

ASA DAPを導入してAnyConnectのMACアドレスを特定する

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[ASAでの設定](#)

[ASDMでの設定](#)

[確認](#)

[シナリオ1:一致するDAPは1つだけです](#)

[シナリオ2:デフォルトのDAPが一致しています](#)

[シナリオ3:複数のDAP\(Action: Continue\)が一致](#)

[シナリオ4:複数のDAP\(Action: Terminate\)が一致しています。](#)

[一般的なトラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、AnyConnect接続に使用されるデバイスのMACアドレスを確認するために、ASDM経由でダイナミックアクセスポリシー(DAP)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。
Cisco Anyconnectとホストスキャンの設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

ASAv 9.18(4)

ASDM 7.20(1)

Anyconnect 4.10.07073

ホストスキャン4.10.07073

Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

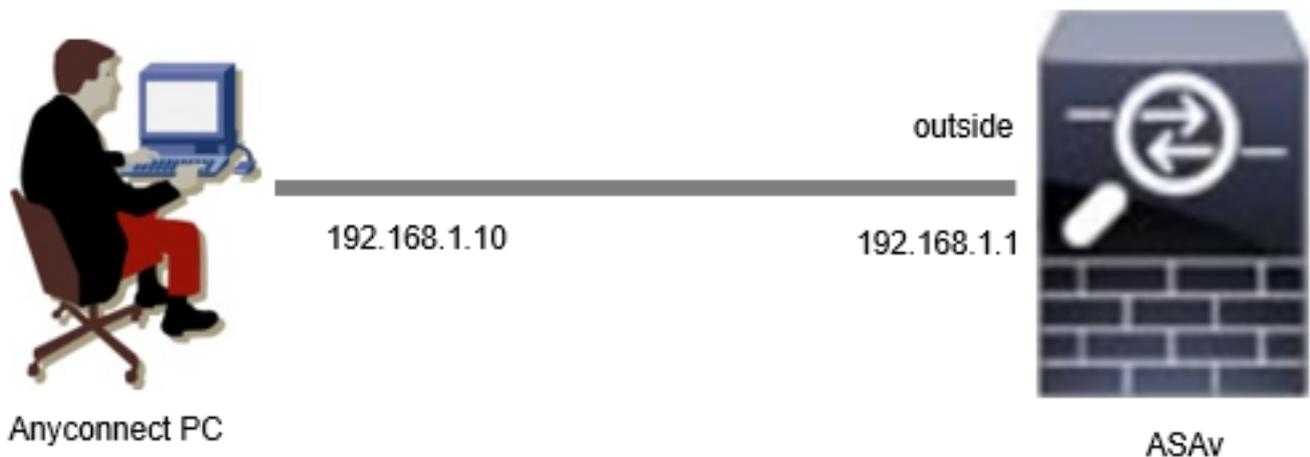
背景説明

HostScanは、AnyConnectセキュアモビリティクライアントがネットワーク上でセキュリティポリシーを適用できるようにするソフトウェアモジュールです。ホストスキャンの処理中に、クライアントデバイスに関するさまざまな詳細が収集され、適応型セキュリティアプライアンス (ASA)に報告されます。これらの詳細には、デバイスのオペレーティングシステム、ウイルス対策ソフトウェア、ファイアウォールソフトウェア、MACアドレスなどが含まれます。ダイナミックアクセスポリシー(DAP)機能を使用すると、ネットワーク管理者はユーザごとにセキュリティポリシーを設定できます。DAPのendpoint.device.MAC属性を使用して、クライアントデバイスのMACアドレスを事前定義されたポリシーと照合したり、照合したりできます。

