Contents

RBAC commands 1

description 1
display role 1
display role feature 8
display role feature-group 11
feature 14
interface policy deny 14
permit interface 15
permit vlan 17
permit vpn-instance 18
role 20
role default-role enable 21
role feature-group 22
rule 22
super 26
super authentication-mode 27
super default role 28
super password 29
super use-login-username 30
vlan policy deny 31
vpn-instance policy deny 32

RBAC commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

description

Use **description** to configure a description for a user role for easy identification.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A user role does not have a description.

Views

User role view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 128 characters.

Examples

Configure the description as **labVIP** for user role **role1**.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] description labVIP
```

Related commands

display role

role

display role

Use **display role** to display user role information.

Syntax

display role [**name** *role-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify a user role name, the command displays information about all user roles, including the predefined user roles.

Examples

Display information about user role **123**.

```
<Sysname> display role name 123
Role: 123
  Description: new role
  VLAN policy: deny
  Permitted VLANs: 1 to 5, 7 to 8
  Interface policy: deny
  Permitted interfaces: Ten-GigabitEthernet1/0/1 to Ten-GigabitEthernet1/0/3,
Vlan-interface1 to Vlan-interface20
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  1       permit RWX   feature-group abc
  2       deny   -W-   feature       ldap
  3       permit       command       system ; radius sc *
  4       permit R--   xml-element   -
  5       permit RW-   oid           1.2.1
  R:Read W:Write X:Execute
```

Display information about all user roles.

```
<Sysname> display role
Role: network-admin
  Description: Predefined network admin role has access to all commands on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       display security-logfile buffer
  sys-6   deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-7   deny         command       security-logfile save
  sys-8   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the device
```

```
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  --------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  --------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   permit       command       system-view ; probe ; display *
  sys-4   deny         command       display history-command all
  sys-5   deny         command       display exception *
  sys-6   deny         command       display cpu-usage configuration
                                     *
  sys-7   deny         command       display kernel exception *
  sys-8   deny         command       display kernel deadloop *
  sys-9   deny         command       display kernel starvation *
  sys-10  deny         command       display kernel reboot *
  sys-13  permit       command       system-view ; local-user *
  sys-16  permit R--   web-menu      -
  sys-17  permit RW-   web-menu      m_device/m_maintenance/
                                     m_changepassword
  sys-18  permit R--   xml-element   -
  sys-19  deny         command       display security-logfile summary
  sys-20  deny         command       display security-logfile buffer
  sys-21  deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-22  deny         command       security-logfile save
  sys-23  deny         command       system-view ; local-user-import
                                     *
  sys-24  deny         command       system-view ; local-user-export
                                     *
  sys-25  permit R--   oid           1
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  --------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  --------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       super *
  sys-6   permit       command       mtrace *
```

```
  R:Read W:Write X:Execute

Role: level-1
  Description: Predefined level-1 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       display *
  sys-6   permit       command       super *
  sys-7   deny         command       display history-command all
  sys-8   permit       command       mtrace *
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-3
  Description: Predefined level-3 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-4
  Description: Predefined level-4 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-5
  Description: Predefined level-5 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-6
  Description: Predefined level-6 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
```

```
  VPN instance policy: permit (default)

Role: level-7
  Description: Predefined level-7 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-8
  Description: Predefined level-8 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-9
  Description: Predefined level-9 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit RWX   feature       -
  sys-2   deny   RWX   feature       device
  sys-3   deny   RWX   feature       filesystem
  sys-4   permit       command       display *
  sys-5   deny         command       display history-command all
  R:Read W:Write X:Execute

Role: level-10
  Description: Predefined level-10 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-11
  Description: Predefined level-11 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-12
  Description: Predefined level-12 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-13
```

```
  Description: Predefined level-13 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-14
  Description: Predefined level-14 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       display security-logfile buffer
  sys-6   deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-7   deny         command       security-logfile save
  sys-8   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for the
security log administrator
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   deny         command       *
  sys-2   permit       command       display security-logfile summary
  sys-3   permit       command       display security-logfile buffer
  sys-4   permit       command       system-view ; info-center
                                     security-logfile directory *
  sys-5   permit       command       security-logfile save
  sys-6   permit       command       cd *
  sys-7   permit       command       copy *
  sys-8   permit       command       delete *
```

```
  sys-9   permit       command       dir *
  sys-10  permit       command       mkdir *
  sys-11  permit       command       more *
  sys-12  permit       command       move *
  sys-13  permit       command       rmdir *
  sys-14  permit       command       pwd
  sys-15  permit       command       rename *
  sys-16  permit       command       undelete *
  sys-17  permit       command       ftp *
  sys-18  permit       command       sftp *
  R:Read W:Write X:Execute

