Contents

Web authentication commands

display web-auth

Use **display web-auth** to display Web authentication configuration and running status on interfaces.

Syntax

display web-auth [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays Web authentication configuration for all interfaces.

Examples

Display Web authentication configuration on GigabitEthernet 1/0/1.

```
<Sysname> display web-auth interface gigabitethernet 1/0/1
 Global Web-auth parameters  :
  Proxy Port Numbers        : Not configured
  Total online web-auth users: 1
 GigabitEthernet1/0/1  is link-up
   Port role               : Authenticator
   Web-auth domain          : my-domain
   Auth-Fail VLAN           : Not configured
   Offline-detect           : Not configured
   Max online users         : 1024
   Web-auth enable          : Enabled


  Total online web-auth users: 1
```

Table 1 Command output

Field	Description
Global Web-auth parameters	Global Web authentication configuration.
Proxy Port Numbers	Port numbers of the Web proxy servers.
Total online web-auth users	Total number of online Web authentication users on the device.
GigabitEthernet1/0/1 is link-up	State of the interface: • **link-up**—The interface is both administratively and physically up. • **link-down**—The interface is down.
Port role	Role of the port. The port functions only as an **Authenticator**.

Web-auth domain	ISP domain used by Web authentication.
Auth-fail VLAN	Auth-Fail VLAN for Web authentication. This field displays **Not configured** if no Auth-Fail VLAN is configured.
Offline-detect	Interval of Web authentication user detection. This field displays **Not configured** if online detection for Web authentication users is disabled.
Max online users	Maximum number of Web authentication users allowed on the interface.
Web-auth enable	State of Web authentication: • Enabled. • Disabled.
Total online web-auth users	Total number of online Web authentication users on the interface.

display web-auth free-ip

Use **display web-auth free-ip** to display Web authentication-free subnets.

Syntax

display web-auth free-ip

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display Web authentication-free subnets.

```
<Sysname> display web-auth free-ip
      Free IP
                      : 1.1.0.0       255.255.0.0
                      : 1.2.0.0       255.255.0.0
```

Related commands

web-auth free-ip

display web-auth server

Use **display web-auth server** to display Web authentication server information.

Syntax

display web-auth server [*server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-name: Specifies a Web authentication server name, a case-sensitive string of 1 to 32 characters. If you do not specify a Web authentication server, this command displays information about all Web authentication servers.

Examples

Display information about Web authentication server **aaa**.

```
<Sysname> display web-auth server aaa
Web-auth server: aaa
  IP                   : 8.8.8.8
  Port                 : 80
  URL                  : http://8.8.8.8/portal/
  Redirect-wait-time   : 5
  URL parameters       : Not configured
```

Table 2 Command output

Field	Description
Web-auth server	Name of the Web authentication server.
IP	IP address of the Web authentication server.
Port	Port number of the Web authentication server.
URL	Redirection URL of the Web authentication server.
Redirect-wait-time	Time before redirecting an authenticated user to the webpage requested by the user.
URL parameters	Parameters in the redirection URL.

display web-auth user

Use **display web-auth user** to display information about online Web authentication users on interfaces.

Syntax

display web-auth user [**interface** *interface-type interface-number* | **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about online Web authentication users on all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays online Web authentication user information for all member devices.

Examples

Display information about online Web authentication users on GigabitEthernet 1/0/1.

```
<Sysname> display web-auth user interface gigabitethernet 1/0/1
  Total online web-auth users: 1

User name: user1
  MAC address: 0000-2700-b076
  Access interface: GigabitEthernet 1/0/1
  Initial VLAN: 1
  Authorization VLAN: N/A
  Authorization ACL ID: N/A
  Authorization user profile: N/A
```

Table 3 Command output

Field	Description
Total online web-auth users	Total number of online Web authentication users.
User Name	Name of the online Web authentication user.
MAC address	MAC address of the online Web authentication user.
Access interface	Access interface of the online Web authentication user.
Initial VLAN	Initial VLAN of the user before the user passes Web authentication.
Authorization VLAN	Authorization VLAN ID of the online Web authentication user.
Authorization ACL ID	Authorization ACL number of the online Web authentication user.
Authorization user profile	Status of user profile of the online Web authentication user: • **N/A**—No user profile is authorized. • **Active**—The authorized user profile is applied to the user access interface successfully. • **Inactive**—The authorized user profile is not applied to the user access interface or the user profile does not exist on the device.

ip

Use **ip** to specify the IP address and port number for a Web authentication server.

