch including network and DPU security modes.

  The admin user can perform tasks in both network and DPU security modes, while all other users are restricted to either network or DPU security mode only. As the admin user has the highest privileges for switch administration, this user can create users and assign valid roles. Thus, the admin user is the default superuser.

Note The superuser can create users with both network-admin and netsecops-admin roles. For troubleshooting service-acceleration issues, it is recommended to troubleshoot the system with users that have both roles assigned.

- **network-admin** - A user who has complete read-and-write access only to the network mode on the N9300 Smart Switches. This user can create all users including network-admins except netsecops-admins and admin and assign any role other than the netsecops-admin role.
- **netsecops-admin** - A user who has complete read-and write access only to the DPU security mode on the N9300 Smart Switches. This user's role is limited to executing commands related to DPU and Hypershield Agent. This user has no privileges to create a user or assign any roles.

  The configuration commands that a netsecops-admin user can perform are attach, username, change-password, configure, service, show, and slot. For attach and slot commands, refer to Commands executed by netsecops-admin. For the rest of the commands, refer to the Configuring User Accounts and RBAC chapter in the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.
- **network-operator** - A user who has read-only access to the entire switch on N9000 Series Switches, but on an N9300 Smart Switch, the access is limited to the network mode on the switch. The network-admin can create this user and assign role. This role allows the user to view operational data but does not provide the rights to configure.
- **priv0-15** - These are privilege roles that can be assigned manually by the network-admin, each with specific command permissions.

Commands executed by netsecops-admin

The netsecops-admin is the only role that has access to the DPU. However, feature service acceleration must be enabled to ensure that the DPU is accessible. The netsecops-admin user can then access the DPU and execute the commands related to DPU. These commands enable advanced management and security operations on the DPUs of the switch.

Use any one of these commands on the supervisor to connect to the DPU and run the DPU commands to check and troubleshoot the DPU firmware version, NPU-DPU port status, state, and so on:

- Use the **attach dpu** *dpu-id* command to attach the user session to one DPU at a time, enabling direct SSH access to the DPU. The netsecops-admin user can then execute commands on the DPU.

  Example

  Use case: The netsecops-admin user wants to verify the firmware version using the **attach dpu** command.

```
switch# attach dpu 1
Attaching to dpu 1 ...
To exit type 'exit'...
dpu1# pdsctl show version
Firmware Version : 1.162.2
Pipeline : rudra
P4 Program : hs-dp-app
Build Time : Mon Aug 3 08:18:19 UTC 2026

dpu1# exit
Connection to dpu1 closed.
switch#
```

- Run the **slot** *slot-num* **dpu** *dpu-id internal-DPU-commands* command. This command allows executing commands directly from the switch Command Line Interface (CLI) without the **attach dpu** *dpu-id* command. It allows targeting a specific DPU in a given slot for command execution or monitoring.

