



# 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.

- [Information About Identity Control Policies, on page 1](#)
- [How to Configure Identity Control Policies, on page 5](#)
- [Configuration Examples for Identity Control Policies, on page 20](#)
- [Feature History for Identity Control Policies, on page 24](#)

## Information About Identity Control Policies

The following sections provide information about how to configure identity control policies.

### Identity-Based Networking Services Configuration

To convert all relevant authentication commands to their Class-Based Policy Language(CPL) control policy equivalents, use the **authentication convert-to new-style** command. This command permanently converts the legacy configuration on the switch to identity-based networking services.



**Note** This configuration is irreversible. It disables the conversion command – **authentication display [legacy | new-style]**.

Use the **authentication display config-mode** command in EXEC mode to display the current configuration mode; *legacy* if it is legacy mode and **new-style** if it is Identity-Based Networking Services configuration mode.

```
(Device)# authentication display config-mode
Current configuration mode is legacy
```

```
Device)# authentication display config-mode
Current configuration mode is new-style
```

## 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 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 5](#)” 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.

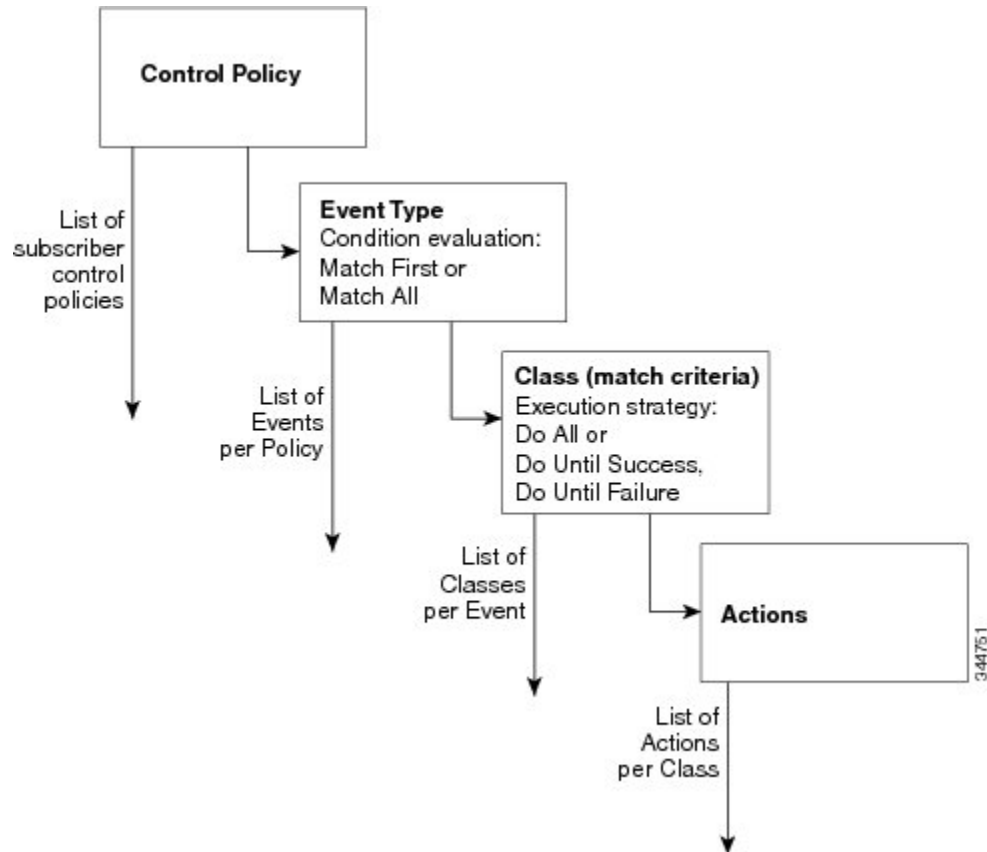
## Control Policies for Identity-Based Networking Services

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 1: 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.

