アイデンティティ サービス テンプレートの設定

アイデンティティ サービス テンプレートには、制御ポリシーにより 1 つ以上の加入者セッションに適用できる一連のポリシー属性や機能、RADIUS Change of Authorization（CoA）要求、またはユーザ プロファイルやサービス プロファイルが含まれます。 このモジュールでは、Identity-Based Networking Services のローカル サービス テンプレートの設定方法に関する情報を提供します。

- 機能情報の確認，1 ページ
- アイデンティティ サービス テンプレートの前提条件，2 ページ
- アイデンティティ サービス テンプレートに関する情報，2 ページ
- アイデンティティ サービス テンプレートの設定方法，3 ページ
- アイデンティティ サービス テンプレートの設定例，6 ページ
- その他の関連資料，8 ページ
- アイデンティティ サービス テンプレートの機能に関する情報，9 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

アイデンティティ サービス テンプレートの前提条件

ダウンロード可能なサービス テンプレートの場合、スイッチは、認証、許可、およびアカウンティング（AAA）サーバ、Cisco Secure Access Control Server（ACS）、Cisco Identity Services Engine（ISE）からサービステンプレートをダウンロードする際にデフォルト パスワード「cisco123」を使用します。 AAA、ACS および ISE サーバのサービス テンプレート設定には、パスワード「cisco123」が含まれている必要があります。

アイデンティティ サービス テンプレートに関する情報

Identity-Based Networking Services 用のサービス テンプレート

サービス テンプレートには、アクセス コントロール リスト（ACL）や VLAN 割り当てなど、一連のサービス関連の属性や機能が含まれています。これらの属性や機能は、セッション ライフサイクル イベントに対応して、1 つ以上の加入者セッションでアクティブ化することができます。テンプレートにより、ネットワーク セッション ポリシー（ポリシーが別個のグループに分類されているか、ロール ベースである）のプロビジョニングとメンテナンスが簡略化されます。

サービス テンプレートは、制御ポリシーの参照、RADIUS Change of Authorization（CoA）要求、またはユーザプロファイルあるいはサービスプロファイルによってセッションに適用されます。ユーザプロファイルは加入者ごとに定義され、サービスプロファイルは複数の加入者に適用できます。

Identity-Based Networking Services は、次の 2 種類のサービス テンプレートをサポートします。

- ダウンロード可能なサービス テンプレート：サービス テンプレートは外部 ACS または AAA サーバに一元的に設定され、オンデマンドでダウンロードされます。
- ローカルで設定されたサービス テンプレート：サービス テンプレートは、Cisco IOS Command-Line Interface（CLI）を使用して、デバイスでローカルに設定されます。

ダウンロード可能なサービス テンプレート

Identity-Based Networking Services は、外部 AAA サーバで定義されたサービス テンプレートをダウンロードできます。 このテンプレートは、AAA 属性の集合を定義します。 これらのテンプレートは、外部 AAA サーバまたは ACS から受信した RADIUS CoA メッセージに含まれるベンダー固有属性（VSA）によってセッションに適用されます。テンプレート名は、処理中にサービステンプレートのダウンロードをトリガーするユーザ プロファイルまたは制御ポリシーで参照されます。

ダウンロード可能なテンプレートはデバイスにキャッシュされ、後続のダウンロードの要求は、使用可能なキャッシュ テンプレートを参照します。ただし、テンプレートがキャッシュされるのは、そのテンプレートがアクティブに使用されている間のみです。 デバイスにキャッシュされた

ダウンロード済みのテンプレートは保護され、コマンドライン インターフェイスやその他のアプリケーションからは削除できません。 これにより、テンプレートが削除されるのは、そのテンプレートに対するアクティブな参照がない場合にのみになります。

ローカルで設定されたサービス テンプレート

サービステンプレートはCLIを使用してローカルで設定できます。 これらのサービステンプレートは、制御ポリシーの参照により、加入者セッションに適用できます。

アクティブなローカル テンプレートが更新されると、そのローカル テンプレートに対する変更は、そのテンプレートがアクティブになっているすべてのセッションに対して反映されます。 テンプレートが削除されると、セッションに対して適用されているそのテンプレートのすべてのコンテンツが削除されます。

アイデンティティ サービス テンプレートの設定方法

ローカル サービス テンプレートの設定

サービス テンプレートは、加入者セッションに適用できるローカル ポリシーを定義します。 該当のローカル ポリシーを適用する必要があるセッションで、このサービス テンプレートをアクティブ化します。

手順の概要

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*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service-template** *template-name* 例： `Device(config)# service-template SVC_2`	サービス テンプレートを作成し、サービス テンプレート コンフィギュレーション モードを開始します。
ステップ 4	**absolute-timer** *minutes* 例： `Device(config-service-template)# absolute-timer 15`	（任意）加入者セッションに対する絶対タイムアウトをイネーブルにします。
ステップ 5	**access-group** *access-list-name* 例： `Device(config-service-template)# access-group ACL_2`	（任意）サービス テンプレートを使用して、セッションにアクセス リストを適用します。
ステップ 6	**description** *description* 例： `Device(config-service-template)# description label for SVC_2`	（任意）サービス テンプレートの説明を追加します。
ステップ 7	**inactivity-timer** *minutes* **[probe]** 例： `Device(config-service-template)# inactivity-timer 15`	（任意）加入者セッションに対して、非アクティブ タイムアウトをイネーブルにします。
ステップ 8	**redirect url** *url* 例： `Device(config-service-template)# redirect url www.cisco.com`	（任意）特定のURLにクライアントを転送します。