Role: guest-manager
  Description: Predefined guest manager role can't access to commands
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   xml-element   useraccounts/approveguest/
  sys-2   permit RWX   xml-element   useraccounts/exportguestaccount/
  sys-3   permit RWX   xml-element   useraccounts/generateguestaccount/
  sys-4   permit RWX   xml-element   useraccounts/guest/
  sys-5   permit RWX   xml-element   useraccounts/guestconfigure/
  sys-6   permit RWX   xml-element   useraccounts/importguestaccount/
  sys-7   permit RWX   xml-element   useraccounts/exportguesttemplet/
  sys-8   permit RWX   xml-element   rpc/
  sys-9   deny         command       *
  R:Read W:Write X:Execute
```

Table 1 Command output

Field	Description
Role	User role name. Predefined user role names: • network-admin. • network-operator. • level-*n* (where *n* represents an integer in the range of 0 to 15). • security-audit. • guest-manager. This user role is not supported in the current software version.
Description	User role description.
VLAN policy	VLAN policy of the user role: • **deny**—Denies access to any VLANs except for permitted VLANs. • **permit (default)**—Default VLAN policy, which enables the user role to access all VLANs.
Permitted VLANs	VLANs accessible to the user role.

Field	Description
Interface policy	Interface policy of the user role: • **deny**—Denies access to any interfaces except for permitted interfaces. • **permit (default)**—Default interface policy, which enables the user role to access all interfaces.
Permitted interfaces	Interfaces accessible to the user role.
VPN instance policy	VPN instance policy of the user role: • **deny**—Denies access to any VPN instances except for permitted VPN instances. • **permit (default)**—Default VPN instance policy, which enables the user role to access all VPN instances.
Permitted VPN instances	VPN instances accessible to the user role.
Rule	User role rule number. Predefined user role rules are identified by sys-*n*, where *n* represents an integer.
Perm	Access control type: • **permit**—User role has access to the items in the **Entity** field. • **deny**—User role does not have access to the items in the **Entity** field.
Type	Controlled type: • **R**—Read-only. • **W**—Write. • **X**—Execute.
Scope	Rule control scope: • **command**—Controls access to the command or commands, as specified in the **Entity** field. • **feature**—Controls access to the commands of the feature, as specified in the **Entity** field. • **feature-group**—Controls access to the commands of the features in the feature group, as specified in the **Entity** field. • **web-menu**—Controls access to Web menus. This rule control scope is not supported in the current software version. • **xml-element**—Controls access to XML elements. • **oid**—Controls access to MIB nodes.
Entity	Command string, feature name, feature group, XML element, or OID specified in the user role rule: • An en dash (–) represents any feature. • An asterisk (*) represents zero or more characters.

Related commands

`role`

display role feature

Use **`display role feature`** to display features available in the system.

Syntax

`display role feature` [**`name`** *`feature-name`* | **`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *feature-name*: Specifies a feature by feature name. The *feature-name* argument represents the feature name, and all letters must be in lower case.

verbose: Displays the commands of each feature.

Usage guidelines

If you do not specify any parameters, the command displays only the list of features available in the system.

Examples

Display the list of feature names.

```
<Sysname> display role feature
Feature: device          (Device configuration related commands)
Feature: interface       (Interface related commands)
Feature: syslog          (Syslog related commands)
…
```

Display the commands of each feature.

```
<Sysname> display role feature verbose
Feature: device          (Device configuration related commands)
  display clock    (R)
  debugging dev    (W)
  display debugging dev    (R)
  display device *    (R)
  display diagnostic-information *    (R)
  display environment *    (R)
  display fan *    (R)
  display alarm *    (R)
  display power *    (R)
  display system-working-mode    (R)
  display hardware-resource *    (R)
  display current-configuration *    (R)
  display saved-configuration *    (R)
  display default-configuration *    (R)
  display startup    (R)
  display this *    (R)
…
```

Display the commands of feature **aaa**.

```
<Sysname> display role feature name aaa
Feature: aaa             (AAA related commands)
  system-view ; domain *    (W)
  system-view ; header *    (W)
  system-view ; aaa *    (W)
```

```
system-view ; probe ; display system internal aaa *    (R)
display domain *    (R)
display aaa *    (R)
system-view ; user-group *    (W)
system-view ; local-user *    (W)
display local-user *    (R)
display user-group *    (R)
display debugging local-server    (R)
debugging local-server *    (W)
super *    (X)
display password-control *    (R)
```

…

Table 2 Command output (display role feature name aaa)

Field	Description
Feature	Displays the name and brief function description of the feature.
system-view ; domain *	All commands that start with the **domain** keyword in system view, and all commands in ISP domain view.
system-view ; header *	All commands that start with the **header** keyword in system view.
system-view ; aaa *	All commands that start with the **aaa** keyword in system view.
display domain *	All commands that start with the **display domain** keywords in user view.
system-view ; user-group *	All commands that start with the **user-group** keyword in system view, and all commands in user group view.
system-view ; local-user *	All commands that start with the **local-user** keyword in system view, and all commands in local user view.
display user-group *	All commands that start with the **display user-group** keywords in user view.
display debugging local-server	All commands that start with the **display debugging local-server** keywords in user view.
debugging local-server *	All commands that start with the **debugging local-server** keywords in user view.
super *	All commands that start with the **super** keyword in user view.
display password-control *	All commands that start with the **display password-control** keywords in user view.
reset password-control *	All commands that start with the **reset password-control** keywords in user view.
system-view ; password-control *	All commands that start with the **password-control** keyword in system view.
(W)	Command type is Write. A write command configures the system.
(R)	Command type is Read. A read command displays configuration or maintenance information.
(X)	Command type is Execute. An execute command executes a specific function.

Related commands

feature

display role feature-group

Use **display role feature-group** to display feature group information.

Syntax

display role feature-group [**name** *feature-group-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *feature-group-name*: Specifies a feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If you do not specify a feature group, the command displays information about all feature groups.

verbose: Displays the commands of each feature in feature groups. If you do not specify this keyword, the command displays only the feature lists of feature groups.

Usage guidelines

Feature groups **L2** and **L3** are predefined feature groups.

Examples

Display the feature lists of feature groups.

