



## **Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)**

**First Published:** January 29, 2013

**Last Modified:** January 29, 2013

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### Session Aware Networking Overview 1

Finding Feature Information 1

Information About Session Aware Networking 1

Understanding Session Aware Networking 1

Features in Session Aware Networking 2

Benefits of Session Aware Networking 2

Web Authentication Support for Common Session ID 3

Web Authentication Support of IPv6 3

Additional References 3

Feature Information for Session Aware Networking Overview 4

---

### CHAPTER 2

#### Configuring Identity Control Policies 5

Finding Feature Information 5

Information About Identity Control Policies 5

Concurrent Authentication Methods 5

Configuration Display Mode 6

Control Policies for Session Aware Networking 6

Control Policy Configuration Overview 7

Parameter Maps for Session Aware Networking 8

Per User Inactivity Handling Across Methods 8

How to Configure Identity Control Policies 8

Enabling the Display Mode for Session Aware Networking 8

Configuring a Control Class 9

Configuring a Control Policy 13

Applying a Control Policy to an Interface 18

Configuring Authentication Features on Ports 19

Configuring a Parameter Map for Web-Based Authentication 20

Configuration Examples for Identity Control Policies 24

Example: Configuring Control Policy for Concurrent Authentication Methods	24
Example: Configuring Control Policy for Sequential Authentication Methods	25
Example: Configuring Parameter Maps	26
Additional References	27
Feature Information for Identity Control Policies	28

---

## CHAPTER 3

### Configuring Identity Service Templates 31

Finding Feature Information	31
Prerequisites for Identity Service Templates	31
Information About Identity Service Templates	32
Service Templates for Session Aware Networking	32
Downloadable Service Templates	32
Locally Configured Service Templates	32
How to Configure Identity Service Templates	33
Configuring a Local Service Template	33
Configuration Examples for Identity Service Templates	35
Example: Activating a Service Template and Replace All	35
Example: Activating a Service Template for Fallback Service	35
Example: Deactivating a Service Template	36
Additional References	37
Feature Information for Identity Service Templates	38

---

## CHAPTER 4

### Change of Authorization Support 39

Finding Feature Information	39
Information About CoA Support	39
RADIUS Change-of-Authorization Support	39
Session Identification	40
CoA Activate Service Command	41
CoA Deactivate Service Command	41
CoA Bounce Host Port Command	42
CoA Disable Host Port Command	42
CoA Session Query Command	42
CoA Session Reauthenticate Command	43
CoA Session Terminate Command	43
Additional References	44

Feature Information for CoA Support 45

---

**CHAPTER 5****Configuring Local Authentication Using LDAP 47**

Finding Feature Information 47

Information About Local Authentication Using LDAP 47

Local Authentication Using LDAP 47

AES Key Wrap 48

How to Configure Local Authentication Using LDAP 48

Configuring Local Authentication Using LDAP 48

Configuring MAC Filtering Support 49

Enabling AES Key Wrap 50

Configuration Examples for Local Authentication Using LDAP 52

Example: Configuring Local Authentication Using LDAP 52

Example: Configuring MAC Filtering Support 52

Example: Configuring AES Key Wrap 52

Additional References 52

Feature Information for Local Authentication Using LDAP 53





## CHAPTER

# 1

# Session Aware Networking Overview

---

Session Aware Networking provides a policy and identity-based framework in which edge devices can deliver flexible and scalable services to subscribers. This module provides information about what Session Aware Networking is and its features and benefits.

- [Finding Feature Information, page 1](#)
- [Information About Session Aware Networking, page 1](#)
- [Additional References, page 3](#)
- [Feature Information for Session Aware Networking Overview, page 4](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

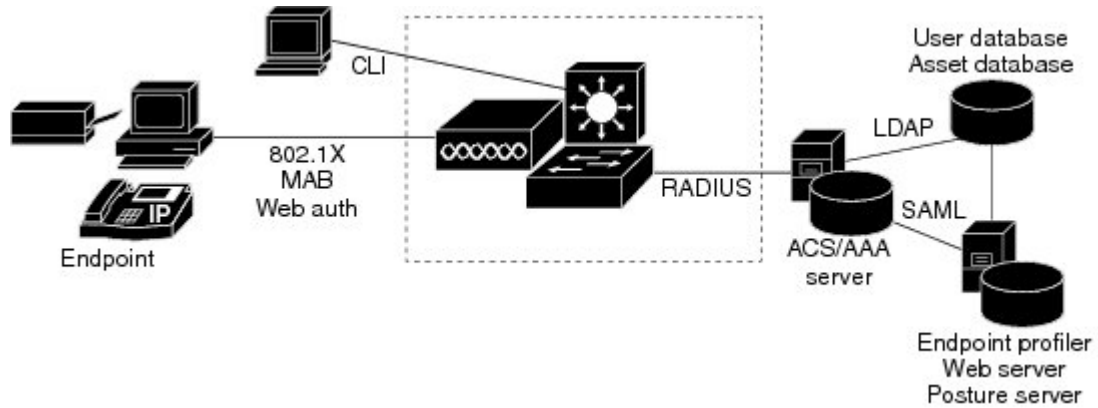
## Information About Session Aware Networking

### Understanding Session Aware Networking

Session Aware Networking provides an identity-based approach to access management and subscriber management. It offers a consistent way to configure features across technologies, a command interface that allows easy deployment and customization of features, and a robust policy control engine with the ability to apply policies defined locally or received from an external server to enforce policy in the network.

The figure below illustrates a typical deployment of Session Aware Networking in a physically distributed enterprise with a campus, branch offices, and remote workers.

**Figure 1: Sample Deployment**



## Features in Session Aware Networking

Session Aware Networking includes the following features:

- Cisco common classification policy language (C3PL)-based identity configuration
- Concurrent authentication methods on a single session, including IEEE 802.1x (dot1x), MAC authentication bypass (MAB), and web authentication
- Downloadable identity service templates
- Extended RADIUS change of authorization (CoA) support for querying, reauthenticating, and terminating a session, port shutdown and port bounce, and activating and deactivating an identity service template.
- Local authentication using Lightweight Directory Access Protocol (LDAP)
- Locally defined identity control policies
- Locally defined identity service templates
- Per-user inactivity handling across methods
- Web authentication support of common session ID
- Web authentication support of IPv6

## Benefits of Session Aware Networking

Identity-based solutions are essential for delivering access control for disparate groups such as employees, contractors, and partners while maintaining low operating expenses. Session Aware Networking provides a consistent approach to operational management through a policy and identity-based infrastructure leading to faster deployment of new features and easier management of switches.

Session Aware Networking provides the following benefits:



- An identity-based framework for session management.
- A robust policy control engine to apply policies defined locally or received from an external AAA server.
- Faster deployment and customization of features across access technologies.
- A simpler and consistent way to configure features across access methods, platforms, and application domains.

## Web Authentication Support for Common Session ID

Session Aware Networking allows a single session identifier to be used for web authentication sessions in addition to all 802.1X and MAB authenticated sessions for a client. This session ID is used for all reporting purposes such as show commands, MIBs, and RADIUS messages and allows users to distinguish messages for one session from messages for other sessions. This common session ID is used consistently across all authentication methods and features applied to a session.

## Web Authentication Support of IPv6

Session Aware Networking introduces IPv6 support for web authentication. IPv6 is supported for web authentication only when Session Aware Networking is explicitly configured. This means that you must permanently convert your configuration to the Cisco common classification policy language (C3PL) display mode by specifically configuring a Session Aware Networking command such as the **policy-map type control subscriber** command.

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Session Aware Networking commands	<a href="#">Cisco IOS Session Aware Networking Command Reference</a>
Address Resolution Protocol (ARP) commands	<a href="#">Cisco IOS IP Addressing Services Command Reference</a>
ARP configuration tasks	<i>IP Addressing - ARP Configuration Guide</i>
Authentication, authorization, and accounting (AAA) configuration tasks	<i>Authentication Authorization and Accounting Configuration Guide</i>
AAA commands	<i>Cisco IOS Security Command Reference</i>

**Standards and RFCs**

Standard/RFC	Title
RFC 5176	<i>Dynamic Authorization Extensions to RADIUS</i>

**Technical Assistance**

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Session Aware Networking Overview

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for Session Aware Networking Overview**

Feature Name	Releases	Feature Information
Web Authentication Support of Common Session ID	Cisco IOS XE Release 3.2SE	Allows a single session identifier to be used for all web authentication sessions in addition to 802.1X and MAB authenticated sessions.



## Configuring Identity Control Policies

Identity control policies define the actions that Session Aware Networking takes in response to specified conditions and subscriber events. A variety of system actions, conditions, and events can be combined using a consistent policy language. This module provides information about how to configure identity control policies for Session Aware Networking.

- [Finding Feature Information, page 5](#)
- [Information About Identity Control Policies, page 5](#)
- [How to Configure Identity Control Policies, page 8](#)
- [Configuration Examples for Identity Control Policies, page 24](#)
- [Additional References, page 27](#)
- [Feature Information for Identity Control Policies, page 28](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Information About Identity Control Policies

#### Concurrent Authentication Methods

Session Aware Networking allows the concurrent operation of IEEE 802.1x (dot1x), MAC authentication bypass (MAB), and web authentication methods, making it possible to invoke multiple authentication methods in parallel on a single subscriber session. This allows the client-supported method to complete at the earliest opportunity without the delays associated with serialization.

Typically, the access control method that is used to authorize a host is left up to the endpoint. For example, a printer without an 802.1x supplicant would be authorized through MAB only, an employee desktop through 802.1x only, and a guest through web authentication only. The default priority order is 802.1x, followed by MAB, then web authentication. When method priorities are the same, the first method that successfully authenticates the session prevails.

