自動 ID

- 自動 ID （1 ページ）

自動 ID

自動 ID 機能は、一連の組み込みポリシーをグローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードで提供します。この機能は、Class-Based Policy Language（CPL）コントロール ポリシーと同等な新しいスタイルのモードでのみ使用できます。関連するすべての認証コマンドをそれらの CPL コントロールポリシーの同様のコマンドに変換するには、 **authentication convert-to new-style** コマンドを使用します。

このモジュールでは、その機能および設定方法について説明します。

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、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース 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検索し、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場合は、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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

自動 ID について

自動 ID の概要

Cisco Identity-Based Networking Services（IBNS）ソリューションは、エッジ デバイスが加入者に対して柔軟かつスケーラブルなサービスを提供できる、ポリシーとアイデンティティ ベースのフレームワークを提供します。IBNS では、IEEE 802.1x（dot1x）、MAC 認証バイパス（MAB）、および Web 認証方式を同時に実行することができます。これにより、1 つの加入

者セッションに対して複数の認証方式を同時に呼び出すことができるようになります。これらの認証方式、dot1x、認証、認可、およびアカウンティング（AAA）、および RADIUS は、グローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードで使用できます。

自動 ID 機能は、Cisco Common Classification Policy Language ベースの設定を使用します。これにより、認証方式とインターフェイス レベルのコマンドを設定するために使用するコマンドの数が大幅に削減されます。自動 ID 機能は、ポリシー マップ、クラス マップ、パラメータ マップ、およびインターフェイステンプレートに基づいた一連の組み込みポリシーを提供します。

グローバル コンフィギュレーション モードでは、**source template AI_GLOBAL_CONFIG_TEMPLATE** コマンドで自動 ID 機能を有効にします。インターフェイス コンフィギュレーション モードでは、AI_MONITOR_MODE、AI_LOW_IMPACT_MODE、または AI_CLOSED_MODE インターフェイス テンプレートを設定し、インターフェイス上でこの機能を有効にします。

複数のテンプレートを設定できますが、**merge** コマンドを使用して、複数のテンプレートをまとめてバインドする必要があります。テンプレートをバインドしなかった場合は、最後に設定したテンプレートが使用されます。テンプレートをバインドする際に、2 つのテンプレートが異なる引数で繰り返された場合、最後に設定したコマンドが使用されます。

（注） また、グローバル コンフィギュレーション モードで **template** *name* コマンドを使用して設定したユーザ定義のテンプレートも有効にできます。

組み込みテンプレートに関する情報を表示するには、**show template interface** または **show template global** コマンドを使用します。組み込みテンプレートは編集できます。組み込みテンプレートを編集した場合は、**show running-config** コマンドの出力に、その組み込みテンプレートの情報が表示されます。編集した組み込みテンプレートを削除すると、その組み込みテンプレートはデフォルトに戻りますが、設定からは削除されません。ただし、ユーザ定義のテンプレートを削除した場合は設定から削除されます。

（注） テンプレートを削除する前に、デバイスに接続されていないことを確認します。

自動 ID グローバル テンプレート

グローバルテンプレートを有効にするには、**source template** *template-name* コマンドを設定します。

（注） RADIUS サーバ コマンドを設定する必要があります。これは、これらのコマンドはグローバルテンプレートが有効になっても、自動的に設定されないためです。

次に、グローバル テンプレートを有効にする例を示します。

```
Switch(config)# source template AI_GLOBAL_CONFIG_TEMPLATE
Switch(config)# radius server ISE
Switch(config-radius-server)# address ipv4 172.20.254.4 auth-port 1645 acct-port 1646
Switch(config-radius-server)# key cisco
Switch(config-radius-server)# end
```

AI_GLOBAL_CONFIG_TEMPLATE は、次のコマンドを自動的に設定します。

```
dot1x system-auth-control
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting identity default start-stop group radius
aaa accounting system default start-stop group radius
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 6 voice 1
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
```

自動 ID インターフェイス テンプレート

自動 ID 機能では、次のインターフェイス テンプレートを使用できます。

- AI_MONITOR_MODE：オープン モードで認証されているセッションを受動的に監視します。
- AI_LOW_IMPACT_MODE：モニタ モードに似ていますが、ポート アクセス コントロール リスト（PACL）など、設定済みスタティック ポリシーを持ちます。
- AI_CLOSED_MODE：認証が完了するまで、データ トラフィックがネットワークに入ることを許可しないセキュア モードです。このモードがデフォルトです。