設定

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。



図

ASAでの設定

これは、ASA CLIでの最小限の設定です。

```
tunnel-group dap_test_tg type remote-access
tunnel-group dap_test_tg general-attributes
default-group-policy dap_test_gp
tunnel-group dap_test_tg webvpn-attributes
group-alias dap_test enable
```

```
group-policy dap_test_gp internal
group-policy dap_test_gp attributes
vpn-tunnel-protocol ssl-client
address-pools value ac_pool
webvpn
anyconnect keep-installer installed
always-on-vpn profile-setting
```

```
ip local pool ac_pool 172.16.1.11-172.16.1.20 mask 255.255.255.0
```

```
webvpn
enable outside
hostscan image disk0:/hostscan_4.10.07073-k9.pkg
hostscan enable
anyconnect image disk0:/anyconnect-win-4.10.07073-webdeploy-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

ASDMでの設定

ここでは、ASDMでDAPレコードを設定する方法について説明します。この例では、endpoint.device.MAC属性を条件として使用する3つのDAPレコードを設定します。

- ・ 01_dap_test:endpoint.device.MAC=0050.5698.e608
- ・ 02_dap_test:endpoint.device.MAC=0050.5698.e605 = AnyConnectエンドポイントのMAC
- ・ 03_dap_test:endpoint.device.MAC=0050.5698.e609

1. 01_dap_testという名前の最初のDAPを設定します。

Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policiesの順に移動します。Addをクリックし、図に示すように、Policy Name、AAA Attribute、endpoint attributes、Action、User Messageを設定します。

Edit Dynamic Access Policy

Policy Name: **01_dap_test**

Description: _____ ACL Priority: 0

Selection Criteria
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values... and the following endpoint attributes are satisfied.

| AAA Attribute | Operation/Value | Endpoint ID | Name/Operation/Value |
|--------------------------|----------------------|---------------|-------------------------------------|
| disco.grouppolicy | = dap_test_gp | device | MAC["0050.5698.e608"] = true |

Advanced

Access/Authorization Policy Attributes
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists | Bookmarks | Access Method | Secure Client | Secure Client Custom Attributes
 Action | Network ACL Filters (client) | Webype ACL Filters (clientless) | Functions

Action: Continue Quarantine Terminate

Specify the message that will be displayed when this record is selected.

User Message: **01_dap_test**

OK Cancel Help

最初のDAPの設定

AAA属性のグループポリシーを設定します。

Add AAA Attribute [Close]

AAA Attribute Type: Cisco

Group Policy: = dap_test_gp

Assigned IPv4 Address: =

Assigned IPv6 Address: =

Connection Profile: = DefaultRAGroup

Username: =

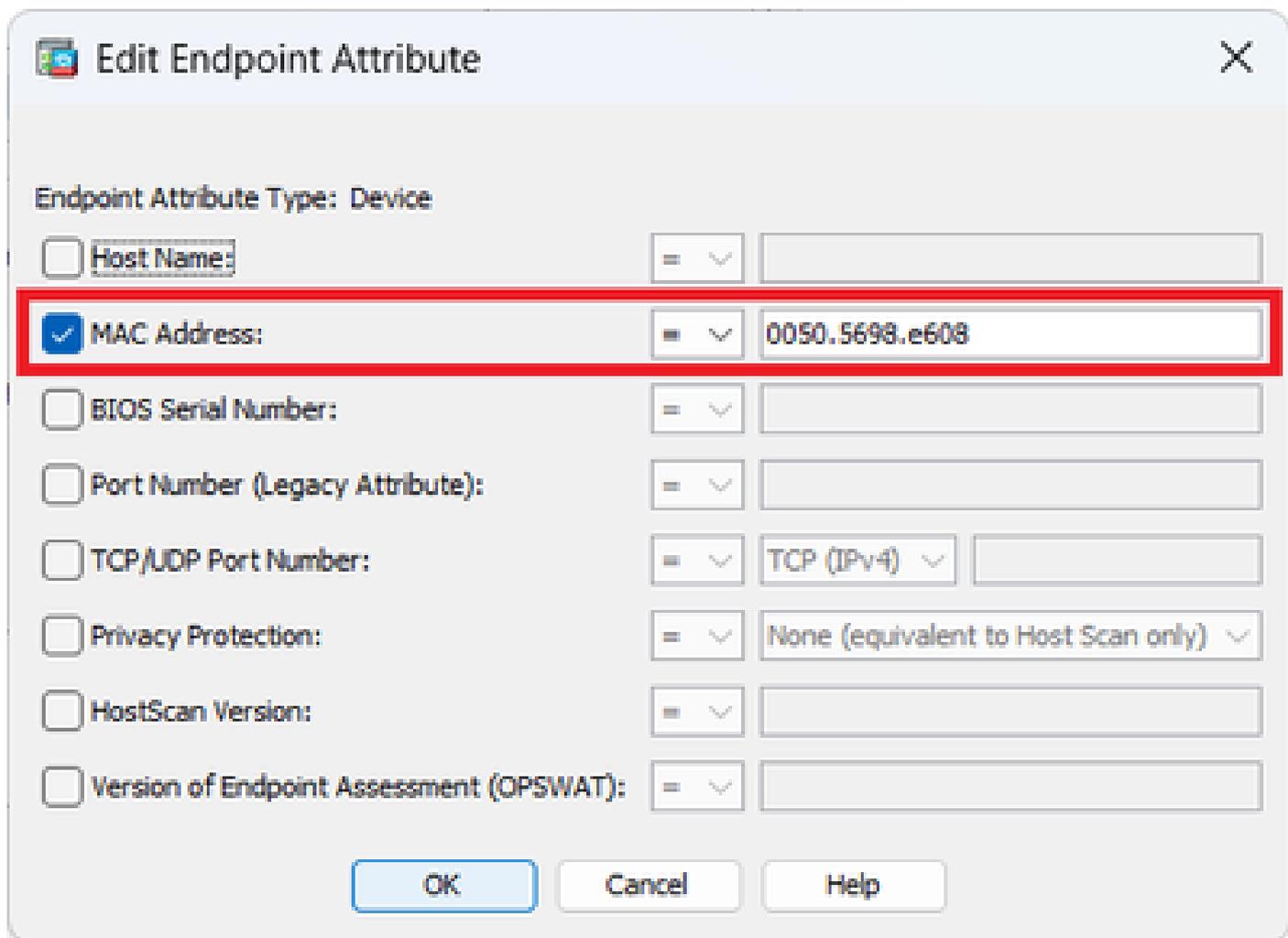
Username2: =

SCEP Required: = true

OK Cancel Help

DAPレコードのグループポリシーの設定

エンドポイント属性のMACアドレスを設定します。

The image shows a dialog box titled "Edit Endpoint Attribute" with a close button (X) in the top right corner. The dialog is set to "Endpoint Attribute Type: Device". It contains several rows of settings, each with a checkbox, a label, a dropdown menu, and a text input field. The "MAC Address" row is highlighted with a red border. The "MAC Address" checkbox is checked, and its value is "0050.5698.e608". Other rows include "Host Name:", "BIOS Serial Number:", "Port Number (Legacy Attribute):", "TCP/UDP Port Number:" (with a sub-dropdown for "TCP (IPv4)"), "Privacy Protection:" (with a sub-dropdown for "None (equivalent to Host Scan only)"), "HostScan Version:", and "Version of Endpoint Assessment (OPSWAT):". At the bottom are "OK", "Cancel", and "Help" buttons.