An example in which more than one method may succeed during the lifetime of a session is when MAB is used to provide interim access pending success of 802.1x. A host could be also be given interim access to a web server to allow credentials to be updated so that 802.1x can succeed after an authentication failure.

## Configuration Display Mode

Session Aware Networking introduces new Cisco IOS commands that replace many of the previously supported authentication and policy commands. These commands are available only after enabling the Cisco common classification policy language (C3PL) display mode that supports Session Aware Networking. Session Aware Networking features such as concurrent authentication and web authentication with IPv6 are not supported in legacy mode.

The device defaults to the legacy configuration mode until you do one of the following:

- Enter the **authentication display new-style** command—This command switches to C3PL display mode, temporarily converting your legacy configuration to a Session Aware Networking configuration so you can see how it looks before you make the conversion permanent. You can switch back to legacy mode by using the **authentication display legacy** command. See the [“Enabling the Display Mode for Session Aware Networking, on page 8”](#) section.
- Enter a Session Aware Networking configuration command—After you enter the first explicit Session Aware Networking command, the configuration converts to C3PL display mode permanently and legacy commands are suppressed. The **authentication display** command is disabled and you can no longer revert to the legacy configuration mode.

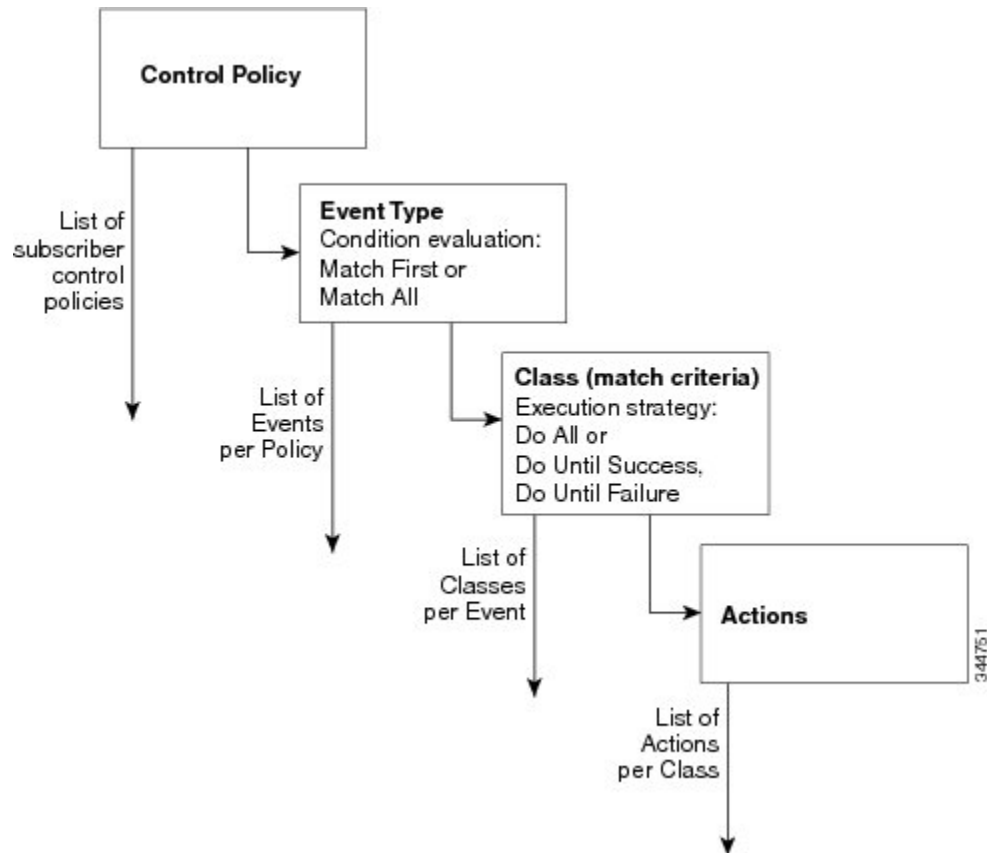
## Control Policies for Session Aware Networking

A control policy defines the handling of different subscriber life-cycle events. For various events, such as session start or session failure, you can specify actions in the control policy. These actions can be executed conditionally for different subscribers based on various match criteria. Control policies are activated on interfaces and typically control the authentication of subscriber identity and the activation of services on sessions. For example, you can configure a control policy to authenticate specific subscribers and then provide them with access to specific services.

A control policy consists of one or more control policy rules and a decision strategy that governs how the policy rules are evaluated. A control policy rule consists of a control class (a flexible condition clause), an event for which the condition is evaluated, and one or more actions. Actions are general system functions, such as “authenticate” or “activate.” You define the specific actions that an event will trigger and some events have default actions.

The figure below illustrates how each control policy contains a list of events that are considered applicable to the subscriber life cycle. Within each event type is a list of control classes with different match criteria for subscriber identity, and under each class is a list of actions to be executed.

**Figure 2: Control Policy Structure**



## Control Policy Configuration Overview

Control policies express system functionality in terms of an event, a condition, and an action. There are three steps in defining a control policy:

- 1 Create one or more control classes—A control class specifies the conditions that must be met for a control policy to be activated. A control class can contain multiple conditions, each of which will evaluate as either true or false. Match directives specify whether all, any, or none of the individual conditions must evaluate true for the class to evaluate true. Or, you can specify the default control class which does not contain any conditions and always evaluates true.
- 2 Create a control policy—A control policy contains one or more control policy rules. A control policy rule consists of a control class, an event that causes the class to be evaluated, and one or more actions. Actions are numbered and executed sequentially.
- 3 Apply the control policy—A control policy is activated by applying it to an interface.

## Parameter Maps for Session Aware Networking

A parameter map allows you to specify parameters that control the behavior of actions specified under a control policy. For Session Aware Networking, an authentication parameter map defines parameters used for the action specified with the **authenticate using webauth** command. You can configure the following types of parameter maps:

- Authentication bypass (This is also called nonresponsive host [NRH] authentication.)
- Consent
- Web authentication
- Web authentication with consent

Parameter maps are optional. If you do not configure a named parameter map, the software uses the default parameters that are specified in the global parameter map.

## Per User Inactivity Handling Across Methods

A common inactivity aging feature extends support for RADIUS attributes 28 (Idle-Timeout) and attribute 29 (Termination-Action) to web authenticated sessions, providing consistent inactivity handling across all authentication methods, including 802.1x, MAC authentication bypass (MAB), and web authentication. The AAA server sends these attributes as part of the user authorization. After a session has been idle for the amount of time specified in attribute 28, or has reached the timeout configured with attribute 29, the session is terminated.

You can also apply the inactivity timeout and absolute timeout to sessions through a locally defined service template. When enabling the inactivity timeout, you can also enable address resolution protocol (ARP) probes that are sent before the session is terminated. For configuration information, see the “[Configuring Identity Service Templates, on page 31](#)” module.

## How to Configure Identity Control Policies

### Enabling the Display Mode for Session Aware Networking

Session Aware Networking features are configured in the Cisco common classification policy language (C3PL) display mode. The legacy authentication manager mode is enabled by default. You can use the following procedure to switch to C3PL display mode and temporarily convert any legacy configuration commands to their C3PL equivalents. This allows you to preview your legacy configuration as a Session Aware Networking configuration before making the conversion permanent. After you enter an explicit Session Aware Networking command, the conversion becomes permanent and you can no longer revert to legacy mode.

#### SUMMARY STEPS

1. **enable**
2. **authentication display {legacy | new-style}**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>authentication display</b> {legacy   new-style}  <b>Example:</b> Device# authentication display new-style	Sets the display mode for authentication and policy configuration.  <ul style="list-style-type: none"> <li>• The default display mode is legacy.</li> <li>• You can use this command to switch between legacy and C3PL display mode until you execute the first explicit Session Aware Networking command. After you enter the first explicit Session Aware Networking command, for example when configuring a control class or control policy, the system displays a prompt to confirm whether you want to continue because this command will be disabled and you cannot revert to legacy mode.</li> </ul> <p><b>Note</b> If you save the configuration while the new-style mode is enabled, and then perform a reload, the display mode is permanently set to new-style. The <b>authentication display</b> command is disabled and you cannot revert to legacy mode.</p> <p>If you boot the standby device while in new-style mode, the standby device will be in new-style mode and after switchover the device remains in new-style mode. To switch back to legacy mode, you must use the <b>authentication display legacy</b> command and reload the standby switch.</p>

## Configuring a Control Class

A control class defines the conditions under which the actions of a control policy are executed. You define whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy. Control classes are evaluated based on the event specified in the control policy.

**Note**

This procedure shows all of the match conditions that you can configure in a control class. You must specify at least one condition in a control class to make it valid. All other conditions, and their corresponding steps, are optional (steps 4 through 18 below).