	コマンドまたはアクション	目的
ステップ 9	**tag** *tag-name* 例： `Device(config-service-template)# tag TAG_2`	（任意）ユーザ定義のタグをサービス テンプレートに関連付けます。
ステップ 10	**vlan** *vlan-id* 例： `Device(config-service-template)# vlan 215`	（任意）サービス テンプレートを使用して、セッションに VLAN を適用します。
ステップ 11	**end** 例： `Device(config-service-template)# end`	サービス テンプレートのコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**show service-template** [*template-name*] 例： `Device# show service-template SVC_2`	設定したサービス・テンプレートに関する情報を表示します。

例：サービス テンプレート

```
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
```

次の作業

加入者セッションでサービステンプレートをアクティブ化するには、制御ポリシーでサービステンプレートを指定します。「制御ポリシーの設定」を参照してください。

アイデンティティ サービス テンプレートの設定例

例：サービス テンプレートのアクティブ化とすべての置き換え

ローカル サービス テンプレートの設定

次の例は、デバイスでローカルに定義されたサービステンプレートの設定を示しています。このテンプレートにはPOSTURE_VALIDATIONという名前の制御ポリシーを使用するセッションに適用される属性が含まれています（以下を参照）。

```
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
```

制御ポリシーの設定

次の例は、replace-allがイネーブルになったDOT1Xという名前のサービス テンプレートをアクティブ化する制御ポリシーを示します。 正常にアクティブ化されたテンプレートは、セッションに以前に適用された、既存の認可データとすべてのサービス テンプレートを置き換えます。

```
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
```

例：フォールバック サービスのサービス テンプレートのアクティブ化

ローカル サービス テンプレートの設定

次の例は、デバイスでローカルに定義されたサービステンプレートの設定を示しています。このテンプレートにはPOSTURE_VALIDATIONという名前の制御ポリシーを使用するセッションに適用される属性が含まれています（以下を参照）。

```
service-template FALLBACK
 description fallback service
 access-group ACL_2
 redirect url www.cisco.com
 inactivity-timer 15
 absolute-timer 15
 tag TAG_2
```

制御ポリシーの設定

次の例は、認証方式 dot1x および MAB を実行する制御ポリシーを示しています。 dot1x 認証が失敗すると、MAB 認証が試行されます。 MAB が失敗すると、FALLBACK テンプレートを使用するデフォルトの許可プロファイルが提供されます。

```
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
```

例：サービス テンプレートの非アクティブ化

アクセス コントロール リストの設定

次の例は、以下の LOW_IMPACT_TEMPLATE という名前のローカル サービス テンプレートで使用されるアクセス コントロール リスト（ACL）の設定を示しています。

```
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
```

ローカル サービス テンプレートの設定

次の例は、認証が失敗した場合でも、すべてのホストに対する限定されたアクセスを提供するローカル サービス テンプレートの設定を示しています。

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

制御ポリシーの設定

次の例は、LOW_IMPACT_TEMPLATE という名前のテンプレートを使用して、認証が失敗した場合でも、すべてのホストに対する限定されたアクセスを提供する制御ポリシーの設定を示しています。 認証が成功すると、ポリシー マネージャはこのサービス テンプレートを削除し、RADIUS サーバからダウンロードされたポリシーに基づいてアクセスを提供します。

```
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
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』
アドレス解決プロトコル（ARP）コマンド	『Cisco IOS IP Addressing Services Command Reference』
ARP 設定作業	『*IP Addressing - ARP Configuration Guide*』
認証、許可、およびアカウンティング（AAA）の設定作業	『*Authentication Authorization and Accounting Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference*』

標準および RFC

標準/RFC	Title
RFC 5176	『*Dynamic Authorization Extensions to RADIUS*』

テクニカル サポート

説明	Link
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

アイデンティティサービステンプレートの機能に関する情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：アイデンティティ サービス テンプレートの機能に関する情報

機能名	リリース	機能情報
ダウンロード可能なアイデンティティ サービス テンプレート	Cisco IOS XE Release 3.2SE	ACS からダウンロードサービス テンプレートと、セッションに対して適用するそのサービス テンプレートの属性をイネーブルにします。

機能名	リリース	機能情報
アイデンティティ サービス テンプレート	Cisco IOS XE Release 3.2SE	アイデンティティ サービス テンプレートのローカルでの設定と、常時利用をイネーブルにします。 導入されたコマンド：**absolute-timer**、**access-group** (service template)、**description** (service template)、**inactivity-timer**、**redirect url**、**service-template**、**show service-template**、**tag** (service template)、**vlan** (service template)。