



A コマンド

この章では、A で始まる Cisco NX-OS Security コマンドについて説明します。

aaa accounting default

アカウントिंगの Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントング) 方式を設定するには、**aaa accounting default** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
aaa accounting default {group group-list | local}
```

```
no aaa accounting default {group group-list | local}
```

シンタックスの説明

group	アカウントングにサーバグループを使用するように指定します。
group-list	サーバグループをスペースで区切って指定します。リストには、次のようなサーバグループを含めることができます。 <ul style="list-style-type: none">• radius — 設定済みのすべての RADIUS サーバ。• 設定済みの任意の RADIUS または TACACS+ サーバグループ名。 リストには、最大 8 つのグループ名を格納できます。
local	アカウントングにローカル データベースを使用するように指定します。

デフォルト

local

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

group group-list 方式は、以前に定義された一連のサーバを指します。ホストサーバを設定するには、**radius-server host** および **tacacs-server host** コマンドを使用します。サーバのネームドグループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバグループを表示するには、**show aaa group** コマンドを使用します。

group 方式、**local** 方式、または両方を指定した場合にそれらの方式が失敗すると、アカウント認証は失敗します。

複数のサーバグループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドにライセンスは必要ありません。

例

次に、AAA アカウンティングに任意の RADIUS サーバを設定する例を示します。

```
switch# config t
switch(config)# aaa accounting default group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA RADIUS サーバグループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa accounting	AAA アカウンティング ステータス情報を表示します。
show aaa group	AAA サーバグループ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa accounting dot1x

802.1X 認証の AAA アカウンティング方式を設定するには、**aaa accounting dot1x** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
aaa accounting dot1x {group group-list | local}
```

```
no aaa accounting dot1x {group group-list | local}
```

シンタックスの説明	
group	アカウンティングにサーバグループを使用するように指定します。
<i>group-list</i>	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバグループを含めることができます。 <ul style="list-style-type: none"> • radius — 設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバグループ名 リストには、最大 8 つのグループ名を格納できます。
local	アカウンティングにローカル データベースを使用するように指定します。

デフォルト local

コマンド モード グローバル コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン **group group-list** 方式は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームドグループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバグループを表示するには、**show aaa group** コマンドを使用します。

group 方式、**local** 方式、または両方を指定した場合にそれらの方式が失敗すると、アカウンティング認証は失敗します。

複数のサーバグループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドにライセンスは必要ありません。

例

次に、AAA アカウンティングに任意の RADIUS サーバを設定する例を示します。

```
switch# config t
switch(config)# aaa accounting default group radius
```

関連コマンド

コマンド	説明
aaa group server radius	AAA RADIUS サーバグループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa accounting	AAA アカウンティング ステータス情報を表示します。
show aaa group	AAA サーバグループ情報を表示します。

aaa authentication cts default group

Cisco TrustSec 認証のデフォルト AAA RADIUS サーバ グループを設定するには、**aaa authentication cts default group** コマンドを使用します。デフォルト AAA 認証サーバ グループ リストからサーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa authentication cts default group group-list

no aaa authentication cts default group group-list

シンタックスの説明	<p><i>group-list</i> RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。</p> <ul style="list-style-type: none"> • radius — 設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 <p>リストには、最大 8 つのグループ名を格納できます。</p>				
デフォルト	なし				
コマンドモード	グローバル コンフィギュレーション				
サポートされるユーザロール	network-admin vdc-admin				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	4.0(1)	このコマンドが導入されました。
リリース	変更内容				
4.0(1)	このコマンドが導入されました。				
使用上のガイドライン	<p>このコマンドを使用するには、feature cts コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。</p> <p><i>group-list</i> は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、radius-server host コマンドを使用します。サーバのネームド グループを作成するには、aaa group server コマンドを使用します。</p> <p>デバイス上の RADIUS サーバ グループを表示するには、show aaa group コマンドを使用します。</p> <p>複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。</p> <p>このコマンドには、Advanced Services ライセンスが必要です。</p>				

例 次に、Cisco TrustSec のデフォルト AAA 認証 RADIUS サーバ グループを設定する例を示します。

```
switch# config t
switch(config)# aaa authentication cts default group RadGroup
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証設定を表示します。
show aaa group	AAA サーバ グループを表示します。

aaa authentication dot1x default group

802.1X の AAA 認証方式を設定するには、**aaa authentication dot1x default group** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
aaa authentication dot1x default group group-list
```

