A through Z

aaa accounting identity

To enable accounting and to create an accounting method list for Session Aware Networking subscriber services, use the **aaa accounting identity** command in global configuration mode. To disable accounting for Session Aware Networking, use the **no** form of this command.

aaa accounting identity {*method-list-name*| **default**} **start-stop [broadcast] group** {*server-group-name*| **radius**| **tacacs+**} [**group**{*server-group-name*| **radius**| **tacacs+**}]

no aaa accounting identity {*method-list-name*| **default**}

Syntax Description

method-list-name	Name of the method list for which to create accounting services by specifying the accounting methods that follow this name.
default	Creates a default method list for accounting services using the accounting methods that follow this keyword.
start-stop	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
broadcast	(Optional) Sends accounting records to multiple authentication, authorization, and accounting (AAA) servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, the device uses the backup servers defined within that group.
group	Specifies one or more server groups to use for accounting services. Server groups are applied in the specified order.
server-group-name	Named subset of RADIUS or TACACS+ servers as defined by the **aaa group server radius** command or **aaa group server tacacs+** command.
radius	Uses the list of all RADIUS servers configured with the **radius-server host** command.
tacacs+	Uses the list of all TACACS+ servers configured with the **tacacs-server host** command.

Command Default Accounting is disabled.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines The **aaa accounting identity** command enables accounting services and creates method lists that define specific accounting methods for Session Aware Networking subscriber services. A method list identifies the list of security servers to which the network access server sends accounting records.

Cisco IOS software supports the following two methods of accounting for Session Aware Networking:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

The default method list is automatically applied to all subscriber sessions except those that have a named method list explicitly defined. A named method list overrides the default method list.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server.

You must enable AAA with the **aaa new-model** command before you can enter the **aaa accounting identity** command.

Examples The following example shows how to configure a default accounting method list where accounting services are provided by a TACACS+ server.

```
aaa new-model
aaa accounting identity default start-stop group tacacs+
```

The following example shows how to configure a named accounting method list, where accounting services are provided by a RADIUS server.

```
aaa new model
aaa accounting identity LIST_1 start-stop group radius
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists.
aaa group server tacacs+	Groups different TACACS+ server hosts into distinct lists.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.

aaa local authentication

To specify the method lists to use for local authentication and authorization from a Lightweight Directory Access Protocol (LDAP) server, use the **aaa local authentication** command in global configuration mode. To return to the default value, use the **no** form of this command.

aaa local authentication {*method-list-name*| **default**} **authorization** {*method-list-name*| **default**}

no aaa local authentication {*method-list-name*| **default**} **authorization** {*method-list-name*| **default**}

Syntax Description

method-list-name	Name of the AAA method list.
default	Uses the default AAA method list.

Command Default

Local LDAP-based authentication is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(1)S	This command was introduced.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **aaa local authentication** command to retrieve Extensible Authentication Protocol (EAP) credentials from local or remote LDAP servers.

Examples

The following example shows how to configure local authentication to use the method list named EAP_LIST:

```
aaa new-model
aaa local authentication EAP_LIST authorization EAP_LIST
```

Related Commands

aaa new-model	Enables the AAA access control model.
ldap server	Defines an LDAP server.

absolute-timer

To enable an absolute timeout for subscriber sessions, use the **absolute-timer** command in service template configuration mode. To disable the timer, use the **no** form of this command.

absolute-timer *minutes*

no absolute-timer

Syntax Description

minutes	Maximum session duration, in minutes. Range: 1 to 65535. Default: 0, which disables the timer.

Command Default

Disabled (the absolute timeout is 0).

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **absolute-timer** command to limit the number of minutes that a subscriber session can remain active. After this timer expires, a session must repeat the process of establishing its connection as if it were a new request.

Examples

The following example shows how to set the absolute timeout to 15 minutes in the service template named SVC_3:

```
service-template SVC_3
 description sample
 access-group ACL_2
 vlan 113
 inactivity-timer 15
 absolute-timer 15
```

Related Commands

Command	Description
event absolute-timeout	Specifies the type of event that triggers actions in a control policy if conditions are met.
inactivity-timer	Enables an inactivity timeout for subscriber sessions.

Command	Description
show service-template	Displays configuration information for service templates.

access-group (service template)

To apply an access list to sessions using a service template, use the **access-group** command in service template configuration mode. To remove the access group, use the **no** form of this command.

access-group *access-list-name*

no access-group *access-list-name*

Syntax Description

access-list-name	Name of the access control list (ACL) to apply.

Command Default

An access list is not applied.

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **access-group** command to apply a locally configured ACL to sessions on which the service template is activated.

Examples

The following example shows how to configure a service template named SVC_2 that applies the access list named ACL_in to sessions:

```
service-template SVC_2
 description label for SVC_2
 access-group ACL_in
 redirect url http://cisco.com match URL_ACL
 tag TAG_1
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.
ip access-list	Defines an IP access control list (ACL).

access-session closed

To prevent preauthentication access on a port, use the **access-session closed** command in interface configuration mode. To return to the default value, use the **no** form of this command.

access-session closed

no access-session closed

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (access is open on the port).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **access-session closed** command closes access to a port, preventing clients or devices from gaining network access before authentication is performed.

Examples

The following example shows how to set port 1/0/2 to closed access.

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

Related Commands

access-session control-direction	Sets the direction of authentication control on a port.
access-session host-mode	Allows hosts to gain access to a controlled port.
access-session port-control	Sets the authorization state of a port.

access-session control-direction

To set the direction of authentication control on a port, use the **access-session control-direction** command in interface configuration mode. To return to the default value, use the **no** form of this command.

access-session control-direction {**both**| **in**}

no access-session control-direction

Syntax Description

both	Enables bidirectional control on the port. This is the default value.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **access-session control-direction** command to set the port control to either unidirectional or bidirectional.

The **in** keyword configures a port as unidirectional, allowing a device on the network to “wake up” the client and force it to reauthenticate. The port can send packets to the host but cannot receive packets from the host.

The **both** keyword configures a port as bidirectional so that access to the port is controlled in both directions. The port cannot send or receive packets.

You can use the **show access-session interface** command to verify the port setting.

Examples

The following example shows how to enable unidirectional control on port 1/0/2:

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

Related Commands

access-session closed	Prevents preauthentication access on a port.
access-session host-mode	Allows hosts to gain access to a controlled port.

access-session port-control	Sets the authorization state of a port.
show access-session	Displays information about authentication sessions.

access-session host-mode

To allow hosts to gain access to a controlled port, use the **access-session host-mode** command in interface configuration mode. To return to the default value, use the **no** form of this command.

access-session host-mode {**multi-auth**| **multi-domain**| **multi-host**| **single-host**}

no access-session host-mode

Syntax Description

multi-auth	Specifies that multiple clients can be authenticated on the port at any given time. This is the default value.
multi-domain	Specifies that only one client per domain (DATA or VOICE) can be authenticated at a time.
multi-host	Specifies that after the first client is authenticated all subsequent clients are allowed access.
single-host	Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected.

Command Default

Access to a port is multi-auth.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Before you use this command, you must enable the **access-session port-control auto** command.

In multi-host mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN (EAPOL) logoff message is received), all attached clients are denied access to the network.

You can use the **show access-session interface** command to verify the port setting.

Examples

The following example shows how to authenticate a single client at a time on port 1/0/2:

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

Related Commands

access-session closed	Prevents preauthentication access on a port.
access-session control-direction	Sets the direction of authentication control on a port.
access-session port-control	Sets the authorization state of a port.
show access-session	Displays information about authentication sessions.

access-session port-control

To set the authorization state of a port, use the **access-session port-control** command in interface configuration mode. To return to the default value, use the **no** form of this command.

access-session port-control {**auto**| **force-authorized**| **force-unauthorized**}

no access-session port-control

Syntax Description

auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This is the default value.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Command Default

The port is set to the force-authorized state.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

Examples

The following example shows how to set the authorization state on port 1/0/2 to automatic:

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

Related Commands

access-session closed	Prevents preauthentication access on a port.
access-session host-mode	Allows hosts to gain access to a controlled port.
access-session port-control	Sets the authorization state of a port.

access-session tunnel vlan

To configure an access session for a VLAN tunnel, use the **access-session tunnel vlan** command in global configuration mode. To remove the access session, use the **no** form of this command.

access-session tunnel vlan *vlan-id*

no access-session tunnel vlan [*vlan-id*]

Syntax Description

vlan-id	Specifies the tunnel VLAN ID. The range is from 1 to 4096.

Command Default

Access to VLAN tunnel is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

Before you use this command, you must configure a VLAN using the **vlan** command.

You can use the **show access-session** command to verify access session settings.

Note If a wired guest access is not being configured, VLAN ID of 325 is used as default.

Examples

The following example shows how to configure access to tunnel a VLAN :

```
Device# configure terminal
Device(config)# vlan 1755
Device(config-vlan)# exit
Device(config)# access-session vlan 1755
```

Related Commands

show access-session	Displays information about access sessions.
vlan (service template)	Assigns a VLAN to subscriber sessions.

activate (policy-map action)

To activate a control policy or service template on a subscriber session, use the **activate** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** *number*] [**replace-all**]}

no *action-number*

Syntax Description

action-number	Action identifier. Actions are executed sequentially within the policy rule.
policy type control subscriber *control-policy-name*	Specifies the name of the control policy to apply to a session, as defined by the **policy-map type control subscriber** command.
service-template *template-name*	Specifies the name of the service template to apply to a session. This template can be defined locally with the **service-template** command or downloaded from an authentication, authorization, and accounting (AAA) server.
aaa-list *list-name*	(Optional) Specifies the name of the AAA method list that identifies the AAA server from which to download the service template. If this is not specified, the template must be locally defined.
precedence *number*	(Optional) Specifies the priority level of the service template. Range: 1 to 254, where 1 is the highest priority and 254 is the lowest.
replace-all	(Optional) Replaces all existing authorization data and services with new data and services.

Command Default

A control policy or service template is not activated for subscriber sessions.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Release	Modification
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **activate** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before actions are executed. Actions are numbered and executed sequentially within a policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions.

Examples

The following example shows how to configure a control policy named SEQ-AUTH-WITH-AUTH-FAIL-VLAN. If authentication fails, and all conditions in the control class DOT1X_FAILED evaluate true, the system activates the service template named VLAN4.

```
class-map type control subscriber DOT1X-FAILED match-any
  match result-type method dot1x authoritative
  match result-type method dot1x agent-not-found
!
class-map type control subscriber MAB-FAILED match-all
  match method mab
  match result-type authoritative
!
policy-map type control subscriber SEQ-AUTH-WITH-AUTH-FAIL-VLAN
  event session-started match-all
   10 class always do-all
    10 authenticate using mab priority 20
  event authentication-failure match-all
   10 class MAB_FAILED do-all
    10 terminate mab
    20 authenticate using dot1x priority 10
   20 class DOT1X_FAILED do-all
    10 activate service-template VLAN4
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
deactivate	Deactivates a control policy or service template on a subscriber session.
event	Specifies the type of event that causes a control class to be evaluated.
service-template	Defines a service template that contains a set of attributes to apply to subscriber sessions.

authenticate using

To initiate the authentication of a subscriber session using the specified method, use the **authenticate using** command in control policy-map action configuration mode. To remove this action from a control policy, use the **no** form of this command.

action-number **authenticate using** {**dot1x**| **mab**| **webauth**}[**aaa** {**authc-list** *authc-list-name*| **authz-list** *authz-list-name*}] **[merge]** [**parameter-map** *parameter-map-name*] [**priority** *priority-number*] [**replace**| **replace-all**] [**retries** *number* {**retry-time** *seconds*}]

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
dot1x	Specifies the IEEE 802.1X authentication method.
mab	Specifies the MAC authentication bypass (MAB) method.
webauth	Specifies the web authentication method.
aaa	(Optional) Indicates that authentication is performed using an authentication, authorization, and accounting (AAA) method list.
authc-list *authc-list-name*	Specifies the name of AAA method list to use for authentication requests.
authz-list *authz-list-name*	Specifies the name of AAA method list to use for authorization requests.
merge	(Optional) Merges the new data and services into the existing authorization data and services.
parameter-map *parameter-map-name*	(Optional) Specifies the name of a parameter map to use for web authentication, as defined by the **parameter map type webauth** command.
priority *priority-number*	(Optional) Specifies the priority of the selected authentication method. Allows a higher priority method to interrupt an authentication in progress with a lower priority method. Range: 1 to 254, where 1 is the highest priority and 254 is the lowest. The default priority order is dot1x, mab, then webauth.
replace	(Optional) Replace existing authorization data with the new authorization data.

replace-all	(Optional) Replace all existing authorization data and services with the new data and services. This is the default behavior.
retries *number*	(Optional) Number of times to retry an authentication method if the initial attempt fails. Range: 1 to 5. Default: 2.
retry-time *seconds*	Number of seconds between authentication attempts. Range: 0 to 65535. Default: 30.

Command Default

Authentication is not initiated.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **authenticate using** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions.

When an AAA method list is configured, the RADIUS or TACACS+ AAA server checks for a valid account by looking at the username and password. The authentication list and the authorization list usually share the same AAA method list; the lists can use different databases but it is not recommended.

Examples

The following example shows the partial configuration of a control policy named CONC_AUTH. When a session starts, the default control class specifies that 802.1X and MAB authentication run concurrently. 802.1X has a higher priority (10) than MAB (20) so 802.1X is used to authenticate the session, unless it fails, and then MAB authentication is used.

```
policy-map type control subscriber CONC_AUTH
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using mab priority 20
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
class-map type control subscriber	Creates a control class, which defines the conditions under which the actions of a control policy are executed.
parameter-map type webauth	Defines a parameter map for web authentication.

authentication-restart

To restart the authentication process after an authentication or authorization failure, use the **authentication-restart** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **authentication-restart** *seconds*

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
seconds	Number of seconds to wait before restarting the authentication process after a failure occurs. Range: 1 to 65535.