（注） マルチ認証ホストモードは、LAN Lite ライセンスではサポートされません。

次に、AI_MONITOR_MODE に組み込まれたコマンドを示します。

```
switchport mode access
 access-session port-control auto
 access-session host-mode multi-auth
 dot1x pae authenticator
 mab
 service-policy type control subscriber AI_DOT1X_MAB_POLICIES
```

次に、AI_LOW_IMPACT_MODE に組み込まれたコマンドを示します。

```
switchport mode access
 access-session port-control auto
 access-session host-mode multi-auth
 dot1x pae authenticator
 mab
 ip access-group AI_PORT_ACL in
 service-policy type control subscriber AI_DOT1X_MAB_POLICIES
```

次に、AI_CLOSED_MODE に組み込まれたコマンドを示します。

```
switchport mode access
 access-session closed
 access-session port-control auto
 access-session host-mode multi-auth
 dot1x pae authenticator
 mab
 service-policy type control subscriber AI_DOT1X_MAB_POLICIES
```

自動 ID 組み込みポリシー

自動 ID 機能では、次の 5 つの組み込みポリシーを使用できます。

- AI_DOT1X_MAB_AUTH：dot1x を使用してフレキシブル認証を有効にしてから、MAC アドレス バイパス（MAB）を有効にします。
- AI_DOT1X_MAB_POLICIES：dot1x を使用してフレキシブル認証を有効にしてから、MAB を有効にします。認証、認可、およびアカウンティング（AAA）サーバに到達できない場合は、クリティカル VLAN を適用します。
- AI_DOT1X_MAB_WEBAUTH：dot1x を使用してフレキシブル認証を有効にしてから、Web 認証を有効にします。
- AI_NEXTGEN_AUTHBYBASS：IP 電話デバイスが検出された場合は認証をスキップします。デバイスを検出するには、**device classifier** コマンドをグローバル コンフィギュレーション モードで、 **voice-vlan** コマンドをインターフェイス コンフィギュレーション モードで有効にします。これは参照ポリシー マップであり、ユーザはこのポリシー マップの内容を別のポリシー マップにコピーできます。
- AI_STANDALONE_WEBAUTH：スタンドアロン Web 認証を定義します。

自動 ID クラス マップ テンプレート

次に、自動 ID 機能でサポートされている組み込みクラス マップを示します。

- AI_NRH：非応答ホスト（NRH）認証方式が有効であることを指定します。
- AI_WEBAUTH_METHOD：Web 認証方式が有効であることを指定します。
- AI_WEBAUTH_FAILED：Web 認証方式が認証に失敗したことを指定します。
- AI_WEBAUTH_NO_RESP：Web 認証クライアントが応答に失敗したことを指定します。
- AI_DOT1X_METHOD-dot1x：dot1x 方式が有効であることを指定します。
- AI_DOT1X_FAILED-dot1x：dot1x 方式が認証に失敗したことを指定します。
- AI_DOT1X_NO_RESP-dot1x：dot1x クライアントが応答に失敗したことを指定します。
- AI_DOT1X_TIMEOUT-dot1x：dot1x クライアントが最初の確認応答（ACK）要求後に応答を停止したことを指定します。
- AI_MAB_METHOD：MAC 認証バイパス（MAB）方式が有効であることを指定します。
- AI_MAB_FAILED-MAB：MAB 方式が認証に失敗したことを指定します。
- AI_AAA_SVR_DOWN_AUTHD_HOST：認証、認可、およびアカウンティング（AAA）サーバがダウンし、クライアントが認可済みの状態になっていることを指定します。
- AI_AAA_SVR_DOWN_UNAUTHD_HOST-AAA：AAA サーバがダウンし、クライアントが認可済みの状態になっていることを指定します。

- AI_IN_CRITICAL_AUTH：クリティカルな認証サービステンプレートが適用されていることを指定します。
- AI_NOT_IN_CRITICAL_AUTH：クリティカルな認証サービス テンプレートが適用されていないことを指定します。
- AI_METHOD_DOT1X_DEVICE_PHONE：方式は dot1x であり、デバイス タイプが IP フォンであることを指定します。
- AI_DEVICE_PHONE：デバイス タイプが IP フォンであることを指定します。

自動 ID パラメータ マップ

次に、自動 ID 機能でサポートされている組み込みパラメータ マップ テンプレートを示します。

- AI_NRH_PMAP：非応答ホスト（NRH）認証を開始します。

  AI_WEBAUTH_PMAP：Web 認証を開始します。

自動 ID サービス テンプレート

サービス テンプレートは、組み込みポリシー マップ内で使用できます。次に、自動 ID 機能でサポートされている組み込みサービス テンプレートを示します。

- AI_INACTIVE_TIMER：非アクティビティ タイマーを起動するテンプレートです。
- AI_CRITICAL_ACL：ダミーテンプレートです。ユーザはこのテンプレートを自分の要件に従って設定できます。

