



## **Identity-Based Networking Services Configuration Guide, Cisco IOS Release 15E**

**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





## CONTENTS

---

### CHAPTER 1

#### **Identity-Based Networking Services Overview 1**

- Finding Feature Information 1
- Information About Identity-Based Networking Services 1
  - Understanding Identity-Based Networking Services 1
  - Features in Identity-Based Networking Services 2
  - Benefits of Identity-Based Networking Services 2
  - Web Authentication Support for Common Session ID 3
  - Web Authentication Support of IPv6 3
- Additional References 3
- Feature Information for Identity-Based Networking Services Overview 4

---

### CHAPTER 2

#### **Change of Authorization Support 5**

- Finding Feature Information 5
- Information About CoA Support 5
  - RADIUS Change-of-Authorization Support 5
  - Session Identification 6
  - CoA Activate Service Command 7
  - CoA Deactivate Service Command 7
  - CoA Bounce Host Port Command 8
  - CoA Disable Host Port Command 8
  - CoA Session Query Command 8
  - CoA Session Reauthenticate Command 9
  - CoA Session Terminate Command 9
- Additional References 10
- Feature Information for CoA Support 11

---

### CHAPTER 3

#### **Configuring Identity Control Policies 13**

- Finding Feature Information 13

Information About Identity Control Policies	13
Concurrent Authentication Methods	13
Configuration Display Mode	14
Control Policies for Identity-Based Networking Services	14
Control Policy Configuration Overview	15
Parameter Maps for Identity-Based Networking Services	16
Per User Inactivity Handling Across Methods	16
How to Configure Identity Control Policies	16
Enabling the Display Mode for Identity-Based Networking Services	16
Configuring a Control Class	17
Configuring a Control Policy	21
Applying a Control Policy to an Interface	26
Configuring Authentication Features on Ports	27
Configuring a Parameter Map for Web-Based Authentication	28
Configuration Examples for Identity Control Policies	32
Example: Configuring Control Policy for Concurrent Authentication Methods	32
Example: Configuring Control Policy for Sequential Authentication Methods	33
Example: Configuring Parameter Maps	34
Additional References	35
Feature Information for Identity Control Policies	36

---

**CHAPTER 4**

<b>Configuring Identity Service Templates</b>	<b>39</b>
Finding Feature Information	39
Prerequisites for Identity Service Templates	39
Information About Identity Service Templates	40
Service Templates for Identity-Based Networking Services	40
Downloadable Service Templates	40
Locally Configured Service Templates	40
How to Configure Identity Service Templates	41
Configuring a Local Service Template	41
Configuration Examples for Identity Service Templates	43
Example: Activating a Service Template and Replace All	43
Example: Activating a Service Template for Fallback Service	43
Example: Deactivating a Service Template	44
Additional References	45

Feature Information for Identity Service Templates 46

---

**CHAPTER 5****eEdge Integration with MACsec 47**

Finding Feature Information 47

Prerequisites for eEdge Integration with MACsec 47

Restrictions for eEdge Integration with MACsec 48

Information About eEdge Integration with MACsec 48

Overview of MACsec 48

MACsec Standard Encryption 48

EAP Implementation of MKA 49

Integrating eEdge with MACsec 49

How to Configure eEdge Integration with MACsec 50

Integrating eEdge with MACsec 50

Identifying Link Layer Security Failures 52

Configuration Examples for eEdge Integration with MACsec 53

Example: Integrating eEdge with MACsec 53

Example: Identifying Linksec Failures 53

Additional References for eEdge Integration with MACsec 54

Feature Information for eEdge Integration with MACsec 54

---

**CHAPTER 6****Critical Voice VLAN Support 57**

Finding Feature Information 57

Restrictions for Critical Voice VLAN Support 57

Information About Critical Voice VLAN Support 58

Critical Voice VLAN Support in Multidomain Authentication Mode 58

Critical Voice VLAN Support in Multiauthentication Mode 58

Critical Voice VLAN Support in a Service Template 58

How to Configure Critical Voice VLAN Support 59

Configuring a Voice VLAN in a Service Template 59

Activating Critical Voice VLAN 61

Configuration Examples for Critical Voice VLAN Support 64

Example: Configuring a Voice VLAN in a Service Template 64

Example: Activating a Critical Voice VLAN on a Service Template 64

Additional References for Critical Voice VLAN Support 64

Feature Information for Critical Voice VLAN Support 65





## CHAPTER

# 1

# Identity-Based Networking Services Overview

---

Identity-Based Networking Services 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 Identity-Based Networking Services is and its features and benefits.

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

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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.

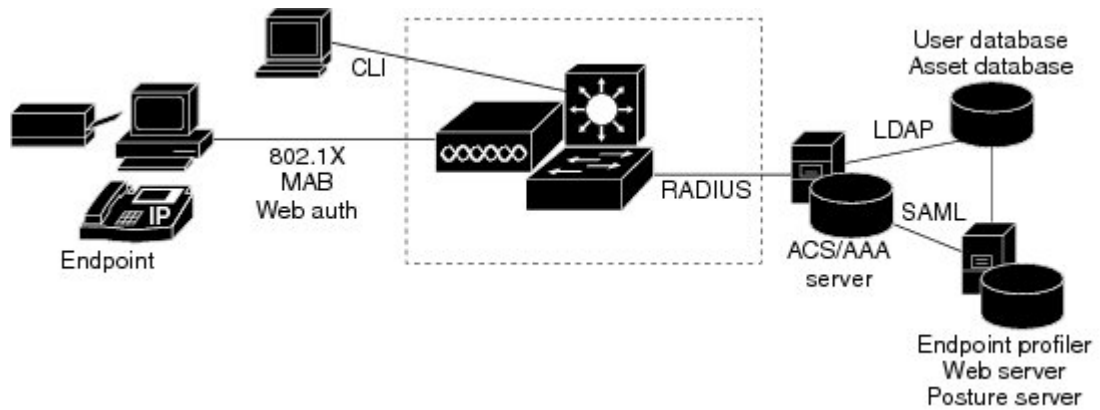
## Information About Identity-Based Networking Services

### Understanding Identity-Based Networking Services

Identity-Based Networking Services 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 Identity-Based Networking Services in a physically distributed enterprise with a campus, branch offices, and remote workers.