| Attribute | Selected | Value |
|--|-------------------------------------|---|
| Host Name: | <input type="checkbox"/> | |
| MAC Address: | <input checked="" type="checkbox"/> | 0050.5698.e608 |
| BIOS Serial Number: | <input type="checkbox"/> | |
| Port Number (Legacy Attribute): | <input type="checkbox"/> | |
| TCP/UDP Port Number: | <input type="checkbox"/> | TCP (IPv4) [] |
| Privacy Protection: | <input type="checkbox"/> | None (equivalent to Host Scan only) [] |
| HostScan Version: | <input type="checkbox"/> | |
| Version of Endpoint Assessment (OPSWAT): | <input type="checkbox"/> | |

DAPのMAC条件の設定

2. 02_dap_testという名前の2番目のDAPを設定します。

Edit Dynamic Access Policy

Policy Name: 02_dap_test

Description: _____ ACL Priority: 0

Selection Criteria
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values... and the following endpoint attributes are satisfied.

| AAA Attribute | Operation/Value | Endpoint ID | Name/Operation/Value |
|--------------------------|----------------------|---------------|-------------------------------------|
| <u>disco.grouppolicy</u> | <u>= dap_test_gp</u> | <u>device</u> | <u>MAC["0050.5698.e605"] = true</u> |

Advanced

Access/Authorization Policy Attributes
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

| Port Forwarding Lists | Bookmarks | Access Method | Secure Client | Secure Client Custom Attributes |
|--|------------------------------|---------------|-----------------------------------|---------------------------------|
| Action | Network ACL Filters (client) | | Webytype ACL Filters (clientless) | Functions |
| Action: <input checked="" type="radio"/> Continue <input type="radio"/> Quarantine <input type="radio"/> Terminate | | | | |
| Specify the message that will be displayed when this record is selected. | | | | |
| User Message: | <u>02_dap_test</u> | | | |

OK Cancel Help

2番目のDAPの設定

3. 3番目のDAPを03_dap_testという名前で設定します。

Edit Dynamic Access Policy

Policy Name: ACL Priority:

Description:

Selection Criteria
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values... and the following endpoint attributes are satisfied.

| AAA Attribute | Operation/Value | Endpoint ID | Name/Operation/Value |
|-------------------|-----------------|-------------|------------------------------|
| disco.grouppolicy | = dap_test_gp | device | MAC["0050.5698.e609"] = true |

Advanced

Access/Authorization Policy Attributes
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists Bookmarks Access Method Secure Client Secure Client Custom Attributes
 Action Network ACL Filters (client) Webytype ACL Filters (clientless) Functions

Action: Continue Quarantine Terminate

Specify the message that will be displayed when this record is selected.

User Message:

OK Cancel Help

3番目のDAPの設定

4. **more flash:/dap.xml** コマンドを使用して、dap.xmlのDAPレコードの設定を確認します。

ASDMで設定されたDAPレコードの詳細は、dap.xmlとしてASAフラッシュに保存されます。これらの設定が完了すると、3つのDAPレコードがdap.xmlに生成されます。dap.xmlで各DAPレコードの詳細を確認できます。

注：DAPが一致する順序は、dap.xmlでの表示順序です。デフォルトのDAP(DfltAccessPolicy)が最後に一致します。