```
no aaa authentication dot1x default group group-list
```

シンタックスの説明	group-list RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 <ul style="list-style-type: none">• radius — 設定済みのすべての RADIUS サーバ• 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。
------------------	--

デフォルト	なし
--------------	----

コマンド モード	グローバル コンフィギュレーション
-----------------	-------------------

サポートされるユーザ ロール	network-admin vdc-admin
-----------------------	----------------------------

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン 802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドにライセンスは必要ありません。

■ aaa authentication dot1x default group

例

次に、802.1X 認証方式を設定する例を示します。

```
switch# config t
switch(config)# aaa authentication dot1x default group Dot1xGroup
```

次に、デフォルトの 802.1X 認証方式に戻す例を示します。

```
switch# config t
switch(config)# no aaa authentication dot1x default group Dot1xGroup
```

関連コマンド

コマンド	説明
feature dot1x	802.1X をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証設定を表示します。
show aaa group	AAA サーバグループを表示します。

aaa authentication eou default group

EAP over UDP (EoU) の AAA 認証方式を設定するには、**aaa authentication eou default group** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
aaa authentication eou default group group-list
```

```
no aaa authentication eou default group group-list
```

シンタックスの説明	group-list RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 <ul style="list-style-type: none">• radius — 設定済みのすべての RADIUS サーバ• 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。
------------------	--

デフォルト	なし
--------------	----

コマンド モード	グローバル コンフィギュレーション
-----------------	-------------------

サポートされるユーザ ロール	network-admin vdc-admin
-----------------------	----------------------------

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン デフォルト EAPoUDP 認証方式を設定する前に、**feature eou** コマンドを使用して EAPoUDP をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドにライセンスは必要ありません。

■ aaa authentication eou default group

例

次に、EAPoUDP 認証方式を設定する例を示します。

```
switch# config t
switch(config)# aaa authentication eou default group EoUGroup
```

次に、デフォルトの EAPoUDP 認証方式に戻す例を示します。

```
switch# config t
switch(config)# no aaa authentication eou default group EoUGroup
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証設定を表示します。
show aaa group	AAA サーバグループを表示します。

aaa authentication login console

コンソール ログインの AAA 認証方式を設定するには、**aaa authentication login console** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
aaa authentication login console {group group-list} [none] | local | none
```

```
no aaa authentication login console {group group-list [none] | local | none}
```

シンタックスの説明

group	認証にサーバグループを使用するように指定します。
<i>group-list</i>	サーバ グループをスペースで区切って指定します。リストには、次のようなサーバグループを含めることができます。 <ul style="list-style-type: none"> • radius — 設定済みのすべての RADIUS サーバ • tacacs+ — 設定済みのすべての TACACS+ サーバ • 設定済みの任意の RADIUS または TACACS+ サーバグループ名
none	認証にユーザ名を使用するように指定します。
local	認証にローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

group radius、**group tacacs+**、および **group group-list** 方式は、以前に定義された RADIUS または TACACS+ サーバを指します。ホスト サーバを設定するには、**radius-server host** または **tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバグループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバグループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認証は失敗する可能性があります。**none** 方式を単独または **group** 方式の後ろに指定した場合、認証は常に成功します。

このコマンドは、デフォルト VDC (VDC 1) でのみ機能します。

このコマンドにライセンスは必要ありません。

例

次に、コンソール ログインの AAA 認証方式を設定する例を示します。

```
switch# config t
switch(config)# aaa authentication login console group radius
```

次に、デフォルトのコンソール ログインの AAA 認証方式に戻す例を示します。

```
switch# config t
switch(config)# no aaa authentication login console group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバグループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
show aaa group	AAA サーバグループを表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login default

デフォルト AAA 認証方式を設定するには、**aaa authentication login default** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
aaa authentication login default {group group-list} [none] | local | none}
```

```
no aaa authentication login default {group group-list [none] | local | none}
```

シンタックスの説明

group	認証に使用するサーバグループ リストを指定します。
<i>group-list</i>	サーバグループをスペースで区切って指定します。リストには、次のようなサーバグループを含めることができます。 <ul style="list-style-type: none"> • radius — 設定済みのすべての RADIUS サーバ • tacacs+ — 設定済みのすべての TACACS+ サーバ • 設定済みの任意の RADIUS または TACACS+ サーバグループ名
none	(任意) 認証にユーザ名を使用するように指定します。
local	認証にローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

group radius、**group tacacs+**、および **group group-list** 方式は、以前に定義された RADIUS または TACACS+ サーバを指します。ホストサーバを設定するには、**radius-server host** または **tacacs-server host** コマンドを使用します。サーバのネームドグループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバグループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバグループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認証は失敗します。**none** 方式を単独または **group** 方式の後ろに指定した場合、認証は常に成功します。

