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, on page 1
- Prerequisites for Identity Service Templates, on page 1
- Information About Identity Service Templates, on page 2
- How to Configure Identity Service Templates, on page 3
- Configuration Examples for Identity Service Templates, on page 5
- Additional References, on page 7
- Feature Information for Identity Service Templates, on page 8

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.

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. 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. `sgt range`
10. `tag tag-name`
11. `vlan vlan-id`
12. `sgt sgt-tag`
13. `end`
14. `show service-template [template-name]`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>service-template template-name</td>
<td>Creates a service template and enters service template configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# service-template SVC_2</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>absolute-timer minutes</td>
<td>(Optional) Enables an absolute timeout for subscriber sessions.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-service-template)# absolute-timer 15</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>5</td>
<td>access-group access-list-name</td>
<td>(Optional) Applies an access list to sessions using a service template.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# access-group ACL_2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>description description</td>
<td>(Optional) Adds a description for a service template.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# description label for SVC_2</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>inactivity-timer minutes [probe]</td>
<td>(Optional) Enables an inactivity timeout for subscriber sessions.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# inactivity-timer 15</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>redirect url url</td>
<td>(Optional) Redirects clients to a particular URL.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# redirect url <a href="http://www.cisco.com">www.cisco.com</a></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>sgt range</td>
<td>(Optional) Associates a Security Group Tag (SGT) with a service template.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# sgt 100</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>tag tag-name</td>
<td>(Optional) Associates a user-defined tag with a service template.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# tag TAG_2</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>vlan vlan-id</td>
<td>(Optional) Applies a VLAN to sessions using a service template.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# vlan 215</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>sgt sgt-tag</td>
<td>(Optional) Adds a Security Group Tag (SGT) using a service template.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# sgt</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>end</td>
<td>Exits service template configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-service-template)# end</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>show service-template [template-name]</td>
<td>Displays information about configured service templates.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show service-template SVC_2</td>
<td></td>
</tr>
</tbody>
</table>
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:

```plaintext
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.

```plaintext
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.

```plaintext
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.

```plaintext
service-template LOW_IMPACT_TEMPLATE
description Service template for Low impact mode
access-group LOW_IMPACT_ACL
```
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.

```plaintext
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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Identity-Based Networking Services commands</td>
<td>Cisco IOS Identity-Based Networking Services Command Reference</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP) commands</td>
<td>Cisco IOS IP Addressing Services Command Reference</td>
</tr>
<tr>
<td>ARP configuration tasks</td>
<td>IP Addressing - ARP Configuration Guide</td>
</tr>
<tr>
<td>Authentication, authorization, and accounting (AAA) configuration tasks</td>
<td>Authentication Authorization and Accounting Configuration Guide</td>
</tr>
</tbody>
</table>
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. An account on Cisco.com is not required.

Table 1: Feature Information for Identity Service Templates

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identity Service Template</td>
<td>Cisco IOS Release 15.2(1)E</td>
<td>Enables identity service templates to be configured locally and available at all times. In Cisco IOS Release 15.2(1)E, this feature is supported on the following platforms:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Catalyst 2960-X Series Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Catalyst 3560-C Series Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Catalyst 3750-X Series Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Catalyst 4500-X Series Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Catalyst 4900 Series Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced: absolute-timer, access-group (service template), description (service template), inactivity-timer, redirect url, service-template, show service-template, tag (service template), vlan (service template).</td>
</tr>
</tbody>
</table>