Command Default

Authentication is not restarted.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **authentication-restart** command configures an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows the partial configuration of a control policy with the **authentication-restart** command configured for the authentication-failure event:

```
class-map type control subscriber match-all DOT1X_TIMEOUT_FAIL
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-all DOT1X_AUTH_FAIL
 match result-type method dot1x authoritative
!
policy-map type control subscriber POLICY
 event session-started match-first
```

```
 10 class always do-all
  10 authenticate using dot1x
event authentication-failure match-all
  .
  .
  .
 50 class DOT1X_AUTH_FAIL do-all
  50 authentication-restart 60
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
resume reauthentication	Resumes reauthentication after an authentication failure.

authentication display

To set the configuration display mode for Session Aware Networking, use the **authentication display** command in privileged EXEC mode.

authentication display {**legacy**| **new-style**}

Syntax Description

legacy	Displays the configuration using the legacy authentication manager style. This is the default mode.
new-style	Displays the configuration using the Cisco common classification policy language (C3PL) style that supports Session Aware Networking.

Command Default

The legacy mode is enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **authentication display** command to enable the configuration display mode that supports Session Aware Networking. This command allows you to switch between the two different display modes until you enter a configuration for Session Aware Networking. After you enter a configuration that is specific to Session Aware Networking, this command is disabled and becomes unavailable.

The **new-style** keyword converts all relevant legacy authentication commands to their new command equivalents. If you save the configuration when new-style mode is enabled, the system writes the configuration in the new style. If you then perform a reload, you will not be able to revert to legacy mode.

Examples

The following example shows how to set the display mode to the style used for Session Aware Networking:

```
Device# authentication display new-style
```

Related Commands

Command	Description
policy-map type control subscriber	Defines a control policy for subscriber sessions.

authorize

To initiate the authorization of a subscriber session, use the **authorize** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **authorize**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

Authorization is not initiated.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **authorize** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions will be executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions.

Examples

The following example shows how to configure a control policy with the authorize action configured for the authentication-failure event:

```
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-any SERVER_DOWN
 match result-type aaa-timeout
!
policy-map type control subscriber POLICY_4
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
 event authentication-failure match-first
  10 class SERVER_DOWN do-all
   10 authorize
  20 class MAB do-all
```

```
 10 authenticate using dot1x priority 10
30 class DOT1X do-all
 10 activate service-template VLAN4
 20 authentication-restart 60
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
class-map type control subscriber	Creates a control class, which defines the conditions under which the actions of a control policy are executed.
policy-map type control subscriber	Defines a control policy for subscriber sessions.
unauthorize	Removes all authorization data from a subscriber session.

banner (parameter-map webauth)

To display a banner on the web-authentication login web page, use the **banner** command in parameter map webauth configuration mode. To disable the banner display, use the **no** form of this command.

banner [**file** *location*:*filename*| **text** *banner-text*]

no banner [**file** *location*:*filename*| **text** *banner-text*]

Syntax Description

file *location*:*filename*	(Optional) Specifies a file that contains the banner to display on the web authentication login page.
text *banner-text*	(Optional) Specifies a text string to use as the banner. You must enter a delimiting character before and after the banner text. The delimiting character can be any character of your choice, such as “c” or “@.”

Command Default

No banner displays on the web-authentication login web page.

Command Modes

Parameter map webauth configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **banner** command allows you to configure one of three possible scenarios:

- The **banner** command without any keyword or argument—Displays the default banner using the name of the device: “Cisco Systems, <device’s hostname> Authentication.”
- The **banner** command with the **file** *filename* keyword-argument pair—Displays the banner from the custom HTML file you supply. The custom HTML file must be stored in the disk or flash of the device.
- The **banner** command with the **text** *banner-text* keyword-argument pair—Displays the text that you supply. The text must include any required HTML tags.

Note If the **banner** command is not enabled, nothing displays on the login page except text boxes for entering the username and password.

Examples

The following example shows that a file in flash named webauth_banner.html is specified for the banner:

```
parameter-map type webauth MAP_1
 type webauth
 banner file flash:webauth_banner.html
```

The following example shows how to configure the message “login page banner” by using “c” as the delimiting character, and it shows the resulting configuration output.

```
Device(config-params-parameter-map)# banner text c login page banner c
parameter-map type webauth MAP_2
 type webauth
 banner text ^c login page banner ^c
```

Note The caret symbol (^) displays in the configuration output before the delimiting character that you entered even though you do not enter it.

Related Commands

Command	Description
consent email	Requests a user’s e-mail address on the web-authentication login web page.
redirect (parameter-map webauth)	Redirects users to a particular URL during web-based authentication.
show ip admission status banner	Displays information about configured banners for web authentication.

class

To associate a control class with one or more actions in a control policy, use the **class** command in control policy-map class configuration mode. To remove the control class from the control policy, use the **no** form of this command.

priority-number **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**]

no *priority-number*

Syntax Description

priority-number	Relative priority of the control class within the policy rule. This priority determines the order in which control policies are applied to a session. Range: 1 to 254, where 1 is the highest priority and 254 is the lowest.
control-class-name	Name of a previously configured control class as defined by the **class-map type control subscriber** command.
always	Creates a default control class that always evaluates true.
do-all	(Optional) Executes all actions.
do-until-failure	(Optional) Executes actions, in order, until one of the actions fails. This is the default behavior.
do-until-success	(Optional) Executes actions, in order, until one of the actions is successful.

Command Default

A control class is not associated with the control policy.

Command Modes

Control policy-map class configuration (config-class-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **class** command associates the conditions in a control class with one or more actions in a control policy. A control class defines the conditions that must be met before a set of actions are executed. The association of a control class and a set of actions is called a control policy rule.

Use the *control-class-name* argument to specify a named control class that was created using the **class-map type control subscriber** command.

Use the **always** keyword to create a default control class that always evaluates true for the given event.

Examples

The following example shows how to configure a control class named DOT1X-NO-AGENT. The **class** command associates DOT1X-NO-AGENT with the control policy named POLICY-1. If DOT1X-NO-AGENT evaluates true, the actions associated with the class are executed.

```
class-map type control subscriber match-first DOT1X-NO-AGENT
 match result-type method dot1x agent-not-found
!
policy-map type control subscriber POLICY-1
 event session-started match-all
  10 class always do-all
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_AGENT do-all
   10 authenticate using mab priority 20
  20 class DOT1X_TIMEOUT do-all
   10 authenticate using mab priority 20
  30 class DOT1X_FAILED do-all
   10 authenticate using mab priority 20
```

Related Commands

Command	Description
class-map type control subscriber	Creates a control class, which defines the conditions under which the actions of a control policy are executed.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

class-map type control subscriber

To create a control class, which defines the conditions under which the actions of a control policy are executed, use the **class-map type control subscriber** command in global configuration mode. To remove a control class, use the **no** form of this command.

class-map type control subscriber {**match-all | match-any | match-none**} *control-class-name*

no class-map type control subscriber {**match-all | match-any | match-none**} *control-class-name*

Syntax Description

match-all	Specifies that all conditions in the control class must evaluate true.
match-any	Specifies that at least one of the conditions in the control class must evaluate true.
match-none	Specifies that all conditions in the control class must evaluate false.
control-class-name	Name of the control class.

Command Default

A control class is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

A control class defines the conditions that must be met for the actions in a control policy to be executed. A control class can contain multiple conditions. Use the **match-any**, **match-all**, or **match-none** keywords to specify which, if any, of the conditions the subscriber session must match for the actions to be executed.

A control policy, which is configured with the **policy-map type control subscriber** command, contains one or more control classes that are evaluated based on the event specified with the **event** command. Use the **class** command to create a policy rule by associating a control class with one or more actions.

Examples

The following example shows the partial configuration for a control class named DOT1X-AUTHORITATIVE, which is associated with the control policy named DOT1X-MAB-WEBAUTH. If an authentication-failure

event occurs, and the session matches all of the conditions in DOT1X-AUTHORITATIVE, the policy executes the authenticate action and attempts to authenticate the session using MAC authentication bypass (MAB).

```
class-map type control subscriber match-all DOT1X-AUTHORITATIVE
  match method dot1x
  match result-type authoritative
!
policy-map type control subscriber DOT1X-MAB-WEBAUTH
  event session-started match-all
   10 class always do-until-failure
    10 authenticate using dot1x retries 3 retry-time 15
  event authentication-failure match-all
   10 class DOT1X_AUTHORITATIVE
    10 authenticate using mab
   .
   .
   .
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

clear-authenticated-data-hosts-on-port

To clear authenticated data hosts on a port after an authentication failure, use the **clear-authenticated-data-hosts-on-port** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **clear-authenticated-data-hosts-on-port**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

Hosts on a port are not cleared.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **clear-authenticated-data-hosts-on-port** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows how to configure a control policy with the clear-authenticated-data-hosts-on-port action configured for the authentication-failure event:

```
policy-map type control subscriber POLICY_Et0/0
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template VLAN123
   20 authorize
   30 pause reauthentication
   40 clear-authenticated-data-hosts-on-port
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class always do-until-failure
```

```
   10 terminate dot1x
   20 authentication-restart 60
event agent-found match-all
 10 class always do-until-failure
   10 authenticate using dot1x priority 10
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
clear-session	Clears an active subscriber session.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.

clear-session

To clear an active subscriber session, use the **clear-session** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **clear-session**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

The session is not cleared.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **clear-session** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows how to configure a control policy with the clear-session action configured for the inactivity-timeout event:

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-all
   10 authenticate using dot1x
 event authentication-failure match-all
  10 class DOT1X_NO_AGENT do-all
   10 activate fallback template VLAN510
 event inactivity-timeout match-all
  10 class always do-all
   10 clear-session
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.

consent email

To request a user's e-mail address on the consent login web page, use the **consent email** command in parameter map webauth configuration mode. To remove the consent parameter file from the map, use the **no** form of this command.

consent email

no consent email

Syntax Description

This command has no arguments or keywords.

Command Default

The e-mail address is not requested on the consent login page.

Command Modes

Parameter map webauth configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **consent email** command to display a text box on the consent login page prompting the user to enter his or her e-mail address for identification. The device sends this e-mail address to the authentication, authorization, and accounting (AAA) server instead of sending the client's MAC address.

The consent feature allows you to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent web page. This web page lists the terms and conditions under which the organization is willing to grant access to end users. Users can connect to the network only after they accept the terms on the consent web page.

If you create a parameter map with the **type** command set to consent, the device does not prompt the user for his or her username and password credentials. Users instead get a choice of two radio buttons: accept or do not accept. For accounting purposes, the device sends the client's MAC address to the AAA server if no username is available (because consent is enabled).

This command is supported in named parameter maps only.

Examples

The following example shows how to enable the consent e-mail feature in a parameter map:

```
parameter-map type webauth PMAP_1
 type consent
 consent email
 banner file flash:consent_page.htm
```

Related Commands

Command	Description
banner (parameter-map webauth)	Displays a banner on the web-authentication login web page.
custom-page	Displays custom web pages during web authentication login.
type (parameter-map webauth)	Defines the methods supported by a parameter map.

custom-page

To display custom web pages during web authentication login, use the **custom-page** command in parameter map webauth configuration mode. To disable custom web pages, use the **no** form of this command.

custom-page {**failure**| **login [expired]**| **success**} **device** *location***:***filename*

no custom-page {**failure**| **login [expired]**| **success**} **device** *location***:***filename*

Syntax Description

failure	Displays the custom web page if the login fails.
login	Displays the custom web page during login.
expired	(Optional) Displays the custom web page if the login expires.
success	Displays the custom web page when the login is successful.
location **:***filename*	Location and name of the locally stored HTML file to use in place of the default HTML file for the specified condition.

Command Default

The internal default web pages are displayed.

Command Modes

Parameter map webauth configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **custom-page** command to display custom web pages during web authentication login. To enable custom web pages:

- You must specify all four custom HTML files. If fewer than four files are specified, the internal default HTML pages are used.
- The four custom HTML files and any images in the custom pages must be stored in the disk or flash of the switch. The maximum size of each HTML file is 256 KB.
- Filenames must start with web_auth.

- To serve custom pages and images from an external server, you must configure a redirect portal IP address by using the **redirect** (parameter-map webauth) command instead of using local custom pages.
- Any external link from a custom page requires an intercept ACL configuration.
- Any name resolution required for external links or images requires an intercept ACL configuration.
- If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.
- Because the custom login page is a public web form, consider the following guidelines for this page:
  - The login form must accept user input for the username and password and must POST the data as uname and pwd.
  - The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

Examples

The following example shows how to configure a named parameter map for web authentication with custom pages enabled:

```
parameter-map type webauth PMAP_WEBAUTH
 type webauth
 custom-page login device flash:webauth_login.html
 custom-page success device flash:webauth_success.html
 custom-page failure device flash:webauth_fail.html
 custom-page login expired device flash:webauth_expire.html
```

Related Commands

Command	Description
banner (parameter-map webauth)	Displays a banner on the web-authentication login web page.
consent email	Requests a user's e-mail address on the consent login web page.
redirect (parameter-map webauth)	Redirects clients to a particular URL during web-based authentication.

deactivate

To deactivate a control policy or service template on a subscriber session, use the **deactivate** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **deactivate** {**policy type control subscriber** *control-policy-name*| **service-template** *template-name*}

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
policy type control subscriber *control-policy-name*	Specifies the name of the control policy to deactivate on the session, as defined by the **policy-map type control subscriber** command.
service-template *template-name*	Specifies the name of the service template to deactivate on the session, as defined by the **service-template** command.

Command Default

A control policy or service template is not deactivated.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **deactivate** command defines an action in a control policy. This command uninstalls all control policies and policy attributes that have been applied on the session.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions.