このコマンドにライセンスは必要ありません。

例

次に、コンソール ログインの AAA 認証方式を設定する例を示します。

```
switch# config t
switch(config)# aaa authentication login default group radius
```

次に、デフォルトのコンソール ログインの AAA 認証方式に戻す例を示します。

```
switch# config t
switch(config)# no aaa authentication login default group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバグループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
show aaa group	AAA サーバグループを表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login error-enable

コンソールに AAA 認証失敗メッセージが表示されるように設定するには、**aaa authentication login error-enable** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login error-enable

no aaa authentication login error-enable

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンドモード グローバル コンフィギュレーション

サポートされるユーザロール network-admin
vdc-admin

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン ログイン時にリモート AAA サーバからの応答がない場合には、ローカル ユーザ データベースへのロールオーバーによってログインが続行されます。そのような場合に、ログイン失敗メッセージの表示がイネーブルになっていると、ユーザ端末に次のメッセージが表示されます。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

このコマンドにライセンスは必要ありません。

例 次に、AAA 認証失敗メッセージのコンソールへの表示をイネーブルにする例を示します。

```
switch# config t
switch(config)# aaa authentication login error-enable
```

次に、AAA 認証失敗メッセージのコンソールへの表示をディセーブルにする例を示します。

```
switch# config t
switch(config)# no aaa authentication login error-enable
```

関連コマンド	コマンド	説明
	show aaa authentication login error-enable	AAA 認証失敗メッセージ表示のステータスを表示します。

aaa authentication login mschap

ログイン時の Microsoft Challenge Handshake Authentication Protocol (MS-CHAP; マイクロソフト チャレンジ ハンドシェーク 認証プロトコル) 認証をイネーブルにするには、**aaa authentication login mschap** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
aaa authentication login mschap
```

```
no aaa authentication login mschap
```

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンドモード グローバル コンフィギュレーション

サポートされるユーザロール network-admin
vdc-admin

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドにライセンスは必要ありません。

例 次に、MSCHAP 認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# aaa authentication login mschap
```

次に、MSCHAP 認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no aaa authentication login mschap
```

関連コマンド	コマンド	説明
	show aaa authentication login mschap	MSCHAP 認証のステータスを表示します。

aaa authorization cts default group

Cisco TrustSec 認可のデフォルト AAA RADIUS サーバ グループを設定するには、**aaa authorization cts default group** コマンドを使用します。デフォルト AAA 認可サーバ グループ リストからサーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa authorization cts default group group-list

no aaa authorization cts default group group-list

シンタックスの説明	<p><i>group-list</i> RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。</p> <ul style="list-style-type: none"> • radius — 設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 <p>リストには、最大 8 つのグループ名を格納できます。</p>				
デフォルト	なし				
コマンドモード	グローバル コンフィギュレーション				
サポートされるユーザロール	network-admin vdc-admin				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	4.0(1)	このコマンドが導入されました。
リリース	変更内容				
4.0(1)	このコマンドが導入されました。				
使用上のガイドライン	<p>このコマンドを使用するには、feature cts コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。</p> <p><i>group-list</i> は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、radius-server host コマンドを使用します。サーバのネームド グループを作成するには、aaa group server コマンドを使用します。</p> <p>デバイス上の RADIUS サーバ グループを表示するには、show aaa group コマンドを使用します。</p> <p>複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。</p> <p>このコマンドには、Advanced Services ライセンスが必要です。</p>				

■ aaa authorization cts default group

例 次に、Cisco TrustSec のデフォルト AAA 認可 RADIUS サーバ グループを設定する例を示します。

```
switch# config t
switch(config)# aaa authorization cts default group RadGroup
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。
show aaa group	AAA サーバグループを表示します。

aaa group server radius

RADIUS サーバグループを作成して、RADIUS サーバグループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。RADIUS サーバグループを削除するには、このコマンドの **no** 形式を使用します。