## SUMMARY STEPS

1. enable
2. configure terminal
3. class-map type control subscriber {match-all | match-any | match-none} control-class-name
4. {match | no-match} activated-service-template template-name
5. {match | no-match} authorization-status {authorized | unauthorized}
6. {match | no-match} authorizing-method-priority {eq | gt | lt} priority-value
7. {match | no-match} client-type {data | switch | video | voice}
8. {match | no-match} current-method-priority {eq | gt | lt} priority-value
9. {match | no-match} ip-address ip-address
10. {match | no-match} ipv6-address ipv6-address
11. {match | no-match} mac-address mac-address
12. {match | no-match} method {dot1x | mab | webauth}
13. {match | no-match} port-type {l2-port | l3-port | dot11-port}
14. {match | no-match} result-type [method {dot1x | mab | webauth}] result-type
15. {match | no-match} service-template template-name
16. {match | no-match} tag tag-name
17. {match | no-match} timer timer-name
18. {match | no-match} username username
19. end
20. show class-map type control subscriber {all | name control-class-name}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>class-map type control subscriber {match-all   match-any   match-none} control-class-name</b>  <b>Example:</b> Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT	Creates a control class and enters control class-map filter mode.  <ul style="list-style-type: none"> <li>• <b>match-all</b>—All of the conditions in the control class must evaluate true.</li> <li>• <b>match-any</b>—At least one of the conditions in the control class must evaluate true.</li> </ul>



	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <b>match-none</b>—All of the conditions in the control class must evaluate false.</li> </ul>
<b>Step 4</b>	<p><b>{match   no-match} activated-service-template <i>template-name</i></b></p> <p><b>Example:</b> Device(config-filter-control-classmap)# match activated-service-template SVC_1</p>	(Optional) Creates a condition that evaluates true based on the service template activated on a session.
<b>Step 5</b>	<p><b>{match   no-match} authorization-status {authorized   unauthorized}</b></p> <p><b>Example:</b> Device(config-filter-control-classmap)# match authorization-status authorized</p>	(Optional) Creates a condition that evaluates true based on a session's authorization status.
<b>Step 6</b>	<p><b>{match   no-match} authorizing-method-priority {eq   gt   lt} <i>priority-value</i></b></p> <p><b>Example:</b> Device(config-filter-control-classmap)# match authorizing-method-priority eq 10</p>	<p>(Optional) Creates a condition that evaluates true based on the priority of the authorization method.</p> <ul style="list-style-type: none"> <li>• <b>eq</b>—Current priority is equal to <i>priority-value</i>.</li> <li>• <b>gt</b>—Current priority is greater than <i>priority-value</i>.</li> <li>• <b>lt</b>—Current priority is less than <i>priority-value</i>.</li> <li>• <b>priority-value</b>—Priority value to match. Range: 1 to 254, where 1 is the highest priority and 254 is the lowest.</li> </ul>
<b>Step 7</b>	<p><b>{match   no-match} client-type {data   switch   video   voice}</b></p> <p><b>Example:</b> Device(config-filter-control-classmap)# match client-type data</p>	(Optional) Creates a condition that evaluates true based on an event's device type.
<b>Step 8</b>	<p><b>{match   no-match} current-method-priority {eq   gt   lt} <i>priority-value</i></b></p> <p><b>Example:</b> Device(config-filter-control-classmap)# match current-method-priority eq 10</p>	(Optional) Creates a condition that evaluates true based on the priority of the current authentication method.
<b>Step 9</b>	<p><b>{match   no-match} ip-address <i>ip-address</i></b></p> <p><b>Example:</b> Device(config-filter-control-classmap)# match ip-address 10.10.10.1</p>	(Optional) Creates a condition that evaluates true based on an event's source IPv4 address.

	Command or Action	Purpose
<b>Step 10</b>	<b>{match   no-match} ipv6-address <i>ipv6-address</i></b>  <b>Example:</b> Device(config-filter-control-classmap)# match ipv6-address FE80::1	(Optional) Creates a condition that evaluates true based on an event's source IPv6 address.
<b>Step 11</b>	<b>{match   no-match} mac-address <i>mac-address</i></b>  <b>Example:</b> Device(config-filter-control-classmap)# match mac-address aabb.cc00.6500	(Optional) Creates a condition that evaluates true based on an event's MAC address.
<b>Step 12</b>	<b>{match   no-match} method {dot1x   mab   webauth}</b>  <b>Example:</b> Device(config-filter-control-classmap)# match method dot1x	(Optional) Creates a condition that evaluates true based on an event's authentication method.
<b>Step 13</b>	<b>{match   no-match} port-type {l2-port   l3-port   dot11-port}</b>  <b>Example:</b> Device(config-filter-control-classmap)# match port-type l2-port	(Optional) Creates a condition that evaluates true based on an event's interface type.
<b>Step 14</b>	<b>{match   no-match} result-type [method {dot1x   mab   webauth}] <i>result-type</i></b>  <b>Example:</b> Device(config-filter-control-classmap)# match result-type agent-not-found	(Optional) Creates a condition that evaluates true based on the specified authentication result.  <ul style="list-style-type: none"> <li>To display the available result types, use the question mark (?) online help function.</li> </ul>
<b>Step 15</b>	<b>{match   no-match} service-template <i>template-name</i></b>  <b>Example:</b> Device(config-filter-control-classmap)# match service-template svc_1	(Optional) Creates a condition that evaluates true based on an event's service template.
<b>Step 16</b>	<b>{match   no-match} tag <i>tag-name</i></b>  <b>Example:</b> Device(config-filter-control-classmap)# match tag tag_1	(Optional) Creates a condition that evaluates true based on the tag associated with an event.
<b>Step 17</b>	<b>{match   no-match} timer <i>timer-name</i></b>  <b>Example:</b> Device(config-filter-control-classmap)# match timer restart	(Optional) Creates a condition that evaluates true based on an event's timer.

	Command or Action	Purpose
<b>Step 18</b>	<b>{match   no-match} username <i>username</i></b>  <b>Example:</b> Device(config-filter-control-classmap)# match username josmiths	(Optional) Creates a condition that evaluates true based on an event's username.
<b>Step 19</b>	<b>end</b>  <b>Example:</b> Device(config-filter-control-classmap)# end	(Optional) Exits control class-map filter configuration mode and returns to privileged EXEC mode.
<b>Step 20</b>	<b>show class-map type control subscriber {all   name <i>control-class-name</i>}</b>  <b>Example:</b> Device# show class-map type control subscriber all	(Optional) Displays information about Session Aware Networking control classes.

### Example: Control Class

The following example shows a control class that is configured with two match conditions:

```
class-map type control subscriber match-all DOT1X_NO_AGENT
  match method dot1x
  match result-type agent-not-found
```

## Configuring a Control Policy

Control policies determine the actions that the system takes in response to specified events and conditions. The control policy contains one or more control policy rules that associate a control class with one or more actions. The actions that you can configure in a policy rule depend on the type of event that you specify.



### Note

This task includes all of the actions that you can configure in a control policy regardless of the event. All of these actions, and their corresponding steps, are optional (steps 6 through 21 below). To display the supported actions for a particular event, use the question mark (?) online help function.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control subscriber** *control-policy-name*
4. **event** *event-name* [**match-all** | **match-first**]
5. *priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**]
6. *action-number* **activate** {**policy type control subscriber** *control-policy-name* [**child** [**no-propagation** | **concurrent**] | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** *number*] [**replace-all**]}]
7. *action-number* **authenticate** using {**dot1x** | **mab** | **webauth**} [**aaa** {**authc-list** *authc-list-name* | **authz-list** *authz-list-name*}] [**merge**] [**parameter-map** *map-name*] [**priority** *priority-number*] [**replace** | **replace-all**] [**retries** *number* {**retry-time** *seconds*}]
8. *action-number* **authentication-restart** *seconds*
9. *action-number* **authorize**
10. *action-number* **clear-authenticated-data-hosts-on-port**
11. *action-number* **clear-session**
12. *action-number* **deactivate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name*}
13. *action-number* **err-disable**
14. *action-number* **pause reauthentication**
15. *action-number* **protect**
16. *action-number* **replace**
17. *action-number* **restrict**
18. *action-number* **resume reauthentication**
19. *action-number* **set-timer** *timer-name* *seconds*
20. *action-number* **terminate** {**dot1x** | **mab** | **webauth**}
21. *action-number* **unauthorize**
22. **end**
23. **show policy-map type control subscriber** {**all** | **name** *control-policy-name*}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>policy-map type control subscriber <i>control-policy-name</i></b>  <b>Example:</b> Device(config)# policy-map type control POLICY_1	Defines a control policy for subscriber sessions.
<b>Step 4</b>	<b>event <i>event-name</i> [match-all   match-first]</b>  <b>Example:</b> Device(config-event-control-policymap)# event session-started	Specifies the type of event that triggers actions in a control policy if conditions are met. <ul style="list-style-type: none"> <li>• <b>match-all</b> is the default behavior.</li> <li>• To display the available event types, use the question mark (?) online help function. For a complete description of event types, see the <b>event</b> command in the <a href="#">Cisco IOS Session Aware Networking Command Reference</a>.</li> </ul>
<b>Step 5</b>	<b>priority-number class {<i>control-class-name</i>   always} [do-all   do-until-failure   do-until-success]</b>  <b>Example:</b> Device(config-class-control-policymap)# 10 class always	Associates a control class with one or more actions in a control policy. <ul style="list-style-type: none"> <li>• A named control class must first be configured before specifying it with the <i>control-class-name</i> argument.</li> <li>• <b>do-until-failure</b> is the default behavior.</li> </ul>
<b>Step 6</b>	<b>action-number activate {policy type control subscriber <i>control-policy-name</i> [child [no-propagation   concurrent]   service-template <i>template-name</i> [aaa-list <i>list-name</i>] [precedence <i>number</i>] [replace-all]}</b>  <b>Example:</b> Device(config-action-control-policymap)# 10 activate service-template FALLBACK	(Optional) Activates a control policy or service template on a subscriber session.
<b>Step 7</b>	<b>action-number authenticate using {dot1x   mab   webauth} [aaa {authc-list <i>authc-list-name</i>   authz-list <i>authz-list-name</i>}] [merge] [parameter-map <i>map-name</i>] [priority <i>priority-number</i>] [replace   replace-all] [retries <i>number</i> {retry-time <i>seconds</i>}]</b>  <b>Example:</b> Device(config-action-control-policymap)# 10 authenticate using dot1x priority 10	(Optional) Initiates the authentication of a subscriber session using the specified method.
<b>Step 8</b>	<b>action-number authentication-restart <i>seconds</i></b>  <b>Example:</b> Device(config-action-control-policymap)# 20 authentication-restart 60	(Optional) Sets a timer to restart the authentication process after an authentication or authorization failure.