```
<#root>
```

```
ciscoasa#
```

```
more flash:/dap.xml
```

```
<dapRecordList> <dapRecord> <dapName> <value>
```

```
01_dap_test
```

```
</value> <--- 1st DAP name </dapName> <dapViewsRelation> <value>and</value> </dapViewsRelation> <dapBas
```

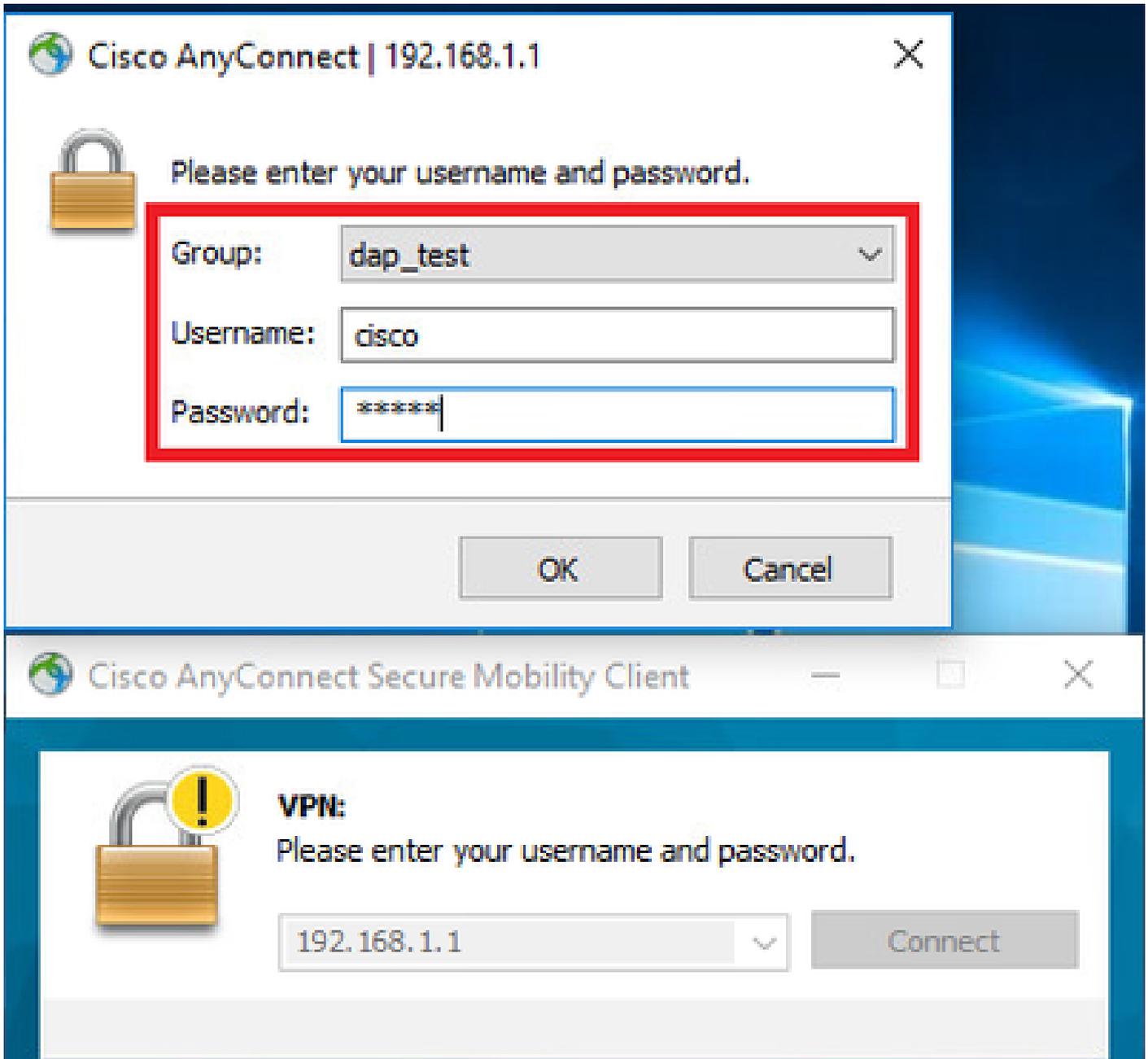
```
dap_test_gp
```

```
</value> <--- 1st DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti
endpoint.device.MAC["0050.5698.e608"]
</name> <--- 1st DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</ope
02_dap_test
</value> <--- 2nd DAP name </dapName> <dapViewsRelation> <value>and</value> </dapViewsRelation> <dapBas
dap_test_gp
</value> <--- 2nd DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti
endpoint.device.MAC["0050.5698.e605"]
</name> <--- 2nd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</ope
03_dap_test
</value> <--- 3rd DAP name </dapName> <dapViewsRelation> <value>and</value> </dapViewsRelation> <dapBas
dap_test_gp
</value> <--- 3rd DAP group policy <operation>EQ</operation> <type>caseless</type> </attr> </dapSelecti
endpoint.device.MAC["0050.5698.e609"]
</name> <--- 3rd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</ope
```

確認

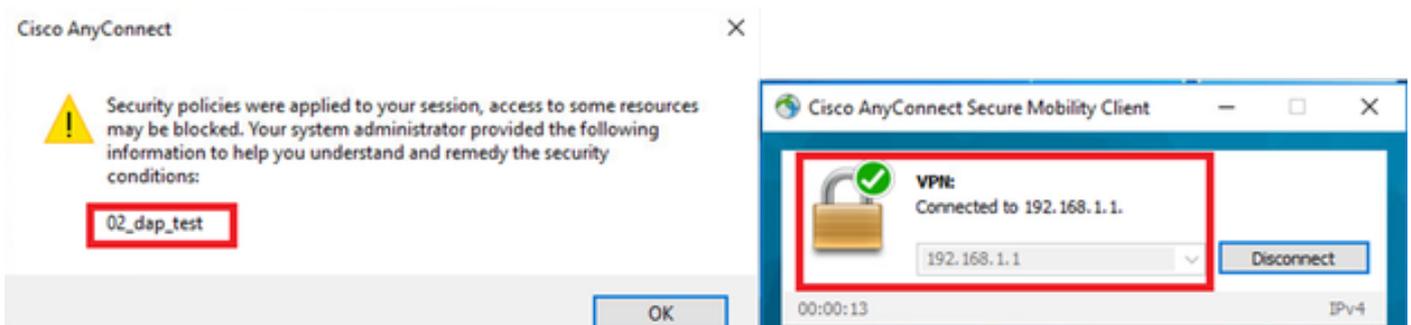
シナリオ1一致するDAPは1つだけです

1. エンドポイントのMACが0050.5698.e605であり、02_dap_testのMAC条件と一致することを確認します。
2. エンドポイントで、Anyconnect接続を実行し、ユーザ名とパスワードを入力します。



ユーザ名とパスワードの入力

3. Anyconnect UIで、02_dap_testが一致していることを確認します。



UIでのユーザメッセージの確認

4. ASA syslogで、02_dap_testが一致していることを確認します。

注：ASAでdebug dap traceが有効になっていることを確認します。