## Single Control Policy for Identity-Based Networking Services

Prior 17.7.1, after the conversion of legacy configuration on the switch to identity-based networking services, the relevant authentication commands are converted to new-style and an identity control policy is generated for each interface. All interfaces have the same configuration as the identity control policy maps. The service templates for each interface are also identical.

Beginning from 17.7.1, to avoid interfaces having the same identity control policy configurations and individual identity control policy, you can configure a single control policy for all interfaces that have identical policy-maps and service-templates. You can also choose to replace all the policy-maps with the specified single control policy map. To use the single control policy map, ensure that the authentication methods on each interface is identical after the conversion.

You can also use the single policy approach if the switch is already in Identity-Based Networking Services configuration mode and you want to replace the existing interface policy-maps with a specific single policy-map.

Use the **authentication convert-to new-style single-policy interface** and **access-session single-policy** commands to apply the configuration of a specific single policy map to the relevant interfaces.

Use the **authentication display config-mode** command in EXEC mode to display the current configuration mode; *legacy* if it is legacy mode and *new-style* if it is Identity-Based Networking Services configuration mode.

# How to Configure Identity Control Policies

The following sections provide information about 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> <code>Device&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>authentication display {legacy   new-style}</b>  <b>Example:</b> <code>Device# authentication display new-style</code>	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>

	Command or Action	Purpose
		<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>For the stack devices and standalone devices to revert to legacy mode, save the new-style configuration in a flash, <b>write erase</b> the device and then perform a <b>reload</b>.</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).

### Procedure

	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</b> <b>{match-all   match-any   match-none}</b> <i>control-class-name</i> <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>	<b>{match   no-match} activated-service-template <i>template-name</i></b> <b>Example:</b> <pre>Device(config-filter-control-classmap) # match activated-service-template SVC_1</pre>	(Optional) Creates a condition that evaluates true based on the service template activated on a session.
<b>Step 5</b>	<b>{match   no-match} authorization-status {authorized   unauthorized}</b> <b>Example:</b> <pre>Device(config-filter-control-classmap) # match authorization-status authorized</pre>	(Optional) Creates a condition that evaluates true based on a session's authorization status.
<b>Step 6</b>	<b>{match   no-match} authorizing-method-priority {eq   gt   lt} <i>priority-value</i></b> <b>Example:</b> <pre>Device(config-filter-control-classmap) # match authorizing-method-priority eq 10</pre>	(Optional) Creates a condition that evaluates true based on the priority of the authorization method. <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>• <i>priority-value</i>—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>	<b>{match   no-match} client-type {data   switch   video   voice}</b> <b>Example:</b> <pre>Device(config-filter-control-classmap) # match client-type data</pre>	(Optional) Creates a condition that evaluates true based on an event's device type.
<b>Step 8</b>	<b>{match   no-match} current-method-priority {eq   gt   lt} <i>priority-value</i></b> <b>Example:</b> <pre>Device(config-filter-control-classmap) # match current-method-priority eq 10</pre>	(Optional) Creates a condition that evaluates true based on the priority of the current authentication method.
<b>Step 9</b>	<b>{match   no-match} ip-address <i>ip-address</i></b> <b>Example:</b> <pre>Device(config-filter-control-classmap) # match ip-address 10.10.10.1</pre>	(Optional) Creates a condition that evaluates true based on an event's source IPv4 address.

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



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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	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>	Enters global configuration mode.