	Command or Action	Purpose
<b>Step 9</b>	<b><i>action-number</i> authorize</b>  <b>Example:</b> Device(config-action-control-policymap) # 10 authorize	(Optional) Initiates the authorization of a subscriber session.
<b>Step 10</b>	<b><i>action-number</i> clear-authenticated-data-hosts-on-port</b>  <b>Example:</b> Device(config-action-control-policymap) # 20 clear-authenticated-data-hosts-on-port	(Optional) Clears authenticated data hosts on a port after an authentication failure.
<b>Step 11</b>	<b><i>action-number</i> clear-session</b>  <b>Example:</b> Device(config-action-control-policymap) # 30 clear-session	(Optional) Clears an active subscriber session.
<b>Step 12</b>	<b><i>action-number</i> deactivate {policy type control subscriber control-policy-name   service-template template-name}</b>  <b>Example:</b> Device(config-action-control-policymap) # 20 deactivate service-template	(Optional) Deactivates a control policy or service template on a subscriber session.
<b>Step 13</b>	<b><i>action-number</i> err-disable</b>  <b>Example:</b> Device(config-action-control-policymap) # 10 err-disable	(Optional) Temporarily disables a port after a session violation event.
<b>Step 14</b>	<b><i>action-number</i> pause reauthentication</b>  <b>Example:</b> Device(config-action-control-policymap) # 20 pause reauthentication	(Optional) Pauses reauthentication after an authentication failure.
<b>Step 15</b>	<b><i>action-number</i> protect</b>  <b>Example:</b> Device(config-action-control-policymap) # 10 protect	(Optional) Silently drops violating packets after a session violation event.
<b>Step 16</b>	<b><i>action-number</i> replace</b>  <b>Example:</b> Device(config-action-control-policymap) # 10 replace	(Optional) Clears the existing session and creates a new session after a violation event.
<b>Step 17</b>	<b><i>action-number</i> restrict</b>  <b>Example:</b> Device(config-action-control-policymap) # 10 restrict	(Optional) Drops violating packets and generates a syslog entry after a session violation event.

	Command or Action	Purpose
<b>Step 18</b>	<b><i>action-number</i> resume reauthentication</b>  <b>Example:</b> Device(config-action-control-policymap)# 20 resume reauthentication	(Optional) Resumes the reauthentication process after an authentication failure.
<b>Step 19</b>	<b><i>action-number</i> set-timer timer-name seconds</b>  <b>Example:</b> Device(config-action-control-policymap)# 20 set-timer RESTART 60	(Optional) Starts a named policy timer.
<b>Step 20</b>	<b><i>action-number</i> terminate {dot1x   mab   webauth}</b>  <b>Example:</b> Device(config-action-control-policymap)# 20 terminate webauth	(Optional) Terminates an authentication method on a subscriber session.
<b>Step 21</b>	<b><i>action-number</i> unauthorize</b>  <b>Example:</b> Device(config-action-control-policymap)# 20 unauthorize	(Optional) Removes all authorization data from a subscriber session.
<b>Step 22</b>	<b>end</b>  <b>Example:</b> Device(config-action-control-policymap)# end	(Optional) Exits control policy-map action configuration mode and returns to privileged EXEC mode.
<b>Step 23</b>	<b>show policy-map type control subscriber {all   name control-policy-name}</b>  <b>Example:</b> Device# show policy-map type control subscriber name POLICY_1	(Optional) Displays information about Session Aware Networking control policies.

### Example: Control Policy

The following example shows a simple control policy with the minimum configuration necessary for initiating authentication:

```
policy-map type control subscriber POLICY_1
  event session-started match-all
  10 class always do-until-failure
  10 authenticate using dot1x
```

For detailed examples of control policies for concurrent and sequential authentication, see the [“Configuration Examples for Identity Control Policies, on page 24”](#) section.

## Applying a Control Policy to an Interface

Control policies typically control the authentication of subscriber identity and the activation of services on sessions. Perform this task to apply a control policy to an interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service-policy type control subscriber** *control-policy-name*
5. **subscriber aging** {**inactivity-timer** *seconds* [**probe**] | **probe**}

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface tengigabitethernet 1/0/1	Specifies an interface and enters interface configuration mode.
<b>Step 4</b>	<b>service-policy type control subscriber</b> <i>control-policy-name</i>  <b>Example:</b> Device(config-if)# service-policy type control subscriber POLICY_1	Applies a previously configured control policy.  <ul style="list-style-type: none"> <li>• To display a list of all configured control policies, use the question mark (?) online help function.</li> </ul>
<b>Step 5</b>	<b>subscriber aging</b> { <b>inactivity-timer</b> <i>seconds</i> [ <b>probe</b> ]   <b>probe</b> }  <b>Example:</b> Device(config-if)# subscriber aging inactivity-timer 60 probe	Enables an inactivity timer for subscriber sessions.



**Example: Applying a Control Policy to an Interface**

```
interface TenGigabitEthernet 1/0/2
 subscriber aging inactivity-timer 60 probe
 service-policy type control subscriber POLICY_1
```

## Configuring Authentication Features on Ports

Perform this task to control access to a port, including the port authorization state, host access mode, preauthentication access, and the authentication direction.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **access-session port-control** {**auto** | **force-authorized** | **force-unauthorized**}
5. **access-session host-mode** {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}
6. **access-session closed**
7. **access-session control-direction** {**both** | **in**}
8. **end**
9. **show access-session interface** *interface-type interface-number* [**details**]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface gigabitethernet 1/0/2	Enters interface configuration mode for the selected interface.
<b>Step 4</b>	<b>access-session port-control</b> { <b>auto</b>   <b>force-authorized</b>   <b>force-unauthorized</b> }  <b>Example:</b> Device(config-if)# access-session port-control auto	Sets the authorization state of a port.  • The default value is <b>force-authorized</b> .
<b>Step 5</b>	<b>access-session host-mode</b> { <b>multi-auth</b>   <b>multi-domain</b>   <b>multi-host</b>   <b>single-host</b> }	Allows hosts to gain access to a controlled port.

	Command or Action	Purpose
	<b>Example:</b> <pre>Device(config-if)# access-session host-mode single-host</pre>	<ul style="list-style-type: none"> <li>To use this command, you must first enable the <b>access-session port-control auto</b> command.</li> <li>The default value is <b>multi-auth</b>.</li> </ul>
<b>Step 6</b>	<b>access-session closed</b>  <b>Example:</b> <pre>Device(config-if)# access-session closed</pre>	Prevents preauthentication access on this port. <ul style="list-style-type: none"> <li>The port is set to open access by default.</li> </ul>
<b>Step 7</b>	<b>access-session control-direction {both   in}</b>  <b>Example:</b> <pre>Device(config-if)# access-session control-direction in</pre>	Sets the direction of authentication control on a port. <ul style="list-style-type: none"> <li>The default value is <b>both</b>.</li> </ul>
<b>Step 8</b>	<b>end</b>  <b>Example:</b> <pre>Device(config-if)# end</pre>	Exits interface configuration mode and returns to privileged EXEC mode.
<b>Step 9</b>	<b>show access-session interface <i>interface-type</i> <i>interface-number</i> [details]</b>  <b>Example:</b> <pre>Device# show access-session interface gigabitethernet 1/0/2 details</pre>	Displays information about subscriber sessions that match the specified client interface.

**Example: Port Authentication**

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

## Configuring a Parameter Map for Web-Based Authentication

A parameter map allows you to modify parameters that control the behavior of actions configured under a control policy. A parameter map for web-based authentication sets parameters that can be applied to subscriber sessions during authentication. If you do not create a parameter map, the policy uses default parameters.

Perform the following steps to define either a global or named parameter map for web-based authentication.

**Note**

The configuration commands available in the global parameter map differ from the commands available in a named parameter map.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type webauth** *{parameter-map-name | global}*
4. **banner** *{file location:filename | text banner-text}*
5. **consent email**
6. **custom-page** *{failure | login [expired] | success}* **device** *location:filename*
7. **max-http-conns** *number*
8. **ratelimit init-state-sessions** *rate-limit*
9. **redirect** *{ {for-login | on-failure | on-success} url | portal {ipv4 ipv4-address | ipv6 ipv6-address} }*
10. **timeout init-state** *min minutes*
11. **type** *{authbypass | consent | webauth | webconsent}*
12. **virtual-ip** *{ipv4 ipv4-address | ipv6 ipv6-address}*
13. **watch-list** *{add-item {ipv4 ipv4-address | ipv6 ipv6-address} | dynamic-expiry-timeout minutes | enabled}*
14. **end**
15. **show ip admission status** *[banners | custom-pages | parameter-map [parameter-map]]*

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>parameter-map type webauth</b> <i>{parameter-map-name   global}</i>  <b>Example:</b> Device(config)# parameter-map type webauth MAP_2	Creates a parameter map and enters parameter-map webauth configuration mode.  <ul style="list-style-type: none"> <li>• The specific configuration commands supported for a global parameter map defined with the <b>global</b> keyword differ from the commands supported for a named parameter map defined with the <i>parameter-map-name</i> argument.</li> </ul>
<b>Step 4</b>	<b>banner</b> <i>{file location:filename   text banner-text}</i>  <b>Example:</b> Device(config-params-parameter-map)# banner file flash:webauth_banner.html	(Optional) Displays a banner on the web-authentication login web page.