```
aaa group server radius group-name
```

```
no aaa group server radius group-name
```

シンタックスの説明	<i>group-name</i> RADIUS サーバグループ名。名前には英数字を使用します。大文字と小文字が区別され、最大 64 文字まで可能です。				
デフォルト	なし				
コマンドモード	グローバル コンフィギュレーション				
サポートされるユーザロール	network-admin vdc-admin				
コマンド履歴	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>4.0(1)</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	4.0(1)	このコマンドが導入されました。
リリース	変更内容				
4.0(1)	このコマンドが導入されました。				
使用上のガイドライン	このコマンドにライセンスは必要ありません。				
例	<p>次に、RADIUS サーバグループを作成し、RADIUS サーバ設定モードを開始する例を示します。</p> <pre>switch# config t switch(config)# aaa group server radius RadServer switch(config-radius)#</pre> <p>次に、RADIUS サーバグループを削除する例を示します。</p> <pre>switch# config t switch(config)# no aaa group server radius RadServer</pre>				
関連コマンド	<table><thead><tr><th>コマンド</th><th>説明</th></tr></thead><tbody><tr><td>show aaa groups</td><td>サーバグループ情報を表示します。</td></tr></tbody></table>	コマンド	説明	show aaa groups	サーバグループ情報を表示します。
コマンド	説明				
show aaa groups	サーバグループ情報を表示します。				

aaa group server tacacs+

TACACS+ サーバ グループを作成して、TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。TACACS+ サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

```
aaa group server tacacs+ group-name
```

```
no aaa group server tacacs+ group-name
```

シンタックスの説明	<i>group-name</i> TACACS+ サーバ グループ名。名前には英数字を使用します。大文字と小文字が区別され、最大 64 文字まで可能です。
------------------	--

デフォルト	なし
--------------	----

コマンドモード	グローバル コンフィギュレーション
----------------	-------------------

サポートされるユーザロール	network-admin vdc-admin
----------------------	----------------------------

コマンド履歴	リリース 変更内容
	4.0(1) このコマンドが導入されました。

使用上のガイドライン	TACACS+ を設定する前に feature tacacs+ コマンドを使用する必要があります。 このコマンドにライセンスは必要ありません。
-------------------	---

例	次に、TACACS+ サーバ グループを作成し、TACACS+ サーバ設定モードを開始する例を示します。 <pre>switch# config t switch(config)# aaa group server tacacs+ TacServer switch(config-radius)#</pre>
----------	---

次に、TACACS+ サーバ グループを削除する例を示します。


```
switch# config t
switch(config)# no aaa group server tacacs+ TacServer
```

関連コマンド	コマンド	説明
	feature tacacs+	TACACS+ をイネーブルにします。
	show aaa groups	サーバグループ情報を表示します。

aaa user default-role

ユーザ ロールを持たないリモート ユーザが、RADIUS または TACACS+ 経由でデフォルト ユーザ ロールを使用してデバイスにログインできるようにするには、**aaa user default-role** コマンドを使用します。リモート ユーザのデフォルト ユーザ ロールをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa user default-role

no aaa user default-role

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト イネーブル

コマンドモード グローバル コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴	リリース	変更内容
	4.0(3)	このコマンドが導入されました。

使用上のガイドライン Virtual Device Context (VDC; バーチャル デバイス コンテキスト) のこの機能は、必要に応じてイネーブルまたはディセーブルにできます。デフォルト VDC の場合、デフォルト ロールは network-operator です。非デフォルト VDC の場合、デフォルト VDC は vdc-operator です。AAA デフォルト ユーザ ロール機能がディセーブルの場合は、ユーザ ロールを持たないリモート ユーザはデバイスにログインできません。

このコマンドにライセンスは必要ありません。

例 次に、リモート ユーザの AAA 認証のデフォルト ユーザ ロールをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa user default-role
```

次に、リモート ユーザの AAA 認証のデフォルト ユーザ ロールをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no aaa user default-role
```

関連コマンド	コマンド	説明
	show aaa user default-role	AAA デフォルト ユーザ ロール機能のステータスを表示します。

absolute

特定の開始日時、特定の終了日時、またはその両方が指定された時間範囲を指定するには、**absolute** コマンドを使用します。絶対時間範囲を削除するには、このコマンドの **no** 形式を使用します。