	Command or Action	Purpose
	Device# configure terminal	
<b>Step 3</b>	<b>policy-map type control subscriber</b> <i>control-policy-name</i>  <b>Example:</b> <pre>Device(config)# policy-map type control POLICY_1</pre>	Defines a control policy for subscriber sessions.
<b>Step 4</b>	<b>event event-name [match-all   match-first]</b>  <b>Example:</b> <pre>Device(config-event-control-policymap)# event session-started</pre>	<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> <p>Specifies the type of event that triggers actions in a control policy if conditions are met.</p>
<b>Step 5</b>	<i>priority-number class {control-class-name  </i> <b>always}</b> [ <b>do-all   do-until-failure  </b> <b>do-until-success]</b>  <b>Example:</b> <pre>Device(config-class-control-policymap)# 10 class always</pre>	<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>	<i>action-number activate {policy type control</i> <b>subscriber control-policy-name [child</b> <b>[no-propagation   concurrent]  </b> <b>service-template template-name [aaa-list</b> <i>list-name] [precedence number] [replace-all]}</i>  <b>Example:</b> <pre>Device(config-action-control-policymap)# 10 activate service-template FALLBACK</pre>	(Optional) Activates a control policy or service template on a subscriber session.
<b>Step 7</b>	<i>action-number authenticate using {dot1x  </i> <b>mab   webauth} [aaa {authc-list</b> <i>authc-list-name   authz-list authz-list-name}]</i> <b>[merge] [parameter-map map-name]</b> <b>[priority priority-number] [replace  </b> <b>replace-all] [retries number {retry-time</b> <i>seconds}]</i>  <b>Example:</b> <pre>Device(config-action-control-policymap)# 10 authenticate using dot1x priority 10</pre>	(Optional) Initiates the authentication of a subscriber session using the specified method.

	Command or Action	Purpose
<b>Step 8</b>	<b><i>action-number authentication-restart seconds</i></b> <b>Example:</b> Device(config-action-control-policymap) # 20 authentication-restart 60	(Optional) Sets a timer to restart the authentication process after an authentication or authorization failure.
<b>Step 9</b>	<b><i>action-number authorize</i></b> <b>Example:</b> Device(config-action-control-policymap) # 10 authorize	(Optional) Initiates the authorization of a subscriber session.
<b>Step 10</b>	<b><i>action-number clear-authenticated-data-hosts-on-port</i></b> <b>Example:</b> Device(config-action-control-policymap) # 20 clear-authenticated-data-hosts-on-port	(Optional) Clears authenticated data hosts on a port after an authentication failure.
<b>Step 11</b>	<b><i>action-number clear-session</i></b> <b>Example:</b> Device(config-action-control-policymap) # 30 clear-session	(Optional) Clears an active subscriber session.
<b>Step 12</b>	<b><i>action-number deactivate {policy type control subscriber control-policy-name   service-template template-name}</i></b> <b>Example:</b> Device(config-action-control-policymap) # 20 deactivate service-template	(Optional) Deactivates a control policy or service template on a subscriber session.
<b>Step 13</b>	<b><i>action-number err-disable</i></b> <b>Example:</b> Device(config-action-control-policymap) # 10 err-disable	(Optional) Temporarily disables a port after a session violation event.
<b>Step 14</b>	<b><i>action-number pause reauthentication</i></b> <b>Example:</b> Device(config-action-control-policymap) # 20 pause reauthentication	(Optional) Pauses reauthentication after an authentication failure.
<b>Step 15</b>	<b><i>action-number protect</i></b> <b>Example:</b> Device(config-action-control-policymap) # 10 protect	(Optional) Silently drops violating packets after a session violation event.
<b>Step 16</b>	<b><i>action-number replace</i></b> <b>Example:</b>	(Optional) Clears the existing session and creates a new session after a violation event.