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

Syntax

ip *ipv4-address* **port** *port-number*

undo ip

Default

No IP address or port number is specified for a Web authentication server.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the Web authentication server. This IP address is that of a Layer 3 interface on the access device and must be routable to and from the Web authentication user.

port *port-number*: Specifies the port number of the Web authentication server, in the range of 1 to 65535.

User guidelines

As a best practice, use the IP address of a loopback interface as the IP address of the Web authentication server. A loopback interface has the following advantages:

- The status of a loopback interface is stable. This can avoid authentication page access failures caused by interface failures.
- A loopback interface does not forward received packets. This can avoid impacting system performance when there are many network access requests.

The port number of the Web authentication server must be the same as the listening port of the local portal Web service. For more information about the local portal Web service configuration, see portal authentication in *Security Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enter the view of Web authentication server **wbs**.

```
<Sysname> system-view
[Sysname] web-auth server wbs
```

Specify 192.168.1.1 as the IP address and 8080 as the port number for Web authentication server **wbs**.

```
[Sysname-web-auth-server-wbs] ip 192.168.1.1 port 8080
```

Related commands

url

tcp-port

redirect-wait-time

Use **redirect-wait-time** to set the redirection wait time. After a user passes Web authentication, the device waits for the specified period of time before redirecting the user to the specified webpage.

Use **undo redirect-wait-time** to restore the default.

Syntax

redirect-wait-time *period*

undo redirect-wait-time

Default

The redirection wait time is 5 seconds.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

period: Specifies the redirection wait time in the range of 1 to 90 seconds.

Usage guidelines

After a user passes Web authentication and is assigned an authorization VLAN, the user might need to change the IP address of the authentication client. To ensure that the redirection URL can be successfully opened, set the redirection wait time to be greater than the time that the user takes to update the IP address of the client.

Examples

Set the redirection wait time for authenticated users to 10 seconds.

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs] redirect-wait-time 10
```

url

Use **url** to specify the redirection URL for a Web authentication server.

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

Syntax

url *url-string*

undo url

Default

No redirection URL is specified for a Web authentication server.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

url-string: Specifies the redirection URL for the Web authentication server, a case-sensitive string of 1 to 256 characters.

Usage guidelines

The redirection URL is a URL that can be accessed through standard HTTP or HTTPS. The redirection URL should start with http:// or https://. If the redirection URL does not start with http:// or https://, the system determines that the URL begins with http://.

The IP address and port number in the URL must be the same as the IP address and port number of the Web authentication server.

Examples

Specify **http://192.168.1.1/portal/** as the redirection URL for Web authentication server **wbs**.

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs] url http://192.168.1.1:80/portal/
```

Related commands

ip

tcp-port

url-parameter

Use **url-parameter** to add parameters to the redirection URL of Web authentication.

Use **undo url-parameter** to delete parameters from the redirection URL of Web authentication.

Syntax

url-parameter *parameter-name* { **original-url** | **source-address** | **source-mac** | **value** *expression* }

undo url-parameter *parameter-name*

Default

No URL parameters are added to the redirection URL of Web authentication.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

parameter-name: Specifies a URL parameter name, a case-sensitive string of 1 to 32 characters. Content of the parameter is determined by the following keyword you specify.

original-url: Specifies the URL of the original webpage that a portal user visits.

source-address: Specifies the user IP address.

source-mac: Specifies the user MAC address.

value *expression*: Specifies a custom case-sensitive string of 1 to 256 characters.

Usage guidelines

You can repeat this command to add multiple URL parameters to the redirection URL of Web authentication. For example, to add the user IP address and a custom string of **http://www.abc.com/welcome** to the redirection URL, execute the following commands:

- **url-parameter userip source-address**.
- **url-parameter userurl value http://www.abc.com/welcome**.

The device will redirect Web requests from IP address 1.1.1.1 to the URL at **http://192.168.1.1/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome**.