**Figure 1: Sample Deployment**



## Features in Identity-Based Networking Services

Identity-Based Networking Services 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 Identity-Based Networking Services

Identity-based solutions are essential for delivering access control for disparate groups such as employees, contractors, and partners while maintaining low operating expenses. Identity-Based Networking Services 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.

Identity-Based Networking Services 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

Identity-Based Networking Services 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

Identity-Based Networking Services introduces IPv6 support for web authentication. IPv6 is supported for web authentication only when Identity-Based Networking Services 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 Identity-Based Networking Services 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>
Identity-Based Networking Services commands	<a href="#">Cisco IOS Identity-Based Networking Services 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-Based Networking Services 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 Identity-Based Networking Services 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.



## CHAPTER 2

# Change of Authorization Support

---

Identity-Based Networking Services 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 Identity-Based Networking Services.

- [Finding Feature Information, page 5](#)
- [Information About CoA Support, page 5](#)
- [Additional References , page 10](#)
- [Feature Information for CoA Support, page 11](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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 Identity-Based Networking Services. All CoA commands must include the session identifier between the device and the CoA client.

**Table 2: RADIUS CoA Commands Supported by Identity-Based Networking Services**

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 6](#)” 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 6](#)” 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 6”](#) 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 6”](#) 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 6”](#) 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, reenable 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>
Identity-Based Networking Services commands	<a href="#">Cisco IOS Identity-Based Networking Services 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 3: 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>





## Configuring Identity Control Policies

Identity control policies define the actions that Identity-Based Networking Services 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 Identity-Based Networking Services.

- [Finding Feature Information](#), page 13
- [Information About Identity Control Policies](#), page 13
- [How to Configure Identity Control Policies](#), page 16
- [Configuration Examples for Identity Control Policies](#), page 32
- [Additional References](#) , page 35
- [Feature Information for Identity Control Policies](#), page 36

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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

Identity-Based Networking Services 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

Identity-Based Networking Services 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 Identity-Based Networking Services. Identity-Based Networking Services 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 Identity-Based Networking Services 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 Identity-Based Networking Services, on page 16](#)” section.
- Enter a Identity-Based Networking Services configuration command—After you enter the first explicit Identity-Based Networking Services 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.

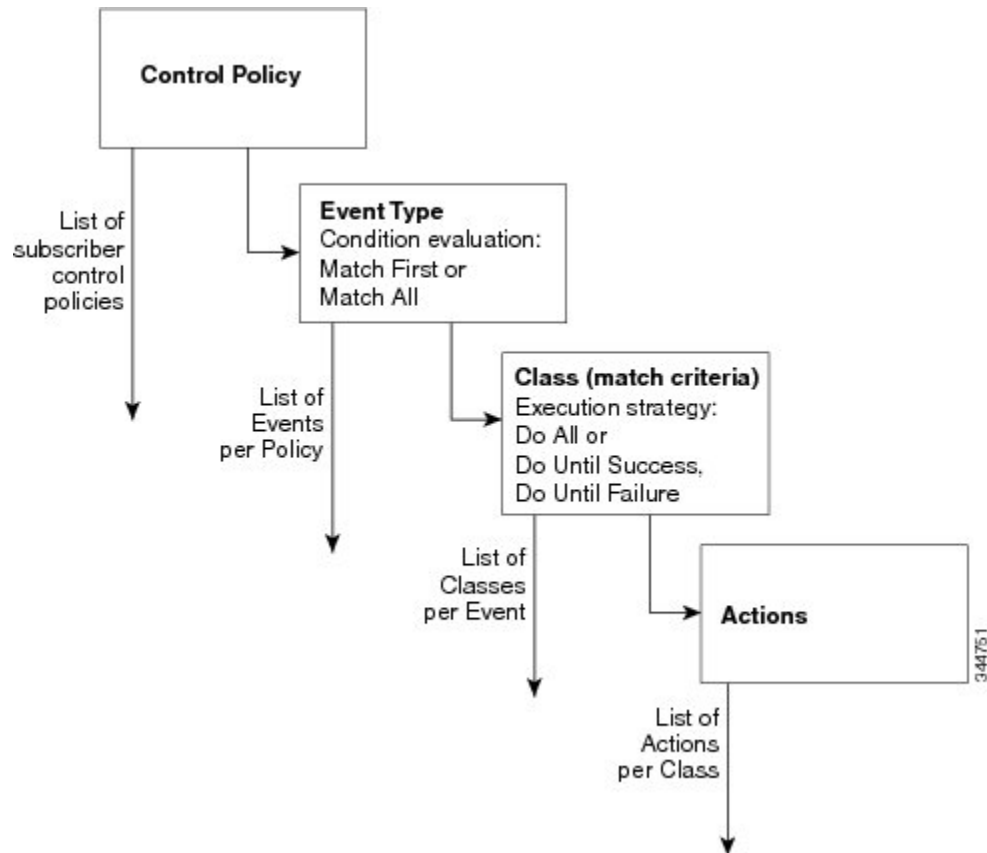
## Control Policies for Identity-Based Networking Services

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 Identity-Based Networking Services

A parameter map allows you to specify parameters that control the behavior of actions specified under a control policy. For Identity-Based Networking Services, 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 39](#)” module.