Examples

The following example shows how to configure a control policy that provides limited access to all hosts even when authentication fails. If authentication succeeds, the policy manager deactivates the service template

named LOW_IMPACT_TEMPLATE and provides access based on the policies downloaded by the RADIUS server.

```
class-map type control subscriber match-all DOT1X_MAB_FAILED
 no-match result-type method dot1x success
 no-match result-type method mab success
!
policy-map type control subscriber CONCURRENT_DOT1X_MAB_LOW_IMP_MODE
 event session-started match-all
  10 class always do-until-failure
   10 authorize
   20 activate service-template LOW_IMPACT_TEMPLATE
   30 authenticate using mab
   40 authenticate using dot1x
 event authentication-success match-all
  10 class always do-until-failure
   10 deactivate service-template LOW_IMPACT_TEMPLATE
 event authentication-failure match-first
  10 class DOT1X_MAB_FAILED do-until-failure
   10 authorize
   20 terminate dot1x
   30 terminate mab
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.
service-template	Defines a service template that contains a set of policy attributes to apply to subscriber sessions.

debug access-session

To display debugging information about Session Aware Networking sessions, use the **debug access-session** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug access-session [**feature** *feature-name*] {**all**| **detail**| **errors**| **events**| **sync**}

no debug access-session [**feature** *feature-name*] {**all**| **detail**| **errors**| **events**| **sync**}

Syntax Description

feature *feature-name*	(Optional) Displays debugging information about specific features. To display the valid feature names, use the question mark (**?**) online help function.
all	Displays all debugging information for Session Aware Networking.
detail	Displays detailed debugging information.
errors	Displays debugging information about errors.
events	Displays debugging information about events.
sync	Displays debugging information about stateful switchovers (SSOs) or In Service Software Upgrades (ISSUs).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **debug access-session** command to troubleshoot Session Aware Networking sessions.

Related Commands

Command	Description
debug authentication	Displays debugging information about the Authentication Manager.
debug dot1x	Displays 802.1x debugging information.

Command	Description
show access-session	Displays information about Session Aware Networking sessions.

debug ip admission

To display web authentication debugging information, use the **debug ip admission** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

Cisco IOS XE Release 3SE and Later Releases

debug ip admission {**aaa**| **acl**| **all**| **dos**| **eapoudp**| **error**| **ha**| **httpd**| **idle**| **input-feature**| **io**| **page**| **qualify**| **session**| **sm**| **state**| **timer**}

no debug ip admission {**aaa**| **acl**| **all**| **dos**| **eapoudp**| **error**| **ha**| **httpd**| **idle**| **input-feature**| **io**| **page**| **qualify**| **session**| **sm**| **state**| **timer**}

All Other Releases

debug ip admission {**api**| **consent**| **detailed**| **dos**| **eapoudp**| **error**| **ezvpn**| **fallback**| **function-trace**| **httpd**| **object-creation**| **object-deletion**| **timers**}

no debug ip admission {**api**| **consent**| **detailed**| **dos**| **eapoudp**| **error**| **ezvpn**| **fallback**| **function-trace**| **httpd**| **object-creation**| **object-deletion**| **timers**}

Syntax Description

aaa	Displays IP admission authentication, authorization, and accounting (AAA) events.
acl	Displays IP admission access control list (ACL) events.
all	Displays all IP admission debugging information.
dos	Displays authentication proxy DOS prevention events.
eapoudp	Displays information about Extensible Authentication Protocol over User Datagram Protocol (UDP) (EAPoUDP) network admission control events.
error	Displays web authentication error messages.
ha	Displays high availability (HA) events.
httpd	Displays web authentication HTTP Daemon information.
idle	Displays Layer 3 (L3) idle timer events.
input-feature	Displays IP admission input-feature events.
io	Displays IP admission HTTP proxy daemon input/output events.
page	Displays IP admission HTTP page events.

qualify	Displays IP admission packet qualification.
session	Displays IP admission session events.
sm	Displays IP admission session manager events.
state	Displays IP admission state transitions.
timers	Displays authentication proxy timer-related events.
api	Displays IP Admission API events.
consent	Displays web authentication consent page information.
detailed	Displays details of the TCP events during an authentication proxy process. The details are generic to all FTP, HTTP, and Telnet protocols.
ezvpn	Displays authentication proxy Easy VPN (EzVPN)-related events
fallback	Displays IP admission fallback events.
function-trace	Displays the authentication proxy functions.
object-creation	Displays additional entries to the authentication proxy cache.
object-deletion	Displays deletion of cache entries for the authentication proxy.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.2SE	This command was modified. The **aaa**, **acl**, **all**, **dos**, **ha**, **idle**, **input-feature**, **io**, **page**, **qualify**, **session**, **sm**, and **state** keywords were added.

Usage Guidelines

Use the **debug ip admission** command to troubleshoot web authentication.

Examples

The following is sample output from the **debug ip admission eapoudp** command:

```
Device# debug ip admission eapoudp

Posture validation session created for client mac= 0001.027c.f364 ip= 10.0.0.1
Total Posture sessions= 1 Total Posture Init sessions= 1
*Apr  9 19:39:45.684: %AP-6-POSTURE_START_VALIDATION: IP=10.0.0.1|
Interface=FastEthernet0/0.420
*Apr  9 19:40:42.292: %AP-6-POSTURE_STATE_CHANGE: IP=10.0.0.1| STATE=POSTURE ESTAB
*Apr  9 19:40:42.292: auth_proxy_posture_parse_aaa_attributes:
CiscoDefined-ACL name= #ACSACL#-IP-HealthyACL-40921e54
Apr  9 19:40:42.957: %AP-6-POSTURE_POLICY: Apply access control list
(xACSACLx-IP-HealthyACL-40921e54) policy for host (10.0.0.1)
```

Related Commands

debug access-session	Displays debugging information about Session Aware Networking sessions.
show ip admission	Displays the network admission control (NAC) cache entries or the NAC configuration.

description (service template)

To add a description to a service template, use the **description** command in service template configuration mode. To remove the description, use the **no** form of this command.

description *description*

no description *description*

Syntax Description

description	Description of the service template.

Command Default

A description does not display for the service template.

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **description** command to provide additional information about the service template when you display the service template configuration.

Examples

The following example shows how to configure a service template with a description:

```
service-template SVC_2
 description label for SVC_2
 access-group ACL_2
 redirect url http://www.cisco.com
 inactivity-timer 15
 tag TAG_2
```

Related Commands

Command	Description
show service-template	Displays information about service templates.

err-disable

To disable a port after a security violation occurs, use the **err-disable** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **err-disable**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

The port is not disabled.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **err-disable** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the policy can execute the actions. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that you can define in a policy rule depend on the type of event that you specify with the **event** command.

After the policy executes this action, the port remains disabled until the interval set with the **error recovery interval** command expires (default is 300 seconds). If you have not enabled error recovery with the **errdisable recovery cause security-violation** command, the port remains disabled indefinitely.

Examples

The following example shows how to configure a control policy with the err-disable action configured:

```
policy-map type control subscriber POLICY_1
 event violation match-all
  10 class always do-until-failure
   10 err-disable
```

Related Commands

Command	Description
errdisable recovery	Configures recovery mechanism variables.

Command	Description
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
restrict	Drops violating packets and generates a syslog message after a security violation on a port.

event

To specify the type of event that triggers actions in a control policy if conditions are met, use the **event** command in control policy-map event configuration mode. To remove the event condition, use the **no** form of this command.

event *event-name* [**match-all** | **match-first**]

no event *event-name* [**match-all** | **match-first**]

Syntax Description

event-name	Event type that triggers actions after conditions in the control class are met. Valid keywords are: • **aaa-available—**A previously unreachable authentication, authorization, and accounting (AAA) server is available. • **absolute-timeout—**Absolute timer has expired on the session. This timer is configured with the **absolute-timer** command. • **agent-found—**Agent for authentication method is successfully detected. • **authentication-failure—**Session authentication has failed. • **authentication-success—**Session is successfully authenticated. • **authorization-failure—**Port authorization has failed. • **inactivity-timeout—**Inactivity timer has expired for the session. This timer is configured with the **inactivity-timer** command. • **remote-authentication-failure—**Remote session authentication failed. • **remote-authentication-success—**Remote session successfully authenticated.

	• **session-started—**Port-up event resulted in creating a session. This event is triggered when a new MAC address is detected on the relevant interface. • **tag-added—**A service template tag was added. This tag is specified with the **tag** (service-template) command. • **tag-removed—**A service template tag was removed. • **template-activated—**A service template is activated on the session. • **template-activation-failed—**Activating a service template on the session failed. • **template-deactivated—**A service template is deactivated on the session. • **template-deactivation-failed—**Deactivating a service template on the session failed. • **timer-expiry—**A timer that was started on the session expired. This timer is started with the **set-timer** command. • **violation—**Session violation detected.
match-all	(Optional) Evaluates all control classes. This is the default behavior.
match-first	(Optional) Evaluates only the first control class.

Command Default

The event evaluates all control classes in a control policy.

Command Modes

Control policy-map event configuration (config-event-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.
Cisco IOS XE Release 3.3SE	This command was modified. The **remote-authentication-failure** and **remote-authentication-success** keywords were added.

Usage Guidelines

The **event** command configures an event condition in a control policy. After the specified event occurs, the system evaluates the control classes. Control classes specify the conditions that must be met to execute the actions in the control policy. The **class** command creates a policy rule by associating a control class with one or more actions.

The **event** command determines the actions that can be defined in a policy rule. For example, the action defined with the **err-disable** command can only be configured for a violation event.

The table below lists the events that have default actions.

Table 1: Events with Default Actions

Event	Default Action
authentication-failure	Session manager checks for a violation and unauthorizes the session if no other method is still running, unless the control policy explicitly specifies authorization.
authentication-success	Session manager authorizes the session, unless the control policy explicitly specifies unauthorization.
authorization-failure	Session manager unauthorizes the session, unless the control policy explicitly specifies authorization.
violation	Session manager generates a restrict violation on the port, unless the control policy explicitly specifies a different action.

Note The **remote-authentication-failure** and **remote-authentication-success** keywords are generated when web authentication success or failure occurs at the Guest Controller (GC) when a user configures CGA and provisions web authentication at the GC. This information is propagated from GC to the access switch.

Examples

The following example shows how to configure a control policy named POLICY-3. This control policy has two events associated with it; one for session creation and the other for authentication failures. The authentication-failure event has two control classes associated with it.

```
class-map type control subscriber match-all MAB-FAILED
 match method mab
 match result-type authoritative
!
policy-map type control subscriber POLICY-3
 event session-started match-all
  10 class always do-all
   10 authenticate using mab priority 20
  !
 !
 event authentication-failure match-all
  10 class MAB-FAILED do-all
   10 authenticate using dot1x priority 10
```

```
!
20 class DOT1X-FAILED do-all
 10 terminate dot1x
 20 activate service-template VLAN4
```

Related Commands

Command	Description
class-map type control subscriber	Defines a control class, which specifies conditions that must be met to execute actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

guest-lan

To configure the wireless guest LAN, use the **guest-lan** command in global configuration mode. To remove the wireless guest LAN configuration, use the **no** form of this command.

guest-lan *profile-name* [*lan-id*]

no guest-lan *profile-name* [*lan-id*]

Syntax Description

profile-name	Specifies the wireless guest profile name.
lan-id	(Optional) Specifies the guest LAN identifier. The range is from 1 to 5.

Command Default

The wireless guest LAN is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

Use the **guest-lan** command to specify a wireless guest profile. This wireless guest profile is used in the **tunnel type capwap** command to configure a a CAPWAP tunnel within a service template and configure wired guest access for guest users of an enterprise network.

Examples

The following example shows how to configure access to tunnel a VLAN :

```
Device# configure terminal
Device(config)# guest-lan guest-lan-name 1
```

Related Commands

tunnel type capwap	Configures a CAPWAP tunnel in a service template.

inactivity-timer

To enable an inactivity timeout for subscriber sessions, use the **inactivity-timer** command in service template configuration mode. To disable the timer, use the **no** form of this command.

inactivity-timer *minutes* **[probe]**

no inactivity-timer

Syntax Description

minutes	Maximum number of minutes that a session can be inactive. Range: 0 to 65535. Default: 0, which disables the timer.
probe	(Optional) Enables address resolution protocol (ARP) probes. These probes are sent before terminating the session.

Command Default

Disabled (the inactivity timeout is 0).

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **inactivity-timer** command to set the maximum amount of time that a subscriber session can exist with no activity or data from the end client. If this timer expires before there is any activity or data, the session is cleared.

The **probe** keyword enables ARP probes. The IP device tracking table maintains a list of known host devices and periodically probes those devices to verify that they are still active. If all probes go unanswered, the session is cleared. Because the host is removed from the IP device tracking table after the inactivity timeout, no further probes are sent, and the inactive end host must send ARP traffic to reinitiate the session.

To set the number and time interval of ARP probes, use the **ip device tracking probe** command.

Examples

The following example shows how to configure a service template with the activity timer set to 15 minutes:

```
service-template SVC_2
 description label for SVC_2
 access-group ACL_2
 redirect url http://www.cisco.com
 inactivity-timer 15
```

Related Commands

Command	Description
absolute-timer	Enables an absolute timeout for subscriber sessions.
authenticate using	Authenticates a subscriber session using the specified method.
ip device tracking probe	Enables the tracking of device probes.
show service-template	Displays information about service templates.

key-wrap enable

To enable Advanced Encryption Standard (AES) key wrap on a RADIUS server, use the **key-wrap enable** command in server group configuration mode. To disable key wrap, use the **no** form of this command.

key-wrap enable

no key-wrap enable

Syntax Description

This command has no arguments or keywords.

Command Default

The key wrap feature is disabled.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **key-wrap enable** command to enable AES key-wrap functionality. The AES key-wrap feature makes the shared secret between the controller and the RADIUS server more secure. AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.

Examples

The following example shows how to configure a RADIUS server group named LAB_RAD with key-wrap support enabled:

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

Related Commands

Command	Description
mac-delimiter	Specifies the MAC delimiter for RADIUS compatibility mode.
radius-server host	Specifies a RADIUS server host.
subscriber mac-filtering security-mode	Specifies the RADIUS compatibility mode for MAC filtering.

linksec policy (service template)

To set a data link layer security policy, use the **linksec policy** command in service template configuration mode. To remove the link layer security policy, use the **no** form of this command.

linksec policy {**must-not-secure | must-secure | should-secure**}

no linksec policy

Syntax Description

must-not-secure	Specifies that the session must not be secured with Media Access Control Security (MACsec) standard.
must-secure	Specifies that the device port must be authorized only if a secure MACsec session is established.
should-secure	Specifies that the link security policy has optionally secured sessions. If an attempt to establish a MACsec session fails, an authorization failure message is not sent.

Command Default

A data link layer security policy is not configured.

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

Configure the link layer security policy within a service template and its associated policy action.

Examples

The following example shows how to configure the link security policy so that the device port is authorized only if a secure MACsec session is established:

```
Device(config)# service-template dot1x-macsec-policy
Device(config-service-template)# linksec policy must-secure
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.