```
<Sysname> display role feature-group
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
Feature: mld-snooping    (MLD-Snooping related commands)
Feature: lacp            (LACP related commands)
Feature: stp             (STP related commands)
Feature: lldp            (LLDP related commands)
Feature: dldp            (DLDP related commands)
Feature: cfm             (CFM related commands)
Feature: eoam            (EOAM related commands)
Feature: smart-link      (Smart-link related commands)
Feature: monitor-link    (Monitor-link related commands)
Feature: loopbk-detect   (Loopback-detection related commands)
Feature: vlan            (Virtual LAN related commands)
Feature: evb             (EVB related commands)
Feature: trill           (TRILL related commands)
Feature: evi             (EVI related commands)
Feature: mvrp            (MVRP related commands )
Feature: qcn             (QCN related commands)
Feature: oap             (OAP related commands)
Feature: rrpp            (RRPP related commands)
Feature: erps            (ERPS related commands)
```

```
Feature: ptp             (PTP related commands)
Feature: pbb             (PBB related commands)
Feature: ofp             (OFP related commands)
Feature: spbm            (SPBM related commands)
Feature: port-security   (Port-security related commands)
Feature: macsec          (MACSEC related commands)
Feature: l2pt            (L2PT related commands)
Feature: rpr             (RPR related commands)

Feature group: L3
Feature: route           (Route management related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: mt              (Multiple-topology related commands)
Feature: multicast       (Multicast related commands)
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
Feature: mcast-domain    (Multicast Domain related commands)
Feature: msdp            (Multicast Source Discovery Protocol related commands)
Feature: mip             (Mobile IP related commands)
```

Display the commands in each feature group. For more information about the wildcards and marks used in the command list, see Table 2.

```
<Sysname> display role feature-group verbose
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
  system-view ; igmp-snooping *    (W)
  system-view ; multicast-vlan *    (W)
  system-view ; vlan * ; igmp-snooping *    (W)
  system-view ; vlan * ; pim-snooping *    (W)
  system-view ; vsi * ; igmp-snooping *    (W)
  system-view ; vsi * ; pim-snooping *    (W)
  system-view ; interface * ; igmp-snooping *    (W)
  system-view ; interface * ; port multicast-vlan *    (W)
  display igmp-snooping *    (R)
  display pim-snooping *    (R)
  display multicast-vlan *    (R)
  display l2-multicast *    (R)
  system-view ; probe ; display system internal l2-multicast *    (R)
  system-view ; probe ; display system internal multicast-vlan *    (R)
  reset igmp-snooping *    (W)
  reset pim-snooping *    (W)
  reset multicast-vlan *    (W)
  reset l2-multicast *    (W)
```

```
  debugging igmp-snooping *    (W)
  display debugging igmp-snooping *    (R)
  system-view ; probe ; debugging system internal igmp-snooping *    (W)
Feature: mld-snooping    (MLD-Snooping related commands)
  system-view ; mld-snooping *    (W)
  system-view ; ipv6 multicast-vlan *    (W)
  system-view ; vlan * ; mld-snooping *    (W)
  system-view ; vlan * ; ipv6 pim-snooping *    (W)
  system-view ; vsi * ; mld-snooping *    (W)
  system-view ; vsi * ; ipv6 pim-snooping *    (W)
  system-view ; interface * ; mld-snooping *    (W)
  system-view ; interface * ; ipv6 port multicast-vlan *    (W)
  display mld-snooping *    (R)
  display ipv6 pim-snooping *    (R)
  display ipv6 multicast-vlan *    (R)
  display ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 multicast-vlan *    (R)
  reset mld-snooping *    (W)
  reset ipv6 pim-snooping *    (W)
  reset ipv6 multicast-vlan *    (W)
  reset ipv6 l2-multicast *    (W)
  debugging mld-snooping *    (W)
  display debugging mld-snooping *    (R)
  system-view ; probe ; debugging system internal mld-snooping *    (W)
…
```

Display the feature list of the **L3** feature group.

```
<Sysname> display role feature-group name L3
Feature group: L3
Feature: route           (Route management related commands)
Feature: usr             (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: lisp            (LISP protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: mt              (Multiple-topology related commands)
Feature: multicast       (Multicast related commands)
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
Feature: mcast-domain    (Multicast Domain related commands)
Feature: msdp            (Multicast Source Discovery Protocol related commands)
Feature: mip             (Mobile IP related commands)
```

Related commands

`feature`

role feature-group

feature

Use **feature** to add a feature to a feature group.

Use **undo feature** to remove a feature from a feature group.

Syntax

feature *feature-name*

undo feature *feature-name*

Default

A user-defined feature group does not have any features.

Views

Feature group view

Predefined user roles

network-admin

Parameters

feature-name: Specifies a feature name. You must enter the feature name in lower case.

Usage guidelines

Repeat the **feature** command to add multiple features to a feature group.

Examples

Add the AAA and ACL features to feature group **security-features**.

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features] feature aaa
[Sysname-featuregrp-security-features] feature acl
```

Related commands

display role feature

display role feature-group

role feature-group

interface policy deny

Use **interface policy deny** to enter user role interface policy view.