## How to Configure Identity Control Policies

### Enabling the Display Mode for Identity-Based Networking Services

Identity-Based Networking Services 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 Identity-Based Networking Services configuration before making the conversion permanent. After you enter an explicit Identity-Based Networking Services 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> <b>{legacy   new-style}</b>  <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 Identity-Based Networking Services command. After you enter the first explicit Identity-Based Networking Services 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
<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>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</b> <i>template-name</i></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} priority-value</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} priority-value</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 ip-address</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>	<p><b>{match   no-match} ipv6-address</b> <i>ipv6-address</i></p> <p><b>Example:</b>  Device(config-filter-control-classmap)# match  ipv6-address FE80::1</p>	(Optional) Creates a condition that evaluates true based on an event's source IPv6 address.
<b>Step 11</b>	<p><b>{match   no-match} mac-address</b> <i>mac-address</i></p> <p><b>Example:</b>  Device(config-filter-control-classmap)# match  mac-address aabb.cc00.6500</p>	(Optional) Creates a condition that evaluates true based on an event's MAC address.
<b>Step 12</b>	<p><b>{match   no-match} method</b> {dot1x   mab   webauth}</p> <p><b>Example:</b>  Device(config-filter-control-classmap)# match  method dot1x</p>	(Optional) Creates a condition that evaluates true based on an event's authentication method.
<b>Step 13</b>	<p><b>{match   no-match} port-type</b> {l2-port   l3-port   dot11-port}</p> <p><b>Example:</b>  Device(config-filter-control-classmap)# match  port-type l2-port</p>	(Optional) Creates a condition that evaluates true based on an event's interface type.
<b>Step 14</b>	<p><b>{match   no-match} result-type</b> [method {dot1x   mab   webauth}] <i>result-type</i></p> <p><b>Example:</b>  Device(config-filter-control-classmap)# match  result-type agent-not-found</p>	<p>(Optional) Creates a condition that evaluates true based on the specified authentication result.</p> <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>	<p><b>{match   no-match} service-template</b> <i>template-name</i></p> <p><b>Example:</b>  Device(config-filter-control-classmap)# match  service-template svc_1</p>	(Optional) Creates a condition that evaluates true based on an event's service template.
<b>Step 16</b>	<p><b>{match   no-match} tag</b> <i>tag-name</i></p> <p><b>Example:</b>  Device(config-filter-control-classmap)# match tag  tag_1</p>	(Optional) Creates a condition that evaluates true based on the tag associated with an event.
<b>Step 17</b>	<p><b>{match   no-match} timer</b> <i>timer-name</i></p> <p><b>Example:</b>  Device(config-filter-control-classmap)# match  timer restart</p>	(Optional) Creates a condition that evaluates true based on an event's timer.

	Command or Action	Purpose
<b>Step 18</b>	<p><code>{match   no-match} username <i>username</i></code></p> <p><b>Example:</b>  Device (config-filter-control-classmap)# match  username josmiths</p>	(Optional) Creates a condition that evaluates true based on an event's username.
<b>Step 19</b>	<p><code>end</code></p> <p><b>Example:</b>  Device (config-filter-control-classmap)# end</p>	(Optional) Exits control class-map filter configuration mode and returns to privileged EXEC mode.
<b>Step 20</b>	<p><code>show class-map type control subscriber {all   name <i>control-class-name</i>}</code></p> <p><b>Example:</b>  Device# show class-map type control subscriber  all</p>	(Optional) Displays information about Identity-Based Networking Services 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>	<p><b>policy-map type control subscriber</b> <i>control-policy-name</i></p> <p><b>Example:</b> Device(config)# policy-map type control POLICY_1</p>	Defines a control policy for subscriber sessions.
<b>Step 4</b>	<p><b>event</b> <i>event-name</i> [<b>match-all</b>   <b>match-first</b>]</p> <p><b>Example:</b> Device(config-event-control-policymap)# event session-started</p>	<p>Specifies the type of event that triggers actions in a control policy if conditions are met.</p> <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.</li> </ul>
<b>Step 5</b>	<p><i>priority-number</i> <b>class</b> {<i>control-class-name</i>   <b>always</b>} [<b>do-all</b>   <b>do-until-failure</b>   <b>do-until-success</b>]</p> <p><b>Example:</b> Device(config-class-control-policymap)# 10 class always</p>	<p>Associates a control class with one or more actions in a control policy.</p> <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>	<p><i>action-number</i> <b>activate</b> {<b>policy type control subscriber</b> <i>control-policy-name</i> [<b>child</b> [<b>no-propagation</b>   <b>concurrent</b>]   <b>service-template</b> <i>template-name</i> [<b>aaa-list</b> <i>list-name</i>] [<b>precedence</b> <i>number</i>] [<b>replace-all</b>]}]</p> <p><b>Example:</b> Device(config-action-control-policymap)# 10 activate service-template FALLBACK</p>	(Optional) Activates a control policy or service template on a subscriber session.
<b>Step 7</b>	<p><i>action-number</i> <b>authenticate using</b> {<b>dot1x</b>   <b>mab</b>   <b>webauth</b>} [<b>aaa</b> {<b>authc-list</b> <i>authc-list-name</i>   <b>authz-list</b> <i>authz-list-name</i>}] [<b>merge</b>] [<b>parameter-map</b> <i>map-name</i>] [<b>priority</b> <i>priority-number</i>] [<b>replace</b>   <b>replace-all</b>] [<b>retries</b> <i>number</i> {<b>retry-time</b> <i>seconds</i>}]</p> <p><b>Example:</b> Device(config-action-control-policymap)# 10 authenticate using dot1x priority 10</p>	(Optional) Initiates the authentication of a subscriber session using the specified method.
<b>Step 8</b>	<p><i>action-number</i> <b>authentication-restart</b> <i>seconds</i></p> <p><b>Example:</b> Device(config-action-control-policymap)# 20 authentication-restart 60</p>	(Optional) Sets a timer to restart the authentication process after an authentication or authorization failure.