```
[sequence-number] absolute [start time date] [end time date]
```

```
no {sequence-number | absolute [start time date] [end time date]}
```

シンタックスの説明

<i>sequence-number</i>	<p>(任意) ルールのシーケンス番号。この番号により、時間範囲内の番号が振られた場所にデバイスがコマンドを挿入します。時間範囲内のルールの順序は、シーケンス番号によって維持されます。</p> <p>シーケンス番号には、1 から 4294967295 までの任意の整数を使用できます。</p> <p>時間範囲内の最初のルールは、デフォルトでシーケンス番号 10 を持ちます。</p> <p>シーケンス番号を指定しない場合は、デバイスによってそのルールが時間範囲の最後に追加され、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号が割り当てられます。</p> <p>ルールにシーケンス番号を再割り当てするには、resequence コマンドを使用します。</p>
<i>start time date</i>	<p>(任意) デバイスが、時間範囲に関連付けられた permit (許可) ルールおよび deny (拒否) ルールの実行を開始する正確な日時を指定します。開始日時を指定しない場合、デバイスは permit ルールまたは deny ルールを即座に実行します。</p> <p><i>time</i> 引数と <i>date</i> 引数の値についての詳細は、「使用上のガイドライン」セクションを参照してください。</p>
<i>end time date</i>	<p>(任意) デバイスが、時間範囲に関連付けられた permit コマンドおよび deny コマンドの実行を停止する正確な日時を指定します。終了日時を指定しない場合、デバイスは毎回、開始日時が過ぎた時点で permit ルールまたは deny ルールを実行します。</p> <p><i>time</i> 引数と <i>date</i> 引数の値についての詳細は、「使用上のガイドライン」セクションを参照してください。</p>

デフォルト

なし

コマンド モード

時間範囲コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン デバイスは、すべての時間範囲ルールを現地時間で解釈します。

start キーワードおよび *end* キーワードの両方を省略すると、デバイスは絶対時間範囲が常にアクティブであるとみなします。

time 引数は、*hours:minutes* または *hours:minutes:seconds* の形式で 24 時間表記で指定します。たとえば、24 時間表記では 8:00 a.m. は 8:00、8:00 p.m. は 20:00 になります。

date 引数は、*day month year* の形式で指定します。最小有効開始日時は 00:00:00 1 January 1970、最大有効開始日時は 23:59:59 31 December 2037 です。

このコマンドにライセンスは必要ありません。

例 次に、2007 年 9 月 17 日の午前 7 時に開始され、2007 年 9 月 19 日の午後 11 時 59 分 59 秒に終了する絶対時間ルールを作成する例を示します。

```
switch# config t
switch(config)# time-range conference-remote-access
switch(config-time-range)# absolute start 07:00 17 September 2007 end 23:59:59 19
September 2007
```

関連コマンド

コマンド	説明
periodic	定期的な時間範囲ルールを設定します。
time-range	IPv4 ACL で使用される時間範囲を設定します。

accept-lifetime

別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間を指定するには、**accept-lifetime** コマンドを使用します。期間を削除するには、このコマンドの **no** 形式を使用します。

accept-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

no accept-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

シンタックスの説明

local	(任意) デバイスが設定された時間を現地時間として扱うように指定します。デフォルトでは、デバイスは <i>start-time</i> 引数および <i>end-time</i> 引数を UTC として扱います。
<i>start-time</i>	デバイスがキーの受け入れを開始する時刻と日付。 <i>start-time</i> 引数の値についての詳細は、「使用上のガイドライン」セクションを参照してください。
duration <i>duration-value</i>	(任意) ライフタイムの長さを秒単位で指定します。最大値は 2147483646 秒です (約 68 年)。
infinite	(任意) キーが期限切れにならないように指定します。
<i>end-time</i>	(任意) デバイスがキーの受け入れを停止する時刻と日付。 <i>time of day</i> 引数と <i>date</i> 引数の値についての詳細は、「使用上のガイドライン」セクションを参照してください。

デフォルト

infinite

コマンドモード

キー コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトで、デバイスはすべての時間範囲ルールを UTC で解釈します。

デフォルトでは、別のデバイスとのキー交換時にデバイスがキーを受け入れる期間 (受け入れライフタイム) は **infinite** です。つまり、キーは永久に有効です。

start-time 引数および *end-time* 引数の両方に、次の形式で時間と日付の要素が必要です。

hour[:*minute*[:*second*]] *month day year*

24 時間表記で指定します。たとえば、24 時間表記では 8:00 a.m. は 8:00、8:00 p.m. は 20:00 になります。最小有効 *start-time* は 00:00:00 Jan 1 1970 であり、最大有効 *start-time* は 23:59:59 Dec 31 2037 です。

このコマンドにライセンスは必要ありません。

例 次に、2008年6月13日の午前零時に開始され、2008年8月12日の午後11時59分59秒に終了する受け入れライフタイムを作成する例を示します。

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2008 23:59:59 Sep 12 2008
switch(config-keychain-key)#
```