Use **undo interface policy deny** to restore the default.

Syntax

interface policy deny

undo interface policy deny

Default

A user role has access to all interfaces.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the interface access of a user role to a set of interfaces, perform the following tasks:

1. Use **interface policy deny** to enter user role interface policy view.
2. Use **permit interface** to specify accessible interfaces.

NOTE:

The **interface policy deny** command denies the access of the user role to any interfaces if the **permit interface** command is not configured.

To configure an interface, make sure the interface is permitted by the user role interface policy in use. You can perform the following tasks on an accessible interface:

- Create, remove, or configure the interface.
- Enter interface view.
- Specify the interface in feature commands.

The create and remove operations are available only for logical interfaces.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] quit
```

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces except for Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface ten-gigabitethernet 1/0/1 to
ten-gigabitethernet 1/0/4
```

Related commands

display role

permit interface

role

permit interface

Use **permit interface** to configure a list of interfaces accessible to a user role.

Use **undo permit interface** to disable the access of a user role to specific interfaces.

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

Default

No permitted interfaces are configured in user role interface policy view.

Views

User role interface policy view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 interface items. Each interface item specifies one interface in the *interface-type interface-number* form or a range of interfaces in the *interface-type interface-number* **to** *interface-type interface-number* form. If you specify an interface range, the end interface must meet the following requirements:

- Be the same type as the start interface.
- Have a higher interface number than the start interface.

Usage guidelines

To permit a user role to access an interface after you configure the **interface policy deny** command, you must add the interface to the permitted interface list of the policy. With the user role, you can perform the following tasks to the interfaces in the permitted interface list:

- Create, remove, or configure the interfaces.
- Enter the interface views.
- Specify the interfaces in feature commands.

The create and remove operations are available only for logical interfaces.

You can repeat the **permit interface** command to add multiple permitted interfaces to a user role interface policy.

The **undo permit interface** command removes the entire list of permitted interfaces if you do not specify an interface.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

Permit user role **role1** to execute all commands available in interface view and VLAN view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; interface *
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

Permit the user role to access Ten-GigabitEthernet 1/0/1, and Ten-GigabitEthernet 1/0/3 to Ten-GigabitEthernet 1/0/5.

```
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface ten-gigabitethernet 1/0/1
ten-gigabitethernet 1/0/3 to ten-gigabitethernet 1/0/5
[Sysname-role-role1-ifpolicy] quit
```

```
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any interfaces except for Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/3 to Ten-GigabitEthernet 1/0/5:

   # Verify that you can enter Ten-GigabitEthernet 1/0/1 interface view.

```
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] quit
```

   # Verify that you can assign Ten-GigabitEthernet 1/0/5 to VLAN 10. In this example, the user role can access all VLANs because the default VLAN policy of the user role is used.

```
[Sysname] vlan 10
[Sysname-vlan10] port ten-gigabitethernet 1/0/5
[Sysname-vlan10] quit
```

   # Verify that you cannot enter interface view of Ten-GigabitEthernet 1/0/2.

```
[Sysname] interface ten-gigabitethernet 1/0/2
Permission denied.
```

Related commands

display role

interface policy deny

role

permit vlan

Use **permit vlan** to configure a list of VLANs accessible to a user role.

Use **undo permit vlan** to remove the permission for a user role to access specific VLANs.

Syntax

permit vlan *vlan-id-list*

undo permit vlan [*vlan-id-list*]

Default

No permitted VLANs are configured in user role VLAN policy view.

Views

User role VLAN policy view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the VLAN IDs is 1 to 4094. If you specify a VLAN range, the value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument.

Usage guidelines

To permit a user role to access a VLAN after you configure the **vlan policy deny** command, you must add the VLAN to the permitted VLAN list of the policy. With the user role, you can perform the following tasks on the VLANs in the permitted VLAN list:

- Create, remove, or configure the VLANs.
- Enter the VLAN views.

- Specify the VLANs in feature commands.

You can repeat the **permit vlan** command to add multiple permitted VLANs to a user role VLAN policy.

The **undo permit vlan** command removes the entire list of permitted VLANs if you do not specify a VLAN.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

By default, all access ports belong to VLAN 1. To assign an access port to any other VLAN by using the **port access vlan** command, make sure you have a user role that can access both VLAN 1 and the new VLAN.

Examples

1. Configure user role **role1**:

Permit user role **role1** to execute all commands available in interface view and VLAN view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; interface *
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

Permit user role **role1** to access VLANs 1, 2, 4, and 50 to 100.