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

	Command or Action	Purpose
<b>Step 18</b>	<p><i>action-number</i> <b>resume reauthentication</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# 20 resume reauthentication</p>	(Optional) Resumes the reauthentication process after an authentication failure.
<b>Step 19</b>	<p><i>action-number</i> <b>set-timer timer-name seconds</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# 20 set-timer RESTART 60</p>	(Optional) Starts a named policy timer.
<b>Step 20</b>	<p><i>action-number</i> <b>terminate {dot1x   mab   webauth}</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# 20 terminate webauth</p>	(Optional) Terminates an authentication method on a subscriber session.
<b>Step 21</b>	<p><i>action-number</i> <b>unauthorize</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# 20 unauthorize</p>	(Optional) Removes all authorization data from a subscriber session.
<b>Step 22</b>	<p><b>end</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# end</p>	(Optional) Exits control policy-map action configuration mode and returns to privileged EXEC mode.
<b>Step 23</b>	<p><b>show policy-map type control subscriber {all   name control-policy-name}</b></p> <p><b>Example:</b> Device# show policy-map type control subscriber name POLICY_1</p>	(Optional) Displays information about identity 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 32”](#) 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.  • 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 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.  • To display a list of all configured control policies, use the question mark (?) online help function.
<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> }	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> Device(config-if)# access-session host-mode single-host	<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> Device(config-if)# access-session closed	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> Device(config-if)# access-session control-direction in	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> Device(config-if)# end	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> Device# show access-session interface gigabitEthernet 1/0/2 details	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
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>parameter-map type webauth</b> { <i>parameter-map-name</i>   <b>global</b> }	Creates a parameter map and enters parameter-map webauth configuration mode.  • 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.
Step 4	<b>banner</b> { <b>file</b> <i>location:filename</i>   <b>text</b> <i>banner-text</i> }	(Optional) Displays a banner on the web-authentication login web page.
	<b>Example:</b> Device(config-params-parameter-map)# banner file flash:webauth_banner.html	

	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 21](#)” 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>
Identity-Based Networking Services commands	<a href="#">Cisco IOS Identity-Based Networking Services 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 4: 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 Identity-Based Networking Services.

- [Finding Feature Information, page 39](#)
- [Prerequisites for Identity Service Templates, page 39](#)
- [Information About Identity Service Templates, page 40](#)
- [How to Configure Identity Service Templates, page 41](#)
- [Configuration Examples for Identity Service Templates, page 43](#)
- [Additional References, page 45](#)
- [Feature Information for Identity Service Templates, page 46](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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 Identity-Based Networking Services

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.

Identity-Based Networking Services 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

Identity-Based Networking Services 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 command line interface 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
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>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.
Step 4	<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 21.”](#)

## 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>
Identity-Based Networking Services commands	<a href="#">Cisco IOS Identity-Based Networking Services 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 5: 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).



## eEdge Integration with MACsec

The Media Access Control Security (MACsec) standard is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. The eEdge Integration with MACsec feature allows you to integrate the MACsec standard with enterprise edge (eEdge) devices to enhance Session Aware Networking capabilities. Session Aware Networking provides a policy and identity-based framework for edge devices to deliver flexible and scalable services to subscribers.

- [Finding Feature Information, page 47](#)
- [Prerequisites for eEdge Integration with MACsec, page 47](#)
- [Restrictions for eEdge Integration with MACsec, page 48](#)
- [Information About eEdge Integration with MACsec, page 48](#)
- [How to Configure eEdge Integration with MACsec, page 50](#)
- [Configuration Examples for eEdge Integration with MACsec, page 53](#)
- [Additional References for eEdge Integration with MACsec, page 54](#)
- [Feature Information for eEdge Integration with MACsec, page 54](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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 eEdge Integration with MACsec

- Layer 2 encryption protocols like the IEEE 802.1AE Media Access Control Security (MACsec) standard must register with the eEdge session manager to receive disconnect notifications and perform cleanup.

- You must provision one virtual interface per secure association.

## Restrictions for eEdge Integration with MACsec

- The Media Access Control Security (MACsec) standard is supported only in single-host and multihost modes. If a link layer security policy is configured as must-secure and the host mode is not configured as a single host or a multihost, the connection is closed.
- The MACsec standard is not supported in multi-authentication mode.
- The MACsec standard supports the 802.1AE encryption with MACsec Key Agreement (MKA) only on downlink ports for encryption between a MACsec-capable device and host devices.

## Information About eEdge Integration with MACsec

### Overview of MACsec

Media Access Control Security (MACsec) is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Implementing the MACsec encryption standard enables support for the 802.1AE encryption with MACsec Key Agreement (MKA) on downlink ports for encryption between a MACsec-capable device and host devices. The MACsec-capable device also supports MACsec link layer device-to-device security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. Link layer security includes both packet authentication between devices and MACsec encryption between devices (encryption is optional).

### MACsec Standard Encryption

The Media Access Control Security (MACsec) standard provides data link layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) protocol provides the required session keys and manages the encryption keys. MKA and MACsec are implemented after a successful authentication by using the 802.1X Extensible Authentication Protocol (EAP) framework. Only host-facing links (links between network access devices and endpoint devices such as a PC or an IP phone) can be secured using MACsec.