Command	Description
policy-map type control subscriber	Defines a control policy for subscriber sessions.

mac-delimiter

To specify the MAC delimiter for RADIUS compatibility mode, use the **mac-delimiter** command in server group configuration mode. To return to the default value, use the **no** form of this command.

mac-delimiter {**colon**| **hyphen**| **none**| **single-hyphen**}

no mac-delimiter {**colon**| **hyphen**| **none**| **single-hyphen**}

Syntax Description

colon	Sets the delimiter to a colon, in the format xx:xx:xx:xx:xx:xx.
hyphen	Sets the delimiter to a hyphen (-), in the format xx-xx-xx-xx-xx-xx.
none	Sets the delimiter to none, in the format xxxxxxxxxxxx. This is the default value.
single-hyphen	Sets the delimiter to a single hyphen, in the format xxxxxx-xxxxxx.

Command Default

The MAC delimiter is set to none.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **mac-delimiter** command to set the delimiter that is used in MAC addresses that are sent to the RADIUS authentication server.

Examples

The following example shows how to configure a RADIUS server group with the MAC delimiter set to a colon:

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

Related Commands

Command	Description
key-wrap enable	Enables AES key wrap.

Command	Description
subscriber mac-filtering security-mode	Specifies the RADIUS compatibility mode for MAC filtering.

match activated-service-template

To create a condition that evaluates true based on the service template activated on a session, use the **match activated-service-template** command in control class-map filter configuration mode. To create a condition that evaluates true if the service template activated on a session does not match the specified template, use the **no-match activated-service-template** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match activated-service-template *template-name*

no-match activated-service-template *template-name*

no {**match| no-match**} **activated-service-template** *template-name*

Syntax Description

template-name	Name of a configured service template as defined by the **service-template** command.

Command Default

The control class does not contain a condition based on the service template.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match activated-service-template** command configures a match condition in a control class based on the service template applied to a session. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true for the actions of the control policy to be executed.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match activated-service-template SVC_1** command, all template values except SVC_1 are accepted as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the service template named VLAN_1 is activated on the session:

```
class-map type control subscriber match-all CLASS_1
 match activated-service-template VLAN_1
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.
class	Associates a control class with one or more actions in a control policy.
match service-template	Creates a condition that evaluates true based on an event's service template.
service-template	Defines a template that contains a set of service policy attributes to apply to subscriber sessions.

match authorization-failure

To create a condition that returns true, based on the type of authorization failure of a session, use the **match authorization-failure** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match authorization-failure {**domain-change-failed | linksec-failed | tunnel-return**}

no match authorization-failure {**domain-change-failed | linksec-failed | tunnel-return**}

Syntax Description

domain-change-failed	Specifies that the domain change has failed.
linksec-failed	Specifies that the data link security has failed.
tunnel-return	Specifies that the Converged Guest Access (CGA) tunnel authorization has failed.

Command Default

The control class does not contain a condition based on the type of authorization failure.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
15.2(1)E	This command was introduced.
Cisco IOS XE Release 3.3SE	This command was integrated into Cisco IOS XE Release 3.3SE.

Usage Guidelines

The **match authorization-failed** command configures a match condition in a control class based on the type of authorization failure that is configured for a session. Authorization failure can be either a data link layer security failure or a domain change failure. A control class can contain multiple conditions, that are evaluated as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if a session failure is caused by the data link layer security failure:

```
Device(config)# class-map type control subscriber match-all CLASS-1
Device(config-filter-control-classmap)# match authorization-failure linksec-failed
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
class-map type control subscriber	Creates a control class that defines the conditions that execute actions of a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match authorization-status

To create a condition that evaluates true based on a session's authorization status, use the **match authorization-status** command in control class-map filter configuration mode. To create a condition that evaluates true if a session's authorization status does not match the specified status, use the **no-match authorization-status** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match authorization-status {**authorized**| **unauthorized**}

no-match authorization-status {**authorized**| **unauthorized**}

no {**match**| **no-match**} **authorization-status** {**authorized**| **unauthorized**}

Syntax Description

authorized	Specifies that the subscriber has been authenticated.
unauthorized	Specifies that the subscriber has not been authenticated.

Command Default

The control class does not contain a condition based on the authorization status.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match authorization-status** command configures a match condition in a control class based on the session's authorization status. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match authorization-status authorized** command, a status value of unauthorized is accepted as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if a session's status is authorized:

```
class-map type control subscriber match-all CLASS_1
 match authorization-status authorized
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
class-map type control subscriber	Defines a control class, which specifies conditions that must be met to execute actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match authorizing-method-priority

To create a condition that evaluates true based on the priority of the authorization method that resulted in authorization, use the **match authorizing-method-priority** command in control class-map filter configuration mode. To create a condition that evaluates true if the priority of the authorization method that resulted in authorization does not match the specified priority, use the **no-match authorizing-method-priority** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match authorizing-method-priority {**eq**| **gt**| **lt**} *priority-value*

no-match authorizing-method-priority {**eq**| **gt**| **lt**} *priority-value*

no {**match**| **no-match**} **authorizing-method-priority** {**eq**| **gt**| **lt**} *priority-value*

Syntax Description

eq	Specifies that the current priority value is equal to *priority-value*.
gt	Specifies that the current priority value is greater than *priority-value*. **Note** The higher the number, the lower the priority.
lt	Specifies that the current priority value is less than *priority-value*. **Note** The lower the number, the higher the priority.
priority-value	Priority value to match. Range: 1 to 254, where 1 is the highest priority and 254 is the lowest.

Command Default

The control class does not contain a condition based on the priority of the authentication method.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match authorizing-method-priority** command configures a match condition in a control class based on the priority of the authentication method that resulted in authorization. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match authorizing-method-priority eq 10** command, all priority values except 10 are accepted as a successful match.

The **class** command associates a control class with a policy control.

Examples

The following example shows how to configure a control class that evaluates true if the priority number of the authorization method is less than 20:

```
class-map type control subscriber match-all CLASS_1
 match authorizing-method-priority lt 20
```

Related Commands

Command	Description
authenticate using	Initiates the authentication of a subscriber session using the specified method.
class	Associates a control class with one or more actions in a control policy.
match current-method-priority	Creates a condition that evaluates true based on the priority of the current authentication method.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match client-type

To create a condition that evaluates true based on an event's device type, use the **match client-type** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's device type does not match the specified device type, use the **no-match client-type** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match client-type {**data**| **switch**| **video**| **voice**}

no-match client-type {**data**| **switch**| **video**| **voice**}

no{**match**| **no-match**} **client-type** {**data**| **switch**| **video**| **voice**}

Syntax Description

data	Specifies a data device.
switch	Specifies a switch device.
video	Specifies a video device.
voice	Specifies a voice device.

Command Default

The control class does not contain a condition based on the device type.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match client-type** command configures a match condition in a control class based on an event's device type. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match client-type voice** command, all device values except voice are accepted as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the client type is data:

```
class-map type control subscriber match-all CLASS_1
 match client-type data
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match current-method-priority

To create a condition that evaluates true based on the priority of the current authentication method, use the **match current-method-priority** command in control class-map filter configuration mode. To create a condition that evaluates true if the priority of the current authentication method does not match the specified method, use the **no-match current-method-priority** command in control class-map filter configuration mode.To remove the condition, use the **no** form of this command.

match current-method-priority {**eq**| **gt**| **lt**} *priority-value*

no-match current-method-priority {**eq**| **gt**| **lt**} *priority-value*

no {**match**| **no-match**}**current-method-priority** {**eq**| **gt**| **lt**} *priority-value*

Syntax Description

eq	Specifies that the current priority value is equal to *priority-value*.
gt	Specifies that the current priority value is greater than *priority-value*. The higher the value, the lower the priority. **Note** The higher the number, the lower the priority.
lt	Specifies that the current priority value is less than *priority-value*. The lower the value, the higher the priority. **Note** The lower the number, the higher the priority.
priority-value	Priority value to match. Range: 1 to 254, where 1 is the highest priority and 254 is the lowest.

Command Default

The control class does not contain a condition based on the priority of the authentication method.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match current-method-priority** command configures a match condition in a control class based on the priority of the authentication method. A control class can contain multiple conditions, each of which will

evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match current-method-priority eq 10** command, the control class accepts any priority value except 10 as a successful match.

The **class** command associates a control class with a policy control.

Examples

The following example shows how to configure a control class that evaluates true if the priority number of the current authentication method is greater than 20:

```
class-map type control subscriber match-all CLASS_1
 match current-method-priority gt 20
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
match authorizing-method-priority	Creates a condition that evaluates true based on the priority of the authorization method.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match ip-address

To create a condition that evaluates true based on an event's source IPv4 address, use the **match ip-address** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's source IP address does not match the specified IP address, use the **no-match ip-address** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match ip-address *ip-address*

no-match ip-address *ip-address*

no {**match**| **no-match**} **ip-address** *ip-address*

Syntax Description

ip-address	IPv4 address to match.

Command Default

The control class does not contain a condition based on the source IPv4 address.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match ip-address** command configures a match condition in a control class based on an event's IP address. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match ip-address 10.10.10.1** command, all IPv4 addresses except 10.10.10.1 are accepted as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the IP address is 10.10.10.1:

```
class-map type control subscriber match-all CLASS_1
 match ip-address 10.10.10.1
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
match ipv6-address	Creates a condition that evaluates true based on an event's source IPv6 address.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match ipv6-address

To create a condition that evaluates true based on an event's source IPv6 address, use the **match ipv6-address** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's source IP address does not match the specified IP address, use the **no-match ipv6-address** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match ipv6-address *ipv6-address subnet-mask*

no-match ipv6-address *ipv6-address subnet-mask*

no {**match| no-match**} **ipv6-address** *ipv6-address subnet-mask*

Syntax Description

ipv6-address	IPv6 address to match.
subnet-mask	Subnet mask.

Command Default

The control class does not contain a condition based on the source IPv6 address.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match ipv6-address** command configures a match condition in a control class based on the subscriber's IPv6 address. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match ipv6-address FE80::1** command, the control class accepts any IPv6 address except FE80::1 as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the IP address is FE80::1:

```
class-map type control subscriber match-all CLASS_1
 match ipv6-address FE80::1
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
match ip-address	Creates a condition that evaluates true based on an event's source IPv4 address.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match mac-address

To create a condition that evaluates true based on an event's MAC address, use the **match mac-address** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's MAC address does not match the specified MAC address, use the **no-match mac-address** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match mac-address *mac-address*

no-match mac-address *mac-address*

no {**match| no-match**}**mac-address** *mac-address*

Syntax Description

mac-address	MAC address to match.

Command Default

The control class does not contain a condition based on the MAC address.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match mac-address** command configures a match condition in a control class based on an event's MAC address. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match mac-address 0030.94C2.D5CA** command, the control class accepts any MAC address except 0030.94C2.D5CA as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the MAC address is 0030.94C2.D5CA:

```
class-map type control subscriber match-all CLASS_1
 match mac-address 0030.94C2.D5CA
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match method

To create a condition that evaluates true based on the authentication method of an event, use the **match method** command in control class-map filter configuration mode. To create a condition that evaluates true if the authentication method of an event does not match the specified method, use the **no-match method** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match method {**dot1x**| **mab**| **webauth**}

no-match method {**dot1x**| **mab**| **webauth**}

no {**match**| **no-match**} **method** {**dot1x**| **mab**| **webauth**}

Syntax Description

dot1x	Specifies the IEEE 802.1X authentication method.
mab	Specifies the MAC authentication bypass (MAB) method.
webauth	Specifies the web authentication method.

Command Default

The control class does not contain a condition based on the authentication method.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match method** command configures a match condition in a control class based on the authentication method. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match method dot1x** command, the control class accepts any authentication method except dot1x as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class with two conditions: the control class evaluates true if the authentication method is 802.1X and that method times out:

```
class-map type control subscriber match-all DOT1X_TIMEOUT
  match method dot1x
  match result-type method-timeout
```

Related Commands

Command	Description
authenticate using	Initiates the authentication of a subscriber session using the specified method.
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match port-type (class-map filter)

To create a condition that evaluates true based on an event's interface type, use the **match port-type** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's interface type does not match the specified type, use the **no-match ip-address** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match port-type {**l2-port**| **l3-port**| **dot11-port**}

no-match port-type {**l2-port**| **l3-port**| **dot11-port**}

no {**match**| **no-match**} **port-type** {**l2-port**| **l3-port**| **dot11-port**}

Syntax Description

dot11-port	Specifies the 802.11 interface.
l2-port	Specifies the Layer 2 interface.
l3-port	Specifies the Layer 3 interface.

Command Default

The control class does not contain a condition based on the interface type.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match port-type** command configures a match condition in a control class based on the interface type. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match port-type l2-port** command, the control class accepts any interface value except l2-port as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the port type is Layer 2:

```
class-map type control subscriber match-all CLASS_1
 match port-type l2-port
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match result-type

To create a condition that evaluates true based on the specified authentication result, use the **match result-type** command in control class-map filter configuration mode. To create a condition that evaluates true if the authentication result does not match the specified result, use the **no-match result-type** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match result-type [**method** {**dot1x | mab | webauth**}] *result-type*

no-match result-type [**method** {**dot1x | mab | webauth**}] *result-type*

no {**match | no-match**} **result-type** [**method** {**dot1x | mab| webauth**}] *result-type*

Syntax Description

method	(Optional) Matches results for the specified authentication method only. If you do not specify a method, the policy matches the method associated with the current event.
dot1x	(Optional) Specifies the IEEE 802.1X authentication method.
mab	(Optional) Specifies the MAC authentication bypass (MAB) method.
webauth	(Optional) Specifies the web authentication method.
result-type	Type of authentication result. Valid keywords for *result-type* are: • **aaa-timeout—**authentication, authorization, and accounting (AAA) server timed out. • **agent-not-found—** The agent for the authentication method was not detected. • **authoritative—**Authorization failed. • **method-timeout—**The authentication method timed out. • **none—**No result. • **success—**Authentication was successful.

Command Default

The control class does not contain a condition based on the result type.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **match result-type** command configures a match condition in a control class based on the result of the authentication request. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match result-type method dot1x method-timeout** command, the control class accepts any result value except dot1x method-timeout as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class named ALL-FAILED that includes no-match conditions based on the authentication result:

```
class-map type subscriber control match-all ALL-FAILED
 no-match result-type method dot1x none
 no-match result-type method dot1x success
 no-match result-type method mab none
 no-match result-type method mab success
 no-match result-type method webauth none
 no-match result-type method webauth success
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
class-map type control subscriber	Defines a control class, which specifies conditions that must be met to execute actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

match service-template

To create a condition that evaluates true based on an event's service template, use the **match service-template** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's service template does not match the specified template, use the **no-match service-template** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match service-template *template-name*

no-match service-template *template-name*

no {**match**| **no-match**} **service-template** *template-name*

Syntax Description

template-name	Name of a configured service template as defined by the **service-template** command.