```
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 1 2 4 50 to 100
[Sysname-role-role1-vlanpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any VLANs except for VLANs 1, 2, 4, and 50 to 100:

Verify that you can create VLAN 100 and enter VLAN view.

```
[Sysname] vlan 100
[Sysname-vlan100] quit
```

Verify that you can add Ten-GigabitEthernet 1/0/1 to VLAN 100 as an access port.

```
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] port access vlan 100
[Sysname-Ten-GigabitEthernet1/0/1] quit
```

Verify that you cannot create VLAN 101 or enter VLAN view.

```
[Sysname] vlan 101
Permission denied.
```

Related commands

display role

role

vlan policy deny

permit vpn-instance

Use **permit vpn-instance** to configure a list of MPLS L3VPN instances accessible to a user role.

Use **undo permit vpn-instance** to disable the access of a user role to specific MPLS L3VPN instances.

Syntax

permit vpn-instance *vpn-instance-name*&<1-10>

undo permit vpn-instance [*vpn-instance-name*&<1-10>]

Default

No permitted VPN instances are configured in user role VPN instance policy.

Views

User role VPN instance policy view

Predefined user roles

network-admin

Parameters

vpn-instance-name&<1-10>: Specifies a space-separated list of up to 10 MPLS L3VPN instance names. Each name is a case-sensitive string of 1 to 31 characters.

Usage guidelines

To permit a user role to access a VPN instance after you configure the **vpn-instance policy deny** command, you must add the VPN instance to the permitted VPN instance list of the policy. With the user role, you can perform the following tasks on the VPN instances in the permitted VPN instance list:

- Create, remove, or configure the VPN instances.
- Enter the VPN instance views.
- Specify the VPN instances in feature commands.

You can repeat the **permit vpn-instance** command to add multiple permitted VPN instances to a user role VPN instance policy.

The **undo permit vpn-instance** command removes the entire list of permitted VPN instances if you do not specify a VPN instance.

Any change to a user role VPN instance policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

Permit the user role to execute all commands available in system view and in the child views of system view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; *
```

Permit the user role to access VPN instance **vpn1**.

```
[Sysname-role-role1] vpn policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn1
[Sysname-role-role1-vpnpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any VPN instances except for **vpn1**:

Verify that you can enter the view of **vpn1**.

```
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] quit
```

Verify that you can specify the primary accounting server at 10.110.1.2 in VPN instance **vpn1** for RADIUS scheme **radius1**.

```
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 vpn-instance vpn1
[Sysname-radius-radius1] quit
```

Verify that you cannot create VPN instance **vpn2** or enter VPN instance view.

```
[Sysname] ip vpn-instance vpn2
Permission denied.
```

Related commands

display role

role

vpn-instance policy deny

role

Use **role** to create a user role and enter its view, or enter the view of an existing user role.

Use **undo role** to delete a user role.

Syntax

role name *role-name*

undo role name *role-name*

Default

The system has the following predefined user roles: network-admin, network-operator, level-*n* (where *n* represents an integer in the range of 0 to 15), and security-audit.

Views

System view

Predefined user roles

network-admin

Parameters

name *role-name*: Specifies a username. The *role-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can create a maximum of 64 user roles in addition to the predefined user roles.

You cannot delete the predefined user roles or change the permissions assigned to network-admin, network-operator, level-15, or security-audit.

You cannot assign the security-audit user role to non-AAA authentication users.

The access permissions of the level-0 to level-14 user roles can be modified through user role rules and resource access policies. However, you cannot make changes on the predefined access permissions of these user roles. For example, you cannot change the access permission of these user roles to the **display history-command all** command.

Examples

Create user role **role1** and enter its view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1]
```

Related commands

display role

interface policy deny

rule

vlan policy deny

vpn-instance policy deny

role default-role enable

Use **role default-role enable** to enable the default user role feature for remote AAA users.

Use **undo role default-role enable** to restore the default.

Syntax

role default-role enable [*role-name*]

undo role default-role enable

Default

The default user role feature is disabled. AAA users who do not have a user role cannot log in to the device.

Views

System view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role by its name for the default user role. The user role must already exist. The argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

The default user role feature assigns the default user role to AAA-authenticated users if the authentication server (local or remote) does not assign any user roles to the users. These users are allowed to access the system with the default user role.

For local authorization, this command is required if you do not use the **authorization-attribute user role** command to assign user roles to local users.

If AAA users have been assigned user roles, they log in with the user roles.

If you do not specify the *role-name* argument, the default user role is network-operator.

Examples

Enable the default user role feature.

```
<Sysname> system-view
[Sysname] role default-role enable
```

Related commands

role

role feature-group

Use **role feature-group** to create a user role feature group and enter its view, or enter the view of an existing user role feature group.

Use **undo role feature-group** to delete a user role feature group.

Syntax

role feature-group name *feature-group-name*

undo role feature-group name *feature-group-name*

Default

Two user role feature groups **L2** and **L3** exist.

Views

System view

Predefined user roles

network-admin

Parameters

name *feature-group-name*: Specifies a feature group name. The *feature-group-name* argument is a case-sensitive string of 1 to 31 characters.

Usage guidelines

The **L2** feature group includes all Layer 2 feature commands, and the **L3** feature group includes all Layer 3 feature commands. These predefined feature groups are not user configurable.

In addition to the predefined feature groups **L2** and **L3**, you can create a maximum of 64 user role feature groups.

Examples

Create feature group **security-features** and enter its view.

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features]
```

Related commands

display role feature

display role feature-group

feature

rule

Use **rule** to create or change a user role rule.