A device that uses MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the client. MACsec frames are encrypted and protected with an integrity check value (ICV). When the device receives frames from the client, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The device compares the calculated value of the ICV to the ICV within the frame. If they are not identical, the frame is dropped. The device also encrypts and adds an ICV to any frame that is sent over a secured port (the access point used to provide the secure MAC service to a client) using the current session key.

The MKA protocol manages the encryption keys used by the underlying MACsec protocol. The basic requirements of MKA are defined in 802.1X-2010. The MKA protocol extends 802.1X to allow peer discovery with confirmation of mutual authentication and sharing of MACsec secret keys to protect data exchanged by peers.

## EAP Implementation of MKA

The Extensible Authentication Protocol (EAP) framework implements MKA as a newly defined EAP-over-LAN (EAPOL) packet. EAP authentication produces a master session key (MSK) that is shared by both partners in the data exchange. Entering the EAP session ID generates a secure connectivity association key name (CKN). Because the device is the authenticator, it is also the key server, generating a random 128-bit secure association key (SAK), which it sends to the client partner. The client is never a key server and can only interact with a single MKA entity, the key server. After key derivation and generation, the device sends periodic transports to the partner at a default interval of 2 seconds.

The packet body in an EAPOL Protocol Data Unit (PDU) is referred to as a MACsec Key Agreement PDU (MKPDU). MKA sessions and participants are deleted when the MKA lifetime (6 seconds) passes and no MKPDU is received from a participant. For example, if a client disconnects, the participant on the device continues to operate MKA until 6 seconds have elapsed after the last MKPDU is received from the client.

## Integrating eEdge with MACsec

In enterprise edge (eEdge) devices the encryption protocol is implemented as a session manager client and an Enterprise Policy Manager (EPM) plugin.

When you implement EPM plugin and the session manager client, the data link layer security is implemented as an EPM feature, which returns an asynchronous result to EPM when authentication is successful.

When the data link layer security user profile is applied and sessions are configured as either must-secure or should-secure using the **linksec policy {must-secure | should-secure}** command, the MACsec Key Agreement (MKA) processing starts.

The Media Access Control Security (MACsec) encryption standard is a data link layer security protocol. On eEdge devices, you must explicitly configure the protocol within a service template and an associated policy action.

The eEdge Integration with MACsec feature enables integrating the MACsec standard on a device using a service template.

# How to Configure eEdge Integration with MACsec

## Integrating eEdge with MACsec

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service-template** *template-name*
4. **linksec policy** {**must-not-secure** | **must-secure** | **should-secure**}
5. **exit**
6. **policy-map type control subscriber** *control-policy-name*
7. **event authentication-success** [**match-all** | **match-any**]
8. **priority-number class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**]
9. **action-number activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** [**replace-all**]]}
10. **end**

### 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>service-template</b> <i>template-name</i>  <b>Example:</b> Device(config)# service-template dot1x-macsec-policy	Defines a template that contains a set of service policy attributes to apply to subscriber sessions and enters service template configuration mode.
<b>Step 4</b>	<b>linksec policy</b> { <b>must-not-secure</b>   <b>must-secure</b>   <b>should-secure</b> }	Sets the link security policy as must-secure.  • Must-secure policy authorizes the eEdge device port only if a secure MACsec session is established.
	<b>Example:</b> Device(config-service-template)# linksec policy must-secure	

	Command or Action	Purpose
Step 5	<b>exit</b>  <b>Example:</b> Device(config-service-template)# exit	Exits service template configuration mode and returns to global configuration mode.
Step 6	<b>policy-map type control subscriber <i>control-policy-name</i></b>  <b>Example:</b> Device(config)# policy-map type control subscriber cisco-subscriber	Defines a control policy for subscriber sessions and enters control policy-map event configuration mode.
Step 7	<b>event authentication-success [match-all   match-any]</b>  <b>Example:</b> Device(config-event-control-policymap)# event authentication-success match-all	Specifies the type of event that triggers actions in a control policy if all authentication events are a match and enters control policy-map class configuration mode.
Step 8	<b><i>priority-number</i> 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 do-until-failure	Specifies that the control class should execute the actions in a control policy, in the specified order, until one of the actions fails, and enters control policy-map action configuration mode.
Step 9	<b><i>action-number</i> activate {policy type control subscriber <i>control-policy-name</i>   service-template <i>template-name</i> [aaa-list <i>list-name</i>] [precedence [replace-all]]}</b>  <b>Example:</b> Device(config-action-control-policymap)# 10 activate service-template dot1x-macsec-policy	Activates a control policy on a subscriber session.
Step 10	<b>end</b>  <b>Example:</b> Device(config-action-control-policymap)# end	Exits control policy-map action configuration mode and enters privileged EXEC mode.

# Identifying Link Layer Security Failures

## SUMMARY STEPS

1. **configure terminal**
2. **class-map type control subscriber** {*match-all* | *match-any* | *match-none*} *control-class-name*
3. **match authorization-failure** {*domain-change-failed* | *linksec-failed*}
4. **exit**
5. **policy-map type control subscriber** *control-policy-name*
6. **event authentication-failure** [*match-all* | *match-any*]
7. *priority-number* **class** {*control-class-name* | *always*} [*do-all* | *do-until-failure* | *do-until-success*]
8. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>class-map type control subscriber</b> { <i>match-all</i>   <i>match-any</i>   <i>match-none</i> } <i>control-class-name</i>  <b>Example:</b> Device(config)# <code>class-map type control subscriber match-all linksec-failed</code>	Creates a control class, which defines the conditions under which the actions of a control policy are executed and enters control class-map filter configuration mode.
<b>Step 3</b>	<b>match authorization-failure</b> { <i>domain-change-failed</i>   <i>linksec-failed</i> }  <b>Example:</b> Device(config-filter-control-classmap)# <code>match authorization-failure linksec-failed</code>	Configures a match condition in a control class based on the type of authorization failure received from an authorization failed event of a link layer security failure.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> Device(config-class-control-policymap)# <code>exit</code>	Exits control class-map filter configuration mode and enters global configuration mode.
<b>Step 5</b>	<b>policy-map type control subscriber</b> <i>control-policy-name</i>  <b>Example:</b> Device(config)# <code>policy-map type control subscriber cisco-subscriber</code>	Defines a control policy for subscriber sessions and enters control policy-map event configuration mode.