自動 ID の設定方法

自動 ID のグローバル設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 • 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： `Switch# 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	**sourcetemplate** {**AI_GLOBAL_CONFIG_TEMPLATE** | *template-name*} 例：	自動 ID テンプレートを設定します。 • **AI_GLOBAL_CONFIG_TEMPLATE** は組み込みのテンプレートです。

	コマンドまたはアクション	目的
	`Switch(config)# source template AI_GLOBAL_CONFIG_TEMPLATE`	• *template-name* はユーザ定義のテンプレートです。
ステップ 4	**aaa new-model** 例： `Switch(config)# aaa new-model`	認証、認可、およびアカウンティング（AAA）アクセス コントロール モードを有効にします。
ステップ 5	**radius server** *name* 例： `Switch(config)# radius server ISE`	RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 6	**address ipv4** {*hostname* | *ipv4-address*} 例： `Switch(config-radius-server)# address ipv4 10.1.1.1`	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。 （注） このコマンドはグローバル テンプレートの一部ではないため、設定する必要があります。
ステップ 7	**key ipv4** { **0** *string* | **7** *string*} *string* 例： `Switch(config-radius-server)# key ipv4 cisco`	デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。 （注） このコマンドはグローバル テンプレートの一部ではないため、設定する必要があります。
ステップ 8	**end** 例： `Switch(config-radius-server)# end`	RADIUS サーバ 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。

インターフェイス レベルでの自動 ID の設定

2 つのインターフェイステンプレートを設定する場合は、**merge** キーワードを設定する必要があります。このキーワードを設定しない場合、最後に設定したテンプレートが使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Switch# 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	**interface** *type number* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイスを設定し、インターフェイス 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	**source template** {**AI_CLOSED_MODE** | **AI_LOW_IMPACT_MODE** | **AI_MONITOR_MODE** | *template-name*} [**merge**] 例： `Switch(config-if)# source template AI_CLOSED_MODE`	インターフェイスにソース テンプレートを設定します。
ステップ 5	**source template** {**AI_CLOSED_MODE** | **AI_LOW_IMPACT_MODE** | **AI_MONITOR_MODE** | *template-name*} [**merge**] 例： `Switch(config-if)# source template AI_MONITOR_MODE merge`	（任意）インターフェイスのソース テンプレートを設定し、このテンプレートを以前に設定したテンプレートとマージします。 • 2 つのテンプレートを設定したときに **merge** キーワードを設定しなかった場合は、最後に設定したテンプレートが使用されます。
ステップ 6	**switchport access vlan** *vlan-id* 例： `Switch(config-if)# switchport access vlan 100`	インターフェイスがアクセス モードのときに VLAN を設定します。
ステップ 7	**switchport voice vlan** *vlan-id* 例： `Switch(config-if)# switchport voice vlan 101`	複数の VLAN アクセス ポートで音声 VLAN を設定します。
ステップ 8	自動 ID 機能を設定する必要があるすべてのインターフェイスで手順 4、6、および 7 を繰り返します。	—
ステップ 9	**end** 例： `Switch(config-if)# end`	インターフェイス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。

自動 ID の設定例

例：自動 ID のグローバル設定

```
Switch> enable
Switch# configure terminal
Switch(config)# source template AI_GLOBAL_CONFIG_TEMPLATE
Switch(config)# aaa new-model
Switch(config)# radius server ISE
Switch(config-radius-server)# address ipv4 10.1.1.1
Switch(config-radius-server)# key ipv4 cisco
Switch(config-radius-server)# end
```

例：インターフェイス レベルでの自動 ID の設定

```
Switch> enable
Switch# configure terminal
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# source template AI_CLOSED_MODE
Switch(config-if)# source template AI_MONITOR_MODE merge
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

自動 ID の確認

手順

ステップ 1 **enable**

例：

```
Switch> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **show template interface source built-in all**

すべての設定済みの組み込みインターフェイス テンプレートを表示します。

例：

```
Switch# show template interface source built-in all

Template Name       : AI_CLOSED_MODE
Modified            : No
Template Definition :
 dot1x pae authenticator
 switchport mode access
```

```
 mab
 access-session closed
 access-session port-control auto
 service-policy type control subscriber AI_DOT1X_MAB_POLICIES
!
Template Name       : AI_LOW_IMPACT_MODE
Modified            : No
Template Definition :
 dot1x pae authenticator
 switchport mode access
 mab
 access-session port-control auto
 service-policy type control subscriber AI_DOT1X_MAB_POLICIES
 ip access-group AI_PORT_ACL in
!
Template Name       : AI_MONITOR_MODE
Modified            : No
Template Definition :
 dot1x pae authenticator
 switchport mode access
 mab
 access-session port-control auto
 service-policy type control subscriber AI_DOT1X_MAB_POLICIES
!
```