	Command or Action	Purpose
	Device(config-action-control-policy-map)# 10 replace	
<b>Step 17</b>	<b>action-number restrict</b>  <b>Example:</b> Device(config-action-control-policy-map)# 10 restrict	(Optional) Drops violating packets and generates a syslog entry after a session violation event.
<b>Step 18</b>	<b>action-number resume reauthentication</b>  <b>Example:</b> Device(config-action-control-policy-map)# 20 resume reauthentication	(Optional) Resumes the reauthentication process after an authentication failure.
<b>Step 19</b>	<b>action-number set-timer timer-name seconds</b>  <b>Example:</b> Device(config-action-control-policy-map)# 20 set-timer RESTART 60	(Optional) Starts a named policy timer.
<b>Step 20</b>	<b>action-number terminate {dot1x   mab   webauth}</b>  <b>Example:</b> Device(config-action-control-policy-map)# 20 terminate webauth	(Optional) Terminates an authentication method on a subscriber session.
<b>Step 21</b>	<b>action-number unauthorize</b>  <b>Example:</b> Device(config-action-control-policy-map)# 20 unauthorize	(Optional) Removes all authorization data from a subscriber session.
<b>Step 22</b>	<b>end</b>  <b>Example:</b> Device(config-action-control-policy-map)# end	(Optional) Exits control policy-map action configuration mode and returns to privileged EXEC mode.
<b>Step 23</b>	<b>show policy-map type control subscriber {all   name control-policy-name}</b>  <b>Example:</b> Device# show policy-map type control subscriber name POLICY_1	(Optional) Displays information about 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 20”](#) 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.