```
<#root>
```

```
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["
```

```
0050.5698.e605
```

```
"] = "true"
```

```
Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:
```

```
Selected DAPs
```

```
: ,
```

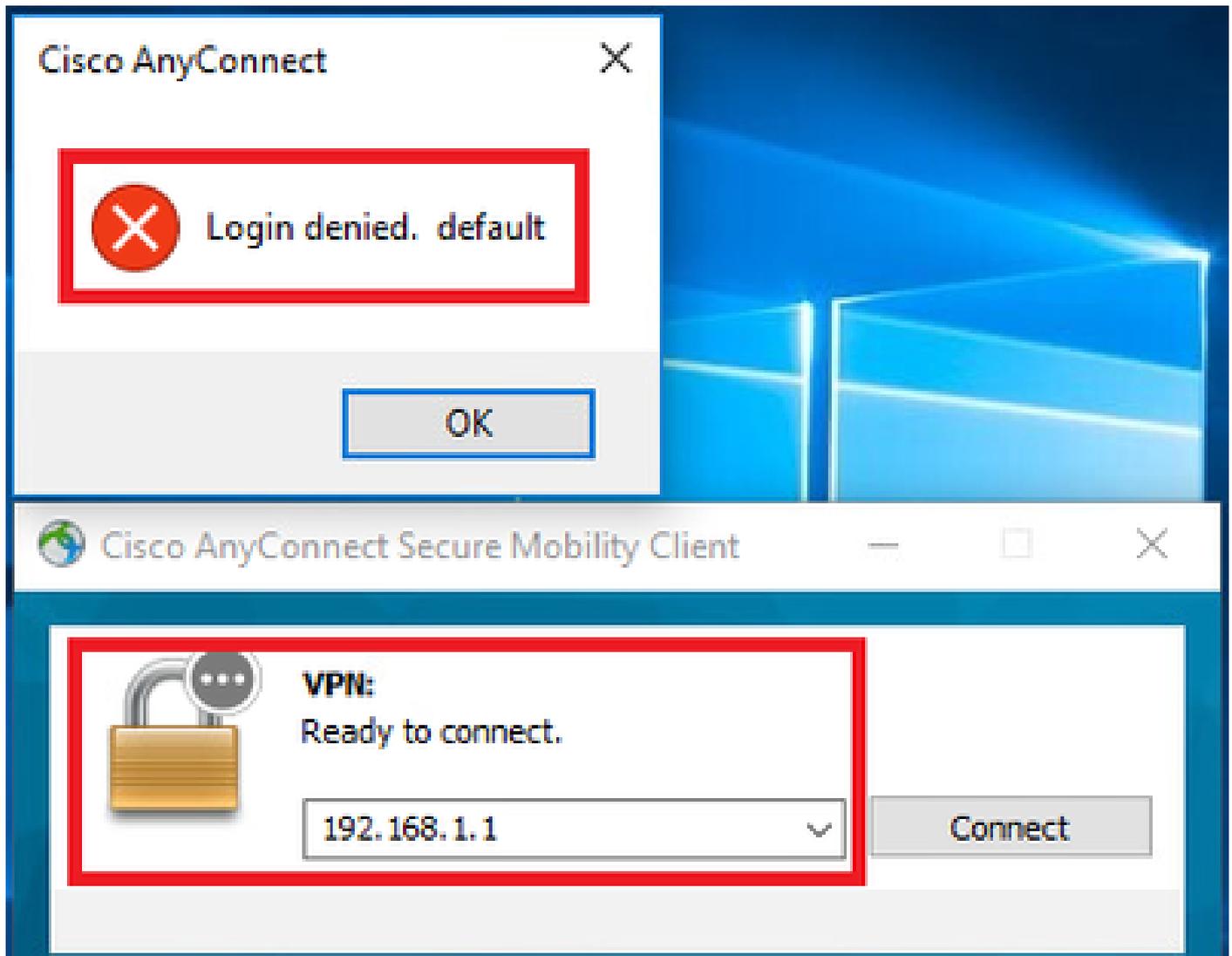
02_dap_test

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Dec 30 2023 11:46:11: %ASA-4-711001: dap_process_selected 1 records

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:

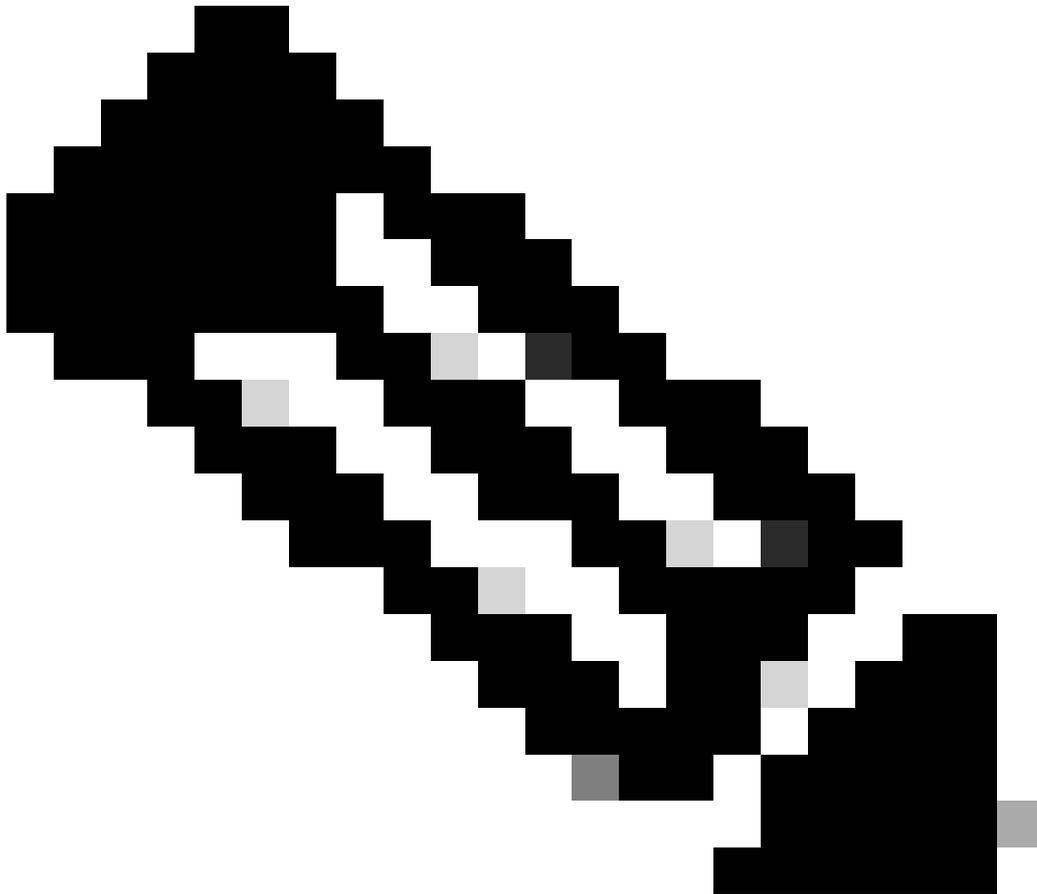
シナリオ2:デフォルトのDAPが一致しています

1. 02_dap_testのendpoint.device.MACの値を、エンドポイントのMACと一致しない0050.5698.e607に変更します。
2. エンドポイントで、Anyconnect接続を実行し、ユーザ名とパスワードを入力します。
3. Anyconnect接続が拒否されたことを確認します。



UIでのユーザメッセージの確認

4. ASA syslogで、DfltAccessPolicyが一致していることを確認します。



注：デフォルトでは、DfltAccessPolicyのアクションはTerminateです。

<#root>

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true"

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001: S
Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Dec 30 2023 12:13:39: %ASA-4-711001: dap_process_select

selected 0 records

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001:

Selected DAPs

:

DfltAccessPolicy

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001: D

シナリオ3:複数のDAP(Action : Continue)が一致

1. 各DAPのアクションと属性を変更します。

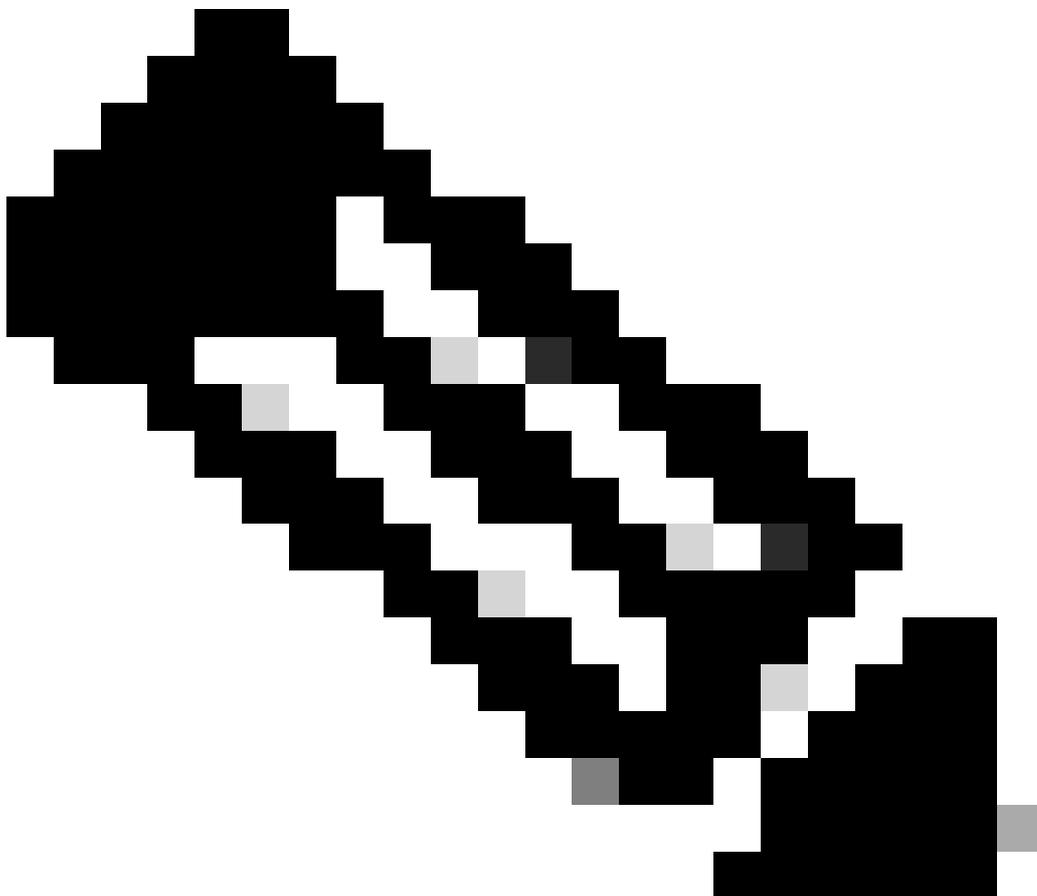
- ・ 01_dap_test:
dapSelection (MACアドレス) = endpoint.device.MAC[0050.5698.e605] = AnyConnectエンドポイントのMAC
アクション=続行
- ・ 02_dap_test:

dapSelection (ホスト名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnectエンドポイントのホスト名
アクション=続行

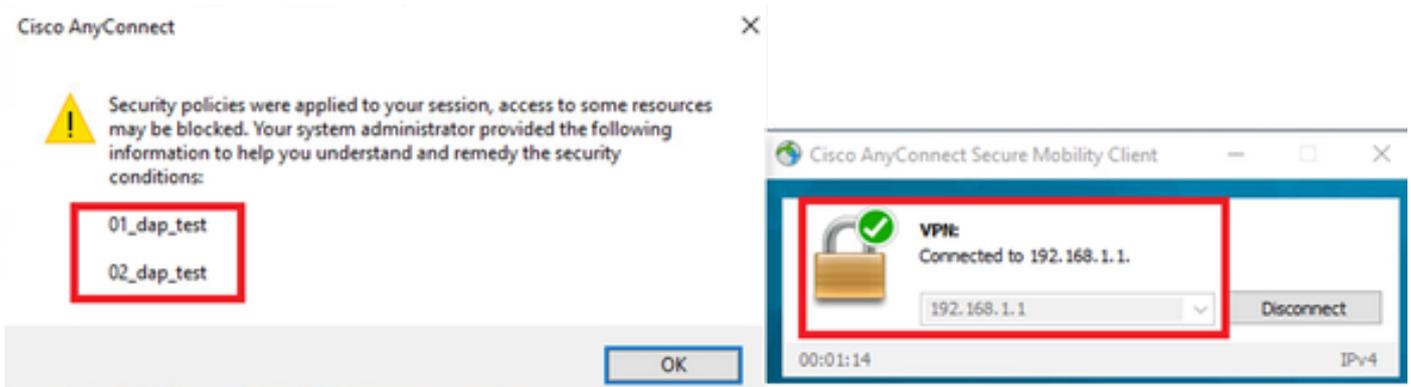
・ 03_dap_test DAPレコードの削除

2. エンドポイントで、Anyconnect接続を実行し、ユーザ名とパスワードを入力します。

3. Anyconnect UIで、2つのDAPがすべて一致していることを確認します



注：接続が複数のDAPに一致する場合、複数のDAPのユーザメッセージが統合され、Anyconnect UIに同時に表示されま
す。



UIでのユーザメッセージの確認

4. ASA syslogで、2つのDAPがすべて一致していることを確認します。

<#root>

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

] = "true"