Use **undo rule** to delete user role rules.

Syntax

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* | **oid** *oid-string* | **xml-element** [*xml-string*] } }

undo rule { *number* | **all** }

Default

A user-defined user role does not have any rules and cannot access any resources.

Views

User role view

Predefined user roles

network-admin

Parameters

number: Specifies a rule number in the range of 1 to 256.

deny: Denies access to the specified commands, XML elements, or MIB nodes.

permit: Permits access to the specified commands, XML elements, or MIB nodes.

command *command-string*: Specifies a command string. The command string can represent a command or a group of commands. The *command-string* argument is a case-sensitive string of 1 to 128 characters, including the following characters:

- The wildcard asterisk (*).
- The delimiters space and tab.
- All printable characters.

execute: Specifies the execute commands, XML elements, or MIB nodes to execute a specific function or program. The **ping** command is an example of execute commands.

read: Specifies the read commands, XML elements, or MIB nodes to display configuration or maintenance information. The **display**, **dir**, **more**, and **pwd** commands are examples of read commands.

write: Specifies the write commands, XML elements, or MIB nodes to configure the system. The **ssh server enable** command is an example of write commands.

feature [*feature-name*]: Specifies one or all features. The *feature-name* argument is a case-sensitive character string. If you do not specify a feature name, you specify all the features in the system.

feature-group *feature-group-name*: Specifies a user-defined or predefined feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If the feature group has not been created, the rule takes effect after the group is created. To display the feature groups that have been created, use the **display role feature-group** command.

oid *oid-string*: Specifies an OID of a MIB node. The *oid-string* argument represents the OID, a case-insensitive string of 1 to 255 characters. The OID is a dotted numeric string that uniquely identifies the path from the root node to this node. For example, 1.3.6.1.4.1.25506.8.35.14.19.1.1.

xml-element [*xml-string*]: Specifies an XML element. The *xml-string* argument represents the XPath of the XML element, a case-insensitive string of 1 to 255 characters. Use the forward slash (/) to separate Xpath items, for example, Interfaces/Index/Name. If you do not specify an XML element, the rule applies to all XML elements.

all: Specifies all the user role rules.

Usage guidelines

You can define the following types of rules for different access control granularities:

- **Command rule**—Controls access to a command or a set of commands that match a regular expression.
- **Feature rule**—Controls access to the commands of a feature by command type.

- **Feature group rule**—Controls access to the commands of a group of features by command type.
- **XML element rule**—Controls access to XML elements by element type.
- **OID rule**—Controls access to the specified MIB node and its child nodes by node type.

A user role can access the set of permitted resources specified in the user role rules. User role rules include predefined (identified by sys-n) and user-defined user role rules.

You can configure a maximum of 256 user-defined rules for a user role. The total number of user-defined user role rules cannot exceed 1024.

Any rule modification, addition, or removal for a user role takes effect only on the users who log in with the user role after the change.

Access to the file system commands is controlled by both the file system command rules and the file system feature rule.

A command with output redirection to the file system is permitted only when the command type write is assigned to the file system feature.

The following guidelines apply to non-OID rules:

- If two user-defined rules of the same type conflict, the rule with the higher ID takes effect. For example, a user role can use the **`tracert`** command but not the **`ping`** command if the user role contains rules configured by using the following commands:
  - **`rule`** *`1`* **`permit command`** *`ping`*
  - **`rule`** *`2`* **`permit command`** *`tracert`*
  - **`rule`** *`3`* **`deny command`** *`ping`*
- If a predefined user role rule and a user-defined user role rule conflict, the user-defined user role rule takes effect.

The following guidelines apply to OID rules:

- The system compares an OID with the OIDs specified in rules, and it uses the longest match principle to select a rule for the OID. For example, a user role cannot access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
  - **`rule`** *`1`* **`permit read write oid`** *`1.3.6`*
  - **`rule`** *`2`* **`deny read write oid`** *`1.3.6.1.4.1`*
  - **`rule`** *`3`* **`permit read write oid`** *`1.3.6.1.4`*
- If the same OID is specified in multiple rules, the rule with the higher ID takes effect. For example, a user role can access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
  - **`rule`** *`1`* **`permit read write oid`** *`1.3.6`*
  - **`rule`** *`2`* **`deny read write oid`** *`1.3.6.1.4.1`*
  - **`rule`** *`3`* **`permit read write oid`** *`1.3.6.1.4.1`*

When you specify a command string, follow the guidelines in Table 3.