ステップ 3 show template global source built-in all

すべての設定済みのグローバル組み込みテンプレートを表示します。

例：

```
Switch# show template global source built-in all

Global Template Name       : AI_GLOBAL_CONFIG_TEMPLATE
Modified                   : No
Global Template Definition : global
 dot1x system-auth-control
 aaa new-model
 aaa authentication dot1x default group radius
 aaa authorization network default group radius
 aaa authorization auth-proxy default group radius
 aaa accounting identity default start-stop group radius
 aaa accounting system default start-stop group radius
 radius-server attribute 6 on-for-login-auth
 radius-server attribute 6 support-multiple
 radius-server attribute 6 voice 1
 radius-server attribute 8 include-in-access-req
 radius-server attribute 25 access-request include
!
```

ステップ 4 show derived-config | include aaa |radius-server

インターフェイスに適用されているすべてのコンフィギュレーション コマンドの複合された結果を表示します。これには、スタティック テンプレート、ダイナミック テンプレート、ダイヤラ インターフェイス、ならびに認証、認可、およびアカウンティング（AAA）のユーザ単位の属性など、送信元からのコマンドが含まれます。

例：

```
Switch# show derived-config | inc aaa| radius-server
```

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting identity default start-stop group radius
aaa accounting system default start-stop group radius
aaa session-id common
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 6 voice 1
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host 10.25.18.42 key cisco
```

ステップ 5 **show derived-config | interface** *type-number*

インターフェイスのすべての設定の複合された結果を表示します。

例：

```
Switch# show derived-config | interface gigabitethernet2/0/6

Building configuration...

Derived configuration : 267 bytes
!
interface GigabitEthernet2/0/6
 switchport mode access
 switchport voice vlan 100
 access-session closed
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast edge
 service-policy type control subscriber AI_DOT1X_MAB_POLICIES
end
```

ステップ 6 **show access-session | interface** *interface-type-number* **details**

インターフェイスに適用されているポリシーを表示します。

例：

```
Switch# show access-session interface gigabitethernet2/0/6 details

Interface:  GigabitEthernet2/0/6
          MAC Address:  c025.5c43.be00
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  CP-9971-SEPC0255C43BE00
          Device-type:  Cisco-IP-Phone-9971
               Status:  Authorized
               Domain:  VOICE
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  091A1C5B00000017002003EE
      Acct Session ID:  0x00000005
               Handle:  0xBB00000B
       Current Policy:  AI_DOT1X_MAB_POLICIES
```

```
Local Policies:

Server Policies:
           Vlan Group:  Vlan: 100
      Security Policy:  Must Not Secure
      Security Status:  Link Unsecure


Method status list:
       Method           State
       dot1x            Authc Success
```

ステップ 7 **show running-config interface** *type-number*

現在の実行コンフィギュレーション ファイルまたはインターフェイスの設定を表示します。

例：

```
Switch# show running-config interface gigabitethernet2/0/6

Building configuration...

Current configuration : 214 bytes
!
interface GigabitEthernet2/0/6
 switchport mode access
 switchport voice vlan 100
 access-session port-control auto
 spanning-tree portfast edge
 service-policy type control subscriber AI_NEXTGEN_AUTHBYPASS
end
```

ステップ 8 **show lldp neighbor**

Link Layer Discovery Protocol（LLDP）を使用して検出した 1 つまたはすべてのネイバー デバイスの情報を表示します。

例：

```
Switch# show lldp neighbor

Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
SEPC0255C43BE00     Gi2/0/6        180        B,T             C0255C43BE00:P1

Total entries displayed: 1
```

自動 ID の機能情報

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、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 リリースだけを示しています。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*: 自動 *ID* の機能情報

機能名	リリース	機能情報
自動 ID	Cisco IOS リリース 15.2(4)E	自動 ID 機能は、一連の組み込みポリシーをグローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードで提供します。この機能は、Class-Based Policy Language（CPL）コントロール ポリシーと同等な新しいスタイルのモードでのみ使用できます。 この機能は、Cisco IOS リリース 15.2(4)E で Cisco Catalyst 2960–X シリーズ スイッチ、Catalyst 3750–X シリーズ スイッチ、および Cisco Catalyst 4500E Supervisor Engine 7-E に実装されました。 次のコマンドが導入または変更されました。**source-template**