

ISEポスチャを使用したAnyconnectセキュアリモートアクセスとのDuo SAML SSOの統合

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[Traffic flow](#)

[コンフィギュレーション](#)

[- Duo Adminポータルの設定](#)

[- Duo Access Gateway\(DAG\)の設定](#)

[-ASA の設定](#)

[-ISE 設定](#)

[確認](#)

[ユーザ エクスペリエンス](#)

[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、Duo SAML SSOと適応型セキュリティアプライアンス(ASA)のCisco AnyConnectセキュアモバイルクライアントアクセスを統合し、Cisco ISEを活用して詳細なポスチャアセスメントを行うための設定例について説明します。Duo SAML SSOは、Duo Access Gateway(DAG)を使用して実装されます。DAGは、初期ユーザ認証ではActive Directoryと通信し、多要素認証ではDuo Security (クラウド)と通信します。Cisco ISEは、ポスチャ評価を使用してエンドポイント検証を行うための認証サーバとして使用されます。

著者 : Cisco HTTPSエンジニア、Dinesh MoudgilおよびPulkit Saxena

前提条件

要件

このドキュメントでは、ASAが完全に動作していて、Cisco Adaptive Security Device Manager(ASDM)またはコマンドラインインターフェイス(CLI)で設定を変更できるように設定されていることを前提としています。


次の項目に関する知識があることが推奨されます。

- Duo Access GatewayとDuo Securityの基礎
- ASAでのリモートアクセスVPN設定に関する基本的な知識
- ISEサービスとポスチャサービスに関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

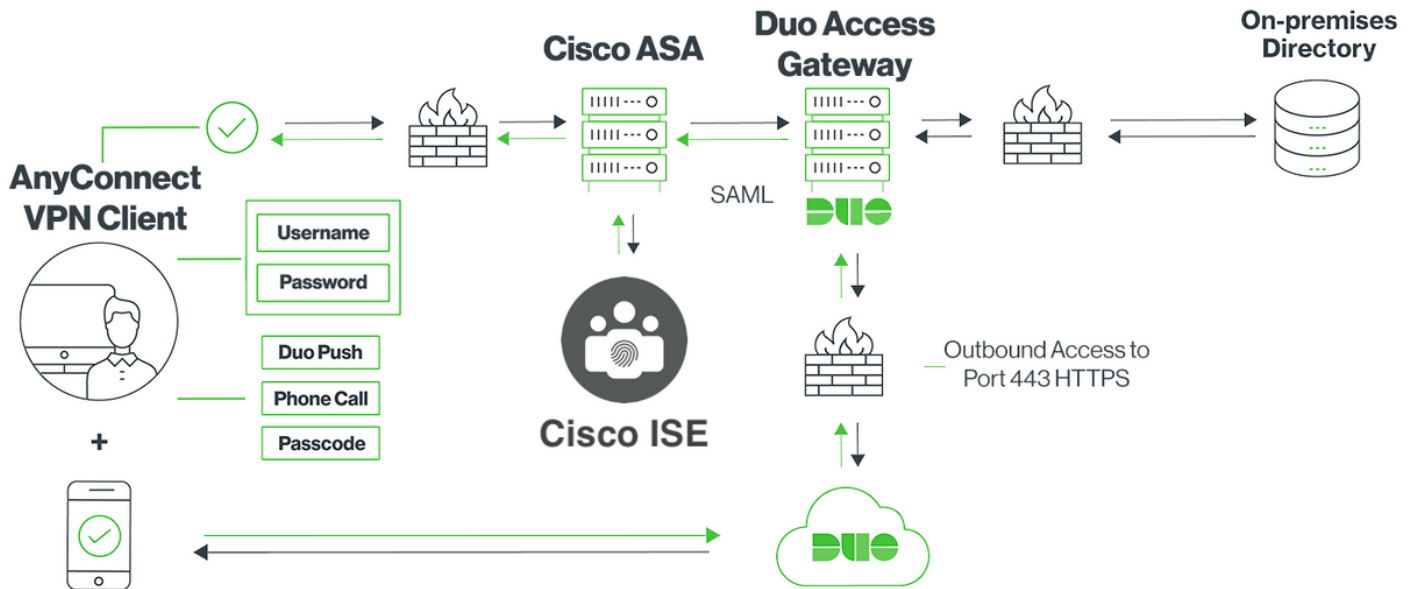
- Cisco適応型セキュリティアプライアンスソフトウェアバージョン9.12(3)12
- Duoアクセスゲートウェイ
- Duo Security
- Cisco Identity Services Engine(ISE)バージョン2.6以降
- AnyConnectバージョン4.8.03052が稼働するMicrosoft Windows 10

 注：この実装で使用されるAnyConnect組み込みブラウザでは、各リリースの9.7(1)24、9.8(2)28、9.9(2)1以降のバージョン、およびAnyConnectバージョン4.6以降でASAが必要です。