	Command or Action	Purpose
<b>Step 5</b>	<b>consent email</b>  <b>Example:</b> Device(config-params-parameter-map)# consent email	(Optional) Requests a user's e-mail address on the web-authentication login web page.  <ul style="list-style-type: none"> <li>This command is supported in named parameter maps only.</li> </ul>
<b>Step 6</b>	<b>custom-page {failure   login [expired]   success} device location:filename</b>  <b>Example:</b> Device(config-params-parameter-map)# custom-page login device flash:webauth_login.html Device(config-params-parameter-map)# custom-page login expired device flash:webauth_expire.html Device(config-params-parameter-map)# custom-page success device flash:webauth_success.html Device(config-params-parameter-map)# custom-page failure device flash:webauth_fail.html	(Optional) Displays custom authentication proxy web pages during web-based authentication.  <ul style="list-style-type: none"> <li>You must configure all four custom HTML files. If fewer than four files are configured, the internal default HTML pages will be used.</li> </ul>
<b>Step 7</b>	<b>max-http-conns number</b>  <b>Example:</b> Device(config-params-parameter-map)# max-http-conns 5	(Optional) Limits the number of HTTP connections for each web authentication client.
<b>Step 8</b>	<b>ratelimit init-state-sessions rate-limit</b>  <b>Example:</b> Device(config-params-parameter-map)# ratelimit init-state-sessions 500	(Optional) Limits the number of web-based authentication sessions in the Init state.  <ul style="list-style-type: none"> <li>This command is supported in the global parameter map only.</li> </ul>
<b>Step 9</b>	<b>redirect {{for-login   on-failure   on-success} url   portal {ipv4 ipv4-address   ipv6 ipv6-address}}</b>  <b>Example:</b> Device(config-params-parameter-map)# redirect portal ipv6 FE80::1 Device(config-params-parameter-map)# redirect on-failure http://10.10.3.34/~sample/failure.html	(Optional) Redirects users to a particular URL during web-based authentication.
<b>Step 10</b>	<b>timeout init-state min minutes</b>  <b>Example:</b> Device(config-params-parameter-map)# timeout init-state min 15	(Optional) Sets the Init state timeout for web-based authentication sessions.
<b>Step 11</b>	<b>type {authbypass   consent   webauth   webconsent}</b>  <b>Example:</b> Device(config-params-parameter-map)# type consent	(Optional) Defines the methods supported by a web-based authentication parameter map.  <ul style="list-style-type: none"> <li>This command is supported in named parameter maps only.</li> </ul>

	Command or Action	Purpose
<b>Step 12</b>	<b>virtual-ip</b> { <b>ipv4</b> <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> }  <b>Example:</b> Device(config-params-parameter-map)# virtual-ip ipv6 FE80::1	(Optional) Specifies a virtual IP address for web-based authentication clients.  <ul style="list-style-type: none"> <li>This command is supported in the global parameter map only.</li> </ul>
<b>Step 13</b>	<b>watch-list</b> { <b>add-item</b> { <b>ipv4</b> <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> }   <b>dynamic-expiry-timeout</b> <i>minutes</i>   <b>enabled</b> }  <b>Example:</b> Device(config-params-parameter-map)# watch-list enabled Device(config-params-parameter-map)# watch-list dynamic-expiry-timeout 20 Device(config-params-parameter-map)# watch-list add-item ipv6 FE80::1	(Optional) Enables a watch list of web-based authentication clients.  <ul style="list-style-type: none"> <li>This command is supported in the global parameter map only.</li> </ul>
<b>Step 14</b>	<b>end</b>  <b>Example:</b> Device(config-params-parameter-map)# end	(Optional) Exits parameter-map configuration mode and returns to privileged EXEC mode.
<b>Step 15</b>	<b>show ip admission status</b> [ <b>banners</b>   <b>custom-pages</b>   <b>parameter-map</b> [ <i>parameter-map</i> ]]  <b>Example:</b> Device# show ip admission status custom-pages	(Optional) Displays information about configured banners and custom pages.

### Example: Parameter Map for Web-Based Authentication

```
parameter-map type webauth PMAP_2
 type webconsent
 timeout init-state min 15
 max-http-conns 5
 consent email
 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
```

### What to Do Next

Apply the parameter map to sessions by specifying it in the **authenticate using** command when configuring a Control Policy. See the “[Configuring a Control Policy, on page 13](#)” section.

# Configuration Examples for Identity Control Policies

## Example: Configuring Control Policy for Concurrent Authentication Methods

The following example shows a control policy that is configured to allow concurrent authentication. All three methods (dot1x, MAB, and web authentication) are run simultaneously when a session is started. The dot1x method is set to the highest priority and web authentication has the lowest priority, which means that if multiple methods succeed, the highest priority method is honored.

If authentication fails, the session manager checks whether all methods have failed, and if so, it sets the restart timer to 60 seconds, after which it attempts to start all three methods again. On authentication success, the session manager terminates any lower priority methods; for dot1x, this is MAB and webauth; for MAB it is webauth. Lastly, if session manager detects a dot1x client (agent-found) it triggers only dot1x to run.

The class map named ALL-FAILED checks that all three methods have run to completion (result type is none until then) and that none of them was successful. In other words, all three methods have completed and failed.



### Note

When configuring a control policy for concurrent authentication, you must include a policy rule that explicitly terminates one method after another method of a higher priority succeeds.

```
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
!
class-map type control subscriber match-all DOT1X
match method dot1x
!
class-map type control subscriber match-all MAB
match method mab
!
policy-map type control subscriber CONCURRENT_DOT1X_MAB_WEBAUTH
event session-started match-all
10 class always do-until-failure
10 authenticate using mab priority 20
20 authenticate using dot1x priority 10
30 authenticate using webauth parameter-map WEBAUTH_DEFAULT priority 30
event authentication-failure match-first
10 class ALL_FAILED
10 authentication-restart 60
event authentication-success match-all
10 class DOT1X
10 terminate MAB
20 terminate webauth
20 class MAB
10 terminate webauth
event agent-found match-all
10 class always do-until-failure
10 authenticate using dot1x priority 10
```

## Example: Configuring Control Policy for Sequential Authentication Methods

The following example shows a control policy that is configured to allow sequential authentication methods using 802.1X (dot1x), MAB, and web authentication.

```
parameter-map type webauth WEBAUTH_FALLBACK
  type webauth
!
class-map type control subscriber match-all DOT1X_NO_RESP
  match method dot1x
  match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB_FAILED
  match method mab
  match result-type method mab authoritative
!
policy-map type control subscriber POLICY_Gi3/0/10
  event session-started match-all
    10 class always do-until-failure
    10 authenticate using dot1x priority 10
  event authentication-failure match-first
    10 class DOT1X_NO_RESP do-until-failure
    10 terminate dot1x
    20 authenticate using mab priority 20
    20 class MAB_FAILED do-until-failure
    10 terminate mab
    20 authenticate using webauth parameter-map WEBAUTH_FALLBACK priority 30
    30 class always do-until-failure
    10 terminate dot1x
    20 terminate mab
    30 terminate webauth
    40 authentication-restart 60
  event agent-found match-all
    10 class always do-until-failure
    10 terminate mab
    20 terminate webauth
    30 authenticate using dot1x priority 10
```

The following example shows a control policy that is configured to allow sequential authentication methods using 802.1X and MAB. If authentication fails, a service template for VLAN is activated.

```
service-template VLAN210
  vlan 210
!
class-map type control subscriber match-all DOT1X_FAILED
  match method dot1x
  match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
  match method dot1x
  match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB_FAILED
  match method mab
  match result-type method mab authoritative
!
policy-map type control subscriber POLICY_Gi3/0/14
  event session-started match-all
    10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
  event authentication-failure match-first
    10 class DOT1X_NO_RESP do-until-failure
    10 terminate dot1x
    20 authenticate using mab priority 20
    20 class MAB_FAILED do-until-failure
    10 terminate mab
    20 activate service-template VLAN210
    30 authorize
    30 class DOT1X_FAILED do-until-failure
    10 terminate dot1x
```

```

    20 authenticate using mab priority 20
40 class always do-until-failure
    10 terminate dot1x
    20 terminate mab
    30 authentication-restart 60
event agent-found match-all
    10 class always do-until-failure
    10 terminate mab
    20 authenticate using dot1x retries 2 retry-time 0 priority 10

```

## Example: Configuring Parameter Maps

### Global Parameter Map

The following example shows the configuration of a global parameter map:

```

parameter-map type webauth global
  timeout init-state min 15
  logging enabled
  watch-list enabled
  virtual-ip ipv6 FE80::1
  redirect on-failure http://10.10.3.34/~sample/failure.html
  ratelimit init-state-sessions 500
  max-http-conns 100
  watch-list dynamic-expiry-timeout 5000
  banner file flash:webauth_banner.html

```

### Named Parameter Maps for Web Authentication and Authentication Bypass (nonresponsive host [NRH])

The following example shows the configuration of two named parameter maps; one for web authentication and one for authentication bypass. This example also shows the corresponding control policy configuration.

```

parameter-map type webauth WEBAUTH_BANNER
  type webauth
  banner
!
parameter-map type webauth WEBAUTH_NRH
  type authbypass
!
class-map type control subscriber match-all NRH_FAIL
  match method webauth
  match current-method-priority eq 254
!
policy-map type control subscriber WEBAUTH_NRH
  event session-started match-all
    10 class always do-until-failure
    10 authenticate using webauth parameter-map WEBAUTH_NRH priority 254
  event authentication-failure match-all
    10 class NRH_FAIL do-until-failure
    10 terminate webauth
    20 authenticate using webauth parameter-map WEBAUTH_BANNER priority 30

```

### Named Parameter Map for Web Authentication Using Custom Pages

The following example shows the configuration of a named parameter map for web authentication that defines custom pages for the login process, along with a control policy that uses the parameter map.

```

parameter-map type webauth CUSTOM_WEBAUTH
  type webauth
  custom-page login device flash:login_page.htm
  custom-page success device flash:success_page.htm
  custom-page failure device flash:fail_page.htm
  custom-page login expired device flash:expire_page.htm
!
policy-map type control subscriber CUSTOM_WEBAUTH
  event session-started match-all