### Procedure

	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 <i>type number</i></b>  <b>Example:</b> Device(config)# interface GigabitEthernet 1/0/1	Specifies an interface and enters interface configuration mode.
<b>Step 4</b>	<b>service-policy type control subscriber <i>control-policy-name</i></b>  <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 {inactivity-timer <i>seconds</i> [probe]   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 GigabitEthernet 1/0/2
 subscriber aging inactivity-timer 60 probe
 service-policy type control subscriber POLICY_1
```

## Applying a Single Control Policy to an Interface in Legacy Mode

You can apply a single control policy to an interface during the conversion of switch configuration from legacy to Identity-Based Networking Services configuration mode.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>authentication convert-to new-style single-policy interface</b> <i>interface name</i>  <b>Example:</b> Device(config)# <i>style</i> single-policy interface GigabitEthernet 1/0/1	Specifies the interface to which the single control policy must be applied.
<b>Step 4</b>	<b>authentication convert-to new-style single-policy interface</b> <i>interface name forced</i>  <b>Example:</b> Device(config)# <i>style</i> single-policy interface GigabitEthernet 1/0/1 forced	(Optional) Permanently replaces all the policy-maps in different interfaces with a single policy-map corresponding to the interface that you have selected. This conversion is irreversible.

## Replacing Redundant Control Policies with a Single Control Policy

You can apply a single control policy to an interface if the switch is in the Identity-Based Networking Services configuration mode.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>access-session single-policy interface</b> <i>interface name</i>	Permanently replaces all the redundant policy-maps in different interfaces with a single

	Command or Action	Purpose
	<b>Example:</b> <pre>Device(config)#access session single-policy interface GigabitEthernet 1/0/2</pre>	policy-map that you have selected or policy-map corresponding to the interface that you have selected. The configuration of the redundant policy-map except the one chosen for the conversion will be removed from the current configuration. The system prompts you to choose if you want to proceed or cancel the conversion. This conversion is irreversible.
<b>Step 4</b>	<b>access-session single-policy interface <i>interface name</i> forced</b>  <b>Example:</b> <pre>Device(config)#access-session single-policy interface GigabitEthernet 1/0/2 forced</pre>	(Optional)  Permanently replaces all the policy-maps in different interfaces with a single policy-map that you have selected or policy-map corresponding to the interface that you have selected. The configuration of the redundant policy-map except the one chosen for the conversion will be removed from the current configuration. This conversion is irreversible.
<b>Step 5</b>	<b>access-session single-policy policy-name <i>policy name</i></b>  <b>Example:</b> <pre>Device(config)#access-session single-policy policy-name POLICY_Gi1/0/1</pre>	Permanently replaces all the policy-maps in different interfaces with a single policy-map that you have selected or policy-map corresponding to the interface that you have selected. The configuration of the redundant policy-map except the one chosen for the conversion will be removed from the current configuration. The system prompts you to choose if you want to proceed or cancel the conversion. This conversion is irreversible.
<b>Step 6</b>	<b>access-session single-policy interface <i>policy name</i> forced</b>  <b>Example:</b> <pre>Device(config)#access-session single-policy policy-name POLICY_Gi1/0/1 forced</pre>	(Optional)  Permanently replaces all the policy-maps in different interfaces with a single policy-map that you have selected or policy-map corresponding to the interface that you have selected. The configuration of the redundant policy-map except the one chosen for the conversion will be removed from the current configuration. This conversion is irreversible.

## 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.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i> <b>Example:</b> Device(config)# interface gigabitethernet 1/0/2	Enters interface configuration mode for the selected interface.
<b>Step 4</b>	<b>access-session port-control {auto   force-authorized   force-unauthorized}</b> <b>Example:</b> Device(config-if)# access-session port-control auto	Sets the authorization state of a port. <ul style="list-style-type: none"> <li>• The default value is <b>force-authorized</b>.</li> </ul>
<b>Step 5</b>	<b>access-session host-mode {multi-auth   multi-domain   multi-host   single-host}</b> <b>Example:</b> Device(config-if)# access-session host-mode single-host	Allows hosts to gain access to a controlled port. <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</b> <i>interface-type interface-number</i> [details] <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.

**Procedure**

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

	Command or Action	Purpose
<b>Step 5</b>	<b>consent</b> <b>Example:</b> <pre>Device(config-params-parameter-map)# type consent</pre>	(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>
<b>Step 6</b>	<b>consent email</b> <b>Example:</b> <pre>Device(config-params-parameter-map)# consent email</pre>	(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 7</b>	<b>custom-page {failure   login [expired]   success} device location:filename</b> <b>Example:</b> <pre>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</pre>	(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 8</b>	<b>max-http-conns number</b> <b>Example:</b> <pre>Device(config-params-parameter-map)# max-http-conns 5</pre>	(Optional) Limits the number of HTTP connections for each web authentication client.
<b>Step 9</b>	<b>ratelimit init-state-sessions rate-limit</b> <b>Example:</b> <pre>Device(config-params-parameter-map)# ratelimit init-state-sessions 500</pre>	(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 10</b>	<b>redirect {{for-login   on-failure   on-success} url   portal {ipv4 ipv4-address   ipv6 ipv6-address}}</b> <b>Example:</b> <pre>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</pre>	(Optional) Redirects users to a particular URL during web-based authentication.
<b>Step 11</b>	<b>timeout init-state sec seconds</b> <b>Example:</b>	(Optional) Sets the Init state timeout for web-based authentication sessions.

	Command or Action	Purpose
	Device(config-params-parameter-map) # timeout init-state sec 60	<ul style="list-style-type: none"> <li>The range of seconds is (60-3932100).</li> </ul>
<b>Step 12</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>
<b>Step 13</b>	<b>virtual-ip {ipv4 ipv4-address   ipv6 ipv6-address}</b>  <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 14</b>	<b>watch-list {add-item {ipv4 ipv4-address   ipv6 ipv6-address}   dynamic-expiry-timeout minutes   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 15</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 16</b>	<b>show ip admission status [banners   custom-pages   parameter-map [parameter-map]]</b>  <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 sec 60
 max-http-conns 5
 type consent
 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 9](#)” section.

# Configuration Examples for Identity Control Policies

The following sections provide configuration examples for identity control policies.

## 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

```

**Example: Configuring Parameter Maps**

```

    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 retriess 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
```

## Feature History for Identity Control Policies

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.5.1a	Identity Control Policies	Identity control policies define the actions taken in response to specified events and conditions.  Support for this feature was introduced only on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Fuji 16.8.1a	Identity Control Policies	Identity control policies define the actions taken in response to specified events and conditions.  Support for this feature was introduced on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.



Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.7.1	Single Control Policy	After conversion from legacy configuration mode to Identity Based Network Services mode, a single policy-map can be configured and applied to each relevant interface
Cisco IOS XE Cupertino 17.7.1	Identity Control Policies	Support for this feature was introduced on the C9500X-28C8D model of the Cisco Catalyst 9500 Series Switches.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.