If you execute this command multiple times to configure the same URL parameter, the most recent configuration takes effect.

When you configure the *parameter-name* argument in this command, you must use the URL parameter name supported by the Web browser. Different Web browsers support different URL parameter names.

Examples

Add parameters **userip** and **userurl** to the redirection URL of portal Web server **wbs**.

```
<Sysname> system-view
[Sysname] web-auth server wbs
```

```
[Sysname-web-auth-server-wbs] url-parameter userip source-address
[Sysname-web-auth-server-wbs] url-parameter userurl value http://www.abc.com/welcome
```

Related commands

web-auth server

web-auth auth-fail vlan

Use **web-auth auth-fail vlan** to specify an Auth-Fail VLAN for Web authentication.

Use **undo web-auth auth-fail vlan** to restore the default.

Syntax

web-auth auth-fail vlan *authfail-vlan-id*

undo web-auth auth-fail vlan

Default

No Auth-Fail VLAN is specified for Web authentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authfail-vlan-id: Specifies the Auth-Fail VLAN ID in a range of 1 to 4094. The specified VLAN must already exist.

User guidelines

After you configure this command on an interface, users who failed Web authentication on the interface can access resources in the Auth-Fail VLAN. You must also configure the IP address of the server that provides the resources as an authentication-free IP address.

To make the Auth-Fail VLAN take effect, you must also enable MAC-based VLAN on the interface, and set the subnet of the Auth-Fail VLAN as the Web authentication-free subnet.

Because MAC-based VLAN takes effect only on Hybrid ports, Auth-Fail VLAN also takes effect only on Hybrid ports.

If a user fails Web authentication, the device maps the MAC address of the user to the Auth-Fail VLAN.

You cannot delete the VLAN that has been configured as an Auth-Fail VLAN. To delete this VLAN, first cancel the Auth-Fail VLAN configuration by using **undo web-auth auth-fail vlan** command.

If a VLAN is specified as the super VLAN, do not configure this VLAN as an Auth-Fail VLAN of an interface. If a VLAN is specified as an Auth-Fail VLAN of an interface, do not configure this VLAN as a super VLAN.

Examples

Specify VLAN 5 as Web authentication Auth-Fail VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] port link-type hybrid
[Sysname–GigabitEthernet1/0/1] mac-vlan enable
[Sysname–GigabitEthernet1/0/1] web-auth auth-fail vlan 5
```

Related commands

display web-auth

web-auth domain

Use **web-auth domain** to specify an authentication domain for Web authentication users on an interface.

Use **undo web-auth domain** to restore the default.

Syntax

web-auth domain *domain-name*

undo web-auth domain

Default

No authentication domain is specified for Web authentication users on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies an ISP authentication domain name, a case-insensitive string of 1 to 255 characters.

User guidelines

After you configure this command, the device uses the authentication domain for authentication, authorization and accounting (AAA) of the Web authentication users on the interface.

Examples

Specify domain **my-domain** as the authentication domain of Web authentication users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] web-auth domain my-domain
```

web-auth enable

Use **web-auth enable** to enable Web authentication.

Use **undo web-auth enable** to disable Web authentication.

Syntax

web-auth enable apply server *server-name*

undo web-auth enable

Default

Web authentication is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

server-name: Specifies the Web authentication server name, a case-sensitive string of 1 to 32 characters.

User guidelines

Use this command to enable Web authentication on an interface and specify a Web authentication server.

For Web authentication to operate correctly, do not enable port security or configure the port security mode on the Layer 2 Ethernet interface enabled with Web authentication.

Examples

Enable Web authentication and specify Web authentication server **wbs** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth enable apply server wbs
```

Related commands

web-auth server

web-auth free-ip

Use **web-auth free-ip** to specify a Web authentication-free subnet.

Use **undo web-auth free-ip** to restore the default.

Syntax

web-auth free-ip *ip-address* { *mask-length* | *mask* }

undo web-auth free-ip { *ip-address* { *mask-length* | *mask* } | **all** }

Default

No Web-authentication-free subnets exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the Web authentication-free subnet address.

mask-length: Specifies the mask length of the Web authentication-free subnet address, in the range of 1 to 32.

mask: Specifies a mask for the Web authentication-free subnet in dotted decimal notation.

all: Specifies all Web authentication-free subnets.

User guidelines

Web authentication users can access resources in Web authentication-free subnets without being authenticated.

You can repeat this command to configure multiple Web authentication-free subnets.

Examples

Configure subnet 192.168.0.0/24 as a Web authentication-free subnet.