Command Default

The control class does not contain a condition based on the service template.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match service-template** command configures a match condition in a control class based on an event's service template. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match service-template VLAN_1** command, the control class accepts any service template value except VLAN_1 as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the service template used is named VLAN_1:

```
class-map type control subscriber match-all CLASS_1
 match service-template VLAN_1
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
match activated-service-template	Creates a condition that evaluates true based on the service template activated on a session.
service-template	Defines a template that contains a set of service policy attributes to apply to subscriber sessions.

match tag (class-map filter)

To create a condition that evaluates true based on the tag associated with an event, use the **match tag** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's tag does not match the specified tag, use the **no-match tag** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match tag *tag-name*

no-match tag *tag-name*

no {**match**| **no-match**} **tag** *tag-name*

Syntax Description

tag-name	Tag name, as defined by the **tag** command in a service template.

Command Default

The control class does not contain a condition based on the event tag.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match tag** command configures a match condition in a control class based on an event's tag. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match tag TAG_1** command, the control class accepts any tag value except TAG_1 as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the tag from an event is named TAG_1:

```
class-map type control subscriber match-all CLASS_1
 match tag TAG_1
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.
tag (service template)	Associates a user-defined tag with a service template.

match timer (class-map filter)

To create a condition that evaluates true based on an event's timer, use the **match timer** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's timer does not match the specified timer, use the **no-match timer** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match timer *timer-name*

no-match timer *timer-name*

no {**match**| **no-match**} **timer** *timer-name*

Syntax Description

timer-name	Name of the policy timer as defined in the control policy with the **set-timer** command.

Command Default

The control class does not contain a condition based on an event's timer.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match timer** command configures a match condition in a control class based on an event's timer name. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match timer TIMER_A** command, the control class accepts any timer value except TIMER_A as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if an event's timer is named TIMER_A:

```
class-map type control subscriber match-all CLASS_1
 match timer TIMER_A
!
policy-map type control subscriber RULE_A
 event session-start match-all
  1 class always do-until-failure
   1 set-timer TIMER_A 60
```

```
event timer-expiry match-all
 2 class CLASS_1 do-all
  1 clear-session
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.
set-timer	Starts a named policy timer for a subscriber session.

match username

To create a condition that evaluates true based on an event's username, use the **match username** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's username does not match the specified username, use the **no-match username** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match username *username*

no-match username *username*

no {**match**| **no-match**} **username** *username*

Syntax Description

username	Username.

Command Default

The control class does not contain a condition based on the event's username.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match username** command configures a match condition in a control class based on the username. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match username josmithe** command, the control class accepts any username value except josmithe as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the username is josmithe:

```
class-map type control subscriber match-all CLASS_1
 match username josmithe
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions

max-http-conns

To limit the number of HTTP connections for each web authentication client, use the **max-http-conns** command in parameter map configuration mode. To return to the default value, use the **no** form of this command.

max-http-conns *number*

no max-http-conns *number*

Syntax Description

number	Maximum number of concurrent HTTP client connections allowed. Range: 1 to 200. Default: 30.

Command Default

Maximum concurrent HTTP connections is 30.

Command Modes

Parameter map configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **max-http-conns** command to set the maximum number of HTTP connections allowed for each web authentication client.

If a new value is configured that is less than the previously configured value while the current number of connections exceeds the new maximum value, the HTTP server will not abort any of the current connections. However, the server will not accept new connections until the current number of connections falls below the new configured value.

Examples

The following example shows how to set the maximum number of simultaneous HTTP connections to 100 in the global parameter map for web authentication:

```
parameter-map type webauth global
 timeout init-state min 15
 max-http-conns 100
 banner file flash:webauth_banner1.html
```

Related Commands

Command	Description
timeout init-state min	Sets the Init state timeout for web authentication sessions.

parameter-map type webauth

To define a parameter map for web authentication, use the **parameter-map type webauth** command in global configuration mode. To delete a parameter map, use the **no** form of this command.

parameter-map type webauth {*parameter-map-name*| **global**}

no parameter-map type webauth {*parameter-map-name*| **global**}

Syntax Description

parameter-map-name	Defines a named parameter map for web authentication.
global	Defines global parameters for web authentication.

Command Default

A parameter map for web authentication is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **parameter-map type webauth** command to define a parameter map for web authentication. A parameter map allows you to specify parameters that control the behavior of actions configured under a policy map with the **authenticate using webauth** command.

A global parameter map contains system-wide parameters. This parameter map is not attached to the web authentication action and has parameters for both web authentication and consent. The global parameter map is automatically applied to the authentication action. If you explicitly apply a named parameter map, and there are parameters that are common to both the global and named parameter map, the global parameter map configuration takes precedence.

The configuration parameters supported for a global parameter map defined with the **global** keyword are different from the parameters supported for a named parameter map defined with the *parameter-map-name* argument.

Examples

The following example shows how to configure a parameter map named PMAP_2, which is used by the control policy named POLICY_1 to authenticate users:

```
parameter-map type webauth PMAP_2
 type webconsent
 max-login-attempts 5
 banner file flash:consent_page.htm
```

```
policy-map type control subscriber match-all POLICY_1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using webauth parameter-map PMAP_2
```

Related Commands

Command	Description
authenticate using	Authenticates a subscriber session using the specified method.
policy-map type control subscriber	Defines a control policy for subscriber sessions.
show ip-admission status parameter-map	Displays configuration information for the specified parameter map.
type	Defines the authentication methods supported by a parameter map.

pause reauthentication

To pause the reauthentication process after an authentication failure, use the **pause reauthentication** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **pause reauthentication**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

Reauthentication is not paused.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **pause reauthentication** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows how to configure a control policy with the pause authentication action configured for the authentication-failure event:

```
policy-map type control subscriber POLICY
 event authentication-failure match-all
  1 class SERVER_DEAD_UNAUTHD_HOST do-all
   1 activate template VLAN
   2 authorized
   3 pause reauthentication
  2 class SERVER_DEAD_AUTHD_HOST do-all
   1 pause reauthentication
```

Related Commands

Command	Description
authentication-restart	Restarts the authentication process after an authentication or authorization failure.
class	Associates a control class with one or more actions in a control policy.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
resume reauthentication	Resumes the reauthentication process after an authentication failure.

policy-map type control subscriber

To define a control policy for subscriber sessions, use the **policy-map type control subscriber** command in global configuration mode. To delete the control policy, use the **no** form of this command.

policy-map type control subscriber *control-policy-name*

no policy-map type control subscriber *control-policy-name*

Syntax Description

control-policy-name	Name of the control policy.

Command Default

A control policy is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Control policies define the actions taken in response to specified events and conditions.

A control policy consists of one or more control policy rules. A control policy rule associates a control class with one or more actions. The control class defines the conditions that must be met before the actions are executed. Actions are numbered and executed sequentially.

There are three steps in defining a control policy:

1. Create one or more control classes by using the **class-map type control subscriber** command.
2. Create a control policy by using the **policy-map type control subscriber** command.
3. Apply the control policy to a context by using the **service-policy type control subscriber** command.

Examples

The following example shows how to configure a control policy named DOT1X-MAB-WEBAUTH. If an authentication-failure event occurs, and the session matches all conditions in the control class named DOT1X-AUTHORITATIVE, the policy executes the authenticate action and attempts to authenticate the session using MAC authentication bypass (MAB).

```
class-map type control subscriber match-all DOT1X-AUTHORITATIVE
 match method dot1x
 match result-type authoritative
!
policy-map type control subscriber DOT1X-MAB-WEBAUTH
```

```
event session-started match-all
 10 class always do-until-failure
  10 authenticate using dot1x retries 3 retry-time 15
event authentication-failure match-first
 10 class DOT1X-AUTHORITATIVE do-all
  10 authenticate using mab
 20 class DOT1X-METHOD-TIMEOUT-3 do-all
  10 authenticate using mab
 30 class MAB-AUTHORITATIVE do-all
  10 authenticate using webauth retries 3 retry-time 15
 40 class AAA-TIMEOUT do-all
  10 activate service-template FALLBACK
event aaa-available match-all
 10 class always do-until-failure
  10 authenticate using dot1x
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
class-map type control subscriber	Defines a control class, which specifies conditions that must be met to execute actions in a control policy.
event	Specifies the type of event that causes a control class to be evaluated.
service-policy type control subscriber	Applies a control policy to an interface.

protect (policy-map action)

To silently drop violating packets after a security violation on a port, use the **protect** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **protect**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

No protect action is configured for a violation event.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **protect** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows how to configure a control policy with the protect action configured for the violation event:

```
policy-map type control subscriber POLICY_1
 event violation match-all
  1 class always do-until-failure
   10 protect
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.

Command	Description
err-disable	Temporarily disables a port after a security violation occurs.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

Cisco IOS Release 12.4T and Later Releases

radius-server host {*hostname*| *ip-address*} [**alias**{*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

All Other Releases

radius-server host {*hostname*| *ip-address*} [**alias**{*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**test username** *user-name* **[ignore-acct-port] [ignore-auth-port]** [**idle-time** *minutes*]] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii**| **hex**}]| **pac**] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.
acct-port *port-number*	(Optional) UDP destination port for accounting requests. • The host is not used for authentication if the port number is set to zero. If the port number is not specified, the default port number assigned is 1646.
auth-port *port-number*	(Optional) UDP destination port for authentication requests. • The host is not used for authentication if the port number is set to zero. If the port number is not specified, the default port number assigned is 1645.
non-standard	Parses attributes that violate the RADIUS standard.

timeout *seconds*	(Optional) Time interval (in seconds) that the device waits for the RADIUS server to reply before retransmitting. • The timeout keyword overrides the global value of the **radius-server timeout** command. • If no timeout value is specified, a global value is used; the range is from 1 to 1000.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or there is a delay in responding. • The retransmit keyword overrides the global setting of the **radius-server retransmit** command. • If no retransmit value is specified, a global value is used; the range is from 1 to 100.
test username *user-name*	(Optional) Sets the test username for the automated testing feature for RADIUS server load balancing.
ignore-acct-port	(Optional) Disables the automated testing feature for RADIUS server load balancing on the accounting port.
ignore-auth-port	(Optional) Disables the automated testing feature for RADIUS server load balancing on the authentication port.
idle-time *minutes*	(Optional) Length of time (in minutes) the server remains idle before it is quarantined and test packets are sent out. The range is from 1 to 35791. The default is 60.
backoff exponential	(Optional) Sets the exponential retransmits backup mode.
max-delay *minutes*	(Optional) Sets the maximum delay (in minutes) between retransmits. • **max-delay** *minutes* *minutes*—The range is from 1 to 120. The default value is 3.
key-wrap encryption-key	(Optional) Specifies the key-wrap encryption key.

message-auth-code-key	Specifies the key-wrap message authentication code key.
format	(Optional) Specifies the format of the message authenticator code key. • Valid values are: ◦ **ascii—**Configures the key in ASCII format. ◦ **hex—**Configures the key in hexadecimal format.
backoff-retry *number-of-retransmits*	(Optional) Specifies the exponential backoff retry. • *number-of-retransmits***—**Number of backoff retries. The range is from 1 to 50. The default value is 8.
pac	(Optional) Generates the per-server Protected Access Credential (PAC) key.
key	(Optional) Encryption key used between the device and the RADIUS daemon running on this RADIUS server. • The **key** keyword overrides the global setting of the **radius-server key** command. If no key string is specified, a global value is used. **Note** The **key** keyword is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
encryption-key	Specifies the encryption key. • Valid values for *encryption-key* are: ◦ **0—**Specifies that an unencrypted key follows. ◦ **7—**Specifies that a hidden key follows. ◦ String specifying the unencrypted (clear-text) server key.

Command Default No RADIUS host is specified and RADIUS server load balancing automated testing is disabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	This command was modified. The **alias** keyword was added.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B. The **backoff exponential**, **backoff-retry**, **key**, and **max-delay** keywords and *number-of-retransmits, encryption-key*, and *minutes* arguments were added.
12.2(28)SB	This command was integrated into Cisco release 12.2(28)SB. The **test username** *user-name*, **ignore-auth-port**, **ignore-acct-port**, and **idle-time** *seconds* keywords and arguments were added for configuring the RADIUS server load balancing automated testing functionality.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB apply to Cisco IOS Release 12.2(33)SRA and subsequent 12.2SR releases.
12.4(11)T	This command was modified. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.4(11)T or to subsequent 12.4T releases.
12.2 SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.2SX.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(1)S	This command was modified. The **key-wrap encryption-key**, **message-auth-code-key**, **format**, **ascii**, and **hex** keywords were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

We recommend the use of a test user who is not defined on the RADIUS server for the automated testing of the RADIUS server. This is to protect against security issues that can arise if the test user is not configured correctly.

If you configure one RADIUS server with a nonstandard option and another RADIUS server without the nonstandard option, the RADIUS server host with the nonstandard option does not accept a predefined host. However, if you configure the same RADIUS server host IP address for different UDP destination ports, where one UDP destination port (for accounting requests) is configured using the **acct-port** keyword and another UDP destination port (for authentication requests) is configured using the **auth-port** keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option. This results in resetting all the port numbers. You must specify a host and configure accounting and authentication ports on a single line.

To use separate servers for accounting and authentication, use the zero port value as appropriate.