	Command or Action	Purpose
Step 6	<b>event authentication-failure [match-all   match-any]</b>  <b>Example:</b> Device(config-event-control-policymap)# event authentication-failure match-all	Specifies the type of event that triggers actions in a control policy if session authentication fails and enters control policy-map class configuration mode.
Step 7	<b>priority-number class {control-class-name   always} [do-all   do-until-failure   do-until-success]</b>  <b>Example:</b> Device(config-class-control-policymap)# 10 class linksec-failed do-until-failure	Specifies that the control class must execute the actions in a control policy, in the specified order, until one of the actions fails and enters control policy-map action configuration mode.
Step 8	<b>end</b>  <b>Example:</b> Device(config-action-control-policymap)# end	Exits control policy-map action configuration mode and enters privileged EXEC mode.

## Configuration Examples for eEdge Integration with MACsec

### Example: Integrating eEdge with MACsec

```

Device> enable
Device# configure terminal
Device(config)# service-template dot1x-macsec-policy
Device(config-service-template)# linksec policy must-secure
Device(config-service-template)# exit
Device(config)# policy-map type control subscriber cisco-subscriber
Device(config-event-control-policymap)# event authentication-success match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 activate service-template dot1x-macsec-policy
Device(config-action-control-policymap)# end

```

### Example: Identifying Linksec Failures

```

Device# configure terminal
Device(config)# class-map type control subscriber match-all linksec-failure
Device(config-filter-control-classmap)# match authorization-failure linksec-failed
Device(config-class-control-classmap)# exit
Device(config)# policy-map type control subscriber cisco-subscriber
Device(config-event-control-policymap)# event authentication-failure match-all
Device(config-class-control-policymap)# 10 class linksec-failed do-until-failure
Device(config-action-control-policymap)# end

```

## Additional References for eEdge Integration with MACsec

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Identity-Based Networking Services Command Reference	<a href="#">Cisco IOS Identity-Based Networking Services Command Reference</a>

### Standards and RFCs

Standard/RFC	Title
IEEE 802.1AE Standard	802.1AE - Media Access Control (MAC) Security

### Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature Information for eEdge Integration with MACsec

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 eEdge Integration with MACsec**

Feature Name	Releases	Feature Information
eEdge Integration with MACsec	Cisco IOS Release 15.2(1)E	<p>The eEdge Integration with MACsec feature allows you to integrate the MACsec standard with enterprise edge (eEdge) devices to enhance Session Aware Networking capabilities.</p> <p>The following commands were introduced or modified: <b>linksec policy</b>, <b>match authorization-failure</b>.</p>





## Critical Voice VLAN Support

The Critical Voice VLAN Support feature directs phone traffic to the configured voice VLAN of a port if the authentication server becomes unreachable.

With normal network connectivity, when an IP phone successfully authenticates on a port, the authentication server directs the phone traffic to the voice domain of the port. If the authentication server becomes unreachable, IP phones cannot authenticate the phone traffic. In multidomain authentication (MDA) mode or multiauthentication mode, you can configure the Critical Voice VLAN Support feature to direct phone traffic to the configured voice VLAN of the port. The phone is authorized as an unknown domain. Both data and voice are enabled for the phone.

- [Finding Feature Information, page 57](#)
- [Restrictions for Critical Voice VLAN Support, page 57](#)
- [Information About Critical Voice VLAN Support, page 58](#)
- [How to Configure Critical Voice VLAN Support, page 59](#)
- [Configuration Examples for Critical Voice VLAN Support, page 64](#)
- [Additional References for Critical Voice VLAN Support, page 64](#)
- [Feature Information for Critical Voice VLAN Support, page 65](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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.

### Restrictions for Critical Voice VLAN Support

- Different VLANs must be configured for voice and data.

- The voice VLAN must be configured on a device.
- The Critical Voice VLAN Support feature does not support standard Access Control Lists (ACLs) on the switch port.

## Information About Critical Voice VLAN Support

### Critical Voice VLAN Support in Multidomain Authentication Mode

If a critical voice VLAN is deployed using an interface in multidomain authentication (MDA) mode, the host mode is changed to multihost and the first phone device is installed as a static forwarding entries. Any additional phone devices are installed as dynamic forwarding entry in the Host Access Table (HAT).

For further information about host modes, see the *802.1X Authentication Services Configuration Guide*.



#### Note

If a critical port is already authorized and reauthentication occurs, the switch puts the port in the critical-authentication state in the current VLAN, which might be the one previously assigned by the RADIUS server.



#### Note

Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on a 802.1X port, the features interact as follows: if all RADIUS servers are not available and if a client is connected to a critical port and was previously assigned to a guest VLAN, the switch keeps the port in the guest VLAN.

### Critical Voice VLAN Support in Multiauthentication Mode

If the critical authentication feature is deployed in multiauthentication mode, only one phone device will be allowed and a second phone trying to authorize will trigger a violation.

