



Configuring Identity Service Templates

- [Configuring Identity Service Templates, on page 1](#)

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.

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 Cisco 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

Cisco Identity Based Networking Services (IBNS) 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.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | service-template <i>template-name</i> Example: Device(config)# service-template SVC_2 | Creates a service template and enters service template configuration mode. |
| Step 4 | absolute-timer <i>minutes</i> Example: Device (config-service-template) # absolute-timer 15 | (Optional) Enables an absolute timeout for subscriber sessions. |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 5 | access-group <i>access-list-name</i> Example: Device(config-service-template)# access-group ACL_2 | (Optional) Applies an access list to sessions using a service template. |
| Step 6 | description <i>description</i> Example: Device(config-service-template)# description label for SVC_2 | (Optional) Adds a description for a service template. |
| Step 7 | inactivity-timer <i>minutes</i> [probe] Example: Device(config-service-template)# inactivity-timer 15 | (Optional) Enables an inactivity timeout for subscriber sessions. |
| Step 8 | redirect url <i>url</i> Example: Device(config-service-template)# redirect url www.cisco.com | (Optional) Redirects clients to a particular URL. |
| Step 9 | sgt <i>range</i> Example: Device(config-service-template)# sgt 100 | (Optional) Associates a Security Group Tag (SGT) with a service template. |
| Step 10 | tag <i>tag-name</i> Example: Device(config-service-template)# tag TAG_2 | (Optional) Associates a user-defined tag with a service template. |
| Step 11 | vlan <i>vlan-id</i> Example: Device(config-service-template)# vlan 215 | (Optional) Applies a VLAN to sessions using a service template. |
| Step 12 | end Example: Device(config-service-template)# end | Exits service template configuration mode and returns to privileged EXEC mode. |
| Step 13 | show service-template [<i>template-name</i>] Example: 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](#).

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
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
```

Feature Information for Identity Service Templates

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.

Table 1: Feature Information for Identity Service Templates

| Release | Feature Name | Feature Information |
|--------------------------------|---------------------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Identity Service Template | Enables identity service templates to be configured locally and available at all times. |
| Cisco IOS XE Cupertino 17.7.1 | Identity Service Template | Support for this feature was introduced on the Cisco Catalyst 9600 Series Supervisor 2 Module (C9600X-SUP-2). |