関連コマンド

コマンド	説明
key	キーを設定します。
keychain	キーチェーンを設定します。
key-string	キーstringを設定します。
send-lifetime	キーの送信ライフタイムを設定します。
show key chain	キーチェーン設定を表示します。

action

パケットが VLAN Access Control List (VACL; VLAN アクセス コントロール リスト) の **permit** コマンドと一致した場合にデバイスが実行する処理を指定するには、**action** コマンドを使用します。**action** コマンドを削除するには、このコマンドの **no** 形式を使用します。

action drop [log]

no action drop [log]

action forward [capture]

no action forward [capture]

action redirect {ethernet *slot/port* | port-channel *channel-number.subinterface-number*}

no action redirect {ethernet *slot/port* | port-channel *channel-number.subinterface-number*}

シンタックスの説明

drop	デバイスがパケットをドロップするように指定します。
log	(任意) デバイスが、 drop キーワードに基づいてドロップしたパケットを記録するように指定します。
forward	デバイスがパケットをその宛先ポートに転送するように指定します。
capture	(任意) デバイスが、パケットの宛先ポートに加え、キャプチャ機能がイネーブルになっているポートにパケットを転送するように指定します。
redirect	デバイスがパケットをインターフェイスにリダイレクトするように指定します。
ethernet <i>slot/port</i>	デバイスがパケットをリダイレクトするイーサネット インターフェイスを指定します。
port-channel <i>channel-number.subinterface-number</i>	デバイスがパケットをリダイレクトするポート チャネル インターフェイスを指定します。
	 (注) <i>channel-number</i> 引数と <i>subinterface-number</i> 引数間には、ドット区切り文字が必要です。

デフォルト

なし

コマンドモード

VALN アクセス マップ コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

action コマンドでは、パケットが **match** コマンドによって指定された ACL 内の条件に一致した場合にデバイスが実行する処理を指定します。

このコマンドにライセンスは必要ありません。

例

次に、vlan-map-01 という名前の VLAN アクセス マップを作成し、ip-acl-01 という名前の IPv4 ACL をマップに割り当て、デバイスが ACL と一致したパケットを転送するように指定し、マップと一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch# config t
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
match	VLAN アクセス マップでのトラフィック フィルタリング用の ACL を指定します。
show vlan access-map	すべてまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップの適用方法についての情報を表示します。
statistics	Access Control List (ACL; アクセス コントロール リスト) または VLAN アクセス マップの統計情報をイネーブルにします。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

arp access-list

Address Resolution Protocol (ARP; アドレス解決プロトコル) ACL を作成するか、特定の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始するには、**arp access-list** コマンドを使用します。ARP ACL を削除するには、このコマンドの **no** 形式を使用します。

arp access-list *access-list-name*

no arp access-list *access-list-name*

シンタックスの説明	<i>access-list-name</i>	ARP ACL の名前。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。名前にはスペースまたは引用符を含めることはできません。
------------------	-------------------------	---

デフォルト	なし
--------------	----

コマンドモード	グローバル コンフィギュレーション
----------------	-------------------

サポートされるユーザロール	network-admin vdc-admin
----------------------	----------------------------

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン DHCP スヌーピングを使用できない場合は、ARP ACL を使用して ARP トラフィックをフィルタリングします。

デフォルトでは、ARP ACL は定義されていません。

arp access-list コマンドを使用すると、デバイスによって ARP アクセス リスト コンフィギュレーション モードが開始されます。このモードでは、**ARP deny** コマンドおよび **permit** コマンドを使用して、ACL のルールを設定できます。指定の ACL が存在しない場合は、このコマンドを入力した時点でデバイスによって作成されます。

ARP ACL を VLAN に適用するには、**ip arp inspection filter** コマンドを使用します。

このコマンドにライセンスは必要ありません。

例 次に、arp-acl-01 という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)#
```

関連コマンド	コマンド	説明
	deny (ARP)	ARP ACL の拒否ルールを設定します。
	ip arp inspection filter	ARP ACL を VLAN に適用します。
	permit (ARP)	ARP ACL の許可ルールを設定します。
	show arp access-lists	すべての ARP ACL または特定の ARP ACL を表示します。