The **show authentication sessions** command displays the critical voice client data. A critically authorized voice client in multiauthentication host mode will be in the “authz success” and “authz fail” state.



#### Note

If critical voice is required, then critical data should be configured too. Otherwise, the critical voice client will be displayed in the “authz fail” state while the voice VLAN will be open.

### Critical Voice VLAN Support in a Service Template

On enterprise Edge (eEdge) devices, the critical access of phones is configured by activating a critical service template when the authentication server becomes unreachable. The voice feature plug-in registers with the Enterprise Policy Manager (EPM) by using an authentication, authorization, and accounting (AAA) voice attribute, and it allows unconditional access to the voice VLAN while the AAA services are unavailable.

To enable critical voice VLAN support, the critical authentication of phones must be configured using a combination of control policy rules and a service template.

When the authentication server is unavailable and the host is unauthorized, the AAA attribute `device-traffic-type` is not populated. The phone is authorized as an unknown domain, and both the data and voice VLAN are enabled for this device, allowing the device to handle voice traffic.

# How to Configure Critical Voice VLAN Support

## Configuring a Voice VLAN in a Service Template

Perform this task on a port to configure critical voice VLAN support using a service template.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service-template** *template-name*
4. **vlan** *vlan-id*
5. **exit**
6. **service-template** *template-name*
7. **voice vlan**
8. **exit**
9. **class-map type control subscriber** {**match-all** | **match-any** | **match-none**} *control-class-name*
10. **match result-type** [**method** {**dot1x** | **mab** | **webauth**}] *result-type*
11. **match authorization-status** {**authorized** | **unauthorized**}
12. **exit**
13. **class-map type control subscriber** {**match-all** | **match-any** | **match-none**} *control-class-name*
14. **match result-type** [**method** {**dot1x** | **mab** | **webauth**}] *result-type*
15. **match authorization-status** {**authorized** | **unauthorized**}
16. **end**

### 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>

	Command or Action	Purpose
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>service-template <i>template-name</i></b>  <b>Example:</b> Device(config)# service-template SERVICE-TEMPLATE	Defines a template that contains a set of service policy attributes to apply to subscriber sessions and enters service template configuration mode.
Step 4	<b>vlan <i>vlan-id</i></b>  <b>Example:</b> Device(config-service-template)# vlan 116	Assigns a VLAN to a subscriber session.
Step 5	<b>exit</b>  <b>Example:</b> Device(config-service-template)# exit	Exits service template configuration mode and returns to global configuration mode.
Step 6	<b>service-template <i>template-name</i></b>  <b>Example:</b> Device(config)# service-template CRITICAL-VOICE	Defines a template that contains a set of service policy attributes to apply to subscriber sessions and enters service template configuration mode.
Step 7	<b>voice vlan</b>  <b>Example:</b> Device(config-service-template)# voice vlan	Assigns a critical voice VLAN to a subscriber session.
Step 8	<b>exit</b>  <b>Example:</b> Device(config-service-template)# exit	Exits service template configuration mode and returns to global configuration mode.
Step 9	<b>class-map type control subscriber {match-all   match-any   match-none} <i>control-class-name</i></b>  <b>Example:</b> Device(config)# class-map type control subscriber match-all AAA-SVR-DOWN-UNAUTHD-HOST	Creates a control class, which defines the conditions under which the actions of a control policy are executed and enters control class-map filter configuration mode.
Step 10	<b>match result-type [method {dot1x   mab   webauth}] <i>result-type</i></b>  <b>Example:</b> Device(config-filter-control-classmap)# match result-type aaa-timeout	Creates a condition that returns true based on the specified authentication result.

	Command or Action	Purpose
<b>Step 11</b>	<b>match authorization-status {authorized   unauthorized}</b>  <b>Example:</b> Device(config-filter-control-classmap)# match authorization-status unauthorized	Creates a condition that returns true based on the authorization status of a session.
<b>Step 12</b>	<b>exit</b>  <b>Example:</b> Device(config-filter-control-classmap)# exit	Exits control class-map filter configuration mode and returns to global configuration mode.
<b>Step 13</b>	<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 AAA-SVR-DOWN-AUTHD-HOST	Creates a control class, which defines the conditions under which the actions of a control policy are executed and enters control class-map filter configuration mode.
<b>Step 14</b>	<b>match result-type [method {dot1x   mab   webauth}] result-type</b>  <b>Example:</b> Device(config-filter-control-classmap)# match result-type aaa-timeout	Creates a condition that returns true based on the specified authentication result.
<b>Step 15</b>	<b>match authorization-status {authorized   unauthorized}</b>  <b>Example:</b> Device(config-filter-control-classmap)# match authorization-status authorized	Creates a condition that returns true based on the authorization status of a session.
<b>Step 16</b>	<b>end</b>  <b>Example:</b> Device(config-filter-control-classmap)# end	Exits control class-map filter configuration mode and returns to privileged EXEC mode.

## Activating Critical Voice VLAN

Perform the following task to activate a critical voice VLAN that is configured on a service template.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control subscriber *control-policy-name***
4. **event authentication-failure [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* | service-template *template-name* [aaa-list *list-name*] [precedence [replace-all]]}**
7. ***action-number* activate {policy type control subscriber *control-policy-name* | service-template *template-name* [aaa-list *list-name*] [precedence [replace-all]]}**
8. ***action-number* authorize**
9. ***action-number* pause reauthentication**
10. **exit**
11. ***priority-number* class {*control-class-name* | always} [do-all | do-until-failure | do-until-success]**
12. ***action-number* pause reauthentication**
13. **end**

## 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>policy-map type control subscriber <i>control-policy-name</i></b>  <b>Example:</b> Device(config)# policy-map type control subscriber cisco-subscriber	Defines a control policy for subscriber sessions and enters control policy-map event configuration mode.
Step 4	<b>event authentication-failure [match-all   match-first]</b>  <b>Example:</b> Device(config-event-control-policymap)# event authentication-failure match-first	Specifies the type of event that triggers actions in a control policy if all authentication events are a match and enters control policy-map class configuration mode.
Step 5	<b><i>priority-number</i> class {<i>control-class-name</i>   always} [do-all   do-until-failure   do-until-success]</b>	Specifies that the control class should execute the actions in a control policy, in the specified order, until one of the actions fails, and enters control policy-map action configuration mode.