```



```

10 class always do-until-failure
10 authenticate using webauth parameter-map CUSTOM_WEB retries 2 retry-time 0

```

### Named Parameter Map for Consent

The following example shows the configuration of a named parameter map for consent, along with the corresponding control policy that uses the parameter map:

```

parameter-map type webauth CONSENT
  type consent
!
ip access-list extended GUEST_ACL
  permit ip any 172.30.30.0 0.0.0.255
  permit ip any host 172.20.249.252
!
service-template GUEST_POLICY
  access-group GUEST_ACL
!
policy-map type control subscriber CONSENT
  event session-started match-all
    10 class always do-until-failure
    10 authenticate using webauth parameter-map CONSENT
  event authentication-success match-all
    10 class always do-until-failure
    10 activate service-template GUEST_POLICY

```

### Named Parameter Map for Web Authentication with Consent

The following example shows the configuration of a named parameter map for web authentication with consent, along with the corresponding control policy that uses the parameter map:

```

parameter-map type webauth WEBAUTH_CONSENT
  type webconsent
!
ip access-list extended GUEST_ACL
  permit ip any 172.30.30.0 0.0.0.255
  permit ip any host 172.20.249.252
!
service-template GUEST_POLICY
  access-group GUEST_ACL
!
policy-map type control subscriber WEBAUTH_CONSENT
  event session-started match-all
    10 class always do-until-failure
    10 authenticate using webauth parameter-map CONSENT
  event authentication-success match-all
    10 class always do-until-failure
    10 activate service-template GUEST_POLICY

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Session Aware Networking commands	<a href="#">Cisco IOS Session Aware Networking Command Reference</a>
Address Resolution Protocol (ARP) commands	<a href="#">Cisco IOS IP Addressing Services Command Reference</a>

Related Topic	Document Title
ARP configuration tasks	<i>IP Addressing - ARP Configuration Guide</i>
Authentication, authorization, and accounting (AAA) configuration tasks	<i>Authentication Authorization and Accounting Configuration Guide</i>
AAA commands	<i>Cisco IOS Security Command Reference</i>

### Standards and RFCs

Standard/RFC	Title
RFC 5176	<i>Dynamic Authorization Extensions to RADIUS</i>

### Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Identity Control Policies

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 2: Feature Information for Identity Control Policies**

Feature Name	Releases	Feature Information
Cisco Common Classification Policy Language based Identity Configuration	Cisco IOS XE Release 3.2SE	<p>Identity control policies define the actions taken in response to specified events and conditions.</p> <p>The following commands were introduced: <b>activate</b> (policy-map action), <b>authenticate using</b>, <b>authentication display</b>, <b>authentication-restart</b>, <b>authorize</b>, <b>banner</b> (parameter-map webauth), <b>class</b>, <b>class-map type control subscriber</b>, <b>clear-authenticated-data-hosts-on-port</b>, <b>clear session</b>, <b>consent email custom-page</b>, <b>deactivate</b>, <b>err-disable</b>, <b>event</b>, <b>logging enabled</b> (parameter-map webauth), <b>match</b>, <b>max-http-conns</b>, <b>parameter-map type webauth</b>, <b>pause reauthentication</b>, <b>policy-map type control subscriber</b>, <b>protect</b> (policy-map action), <b>ratelimit init-state-sessions</b>, <b>redirect</b> (parameter-map webauth), <b>replace</b>, <b>restrict</b>, <b>resume reauthentication</b>, <b>service-policy type control subscriber</b>, <b>set-timer</b>, <b>show access-session</b>, <b>show class-map type control subscriber</b>, <b>show policy-map type control subscriber</b>, <b>terminate</b>, <b>type</b> (parameter-map webauth), <b>unauthorize</b>, <b>virtual-ip</b>, <b>watch-list</b>.</p>
Concurrent Authentication	Cisco IOS XE Release 3.2SE	Allows concurrent operation of 802.1x, MAB and web authentication methods, making it possible to invoke multiple authentication methods in parallel on a single session.
Per User Inactivity Handling across Methods	Cisco IOS XE Release 3.2SE	Supports RADIUS attributes 28 (Idle-Timeout) and 29 (Termination-Action).





## Configuring Identity Service Templates

Identity service templates contain a set of policy attributes or features that can be applied to one or more subscriber sessions through a control policy, a RADIUS Change of Authorization (CoA) request, or a user profile or service profile. This module provides information about how to configure local service templates for Session Aware Networking.

- [Finding Feature Information, page 31](#)
- [Prerequisites for Identity Service Templates, page 31](#)
- [Information About Identity Service Templates, page 32](#)
- [How to Configure Identity Service Templates, page 33](#)
- [Configuration Examples for Identity Service Templates, page 35](#)
- [Additional References, page 37](#)
- [Feature Information for Identity Service Templates, page 38](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Prerequisites for Identity Service Templates

For downloadable service templates, the switch uses the default password “cisco123” when downloading the service templates from the authentication, authorization, and accounting (AAA) server, Cisco Secure Access Control Server (ACS), or Cisco Identity Services Engine (ISE). The AAA, ACS, and ISE server must include the password “cisco123” in the service template configuration.

# Information About Identity Service Templates

## Service Templates for Session Aware Networking

A service template contains a set of service-related attributes or features, such as access control lists (ACLs) and VLAN assignments, that can be activated on one or more subscriber sessions in response to session life-cycle events. Templates simplify the provisioning and maintenance of network session policies where policies fall into distinct groups or are role-based.

A service template is applied to sessions through its reference in a control policy, through RADIUS Change of Authorization (CoA) requests, or through a user profile or service profile. User profiles are defined per subscriber; service profiles can apply to multiple subscribers.

Session Aware Networking supports two types of service templates:

- **Downloadable Service Templates**—The service template is configured centrally on an external ACS or AAA server and downloaded on demand.
- **Locally Configured Service Templates**—The service template is configured locally on the device through the Cisco IOS command-line interface (CLI).

## Downloadable Service Templates

Session Aware Networking can download a service template defined on an external AAA server. The template defines a collection of AAA attributes. These templates are applied to sessions through the use of vendor-specific attributes (VSAs) included in RADIUS CoA messages received from the external AAA server or ACS. The name of the template is referenced in a user profile or a control policy, which triggers a download of the service template during processing.

The downloadable template is cached on the device and subsequent requests for a download will refer to the available cached template. The template however is cached only for the duration of its active usage. The downloaded template cached on the device is protected and cannot be deleted through the CLI or through other applications. This ensures that the template is deleted only when there are no active references to it.

## Locally Configured Service Templates

Service templates can be configured locally through the CLI. These service templates can be applied to subscriber sessions by a reference in a control policy.

When an active local template is updated, changes to that local template will be reflected across all sessions for which the template is active. If a template is deleted, all content from that template that is applied against sessions is removed.

# How to Configure Identity Service Templates

## Configuring a Local Service Template

A service template defines the local policies that can be applied to a subscriber session. Activate this service template on sessions on which the local policies must be applied.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service-template** *template-name*
4. **absolute-timer** *minutes*
5. **access-group** *access-list-name*
6. **description** *description*
7. **inactivity-timer** *minutes* [**probe**]
8. **redirect url** *url*
9. **tag** *tag-name*
10. **vlan** *vlan-id*
11. **end**
12. **show service-template** [*template-name*]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>service-template</b> <i>template-name</i>  <b>Example:</b> Device(config)# service-template SVC_2	Creates a service template and enters service template configuration mode.
<b>Step 4</b>	<b>absolute-timer</b> <i>minutes</i>  <b>Example:</b> Device(config-service-template)# absolute-timer 15	(Optional) Enables an absolute timeout for subscriber sessions.

	Command or Action	Purpose
<b>Step 5</b>	<b>access-group</b> <i>access-list-name</i>  <b>Example:</b> Device(config-service-template)# access-group ACL_2	(Optional) Applies an access list to sessions using a service template.
<b>Step 6</b>	<b>description</b> <i>description</i>  <b>Example:</b> Device(config-service-template)# description label for SVC_2	(Optional) Adds a description for a service template.
<b>Step 7</b>	<b>inactivity-timer</b> <i>minutes</i> [ <b>probe</b> ]  <b>Example:</b> Device(config-service-template)# inactivity-timer 15	(Optional) Enables an inactivity timeout for subscriber sessions.
<b>Step 8</b>	<b>redirect url</b> <i>url</i>  <b>Example:</b> Device(config-service-template)# redirect url www.cisco.com	(Optional) Redirects clients to a particular URL.
<b>Step 9</b>	<b>tag</b> <i>tag-name</i>  <b>Example:</b> Device(config-service-template)# tag TAG_2	(Optional) Associates a user-defined tag with a service template.
<b>Step 10</b>	<b>vlan</b> <i>vlan-id</i>  <b>Example:</b> Device(config-service-template)# vlan 215	(Optional) Applies a VLAN to sessions using a service template.
<b>Step 11</b>	<b>end</b>  <b>Example:</b> Device(config-service-template)# end	Exits service template configuration mode and returns to privileged EXEC mode.
<b>Step 12</b>	<b>show service-template</b> [ <i>template-name</i> ]  <b>Example:</b> Device# show service-template SVC_2	Displays information about configured service templates.

**Example: Service Template**

```

service-template SVC_2
description label for SVC_2
access-group ACL_2
redirect url www.cisco.com

```



```
vlan 215
inactivity-timer 15
absolute-timer 15
tag TAG_2
```

### What to Do Next

To activate a service template on a subscriber session, specify the service template in a control policy. See [“Configuring a Control Policy, on page 13.”](#)

## Configuration Examples for Identity Service Templates

### Example: Activating a Service Template and Replace All

#### Local Service Template Configuration

The following example shows the configuration of a service template defined locally on the device. This template contains attributes that are applied to sessions that use the control policy named POSTURE\_VALIDATION, shown below:

```
service-template DOT1X
access-group SVC1_ACL
redirect url www.cisco.com match URL_REDIRECT_ACL
inactivity-timer 60
absolute-timer 300
!
ip access-list extended URL_REDIRECT_ACL
permit tcp any host 5.5.5.5 eq www
```

#### Control Policy Configuration

The following example shows a control policy that activates the service template named DOT1X with replace-all enabled. The successfully activated template will replace the existing authorization data and any service template previously applied to the session.