```
<Sysname> system-view
[Sysname] web-auth free-ip 192.168.0.0 24
```

web-auth max-user

Use **web-auth max-user** to set the maximum number of Web authentication users allowed on an interface.

Use **undo web-auth max-user** to restore the default.

Syntax

web-auth max-user *max-number*

undo web-auth max number

Default

The maximum number of Web authentication users on an interface is 1024.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of Web authentication users allowed on an interface. The value range for this argument is 1 to 2048.

User guidelines

If the specified maximum number is smaller than the number of current online Web authentication users on the interface, the limit can be set successfully. The limit does not impact the online Web authentication users. However, the device does not allow new Web authentication users to log in from the interface until the number drops down below the limit.

This command specifies the maximum number of only IPv4 Web authentication users.

Examples

On GigabitEthernet 1/0/1, set the maximum number of Web authentication users to 32.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth max-user 32
```

Related commands

display web-auth

web-auth offline-detect

Use **web-auth offline-detect** to enable online detection of Web authentication users.

Use **undo web-auth max-user** to disable online detection of Web authentication users.

Syntax

web-auth offline-detect interval *interval*

undo web-auth offline-detect interval

Default

Online detection of Web authentication users is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the Web authentication user detection interval, in the range of 60 to 65535 seconds.

User guidelines

This feature enables the device to detect packets of an online user at the specified detection interval. If no packet from the user is received within the interval, the device logs out the user and notifies the RADIUS server to stop accounting for the user.

To prevent the device from mistakenly logging out users, set the detection interval to be the same as the aging time of MAC address entries.

Examples

On GigabitEthernet 1/0/1, enable online detection of Web authentication users and set the detection interval to 3600 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth offline-detect interval 3600
```

web-auth proxy port

Use **web-auth proxy port** to add the port number of a Web proxy server, so that HTTP requests forwarded by the Web proxy server trigger Web authentication.

Use **undo web-auth proxy port** to delete one or all Web proxy server port numbers.

Syntax

web-auth proxy port *port number*

undo web-auth proxy port { *port-number* | **all** }

Default

No Web proxy server port numbers are configured on the device.

Views

System view

Predefined user roles

network-admin

Parameters

port number: Specifies a Web proxy server TCP port number, in the range of 1 to 65535.

all: Specifies all Web proxy server TCP port numbers.

User guidelines

By default, proxied HTTP requests cannot trigger Web authentication but are silently dropped. To allow such HTTP requests to trigger Web authentication, specify the port numbers of the Web proxy servers on the device.

You can repeat this command to add the port numbers of multiple Web proxy servers.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover Web proxy servers, you must perform the following tasks:

- Add the port numbers of the Web proxy servers on the device.
- Configure authentication-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.
- For Web authentication to support Web proxy:
- You must add the port numbers of the Web proxy servers on the device.
- Users must make sure their browsers that use a Web proxy server do not use the proxy server for the listening IP address of the local portal Web service. Then, HTTP packets that the Web authentication user sends to the local portal Web service are not sent to the Web proxy server.

Examples

Add the Web proxy server TCP port number of 7777 for Web authentication.

```
<Sysname> system-view
[Sysname] web-auth proxy port 7777
```

web-auth server

Use **web-auth server** to create a Web authentication server and enter its view, or enter the view of an existing Web authentication server.

Use **undo web-auth server** to delete a Web authentication server.

Syntax

web-auth server *server-name*

undo web-auth server *server-name*

Default

No Web authentication servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies a Web authentication server name, a case-sensitive string of 1 to 32 characters.

User guidelines

In Web authentication server view, you can configure the following parameters and features for the Web authentication server:

- IP address of the server.
- Redirection URL.
- Parameters to be carried in the redirection URL.

Examples

Create a Web authentication server named **wbs** and enter its view.

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs]
```

Related commands

web-auth enable apply server