RADIUS Server Automated Testing

When you use the **radius-server host** command to enable automated testing for RADIUS server load balancing:

- The authentication port is enabled by default. If the port number is not specified, the default port number (1645) is used. To disable the authentication port, specify the **ignore-auth-port** keyword.
- The accounting port is enabled by default. If the port number is not specified, the default port number (1645) is used. To disable the accounting port, specify the **ignore-acct-port** keyword.

Examples

The following example shows how to specify host1 as the RADIUS server and to use default ports for both accounting and authentication depending on the Cisco release that you are using:

```
radius-server host host1
```

The following example shows how to specify port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example shows how to specify the host with IP address 192.0.2.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to six, sets the retransmit value to five, and sets “rad123” as the encryption key, thereby matching the key on the RADIUS server:

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example shows how to specify the RADIUS server host1 for accounting but not for authentication, and the RADIUS server host2 for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example shows how to specify four aliases on the RADIUS server with IP address 192.0.2.1:

```
radius-server host 192.0.2.1 auth-port 1646 acct-port 1645
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

The following example shows how to enable exponential backoff retransmits on a per-server basis. In this example, assume that the retransmit is configured for three retries and the timeout is configured for five seconds; that is, the RADIUS request will be transmitted three times with a delay of five seconds. Thereafter, the device will continue to retransmit RADIUS requests with a delayed interval that doubles each time until 32 retries have been achieved. The device will stop doubling the retransmit intervals after the interval surpasses the configured 60 minutes; it will transmit every 60 minutes.

The **pac** keyword allows the PAC-Opaque, which is a variable length field, to be sent to the server during the Transport Layer Security (TLS) tunnel establishment phase. The PAC-Opaque can be interpreted only by the server to recover the required information for the server to validate the peer's identity and authentication. For example, the PAC-Opaque may include the PAC-Key and the PAC's peer identity. The PAC-Opaque format and contents are specific to the issuing PAC server.

The following example shows how to configure automatic PAC provisioning on a device. In seed devices, the PAC-Opaque has to be provisioned so that all RADIUS exchanges can use this PAC-Opaque to enable automatic PAC provisioning for the server being used. All nonseed devices obtain the PAC-Opaque during the authentication phase of a link initialization.

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

Examples

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified depending on the Cisco release that you are using:

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces that run PPP.
aaa authorization	Sets parameters that restrict network access to a user.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are to be selected on the interface.

Command	Description
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
radius-server retransmit	Specifies the number of times Cisco software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval that a device waits for a server host to reply.
test aaa group	Tests the RADIUS load balancing server response manually.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

redirect (parameter-map webauth)

To redirect users to a particular URL during web authentication login, use the **redirect** command in parameter-map webauth configuration mode. To remove the URL, use the **no** form of this command.

redirect {{**for-login**| **on-failure**| **on-success**} *url* | **portal** {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*}}

no redirect {**for-login**| **on-failure**| **on-success**| **portal** {**ipv4**| **ipv6**}}

Syntax Description

for-login	Sends users to this URL for login.
on-failure	Sends users to this URL if the login fails.
on-success	Sends users to this URL if the login is successful.
url	Valid URL.
portal	Sends users to this external web server to access the customized login web pages.
ipv4 *ipv4-address*	Specifies the IPv4 address of the portal.
ipv6 *ipv6-address*	Specifies the IPv6 address of the portal.

Command Default

Users are not redirected.

Command Modes

Parameter-map webauth configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **redirect** command to redirect users to custom web pages stored on an external server during the authentication process.

The device redirects the client to the specified portal IP address after it intercepts the initial HTTP request. The device also intercepts the login form sent by the client so it can extract the username and password and authenticates the user.

To display custom web pages that are stored locally, use the **custom-page** command.

When you configure the **redirect portal** command, web authentication creates intercept ACLs that include an entry to deny (not intercept) the redirect portal address. For example, if you configure the command **redirect portal ipv4 10.51.3.34**, the **show ipv4 access-list** command would display the following output:

```
Extended IP access list WA-v4-int-acl-pmap-PA
    10 deny tcp any host 10.51.3.34 eq www
    20 deny tcp any host 10.51.3.34 eq 443
    30 permit tcp any any eq www
    40 permit tcp any any eq 443
```

Examples

The following example shows how to configure a named parameter map that redirects users to custom web pages:

```
parameter-map type webauth PMAP_WEBAUTH
 type webauth
 redirect for-login http://10.10.3.34/~sample/login.html
 redirect on-success http://10.10.3.34/~sample/success.html
 redirect on-failure http://10.10.3.34/~sample/failure.html
 redirect portal ipv4 10.10.3.34
```

Related Commands

Command	Description
custom-page	Displays custom web pages during web authentication login.
show ip admission	Displays the network admission cache entries and information about web authentication sessions.
type (parameter-map webauth)	Defines the authentication methods supported by a parameter map.

redirect url

To redirect clients to a particular URL, use the **redirect url** command in service template configuration mode. To remove the URL, use the **no** form of this command.

redirect url *url* [**match** *access-list-name* [**one-time-redirect**| **redirect-on-no-match**]]

no redirect url *url* [**match** *access-list-name* [**one-time-redirect**| **redirect-on-no-match**]]

Syntax Description

url	Valid URL.
match *access-list-name*	(Optional) Specifies the name of an access control list to match.
one-time-redirect	(Optional) Redirects traffic matching the access list only once.
redirect-on-no-match	(Optional) Redirects traffic not matching the access list.

Command Default

Clients are not redirected.

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **redirect url** command to redirect clients to a particular URL when the service template is activated on a subscriber session.

Examples

The following example shows how to configure a service template named SVC_2 that redirects clients to Cisco.com after authentication if their IP address matches the access list defined in URL_ACL:

```
ip access-list extended URL_ACL
 permit tcp any host 10.10.10.1 eq www
!
service-template SVC_2
 access-group ACL_in
 redirect url http://cisco.com match URL_ACL
 tag TAG_1
!
policy-map type control subscriber POLICY_WEBAUTH
 event authentication-success match-all
```

```
10 class always do-until-failure
 10 activate service-template SVC_2 precedence 20
```

Related Commands

Command	Description
access-group (service template)	Specifies the access group that a service template applies to sessions.
activate (policy-map action)	Activates a control policy or service template on a subscriber session.

replace

To clear the existing session and create a new session after a security violation on a port, use the **replace** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **replace**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

The existing session is not cleared, and a new session is not created.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **replace** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows how to configure a control policy with the replace action configured for the violation event:

```
policy-map type control subscriber POLICY_1
 event violation match-all
  1 class always do-until-failure
   10 replace
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.

Command	Description
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
restrict	Drops violating packets and generates a syslog message after a security violation on a port.

restrict

To drop violating packets and generate a syslog message after a security violation on a port, use the **restrict** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **restrict**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

Violating packets are not dropped, and a syslog message is not generated.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **restrict** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows how to configure a control policy with the restrict action configured for the violation event:

```
policy-map type control subscriber POLICY_1
 event violation match-all
  10 class always do-until-failure
   10 restrict
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.

Command	Description
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
replace	Clears the existing session and creates a new session after a security violation on a port.

resume reauthentication

To resume the reauthentication process after an authentication failure, use the **resume reauthentication** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **resume reauthentication**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

Reauthentication is not resumed.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **resume reauthentication** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows how to configure a control policy with the resume authentication action configured for the aaa-available event:

```
policy-map type control subscriber POLICY
 event aaa-available match-all
  10 class CRITICAL_VLAN do-all
   10 clear-session
  20 class NOT_CRITICAL_VLAN do-all
   10 resume reauthentication
```

Related Commands

Command	Description
authentication-restart	Restarts the authentication process after an authentication or authorization failure.
class	Associates a control class with one or more actions in a control policy.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
pause reauthentication	Pauses the reauthentication process after an authentication failure.

service-policy type control subscriber

To apply a control policy to an interface, use the **service-policy type control subscriber** command in interface configuration mode. To remove the control policy, use the **no** form of this command.

service-policy type control subscriber *control-policy-name*

no service-policy type control subscriber *control-policy-name*

Syntax Description

control-policy-name	Name of a previously configured control policy, as defined with the **policy-map type control subscriber** command. Use the question mark (?) online help function to display a list of all configured control policies.

Command Default

A control policy is not applied to a context.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

A control policy is activated by applying it to one or more interfaces. Control policies apply to all sessions hosted on the interface. Only one control policy may be applied to a given interface.

Examples

The following example shows how to apply a control policy named POLICY_1 to an interface:

```
interface TenGigabitEthernet 1/0/1
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 service-policy type control subscriber POLICY_1
```

Related Commands

Command	Description
class-map type control subscriber	Defines a control class, which specifies conditions that must be met to execute actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

service-template

To define a template that contains a set of service policy attributes to apply to subscriber sessions, use the **service-template** command in global configuration mode. To remove the template, use the **no** form of this command.

service-template *template-name*

no service-template *template-name*

Syntax Description

template-name	Alphanumeric name that identifies the service template.

Command Default

No service templates are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Use the **service-template** command to group attributes that can be applied to subscriber sessions that share the same characteristics.

More than one template can be defined but only one template can be associated with a single subscriber session.

Examples

The following example shows how to configure a service template named SVC-2 that applies the access group ACL-2 to sessions and redirects clients to www.cisco.com:

```
service-template SVC-2
 description label for SVC-2
 access-group ACL-2
 redirect url http://www.cisco.com
 inactivity-timer 15
 tag TAG-2
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.
match activated-service-template	Creates a condition that evaluates true if the service template activated on a session matches the specified template.
match service-template	Creates a condition that evaluates true if an event's service template matches the specified template.

set-timer (policy-map action)

To start a named policy timer for a subscriber session, use the **set-timer** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **set-timer** *timer-name seconds*

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
timer-name	Name of the policy timer, up to 15 characters. This is an arbitrary name defined for this action.
seconds	Timer interval, in seconds. Range: 1 to 65535.

Command Default

A named policy timer is not started.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **set-timer** command configures an action in a control policy. This command starts the named policy timer. After the named timer expires, the system generates the timer-expiry event.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions. The actions that can be defined in a policy rule depend on the type of event that is specified by the **event** command.

Examples

The following example shows how to configure a control policy with the set-timer action configured for the session-start event:

```
class-map type control subscriber match-all CLASS_1
 match timer TIMER_A
!
policy-map type control subscriber RULE_A
 event session-start match-all
  10 class always do-until-failure
```

```
  10 set-timer TIMER_A 60
event timer-expiry match-all
 20 class CLASS_1 do-all
  10 clear-session
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
event	Specifies the type of event that triggers actions in a control policy if conditions are met.
match timer (class-map filter)	Creates a condition that evaluates true based on an event's timer.

show access-session

To display information about Session Aware Networking sessions, use the **show access-session** command in privileged EXEC mode.

show access-session [**[database]** [**handle** *handle-number*| [**method** *method*] [**interface** *interface-type interface-number*]| **mac** *mac-address*| **session-id** *session-id*] | **history** [**min-uptime** *seconds*]| **registrations**| **statistics**] **[details]**

Syntax Description

database	(Optional) Displays session data stored in the session database. This allows you to see information like the VLAN ID which is not cached internally. A warning message displays if data stored in the session database does not match the internally cached data.
handle *handle-number*	(Optional) Displays information about the specified context handle number. Range: 1 to 4294967295.
method *method*	(Optional) Displays information about subscriber sessions using one of the following authentication methods: • **dot1x—**IEEE 802.1X authentication method. • **mab—**MAC authentication bypass (MAB) method. • **webauth—**Web authentication method. If you specify a method, you can also specify an interface.
interface *interface-type interface-number*	(Optional) Displays information about subscriber sessions that match the specified client interface type. To display the valid keywords and arguments for interfaces, use the question mark (**?**) online help function.
mac *mac-address*	(Optional) Displays information about subscriber sessions with the specified client MAC address.
session-id *session-id*	(Optional) Displays information about subscriber sessions with the specified client session identifier.
history	(Optional) Displays session history.
min-uptime *seconds*	(Optional) Displays session history for sessions that have been up for the specified number of seconds. Range: 1 to 4294967295.
registrations	(Optional) Displays information about all registered session manager clients including the registered authentication methods.
statistics	(Optional) Displays information about authentication session statistics.

details	(Optional) Displays detailed information about each session instead of displaying a single-line summary.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

If you enter the **show access-session** command without any keywords or arguments, the information displays for all sessions on the switch. When you specify an identifier, information displays for only those sessions that match the identifier.

Examples

The following is sample output from the **show access-session** command:

```
Device# show access-session

Interface MAC Address Method Domain Status Fg Session ID
Gi1/0/17 0010.189c.19e8 webauth DATA Auth AC14F969000010B13CB02250

Session count = 1

Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker
```

The following is sample output from the **show access-session** command with the **interface** keyword:

```
Device# show access-session interface g1/0/17 details

Interface: GigabitEthernet1/0/17
IIF-ID: 0x1040E00000001DA
MAC Address: 0010.189c.19e8
IPv6 Address: Unknown
IPv4 Address: 9.9.2.5
User-Name: web
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: AC14F969000010B13CB02250
Acct Session ID: Unknown
Handle: 0x180000C6
Current Policy: DEFAULT_WEBAUTH

Server Policies:

Method status list:
Method State
webauth Authc Success
```

The following is sample output from the **show access-session** command with the **registrations** keyword:

```
Device# show access-session registrations

Clients registered with the Session Manager:
Handle Priority Name
1 0 Session Mgr IPDT Shim
2 0 Switch PI (IOU)
3 0 SVM
5 0 dct
6 0 iaf
7 0 Tag
8 0 SM Reauth Plugin
9 0 SM Accounting Feature
12 0 AIM
11 10 mab
10 5 dot1x
4 15 webauth
```

The table below describes the significant fields shown in the displays.

Table 2: show access-session Field Descriptions

Field	Description
Interface	The type and number of the authentication interface.
MAC Address	The MAC address of the client.
Domain	The name of the domain, either DATA or VOICE.
Status	The status of the authentication session. The possible values are: • Authc Failed—An authentication method has run for this session and authentication failed. • Authc Success—An authentication method has run for this session and authentication was successful. • Authz Failed—A feature has failed and the session has terminated. • Authz Success—All features have been applied to the session and the session is active. • Idle—This session has been initialized but no authentication methods have run. This is an intermediate state. • No methods—No authentication method has provided a result for this session. • Running—An authentication method is running for this session.

Field	Description
Fg	These status flags indicate that events are temporarily blocked from being processed on a session, usually because an asynchronous action is in progress. A transient block, from less than a second to a few seconds maximum, is to be expected; a session that remains blocked for more than a few seconds indicates an issue. All flags are mutually exclusive except P which can display with any other flag. Key to Session Events Blocked Status Flags: • A - Applying Policy (multi-line status for details)—A policy action (event) is being carried out and involves asynchronous processing which is in progress. Use the **details** keyword to see the name of the event being processed. • D - Awaiting Deletion—Session deletion has begun. One or more asynchronous actions are currently in progress (either retrieving accounting data from the platform or deleting the IIF ID). • F - Final Removal in progress—The D stage is over but the session has not been deleted yet. • I - Awaiting IIF ID allocation—The IIF ID is a system-wide identifier for a session or any other object the platform must know about. The platform must have the IIF ID before proceeding. • P - Pushed Session—Indicates the session was authenticated earlier and pushed from the wireless controller module (WCM). Session manager only tracks the session rather than performing authentication. This is for wireless sessions only. It is a permanent flag on sessions and can display with other flags. • R - Removing User Profile (multi-line status for details)—User profile is being removed asynchronously by the enforcement policy module (EPM). • U - Applying User Profile (multi-line status for details)—User profile is being applied asynchronously by the EPM. • X - Unknown Blocker—Event is blocked for an unknown reason.

Field	Description
Handle	The context handle.
State	The operating states for the reported authentication sessions. The possible values are: • Not run—The method has not run for this session. • Running—The method is running for this session. • Failed over—The method has failed and the next method is expected to provide a result. • Success—The method has provided a successful authentication result for the session. • Authc Failed—The method has provided a failed authentication result for the session.

Related Commands

Command	Description
policy-map type control subscriber	Defines a control policy for subscriber sessions.
service-policy type control subscriber	Applies a control policy to an interface.

show class-map type control subscriber

To display information about session aware networking control classes, use the **show class-map type control subscriber** command in user EXEC or privileged EXEC mode.

show class-map type control subscriber {**all**| **name** *control-class-name*}

Syntax Description

all	Displays output for all control classes.
name *control-class-name*	Displays output for the named control class.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Control policies define the actions taken in response to specified events and conditions. Use the **show class-map type control subscriber** command to display information about configured control classes, including the number of times each match condition within the class has been executed.

Examples

The following is sample output from the **show class-map type control subscriber** command using the **name** keyword.

```
Device# show class-map type control subscriber name DOT1X_AUTH

Class-map                  Action                        Exec  Hit  Miss  Comp
---------                  ------                        ----  ---  ----  ----
match-all DOT1X_AUTH       match method dot1x               0    0     0     0
match-all DOT1X_AUTH       match result-type authoritati    0    0     0     0

Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
           condition without a need to continue on to the end
```

The fields in the display are self-explanatory.

Related Commands

Command	Description
class-map type control subscriber	Creates a control class, which defines the conditions under which the actions of a control policy are executed.
policy-map type control subscriber	Defines a control policy for subscriber sessions.
show policy-map type control subscriber	Displays information about session aware networking control policies.

show ip admission

To display the network admission cache entries and information about web authentication sessions, use the **show ip admission** command in user EXEC or privileged EXEC mode.

Cisco IOS XE Release 3SE and Later Releases

show ip admission {**cache**| **statistics** [**brief**| **details**| **httpd**| **input-feature**]| **status** [**banners**| **custom-pages**| **httpd**| **parameter-map** [*parameter-map-name*]]| **watch-list**}

All Other Releases

show ip admission {**cache** [**consent**| **eapoudp**| **ip-addr** *ip-address*| **username** *username*]| **configuration**| **httpd**| **statistics**| [**brief**| **details**| **httpd**]| **status [httpd]**| **watch-list**}

Syntax Description

cache	Displays the current list of network admission entries.
statistics	Displays statistics for web authentication.
brief	(Optional) Displays a statistics summary for web authentication.
details	(Optional) Displays detailed statistics for web authentication.
httpd	(Optional) Displays information about web authentication HTTP processes
input-feature	Displays statistics about web authentication packets.
status	Displays status information about configured web authentication features including banners, custom pages, HTTP processes, and parameter maps.
banners	Displays information about configured banners for web authentication.
custom-pages	Displays information about custom pages configured for web authentication. Custom files are read into a local cache and served from the cache. A background process periodically checks if the files need to be re-cached.
parameter-map *parameter-map-name*	Displays information about configured banners and custom pages for all parameter maps or only for the specified parameter map.
watch-list	Displays the list of IP addresses in the watch list.

consent	(Optional) Displays the consent web page cache entries.
eapoudp	(Optional) Displays the Extensible Authentication Protocol over UDP (EAPoUDP) network admission cache entries. Includes the host IP addresses, session timeout, and posture state.
ip-addr *ip-address*	(Optional) Displays information for a client IP address.
username *username*	(Optional) Display information for a client username.
configuration	(Optional) Displays the NAC configuration. **Note** This keyword is not supported in Cisco IOS XE Release 3.2SE and later releases. Use the **show running-config all** command to see the running web authentication configuration and the commands configured with default parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was modified. The output of this command was enhanced to display whether the AAA timeout policy is configured.
12.4(15)T	This command was modified. The **consent** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.3(1)T	This command was modified. The **statistics**, **brief**, **details**, **httpd**, and **status** keywords were added.
Cisco IOS XE Release 3.2SE	This command was modified. The **input-feature**, **banners**, **custom-pages**, and **parameter-map** keywords were added. The **configuration** keyword was removed.

Usage Guidelines

Use the **show ip admission** command to display information about network admission entries and information about web authentication sessions.

Examples

The following is sample output from the **show ip admission cache** command:

```
Device# show ip admission cache

Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 1
 Client MAC 5cf3.fc25.7e3d Client IP 1.150.128.2 IPv6 :: Port 0, State INIT, Method Webauth
```

The following is sample output from the **show ip admission statistics** command:

```
Device# show ip admission statistics

Webauth input-feature statistics:
                                                        IPv4          IPv6
  Total packets received                                46            0
    Delivered to TCP                                    46            0
    Forwarded                                           0             0
    Dropped                                             0             0
    TCP new connection limit reached                    0             0

Webauth HTTPd statistics:

  HTTPd process 1
    Intercepted HTTP requests:                          8
    IO Read events:                                     9
    Received HTTP messages:                             7
    IO write events:                                    11
    Sent HTTP replies:                                  7
    IO AAA messages:                                    4
    SSL OK:                                             0
    SSL Read would block:                               0
    SSL Write would block:                              0
    HTTPd process scheduled count:                      23
```

The following is sample output from the **show ip admission status** command:

```
Device# show ip admission status

IP admission status:
  Enabled interfaces            1
  Total sessions                1
  Init sessions                 1     Max init sessions allowed     100
    Limit reached               0     Hi watermark                  1
  TCP half-open connections     0     Hi watermark                  0
  TCP new connections           0     Hi watermark                  0
  TCP half-open + new           0     Hi watermark                  0
  HTTPD1 Contexts               0     Hi watermark                  1

  Parameter Map: Global
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Custom Pages
      Custom pages not configured
    Banner
      Type: text
        Banner                  " <H2>Login Page Banner</H2> "
        Html                    " <H2>Login Page Banner</H2> "
        Length                  48

  Parameter Map: PMAP_CONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBCONSENT
    Custom Pages
      Custom pages not configured
```

```
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_FLASH
    Custom Pages
      Type: "login"
        File                    flash:webauth_login.html
        File status             Ok - File cached
        File mod time           2012-07-20T02:29:36.000Z
        File needs re-cached    No
        Cache                   0x3AEE1E1C
        Cache len               246582
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "success"
        File                    flash:webauth_success.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:57:28.000Z
        File needs re-cached    No
        Cache                   0x3A529B3C
        Cache len               70
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "failure"
        File                    flash:webauth_fail.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:49.000Z
        File needs re-cached    No
        Cache                   0x3A5BEBC4
        Cache len               67
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "login expired"
        File                    flash:webauth_expire.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:25.000Z
        File needs re-cached    No
        Cache                   0x3AA20090
        Cache len               69
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_EXTERNAL
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured
```

The following is sample output from the **show ip admission status banners** command for a banner configured with the **banner text** command:

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: text
      Banner                    " <H2>Login Page Banner</H2> "
      Html                      " <H2>Login Page Banner</H2> "
      Length                    48
```

The following is sample output from the **show ip admission status banners** command for a banner configured with the **banner file** command:

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured
```

```
  Parameter Map: PMAP_WEBAUTH
    Type: file
      Banner                    <h2>Cisco Systems</h2>
<h3>Webauth Banner from file</h3>

      Length                    60
      File                      flash:webauth_banner1.html
      File status               Ok - File cached
      File mod time             2012-07-24T07:07:09.000Z
      File needs re-cached      No
      Cache                     0x3AF6CEE4
      Cache len                 60
      Cache time                2012-09-19T10:13:59.000Z
      Cache access              0 reads, 1 write
```

The following is sample output from the **show ip admission status custom pages** command:

```
Device# show ip admission status custom pages

IP admission status:
  Parameter Map:  Global
    Custom pages not configured
  Parameter Map:  PMAP_WEBAUTH
    Type: "login"
      File                      flash:webauth_login.html
      File status               Ok - File cached
      File mod time             2012-07-20T02:29:36.000Z
      File needs re-cached      No
      Cache                     0x3B0DCEB4
      Cache len                 246582
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "success"
      File                      flash:webauth_success.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:57:28.000Z
      File needs re-cached      No
      Cache                     0x3A2E9090
      Cache len                 70
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "failure"
      File                      flash:webauth_fail.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:55:49.000Z
      File needs re-cached      No
      Cache                     0x3AF6D1A4
      Cache len                 67
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "login expired"
      File                      flash:webauth_expire.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:55:25.000Z
      File needs re-cached      No
      Cache                     0x3A2E8284
      Cache len                 69
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
  Parameter Map:  PMAP_CONSENT
    Custom pages not configured
```

The following table describes the significant fields shown in the above display.

Table 3: show ip admission Field Descriptions

File mod time	Time stamp when the file was changed on the file system.
Cache time	Time stamp when the file was last read into cache.

The following output displays all the IP admission control rules that are configured on a router:

```
Device# show ip admission configuration

Authentication Proxy Banner not configured
Consent Banner is not configured
Authentication Proxy webpage
        Login page              : flash:test1.htm
        Success page            : flash:test1.htm
        Fail page               : flash:test1.htm
        Login Expire page       : flash:test1.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 5 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

The following output displays the host IP addresses, the session timeout, and the posture states. If the posture statue is POSTURE ESTAB, the host validation was successful.

```
Device# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

The fields in the displays are self-explanatory.

Related Commands

Command	Description
banner (parameter-map webauth)	Displays a banner on the web-authentication login web page.
clear ip admission cache	Clears IP admission cache entries from the router.
custom-page	Displays custom web pages during web authentication login.
ip admission name	Creates a Layer 3 network admission control rule.

show policy-map type control subscriber

To display information about session aware networking control policies, use the **show policy-map type control subscriber** command in user EXEC or privileged EXEC mode.

show policy-map type control subscriber {**all**| **name** *control-policy-name*}

Syntax Description

all	Displays output for all control policies.
name *control-policy-name*	Displays output for the named control policy.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Control policies define the actions taken in response to specified events and conditions. Use the **show policy-map type control subscriber** command to display information about configured control policies, including the number of times each policy-rule within the policy map has been executed.

Examples

The following is sample output from the **show policy-map type control subscriber** command using the **name** keyword.

```
Device# show policy-map type control subscriber name POLICY_1

Control_Policy: POLICY_1
  Event:      event session-started match-all
    Class-map:  10 class always do-until-failure
      Action: 10 authenticate using dot1x retries 3 retry-time 15
      Executed: 0

  Event:      event authentication-failure match-all
    Class-map:  10 class DOT1X_AUTH do-until-failure
      Action: 10 authenticate using mab
      Executed: 0

    Class-map:  20 class DOT1X_METHOD_TIMEOUT do-until-failure
      Action: 10 authenticate using mab
      Executed: 0

    Class-map:  30 class MAB_AUTH do-until-failure
      Action: 10 authenticate using webauth retries 3 retry-time 15
      Executed: 0

    Class-map:  40 class AAA_TIMEOUT do-until-failure
      Action: 10 activate service-template FALLBACK
```

```
      Executed: 0

  Event:      event aaa-available match-all
    Class-map:  10 class always do-until-failure
      Action: 10 authenticate using dot1x
      Executed: 0


Key:
  "Executed" - The number of times this rule action line was executed
```

The fields in the display are self-explanatory.

Related Commands

Command	Description
class-map type control subscriber	Defines a control class, which specifies conditions that must be met to execute actions in a control policy.
event	Specifies the type of event that causes a control class to be evaluated.
policy-map type control subscriber	Defines a control policy for subscriber sessions.
show class-map type control subscriber	Displays information about session aware networking control classes.

show service-template

To display information about configured service templates, use the **show service-template** command in privileged EXEC mode.

show service-template [*template-name*]

Syntax Description

template-name	(Optional) Name of the service template.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Service templates define service policy attributes that can be applied to subscriber sessions. Use the **show service-template** command to display information about configured service templates. Using this command without the *service-template* argument displays a summary of all configured service templates.

Examples

The following is sample output from the **show service-template** command displaying a list of configured service templates:

```
Device# show service-template

  Policy Name     Description
================================================
    L3_default_acce NONE
    SVC_2           label for SVC_2
```

The following is sample output from the **show service-template** command using the *template-name* argument, displaying configuration information for the template named SVC_2:

```
Device# show service-template SVC_2

    Name                      :  SVC_2
    Description               :  label for SVC_2
    VLAN                      :  NONE
    URL_Redirect URL          :  www.cisco.com
    URL-Redirect Match ACL    :  NONE
```

Related Commands

Command	Description
match service-template	Creates a condition that evaluates true if an event's service template matches the specified template.
service-template	Defines a service template.

subscriber aging

To enable an inactivity timer for subscriber sessions, use the **subscriber aging** command in interface configuration mode. To return to the default, use the **no** form of this command.

subscriber aging {**inactivity-timer** *seconds* **[probe]| probe**}

no subscriber aging

Syntax Description

inactivity-timer *seconds*	Maximum amount of time, in seconds, that a session can be inactive. Range: 1 to 65535. Default: 0, which sets the timer to disabled.
probe	Enables an address resolution protocol (ARP) probe.

Command Default

The inactivity timer is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **subscriber aging** command to set the maximum amount of time that a subscriber session can exist with no activity or data from the end client. If this timer expires before there is any activity or data, the session is cleared.

Examples

The following example shows how to set the inactivity timer to 60 seconds on Ten Gigabit Ethernet interface 1/0/2:

```
interface TenGigabitEthernet 1/0/2
 subscriber aging inactivity-timer 60 probe
 service-policy type control subscriber POLICY_1
```

Related Commands

inactivity-timer	Enables an inactivity timeout for subscriber sessions.
ip device tracking probe	Enables the tracking of device probes.
service-policy type control subscriber	Applies a control policy to an interface.

subscriber mac-filtering security-mode

To specify the RADIUS compatibility mode for MAC filtering, use the **subscriber mac-filtering security-mode** command in server group configuration mode. To return to the default value, use the **no** form of this command.

subscriber mac-filtering security-mode {**mac**| **none**| **shared-secret**}

no subscriber mac-filtering security-mode {**mac**| **none**| **shared-secret**}

Syntax Description

mac	Sends the MAC address as the password.
none	Does not send the password attribute. This is the default value.
shared-secret	Sends the shared-secret as the password.

Command Default

The security mode is set to none.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **subscriber mac-filtering security-mode** command to set the type of security used for MAC filtering in RADIUS compatibility mode.

Examples

The following example shows how to configure a server group with MAC filtering to send the MAC address as the password:

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

Related Commands

Command	Description
key-wrap enable	Enables AES key wrap.
mac-delimiter	Specifies the MAC delimiter for RADIUS compatibility mode.

Command	Description
radius-server host	Specifies a RADIUS server host.

tag (service template)

To associate a user-defined tag with a service template, use the **tag** command in service template configuration mode. To remove a tag, use the **no** form of this command.

tag *tag-name*

no tag *tag-name*

Syntax Description

tag-name	Arbitrary text string assigned as the tag name.

Command Default

No tag is associated with the service template.

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **tag** command to associate an identifier tag with a service template. The tag is applied to a session when a control policy activates the service template on the session.

A set of policies can be associated with the tag and if the authentication, authorization, and accounting (AAA) server sends the same tag in response to the authentication response, the policies that are associated with the tag are applied on the host.

Examples

The following example shows how to associate a service template named SVC_1 with TAG_1, which is used as a match condition in the control class named CLASS_1.

```
service-template SVC_1
 description label for SVC_1
 redirect url www.cisco.com match ACL_1
 inactivity-timer 30
 tag TAG_1
!
class-map type control subscriber match-all CLASS_1
  match tag TAG_1
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.

Command	Description
event	Specifies the type of event that causes a control class to be evaluated.
match tag	Creates a condition that evaluates true if an event's tag matches the specified tag.

terminate

To terminate an authentication method on a subscriber session, use the **terminate** command in control policy-map action configuration mode. To remove this action from a control policy, use the **no** form of this command.

action-number **terminate**{**dot1x**| **mab**| **webauth**}

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
dot1x	Specifies the IEEE 802.1X authentication method.
mab	Specifies the MAC authentication bypass (MAB) method.
webauth	Specifies the web authentication method.

Command Default

An authentication method is not terminated.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **terminate** command defines an action in a control policy.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions are executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions.

When configuring a control policy, you must explicitly terminate one authentication method before initiating another method. Session aware networking does not automatically terminate one method before attempting the next method. For concurrent authentication, this means you must configure a policy rule that explicitly terminates one method after another method of a higher priority succeeds.

Examples

The following example shows how to configure a control policy that includes the terminate action:

```
policy-map type control subscriber POLICY_3
 event session-start
  10 class always
   10 authenticate using dot1x
 event agent-not-found
  10 class DOT1X
   10 terminate dot1x
   20 authenticate using mab
 event authentication-success
  10 class DOT1X
   10 terminate mab
   20 terminate web-auth
  20 class MAB
   10 terminate web-auth
```

Related Commands

Command	Description
authenticate using	Initiates authentication of a subscriber session using the specified method.
class	Associates a control class with one or more actions in a control policy.
event	Specifies the type of event that causes a control class to be evaluated.

timeout init-state min

To set the initialize (Init) state timeout for web authentication sessions, use the **timeout init-state min** command in parameter-map type webauth configuration mode. To reset the timeout to the default value, use the **no** form of this command.

timeout init-state min *minutes*

no timeout init-state min *minutes*

Syntax Description

minutes	Maximum duration of Init state, in minutes. Range: 1 to 65535. Default: 2.

Command Default

The Init state timeout is two minutes.

Command Modes

Parameter-map type webauth configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **timeout init-state min** command to limit the number of minutes that a web authentication session can stay in the Init state. A session remains in the Init state until the user enters his or her username and password credentials. If the timer expires before the user enters his or her credentials, the session is cleared.

Examples

The following example shows how to set the Init timeout to 15 minutes in the parameter map named MAP_2:

```
parameter-map type webauth MAP_2
 type webauth
 timeout absolute min 30
 timeout init-state min 15
 max-login-attempts 5
```

Related Commands

Command	Description
max-login-attempts	Limits the number of login attempts for a web authentication session.
timeout absolute min	Sets the absolute timeout for web authentication sessions.

tunnel type capwap (service-template)

To configure a Control And Provisioning of Wireless Access Points protocol (CAPWAP) tunnel in a service template, use the **tunnel type capwap** command in service-template configuration mode. To disable the CAPWAP tunnel, use the **no** form of this command.

tunnel type capwap name *tunnel-name*

no tunnel type capwap name *tunnel-name*

Syntax Description

name *tunnel-name*	Specified the name of the CAPWAP tunnel.

Command Default

CAPWAP tunnel is not configured.

Command Modes

Service-template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

Use this command to create a CAPWAP tunnel to enable wired guest access through a wireless port. For wireless access, guests are directed through a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel to the wireless controller in the DMZ (demilitarized zone) and are provided open or web-authenticated access from the wireless controller.

Examples

The following example shows how to configure a CAPWAP tunnel:

```
Device(config)# service-template GUEST-TUNNEL
Device(config-service-template)# tunnel type capwap name tunnel1
```

Related Commands

Command	Description
service-template	Defines a template that contains a set of service policy attributes to apply to subscriber sessions.

type (parameter-map webauth)

To define the authentication methods supported by a parameter map, use the **type** command in parameter-map webauth configuration mode. To return to the default value, use the **no** form of this command.

type {**authbypass**| **consent**| **webauth**| **webconsent**}

no type {**authbypass**| **consent**| **webauth**| **webconsent**}

Syntax Description

authbypass	Specifies authentication bypass. Allows access using nonresponsive host (NRH) authentication.
consent	Specifies consent only. Allows default access without prompting users for their username and password credentials. Users instead get a choice of two radio buttons: accept or do not accept. For accounting purposes, the device passes the client's MAC address to the authentication, authorization, and accounting (AAA) server.
webauth	Specifies web authentication only. Allows access based on the user's privileges. The device sends the username and password to the AAA server for authentication and accounting. This is the default value.
webconsent	Specifies both web authentication and consent.

Command Default

The type is web authentication (webauth).

Command Modes

Parameter-map webauth configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **type** command to specify the authentication method to which the parameters in the map apply. A parameter map defines parameters that control the behavior of actions specified under a policy map.

This command is supported in named parameter maps only.

Examples

The following example shows how to configure a parameter map with the type set to the default of webauth:

```
parameter-map type webauth PMAP_3
 type webauth
 timeout init-state min 15
 banner file flash:webauth_banner.html
```

Related Commands

Command	Description
banner (parameter-map webauth)	Displays a banner on the web authentication web page.
consent email	Requests a user's e-mail address on the consent login web page.
custom-page	Displays custom web pages during web authentication login.
redirect (parameter-map webauth)	Redirects users to a particular URL during web authentication.

unauthorize

To unauthorize a port and remove any access granted on the basis of previous authorization data, use the **unauthorize** command in control policy-map action configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **unauthorize**

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.

Command Default

Authorization data is not removed.

Command Modes

Control policy-map action configuration (config-action-control-policymap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **unauthorize** command defines an action in a control policy. This command removes any access that was granted based on previous authorization data, including the user profile and any activated service templates.

Control policies determine the actions taken in response to specified events and conditions. The control class defines the conditions that must be met before the actions will be executed. The actions are numbered and executed sequentially within the policy rule.

The **class** command creates a policy rule by associating a control class with one or more actions.

Examples

The following example shows how to configure a control policy with the unauthorize action configured for the inactivity-timeout event:

```
policy-map type control subscriber POLICY
 event inactivity-timeout match-all
  10 class always
   10 unauthorize
```

Related Commands

Command	Description
authorize	Initiates the authorization of a subscriber session.

Command	Description
class	Associates a control class with one or more actions in a control policy.
class-map type control subscriber	Creates a control class, which defines the conditions under which the actions of a control policy are executed.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

virtual-ip

To specify a virtual IP address for web authentication clients, use the **virtual-ip** command in parameter-map webauth configuration mode. To remove the address, use the **no** form of this command.

virtual-ip {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*}

no virtual-ip {**ipv4**| **ipv6**}

Syntax Description

ipv4 *ipv4-address*	Specifies the IPv4 address to use as the virtual IP address.
ipv6 *ipv6-address*	Specifies the IPv6 address to use as the virtual IP address.

Command Default

A virtual IP address is not configured.

Command Modes

Parameter-map webauth configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **virtual-ip** command to specify the virtual IP address to use for web authentication clients.

If you use default or local custom pages, configuring a virtual IP address will cause a logout web page to be presented to clients after they have been successfully authenticated. This allows users to logout by clicking a link in the logout page. The logout request is sent to the virtual IP address, and is intercepted by the device (an ACL is automatically created so that the logout request is intercepted).

To serve custom pages or other files from an external server, you must configure a virtual IP address. When a user enters his or her credentials in the login form, that form is sent to the virtual IP address and is intercepted by the device so that the client can be authenticated.

The virtual IP address must not be an address on the network or an address on the device.

This command is supported in the global parameter map only.

Examples

The following example shows how to set the virtual IP address to FE80::1 in the global parameter map for web authentication:

```
parameter-map type webauth global
 timeout init-state min 15
 watch-list enabled
 virtual-ip ipv6 FE80::1
```

Related Commands

Command	Description
authenticate using	Initiates the authentication of a subscriber session using the specified method.

vlan (service template)

To assign a VLAN to subscriber sessions, use the **vlan** command in service template configuration mode. To disable a VLAN, use the **no** form of this command.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description

vlan-id	VLAN identifier. Range: 1 to 4094.

Command Default

The service template does not assign a VLAN.

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **vlan** command to assign a VLAN to sessions on which the service template is activated.

Examples

The following example shows how to configure a service template that applies a VLAN:

```
service-template SVC_2
 description label for SVC_2
 redirect url www.google.com
 vlan 215
 inactivity-timer 30
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.
tag	Associates a user-defined tag with a service template.

voice vlan (service template)

To assign a voice VLAN to subscriber sessions, use the **voice vlan** command in service template configuration mode. To disable the voice VLAN, use the **no** form of this command.

voice vlan

no voice vlan

Syntax Description

This command has no keywords or arguments.

Command Default

The service template does not assign a voice VLAN.

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **voice vlan** command to assign a voice VLAN to sessions on which the service template is activated.

Examples

The following example shows how to configure a service template that applies a VLAN:

```
Device(config)# service-template CRITICAL-VOICE
Device(config-service-template)# voice vlan
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.

watch-list

To enable a watch list of web authentication clients, use the **watch-list** command in parameter-map webauth configuration mode. To return to the default value, use the **no** form of this command.

watch-list {**add-item** {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*}| **dynamic-expiry-timeout** *minutes*| **enabled**}

no watch-list {**add-item** {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*}| **dynamic-expiry-timeout** *minutes*| **enabled**}

Syntax Description

add-item	Adds an IP address to the watch list.
ipv4 *ipv4-address*	Specifies the IPv4 address of a client to add to the watch list.
ipv6 *ipv6-address*	Specifies the IPv6 address of a client to add to the watch list.
dynamic-expiry-timeout *minutes*	Sets the duration of time, in minutes, that an entry remains in the watch list. Range: 0 to 2147483647. Default: 30. 0 (zero) keeps the entry in the list permanently.
enabled	Enables a watch list.

Command Default

The watch list is disabled.

Command Modes

Parameter-map webauth configuration (config-params-parameter-map)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **watch-list** command to monitor the connections of specific web authentication clients. When you enable the watch list, web authentication dynamically adds clients to the watch list after either of the following events occurs:

- The client exceeds the maximum number of login attempts allowed, as configured with the **ip admission max-login-attempts** command.
- The client exceeds the maximum number of open TCP sessions allowed, as configured with the **max-http-conns** command (default is 30).

After an IP address is added to the watch list, no new connections are accepted from this IP address (to port 80) until the timer that you set with the **dynamic-expiry-timeout** keyword expires.

You can manually add an IP address to the watch list by using the **add-item** keyword.

When you disable a watch list, no new entries are added to the watch list and the sessions are put in the SERVICE_DENIED state.

This command is supported in the global parameter map only.

Examples

The following example shows how to configure the global parameter map with the watch list set to enabled and the timeout set to 20 minutes:

```
parameter-map type webauth global
 watch-list enabled
 watch-list dynamic-expiry-timeout 20
```

Note Entries that you add to the watch list using the **add-item** keyword do not display in the running configuration. To view these entries, use the **show ip admission watch-list** command.

Related Commands

Command	Description
ip admission max-login-attempts	Limits the number of login attempts.
show ip-admission watch-list	Displays the list of IP addresses in the watch list.