	Command or Action	Purpose
	<p><b>Example:</b> Device(config-class-control-policymap)# 10 class AAA-SVR-DOWN-UNAUTHD-HOST do-until-failure</p>	
<b>Step 6</b>	<p><i>action-number</i> <b>activate</b> {<b>policy type control subscriber</b> <i>control-policy-name</i>   <b>service-template</b> <i>template-name</i> [<i>aaa-list list-name</i>] [<b>precedence</b> [<b>replace-all</b>]]}</p> <p><b>Example:</b> Device(config-action-control-policymap)# 10 activate service-template foo-DATA</p>	Activates a control policy associated with the VLAN on a subscriber session.
<b>Step 7</b>	<p><i>action-number</i> <b>activate</b> {<b>policy type control subscriber</b> <i>control-policy-name</i>   <b>service-template</b> <i>template-name</i> [<i>aaa-list list-name</i>] [<b>precedence</b> [<b>replace-all</b>]]}</p> <p><b>Example:</b> Device(config-action-control-policymap)# 10 activate service-template CRITICAL-VOICE</p>	Activates a control policy associated with the voice VLAN on a subscriber session.
<b>Step 8</b>	<p><i>action-number</i> <b>authorize</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# 30 authorize</p>	Initiates the authorization of a subscriber session.
<b>Step 9</b>	<p><i>action-number</i> <b>pause reauthentication</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# 40 pause reauthentication</p>	Pauses the reauthentication process after an authentication failure.
<b>Step 10</b>	<p><b>exit</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# exit</p>	Exits control policy-map action configuration mode and enters control policy-map class configuration mode.
<b>Step 11</b>	<p><i>priority-number</i> <b>class</b> {<i>control-class-name</i>   <b>always</b>} [<b>do-all</b>   <b>do-until-failure</b>   <b>do-until-success</b>]</p> <p><b>Example:</b> Device(config-class-control-policymap)# 20 class AAA-SVR-DOWN-AUTHD-HOST</p>	Specifies that the control class should execute the actions in a control policy, in the specified order, until one of the actions fails, and enters control policy-map action configuration mode.
<b>Step 12</b>	<p><i>action-number</i> <b>pause reauthentication</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# 10 pause reauthentication</p>	Pauses the reauthentication process after an authentication failure.
<b>Step 13</b>	<p><b>end</b></p> <p><b>Example:</b> Device(config-action-control-policymap)# exit</p>	Exits control policy-map action configuration mode and enters privileged EXEC mode.

## Configuration Examples for Critical Voice VLAN Support

### Example: Configuring a Voice VLAN in a Service Template

```

Device> enable
Device# configure terminal
Device(config)# service-template SERVICE-TEMPLATE
Device(config-service-template)# vlan 116
Device(config-service-template)# exit
Device(config)# service-template CRITICAL-VOICE
Device(config-service-template)# voice vlan
Device(config-service-template)# exit
Device(config)# class-map type control subscriber match-all AAA-SVR-DOWN-UNAUTHD-HOST
Device(config-filter-control-classmap)# match result-type aaa-timeout
Device(config-filter-control-classmap)# match authorization-status unauthorized
Device(config-filter-control-classmap)# exit
Device(config)# class-map type control subscriber match-all AAA-SVR-DOWN-AUTHD-HOST
Device(config-filter-control-classmap)# match result-type aaa-timeout
Device(config-filter-control-classmap)# match authorization-status authorized
Device(config-filter-control-classmap)# end

```

### Example: Activating a Critical Voice VLAN on a Service Template

```

Device> enable
Device# configure terminal
Device(config)# policy-map type control subscriber cisco-subscriber
Device(config-event-control-policymap)# event authentication-failure match-first
Device(config-class-control-policymap)# 10 class AAA-SVR-DOWN-UNAUTHD-HOST do-until-failure
Device(config-action-control-policymap)# 10 activate service-template SERVICE-TEMPLATE
Device(config-action-control-policymap)# 10 activate service-template CRITICAL-VOICE
Device(config-action-control-policymap)# 30 authorize
Device(config-action-control-policymap)# 40 pause reauthentication
Device(config-action-control-policymap)# exit
Device(config-class-control-policymap)# 20 class AAA-SVR-DOWN-AUTHD-HOST
Device(config-action-control-policymap)# 10 pause reauthentication
Device(config-action-control-policymap)# end

```

## Additional References for Critical Voice VLAN Support

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Cisco Identity-Based Networking Services commands	<a href="#">Cisco IOS Identity-Based Networking Services Command Reference</a>

**Standards and RFCs**

Standard/RFC	Title
IEEE 802.1X	<i>Port based Network Access Control</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 Critical Voice VLAN 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 7: Feature Information for Critical Voice VLAN Support**

Feature Name	Releases	Feature Information
Critical Voice VLAN Support	15.2(1)E Cisco IOS XE Release 3.3SE	This feature enables critical voice VLAN support, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.  The following command was added or modified: <b>voice vlan</b>