```
policy-map type control subscriber POSTURE_VALIDATION
event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x priority 10
    20 authenticate using webauth priority 20
event authentication-success match-all
  10 class DOT1X do-all
    10 terminate webauth
    20 activate service-template DOT1X replace-all
```

### Example: Activating a Service Template for Fallback Service

#### Local Service Template Configuration

The following example shows the configuration of a service template defined locally on the device. This template contains attributes that are applied to sessions that use the control policy named POSTURE\_VALIDATION, shown below:

```
service-template FALLBACK
description fallback service
access-group ACL_2
redirect url www.cisco.com
```

**Example: Deactivating a Service Template**

```

inactivity-timer 15
absolute-timer 15
tag TAG_2

```

**Control Policy Configuration**

The following example shows a control policy that runs authentication methods dot1x and MAB. If dot1x authentication fails, MAB authentication is attempted. If MAB fails, the system provides a default authorization profile using the FALLBACK template.

```

policy-map type control subscriber POSTURE_VALIDATION
event session-started match-all
  10 class always do-all
    10 authenticate using dot1x
event authentication-failure match-all
  10 class DOT1X do-all
    10 authenticate using mab
  20 class MAB do-all
    10 activate service-template FALLBACK

```

## Example: Deactivating a Service Template

**Access Control List Configuration**

The following example shows the configuration of an access control list (ACL) that is used by the local service template named LOW\_IMPACT\_TEMPLATE, shown below.

```

ip access-list extended LOW_IMPACT_ACL
permit udp any any eq bootps
permit tcp any any eq www
permit tcp any any eq 443
permit ip any 172.30.0.0 0.0.255.255

```

**Local Service Template Configuration**

The following example shows the configuration of the local service template that provides limited access to all hosts even when authentication fails.

```

service-template LOW_IMPACT_TEMPLATE
description Service template for Low impact mode
access-group LOW_IMPACT_ACL
inactivity-timer 60
tag LOW_IMPACT_TEMPLATE

```

**Control Policy Configuration**

The following example shows the configuration of a control policy that uses the template named LOW\_IMPACT\_TEMPLATE to provide limited access to all hosts even when authentication fails. If authentication succeeds, the policy manager removes the service 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

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Session Aware Networking commands	<a href="#">Cisco IOS Session Aware Networking Command Reference</a>
Address Resolution Protocol (ARP) commands	<a href="#">Cisco IOS IP Addressing Services Command Reference</a>
ARP configuration tasks	<i>IP Addressing - ARP Configuration Guide</i>
Authentication, authorization, and accounting (AAA) configuration tasks	<i>Authentication Authorization and Accounting Configuration Guide</i>
AAA commands	<i>Cisco IOS Security Command Reference</i>

### Standards and RFCs

Standard/RFC	Title
RFC 5176	<i>Dynamic Authorization Extensions to RADIUS</i>

**Technical Assistance**

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Identity Service Templates

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 3: Feature Information for Identity Service Templates**

Feature Name	Releases	Feature Information
Downloadable Identity Service Template	Cisco IOS XE Release 3.2SE	Enables a service template to be downloaded from an ACS and its attributes applied against a session.
Identity Service Template	Cisco IOS XE Release 3.2SE	Enables identity service templates to be configured locally and available at all times.  The following commands were introduced: <b>absolute-timer</b> , <b>access-group</b> (service template), <b>description</b> (service template), <b>inactivity-timer</b> , <b>redirect url</b> , <b>service-template</b> , <b>show service-template</b> , <b>tag</b> (service template), <b>vlan</b> (service template).



## Change of Authorization Support

Session Aware Networking supports RADIUS change of authorization (CoA) commands for session query, reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation. This module provides information about the supported CoA commands for Session Aware Networking.

- [Finding Feature Information, page 39](#)
- [Information About CoA Support, page 39](#)
- [Additional References, page 44](#)
- [Feature Information for CoA Support, page 45](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Information About CoA Support

### RADIUS Change-of-Authorization Support

Cisco IOS software supports the RADIUS CoA extensions defined in RFC 5176 that are typically used in a push model to allow the dynamic reconfiguring of sessions from external AAA or policy servers. Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a AAA or policy server) and directed to the device that acts as a listener.

The table below shows the RADIUS CoA commands and vendor-specific attributes (VSAs) supported by Session Aware Networking. All CoA commands must include the session identifier between the device and the CoA client.

**Table 4: RADIUS CoA Commands Supported by Session Aware Networking**

CoA Command	Cisco VSA
Activate service	Cisco:Avpair="subscriber:command=activate-service" Cisco:Avpair="subscriber:service-name=<service-name>" Cisco:Avpair="subscriber:precedence=<precedence-number>" Cisco:Avpair="subscriber:activation-mode=replace-all"
Deactivate service	Cisco:Avpair="subscriber:command=deactivate-service" Cisco:Avpair="subscriber:service-name=<service-name>"
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Session query	Cisco:Avpair="subscriber:command=session-query"
Session reauthenticate	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair="subscriber:reauthenticate-type=last" or Cisco:Avpair="subscriber:reauthenticate-type=rerun"
Session terminate	This is a standard disconnect request and does not require a VSA.

## Session Identification

For disconnect and CoA requests targeted at a particular session, the device locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco VSA)
- Calling-Station-Id (IETF attribute #31, which contains the host MAC address)
- IPv6 Attributes, which can be one of the following:
  - Framed-IPv6-Prefix (IETF attribute #97) and Framed-Interface-Id (IETF attribute #96), which together create a full IPv6 address per RFC 3162
  - Framed-IPv6-Address

- Plain IP Address (IETF attribute #8)

If more than one session identification attribute is included in the message, all of the attributes must match the session or the device returns a Disconnect-NAK or CoA-NAK with the error code “Invalid Attribute Value.”

For CoA requests targeted at a particular enforcement policy, the device returns a CoA-NAK with the error code “Invalid Attribute Value” if any of the above session identification attributes are included in the message.

## CoA Activate Service Command

The CoA activate service command can be used to activate a service template on a session. The AAA server sends the request in a standard CoA-Request message using the following VSAs:

Cisco:Avpair=“subscriber:command=activate-service”

Cisco:Avpair=“subscriber:service-name=<service-name>”

Cisco:Avpair=“subscriber:precedence=<precedence-number>”

Cisco:Avpair=“subscriber:activation-mode=replace-all”

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “[Session Identification, on page 40](#)” section. If the device cannot locate a session, it returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the device locates a session, it initiates an activate template operation for the hosting port and a CoA-ACK is returned. If activating the template fails, a CoA-NAK message is returned with the Error-Code attribute set to the appropriate message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

## CoA Deactivate Service Command

The CoA deactivate service command can be used to deactivate a service template on a session. The AAA server sends the request in a standard CoA-Request message using the following VSAs:

Cisco:Avpair=“subscriber:command=deactivate-service”

Cisco:Avpair=“subscriber:service-name=<service-name>”

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “[Session Identification, on page 40](#)” section. If the device cannot locate a session, it returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the device locates a session, it initiates a deactivate template operation for the hosting port and a CoA-ACK is returned. If deactivating the template fails, a CoA-NAK message is returned with the Error-Code attribute set to the appropriate message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

## CoA Bounce Host Port Command

The CoA bounce host port command terminates a session and bounces the port (initiates a link down event followed by a link up event). The AAA server sends the request in a standard CoA-Request message with the following VSA:

```
Cisco:Avpair="subscriber:command=bounce-host-port"
```

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the [“Session Identification, on page 40”](#) section. If the session cannot be located, the device returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the device disables the hosting port for a period of ten seconds, reenables it (port bounce), and returns a CoA-ACK.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

The CoA bounce port command is useful as a last resort when an endpoint needs to acquire a new IP address after a change in authorization and this is the only way to indicate to the endpoint to restart the DHCP process. This can occur when there is a VLAN change and the endpoint is a device, such as a printer, that does not have a mechanism to detect a change on this authentication port. This command can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port.

## CoA Disable Host Port Command

The CoA disable host port command administratively shuts down the authentication port that is hosting a session, which terminates the session. The AAA server sends the request in a standard CoA-Request message with the following VSA:

```
Cisco:Avpair="subscriber:command=disable-host-port"
```

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the [“Session Identification, on page 40”](#) section. If the device cannot locate the session, it returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the device locates the session, it disables the hosting port and returns a CoA-ACK message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

## CoA Session Query Command

The CoA session query command requests service information about a subscriber session. The AAA server sends the request in a standard CoA-Request message containing the following VSA:

```
Cisco:Avpair="subscriber:command=session-query"
```

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the [“Session Identification, on page 40”](#) section. If the device cannot locate a session, it returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the device locates a session, it performs a session query operation on the session and returns a CoA-ACK message.



If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

## CoA Session Reauthenticate Command

To initiate session authentication, the AAA server sends a standard CoA-Request message containing the following VSAs:

Cisco:Avpair="subscriber:command=reauthenticate"

Cisco:Avpair="subscriber:reauthenticate-type=<last | rerun>"

"reauthenticate-type" defines whether the CoA reauthentication request uses the authentication method that last succeeded on the session or whether the authentication process is completely rerun.

The following rules apply:

- "subscriber:command=reauthenticate" must be present to trigger a reauthentication.
- If "subscriber:reauthenticate-type" is not specified, the default behavior is to rerun the last successful authentication method for the session. If the method reauthenticates successfully, all old authorization data is replaced with the new reauthenticated authorization data.
- "subscriber:reauthenticate-type" is valid only when included with "subscriber:command=reauthenticate." If it is included in another CoA command, the VSA will be silently ignored.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is resent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

## CoA Session Terminate Command

A CoA Disconnect-Request command terminates a session without disabling the host port. This command causes reinitialization of the authenticator state machine for the specified host, but does not restrict the host's access to the network. If the session cannot be located, the device returns a Disconnect-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device terminates the session. After the session has been completely removed, the device returns a Disconnect-ACK.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client.

To restrict a host's access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. When you want to restore network access on the port, reenale it using a non-RADIUS mechanism.

# Additional References

## Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Session Aware Networking commands	<a href="#">Cisco IOS Session Aware Networking Command Reference</a>
Address Resolution Protocol (ARP) commands	<a href="#">Cisco IOS IP Addressing Services Command Reference</a>
ARP configuration tasks	<i>IP Addressing - ARP Configuration Guide</i>
Authentication, authorization, and accounting (AAA) configuration tasks	<i>Authentication Authorization and Accounting Configuration Guide</i>
AAA commands	<i>Cisco IOS Security Command Reference</i>

## Standards and RFCs

Standard/RFC	Title
RFC 5176	<i>Dynamic Authorization Extensions to RADIUS</i>

## Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for CoA Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 5: Feature Information for CoA Support**

Feature Name	Releases	Feature Information
Change of Authorization	Cisco IOS XE Release 3.2SE	<p>Supports CoA requests for initiating the following:</p> <ul style="list-style-type: none"><li>• Activating and deactivating service templates on sessions</li><li>• Port bounce</li><li>• Port shutdown</li><li>• Querying a session</li><li>• Reauthenticating a session</li><li>• Terminating a session</li></ul> <p>These VSAs are sent in a standard CoA-Request message from a AAA server.</p>





## CHAPTER

# 5

## Configuring Local Authentication Using LDAP

Local authentication using Lightweight Directory Access Protocol (LDAP) allows an endpoint to be authenticated using 802.1X, MAC authentication bypass (MAB), or web authentication with LDAP as a backend. Local authentication in Session Aware Networking also supports associating an authentication, authorization, and accounting (AAA) attribute list with the local username. This module provides information about configuring local authentication for Session Aware Networking.

- [Finding Feature Information, page 47](#)
- [Information About Local Authentication Using LDAP, page 47](#)
- [How to Configure Local Authentication Using LDAP, page 48](#)
- [Configuration Examples for Local Authentication Using LDAP, page 52](#)
- [Additional References, page 52](#)
- [Feature Information for Local Authentication Using LDAP, page 53](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Information About Local Authentication Using LDAP

### Local Authentication Using LDAP

Local authentication using LDAP allows an endpoint to be authenticated using 802.1X, MAB, or web authentication with LDAP as a backend. Local authentication also supports additional AAA attributes by associating an attribute list with a local username for wireless sessions.

# AES Key Wrap

The Advanced Encryption Standard (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.

## How to Configure Local Authentication Using LDAP

### Configuring Local Authentication Using LDAP

Perform this task to specify the AAA method list for local authentication and to associate an attribute list with a local username.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa local authentication** *{method-list-name | default}* **authorization** *{method-list-name | default}*
4. **username** *name* **aaa attribute list** *aaa-attribute-list* [**password** *password*]
5. **exit**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>aaa local authentication</b> <i>{method-list-name   default}</i> <b>authorization</b> <i>{method-list-name   default}</i>  <b>Example:</b> Device(config)# aaa local authentication default authorization default	Specifies the method lists to use for local authentication and authorization from a LDAP server.
Step 4	<b>username</b> <i>name</i> <b>aaa attribute list</b> <i>aaa-attribute-list</i> [ <b>password</b> <i>password</i> ]	Associates a AAA attribute list with a local username.

	Command or Action	Purpose
	<b>Example:</b> Device(config)# username USER_1 aaa attribute list LOCAL_LIST password CISCO	
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Device(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

## Configuring MAC Filtering Support

Perform this task to set the RADIUS compatibility mode, the MAC delimiter, and the MAC address as the username to support MAC filtering.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius *group-name***
4. **subscriber mac-filtering security-mode {mac | none | shared-secret}**
5. **mac-delimiter {colon | hyphen | none | single-hyphen}**
6. **exit**
7. **username *mac-address* mac [aaa attribute list *aaa-attribute-list*]**
8. **exit**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>aaa group server radius <i>group-name</i></b>  <b>Example:</b> Device(config)# aaa group server radius RAD_GROUP1	Groups different RADIUS server hosts into distinct lists.
<b>Step 4</b>	<b>subscriber mac-filtering security-mode {mac   none   shared-secret}</b>  <b>Example:</b> Device(config-sg-radius)# subscriber mac-filtering security-mode mac	Specifies the RADIUS compatibility mode for MAC filtering. <ul style="list-style-type: none"> <li>The default value is <b>none</b>.</li> </ul>
<b>Step 5</b>	<b>mac-delimiter {colon   hyphen   none   single-hyphen}</b>  <b>Example:</b> Device(config-sg-radius)# mac-delimiter hyphen	Specifies the MAC delimiter for RADIUS compatibility mode. <ul style="list-style-type: none"> <li>The default value is <b>none</b>.</li> </ul>
<b>Step 6</b>	<b>exit</b>  <b>Example:</b> Device(config-sg-radius)# exit	Exits server group configuration mode and returns to global configuration mode.
<b>Step 7</b>	<b>username <i>mac-address</i> mac [aaa attribute list <i>aaa-attribute-list</i>]</b>  <b>Example:</b> Device(config)# username 00-22-WP-EC-23-3C mac aaa attribute list AAA_list1	Allows a MAC address to be used as the username for MAC filtering done locally.
<b>Step 8</b>	<b>exit</b>  <b>Example:</b> Device(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

## Enabling AES Key Wrap

Advanced Encryption Standard (AES) key wrap makes the shared secret between the controller and the RADIUS server more secure. AES key wrap requires a key-wrap compliant RADIUS authentication server.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host {hostname | ip-address} key-wrap encryption-key encryption-key message-auth-code-key encryption-key [format {ascii | hex}]**
4. **aaa group server radius group-name**
5. **server ip-address [auth-port port-number] [acct-port port-number]**
6. **key-wrap enable**
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>radius-server host {hostname   ip-address} key-wrap encryption-key encryption-key message-auth-code-key encryption-key [format {ascii   hex}]</b>  <b>Example:</b> Device(config)# radius-server host 10.10.1.2 key-wrap encryption-key testkey99 message-auth-code-key testkey123	Defines a RADIUS server host.
<b>Step 4</b>	<b>aaa group server radius group-name</b>  <b>Example:</b> Device(config)# aaa group server radius RAD_GROUP1	Groups different RADIUS server hosts into distinct lists.
<b>Step 5</b>	<b>server ip-address [auth-port port-number] [acct-port port-number]</b>  <b>Example:</b> Device(config-sg-radius)# server 10.10.1.2	Specifies the IP address of the RADIUS server in the server group.
<b>Step 6</b>	<b>key-wrap enable</b>  <b>Example:</b> Device(config-sg-radius)# key-wrap enable	Enables AES key wrap for this RADIUS server.

	Command or Action	Purpose
<b>Step 7</b>	<b>end</b>  <b>Example:</b> Device(config-sg-radius) # end	Exits server group configuration mode and returns to privileged EXEC mode.

## Configuration Examples for Local Authentication Using LDAP

### Example: Configuring Local Authentication Using LDAP

The following example shows a configuration for local authentication:

```
!
username USER_1 password 0 CISCO
username USER_1 aaa attribute list LOCAL_LIST
aaa new-model
aaa local authentication EAP_LIST authorization EAP_LIST
!
```

### Example: Configuring MAC Filtering Support

The following example shows a configuration for MAC filtering:

```
username 00-22-WP-EC-23-3C mac aaa attribute list AAA_list1
!
aaa group server radius RAD_GROUP1
subscriber mac-filtering security-mode mac
mac-delimiter hyphen
```

### Example: Configuring AES Key Wrap

The following example shows a configuration with key wrap enabled for a RADIUS server:

```
aaa group server radius RAD_GROUP1
server 10.10.1.2
key-wrap enable
!
radius-server host 10.10.1.2
!
```

## Additional References

#### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>

Related Topic	Document Title
Session Aware Networking commands	<a href="#">Cisco IOS Session Aware Networking Command Reference</a>
Address Resolution Protocol (ARP) commands	<a href="#">Cisco IOS IP Addressing Services Command Reference</a>
ARP configuration tasks	<i>IP Addressing - ARP Configuration Guide</i>
Authentication, authorization, and accounting (AAA) configuration tasks	<i>Authentication Authorization and Accounting Configuration Guide</i>
AAA commands	<i>Cisco IOS Security Command Reference</i>

### Standards and RFCs

Standard/RFC	Title
RFC 5176	<i>Dynamic Authorization Extensions to RADIUS</i>

### Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Local Authentication Using LDAP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 6: Feature Information for Local Authentication Using LDAP**

Feature Name	Releases	Feature Information
Local Authentication Using LDAP	Cisco IOS XE Release 3.2SE	<p>Introduces support for local authentication using Lightweight Directory Access Protocol (LDAP).</p> <p>The following commands were introduced or modified: <b>aaa local authentication</b>, <b>key-wrap enable</b>, <b>mac-delimiter</b>, <b>radius-server host</b>, <b>subscriber mac-filtering security-mode</b>, <b>username</b>.</p>