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: endpoint.device.ho

DESKTOP-VCKHRG1

"

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: S

01_dap_test

,

02_dap_test

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: dap_process_select

selected 2 records

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: D

シナリオ4:複数のDAP(Action :Terminate)が一致しています

1. 01_dap_testのアクションを変更します。

・ 01_dap_test:

dapSelection (MACアドレス) = endpoint.device.MAC[0050.5698.e605] = AnyConnectエンドポイントのMAC

アクション=終了

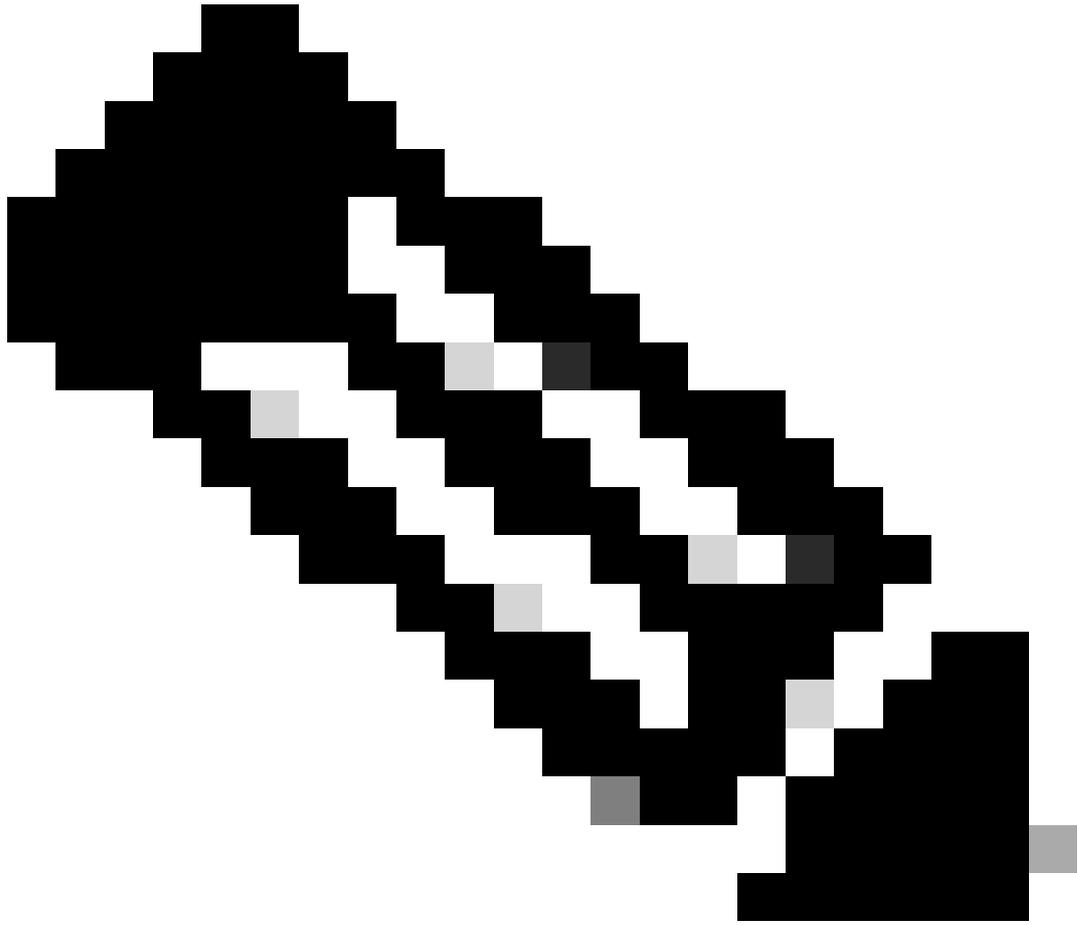
・ 02_dap_test:

dapSelection (ホスト名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnectエンドポイントのホスト名

アクション=続行

2. エンドポイントで、Anyconnect接続を実行し、ユーザ名とパスワードを入力します。

3. Anyconnect UIで、**01_dap_testのみ**が一致していることを確認します。



注：アクションを終了するように設定されたDAPレコードに一致する接続。終了操作の後、後続のレコードが一致しなくなりました。



UIでのユーザメッセージの確認

4. ASA syslogで、01_dap_testのみが一致していることを確認します。

<#root>

```
Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["
```

```
0050.5698.e605
```

```
"] = "true"
```

```
Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.ho
```

```
DESKTOP-VCKHRG1
```

```
" Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:55:37: %ASA-4-711001:
```

```
01_dap_test
```

```
Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: dap_process_selec
```

```
selected 1 records
```

```
Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:55:37: %ASA-4-711001: I
```

一般的なトラブルシューティング

次のデバッグログは、ASAでのDAPの詳細な動作を確認するのに役立ちます。

```
debug dap trace
```

```
debug dap trace errors
```

<#root>

```
Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["0050.5698.e605"] = "true" Feb
```

```
Selected DAPs
```

```
: ,01_dap_test,02_dap_test Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4
```

関連情報

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/108000-dap-deploy-guide.html#toc-hId-981572249>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。