Table 3 Command string configuration rules

Rule	Guidelines
Semicolon (;) is the delimiter.	Use a semicolon to separate the command of each view that you must enter before you access a command or a set of commands. However, do not use a semicolon to separate commands available in user view or any view, for example, **`display`** and **`dir`**. Each semicolon-separated segment must have a minimum of one printable character. To specify the commands in a view but not the commands in the view's subviews, use a semicolon as the last printable character in the last segment. To specify the commands in a view and the view's subviews, the last printable character in the last segment must not be a semicolon. For example, you must enter system view before you enter interface view. To specify all commands starting with the **`ip`** keyword in any interface view, you must use the "system ; interface * ; ip * ;" command string. For another example, the "system ; radius scheme * ;" command string represents all commands that start with the **`radius scheme`** keywords in system view. The "system ; radius scheme *" command string represents all commands that start with the **`radius scheme`** keywords in system view and all commands in RADIUS scheme view.
Asterisk (*) is the wildcard.	An asterisk represents zero or multiple characters. In a non-last segment, you can use an asterisk only at the end of the segment. In the last segment, you can use an asterisk in any position of the segment. If the asterisk appears at the beginning, you cannot specify a printable character behind the asterisk. For example, the "system ; *" command string represents all commands available in system view and all subviews of the system view. The "debugging * event" command string represents all event debugging commands available in user view.
Keyword abbreviation is allowed.	You can specify a keyword by entering the first few characters of the keyword. Any command that starts with this character string matches the rule. For example, "rule 1 deny command dis arp source *" denies access to the commands **display arp source-mac interface** and **display arp source-suppression**.
To control the access to a command, you must specify the command immediately after the view that has the command.	To control access to a command, you must specify the command immediately behind the view to which the command is assigned. The rules that control command access for any subview do not apply to the command. For example, the "rule 1 deny command system ; interface * ; *" command string disables access to any command that is assigned to interface view. However, you can still execute the **acl advanced** command in interface view, because this command is assigned to system view rather than interface view. To disable access to this command, use "rule 1 deny command system ; acl *;".
Do not include the vertical bar (|), greater-than sign (>), or double greater-than sign (>>) when you specify **display** commands in a user role command rule.	The system does not treat the redirect signs and the parameters that follow the signs as part of command lines. However, in user role command rules, these redirect signs and parameters are handled as part of command lines. As a result, no rule that includes any of these signs can find a match. For example, "rule 1 permit command display debugging > log" can never find a match. This is because the system has a **display debugging** command but not a **display debugging > log** command.

Examples

Permit user role **role1** to execute the **display acl** command.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command display acl
```

Permit user role **role1** to execute all commands that start with the **display** keyword.

```
[Sysname-role-role1] rule 2 permit command display *
```

Permit user role **role1** to execute the **radius scheme aaa** command in system view and use all commands assigned to RADIUS scheme view.

```
[Sysname-role-role1] rule 3 permit command system ; radius scheme aaa
```

Deny the access of **role1** to the read or write commands of any features.

```
[Sysname-role-role1] rule 4 deny read write feature
```

Deny the access of **role1** to the read commands of the **aaa** feature.

```
[Sysname-role-role1] rule 5 deny read feature aaa
```

Permit **role1** to access all read, write, and execute commands of feature group **security-features**.

```
[Sysname-role-role1] rule 6 permit read write execute feature-group security-features
```

Permit **role1** to access all read and write MIB nodes starting from the node with OID 1.1.2.

```
[Sysname-role-role1] rule 7 permit read write oid 1.1.2
```

Related commands

display role

display role feature

display role feature-group

role

super

Use **super** to obtain another user role without reconnecting to the device.

Syntax

super [*role-name*]

Views

User view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit. If you do not specify a user role, you obtain the default target user role which is set by using the **super default role** command.

Usage guidelines

The obtained user role is a temporary user role, because this command is effective only on the current login. The next time you are logged in with the user account, the original user role settings take effect.

To enable a user to obtain another user role without reconnecting to the device, you must configure user role authentication.

- If no local password is configured in the local password authentication (**local**), an AUX user can obtain the user role by either entering a string or not entering anything.
- If no local password is configured in the local-then-remote authentication (**local scheme**), the following rules apply:
  - A VTY user performs remote authentication.
  - An AUX user can obtain user role authorization by either entering a string or not entering anything.

Examples

Obtain the user role network-operator.

```
<Sysname> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized to the role can be used.
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

super authentication-mode

Use **super authentication-mode** to set an authentication mode for temporary user role authorization.

Use **undo super authentication-mode** to restore the default.

Syntax

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

Default

Local password authentication applies.

Views

System view

Predefined user roles

network-admin

Parameters

local: Enables local password authentication.

scheme: Enables remote AAA authentication.

Usage guidelines

For local password authentication, use the **super password** command to set a password.

For remote AAA authentication, set the username and password on the RADIUS or HWTACACS server.

If you specify both **local** and **scheme** keywords, the keyword first entered in the command takes precedence.

- **scheme local**—Enables remote-then-local authentication mode. The device first performs AAA authentication to obtain a temporary user role. Local password authentication is performed if the remote HWTACACS or RADIUS server does not respond, or if the AAA configuration on the device is invalid.
- **local scheme**—Enables local-then-remote authentication mode. The device first performs local password authentication. If no password is configured for the user role, the device performs remote authentication for VTY users. An AUX user can obtain another user role by either entering a string or not entering anything.

For more information about AAA, see *Security Configuration Guide*.

Examples

Enable local-only authentication for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super authentication-mode local
```

Enable remote-then-local authentication for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super authentication-mode scheme local
```

Related commands

authentication super (*Security Command Reference*)

super password

super default role

Use **super default role** to specify the default target user role for temporary user role authorization.