  Example

  Use case: The netsecops-admin user does not want to log into the DPU but needs to verify the DPU port state-machine directly, so the user uses the slot dpu command to execute the internal DPU command and also revert to the Supervisor (SUP).

```
switch# slot 1 dpu 1 pdsctl show port fsm

Port ID: 00000111-0000-0000-4242-9ca9b8dd73e0
Timestamp State Duration (sec)
------------------------------------------------------------------
1970-01-01 00:00:10.23 ENABLED -
1970-01-01 00:00:10.124 AN_CFG 0.100659465
1970-01-01 00:00:10.124 SERDES_CFG 0.000001245
1970-01-01 00:00:10.174 WAIT_SERDES_RDY 0.050439400
1970-01-01 00:00:10.174 MAC_CFG 0.000172545
1970-01-01 00:00:10.174 WAIT_PHY_LINK_UP 0.000139070
1970-01-01 00:00:10.174 SIGNAL_DETECT 0.000002575
1970-01-01 00:00:10.174 DFE_TUNING 0.000189905
1970-01-01 00:00:10.174 DFE_START_ICAL 0.000001085
1970-01-01 00:00:10.174 DFE_WAIT_ICAL 0.000001865
1970-01-01 00:00:11.666 DFE_START_PCAL 1.491027795
1970-01-01 00:00:11.666 DFE_WAIT_PCAL 0.000007260
1970-01-01 00:00:11.666 CLEAR_MAC_REMOTE_FAULTS 0.000325270
1970-01-01 00:00:11.666 WAIT_MAC_SYNC 0.000012750
1970-01-01 00:00:11.666 WAIT_MAC_FAULTS_CLEAR 0.000015845
1970-01-01 00:00:11.666 UP 0.000007625


Port ID: 00000211-0000-0000-4242-9ca9b8dd73e0
Timestamp State Duration (sec)
------------------------------------------------------------------
1970-01-01 00:00:10.23 ENABLED -
1970-01-01 00:00:10.225 AN_CFG 0.201410325
1970-01-01 00:00:10.225 SERDES_CFG 0.000001045
1970-01-01 00:00:10.285 WAIT_SERDES_RDY 0.060090520
1970-01-01 00:00:10.285 MAC_CFG 0.000162035
1970-01-01 00:00:10.285 WAIT_PHY_LINK_UP 0.000133370
1970-01-01 00:00:10.285 SIGNAL_DETECT 0.000001940
1970-01-01 00:00:10.285 DFE_TUNING 0.000176350
```

```
1970-01-01 00:00:10.285 DFE_START_ICAL 0.000000830
1970-01-01 00:00:10.285 DFE_WAIT_ICAL 0.000001545
1970-01-01 00:00:11.718 DFE_START_PCAL 1.433245790
1970-01-01 00:00:11.719 DFE_WAIT_PCAL 0.000006890
1970-01-01 00:00:11.719 CLEAR_MAC_REMOTE_FAULTS 0.000316325
1970-01-01 00:00:11.719 WAIT_MAC_SYNC 0.000011745
1970-01-01 00:00:11.719 WAIT_MAC_FAULTS_CLEAR 0.000013710
1970-01-01 00:00:11.719 UP 0.000007615

switch#
```

- Use the **attach console dpu** *dpu-id* command to attach or connect to the console of a DPU within the switch. The console window opens and the netsecops-admin user can interact directly with the DPU's command-line interface for management or troubleshooting purposes.

Note To navigate or close the console, see the instructions on the banner at the bottom of the console. For example, to return to NX-OS, press Ctrl-A, release, then Z, X, and Enter. For more information, refer to the Cisco Hypershield User Documentation and Cisco Hypershield Reference Documentation.

Example

Use case: The netsecops-admin user wants to verify the DPU port status using the console.

```
switch# attach console dpu 1

Welcome to minicom 2.9

OPTIONS: I18n
Compiled on Sep 22 2023, 21:10:41.
Port /dev/dpu00, 00:31:44

Press CTRL-A Z for help on special keys


dpu1# pdsctl show port status
MAC-Info: MAC ID/MAC Channel/Num lanes
FEC-Type: FC - FireCode, RS - ReedSolomon
--------------------------------------------------------------------------------------------------------------------------------------
ID Name IfIndex Speed MAC-Info FEC AutoNeg MTU Pause Pause Debounce State Transceiver
NumLinkDown LinkSM Loopback
Cfg/Oper Cfg/Oper Type Tx/Rx (msecs) Admin/Oper
--------------------------------------------------------------------------------------------------------------------------------------
00000111-0000-0000-4242-9ca9b8dd73e0 Eth1/1 0x11010000 200G 0/0/4 RS/RS F/F 9440 NONE
F/F 0 UP/UP REMOVED 0 UP NONE
00000211-0000-0000-4242-9ca9b8dd73e0 Eth1/2 0x11020000 200G 0/4/4 RS/RS F/F 9440 NONE
F/F 0 UP/UP REMOVED 0 UP NONE

No. of ports : 2

dpu1#
```

- Use the **service system hypershield connect session** *[command]* to open an interactive shell session inside the Hypershield agent container running on the switch.
  - If a *command* is specified, the command is executed non-interactively inside the container and returns the output to the terminal.

    Example- interactive session

```
switch# service system hypershield connect session
HypershieldAgent:/usr/src/app#
```

- If a *command* is not specified, it opens an interactive shell session within the Hypershield agent container.

Example – non-interactive session

```
switch# service system hypershield connect session /usr/src/app/agwctl -v
agwctl version v1.19.0-pre.8-547-gb57fe1ed
```