Use **undo super default role** to restore the default.

Syntax

super default role *role-name*

undo super default role

Default

The default target user role is network-admin.

Views

System view

Predefined user roles

network-admin

Parameters

role-name: Specifies the name of the default target user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit.

Usage guidelines

The default target user role is applied to the **super** or **super password** command when you do not specify a user role for the command.

Examples

Specify **network-operator** as the default target user role for temporary user role authorization.

```
<Sysname> system-view
```

```
[Sysname] super default role network-operator
```

Related commands

super

super password

super password

Use **super password** to set a password for a user role.

Use **undo super password** to delete the password for a user role.

Syntax

In non-FIPS mode:

super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

undo super password [**role** *role-name*]

In FIPS mode:

super password [**role** *role-name*]

undo super password [**role** *role-name*]

Default

No password is set for a user role.

Views

System view

Predefined user roles

network-admin

Parameters

role *role-name*: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit. If you do not specify a user role, the command sets a password for the default target user role which is set by using the **super default role** command.

hash: Specifies a password in hashed form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password. In non-FIPS mode, the plaintext form of the password is a case-sensitive string of 1 to 63 characters. The hashed form of the password is a case-sensitive string of 1 to 110 characters. In FIPS mode, the password must be a case-sensitive plaintext string of 15 to 63 characters. The string must contain four character types including digits, uppercase letters, lowercase letters, and special characters.

Usage guidelines

If you do not specify any parameters, you specify a plaintext password in the interactive mode.

The FIPS mode supports only the interactive mode for setting a password.

Set a password if you configure local password authentication for temporary user role authorization.

It is a good practice to specify different passwords for different user roles.

When the global password control feature is enabled, all history super passwords are stored in hashed form.

- If you set a new super password in plaintext form, make sure the new super password is different from the current one and those stored in the history super password records.
- If you set a new super password in hashed form, the system does not compare the new super password with the current one or those stored in the history super password records.

Examples

Set the password to **123456TESTplat&!** in plaintext form for user role network-operator.

```
<Sysname> system-view
[Sysname] super password role network-operator simple 123456TESTplat&!
```

Set the password to **123456TESTplat&!** in the interactive mode for user role network-operator.

```
<Sysname> system-view
[Sysname] super password role network-operator
Password:
Confirm :
Updating user information. Please wait... ...
```

Related commands

super authentication-mode

super default role

super use-login-username

Use **super use-login-username** to enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

Use **undo super use-login-username** to restore the default.

Syntax

super use-login-username

undo super use-login-username

Default

The device prompts for a username when a login user requests temporary user role authorization from a remote authentication server.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is applicable only to the login from a user line that uses scheme authentication, which requires a username for login.

If the user was logged in from a user line that uses password authentication or no authentication, the device cannot obtain the login username. The request for temporary user role authorization from a remote authentication server will fail.

This command does not take effect on local password authentication for temporary user role authorization.

Examples

Enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

```
<Sysname> system-view
[Sysname] super use-login-username
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

vlan policy deny

Use **vlan policy deny** to enter user role VLAN policy view.

Use **undo vlan policy deny** to restore the default.

Syntax

vlan policy deny

undo vlan policy deny

Default

A user role has access to all VLANs.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the VLAN access of a user role to a set of VLANs, perform the following tasks:

1. Use **vlan policy deny** to enter user role VLAN policy view.
2. Use **permit vlan** to specify accessible VLANs.

NOTE:

The **vlan policy deny** command denies the access of the user role to any VLANs if the **permit vlan** command is not configured.

To configure a VLAN, make sure the VLAN is permitted by the user role VLAN policy in use. You can perform the following tasks on an accessible VLAN:

- Create, remove, or configure the VLAN.
- Enter VLAN view.
- Specify the VLAN in feature commands.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs.

```
<Sysname> system-view
[Sysname] role name role1
```

```
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] quit
```

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs except for VLANs 50 to 100.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 50 to 100
```

Related commands

display role

permit vlan

role

vpn-instance policy deny

Use **vpn-instance policy deny** to enter user role VPN instance policy view.

Use **undo vpn-instance policy deny** to restore the default.

Syntax

vpn-instance policy deny

undo vpn-instance policy deny

Default

A user role has access to all VPN instances.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the VPN instance access of a user role to a set of VPN instances, perform the following tasks:

1. Use **vpn-instance policy deny** to enter user role VPN instance policy view.
2. Use **permit vpn-instance** to specify accessible VPN instances.

NOTE:

The **vpn-instance policy deny** command denies the access of the user role to any VPN instances if the **permit vpn-instance** command is not configured.

To configure a VPN instance, make sure the VPN instance is permitted by the user role VPN instance policy in use. You can perform the following tasks on an accessible VPN instance:

- Create, remove, or configure the VPN instance.
- Enter VPN instance view.
- Specify the VPN instance in feature commands.

Any change to a user role VPN instance policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VPN instance policy view of **role1**, and deny the access of **role1** to any VPN instances.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] quit
```

Enter user role VPN instance policy view of **role1**, and deny the access of **role1** to any VPN instances except for **vpn2**.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn2
```

Related commands

display role

permit vpn-instance

role