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。


設定

ネットワーク図



Traffic flow

1. AnyconnectクライアントがCisco ASAへのSSL VPN接続を開始する
2. Duo Access Gateway(DAG)によるプライマリ認証用に設定されたCisco ASAは、SAML認証用にAnyconnectクライアントの組み込みブラウザをDAGにリダイレクトします
3. AnyconnectクライアントがDuo Access Gatewayにリダイレクトされる
4. AnyConnectクライアントがクレデンシャルを入力すると、SAML認証要求が作成され、Cisco ASAからDuo Access Gatewayに発行されます
5. Duo Access Gatewayは、オンサイトのActive Directoryとの統合を活用して、Anyconnectクライアントのプライマリ認証を実行します
6. プライマリ認証が成功すると、Duo Access GatewayはTCPポート443経由でDuo Securityに要求を送信し、二要素認証を開始します
7. AnyConnectクライアントに「Duo Interactive Prompt」が表示され、ユーザは任意の方式（プッシュまたはパスコード）を使用してDuoの2要素認証を完了します
8. Duo Securityは認証応答を受信し、Duo Access Gatewayに情報を返します
9. 認証応答に基づいて、Duo Access GatewayはSAMLアサーションを含むSAML認証応答を構築し、Anyconnectクライアントに応答します
10. AnyconnectクライアントがCisco ASAとのSSL VPN接続の認証に成功する
11. 認証が成功すると、Cisco ASAはCisco ISEに許可要求を送信します

 注:Duo Access Gatewayは必要な認証を提供するため、Cisco ISEは許可専用を設定されています

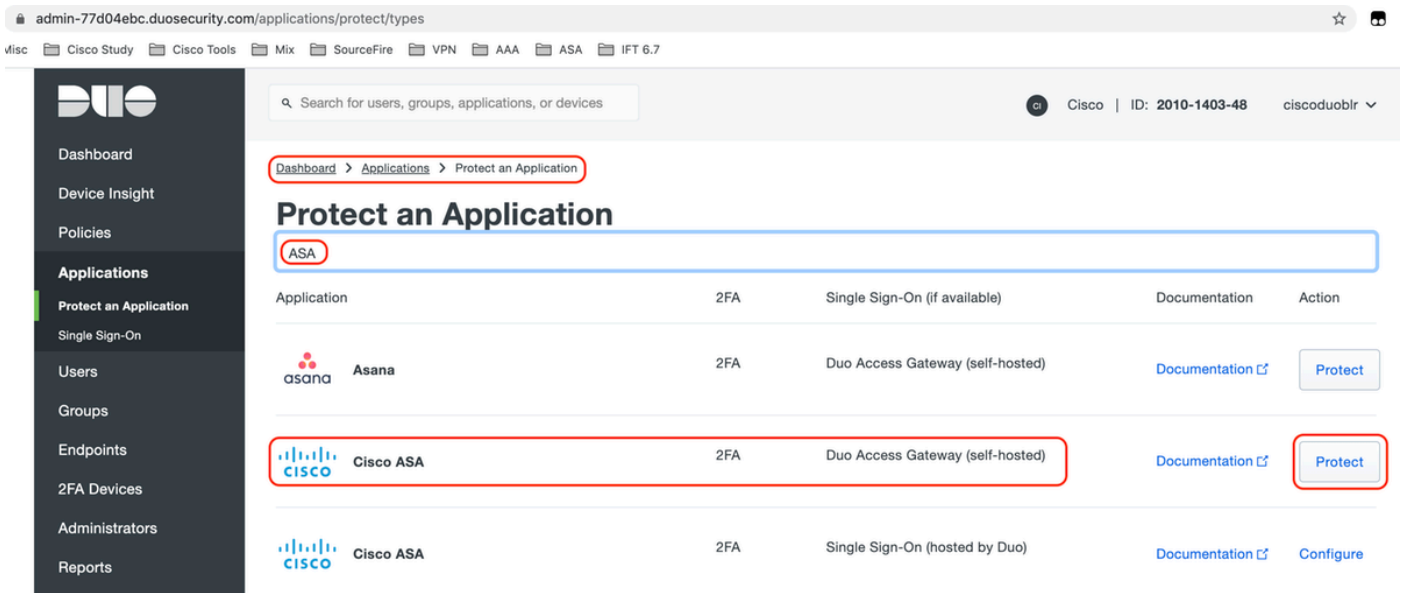
12. Cisco ISEが許可要求を処理し、クライアントポスチャステータスが不明であるため、Cisco ASA経由のAnyconnectクライアントへの制限付きアクセスでポスチャリダイレクトを返します
13. Anyconnectクライアントにコンプライアンスモジュールがない場合は、ポスチャ評価を進めるためにダウンロードするように求められます
14. Anyconnectクライアントにコンプライアンスモジュールがある場合、Cisco ASAとのTLS接続が確立され、ポスチャフローが開始されます
15. ISEで設定されたポスチャ条件に応じて、ポスチャチェックが実行され、詳細がAnyconnectクライアントからCisco ISEに送信されます
16. クライアントポスチャステータスが不明から準拠が変わると、Cisco ISEからCisco ASAに認可変更(CoA)要求が送信され、クライアントへのフルアクセスが許可され、VPNが完全に確立されます

コンフィギュレーション




- Duo Adminポータルの設定

このセクションでは、Duo Admin PortalでASAアプリケーションを設定します。

1. 「Duo Admin Portal」にログインし、「Applications > Protect an Application」に移動して、保護タイプが「2FA with Duo Access Gateway, self-hosted」の「ASA」を検索します。右端の「Protect」をクリックして、Cisco ASAを設定します



The screenshot shows the Duo Admin Portal interface. The breadcrumb navigation is "Dashboard > Applications > Protect an Application". The search bar contains "ASA". The table below lists applications:

Application	2FA	Single Sign-On (if available)	Documentation	Action
 Asana	2FA	Duo Access Gateway (self-hosted)	Documentation	Protect
 Cisco ASA	2FA	Duo Access Gateway (self-hosted)	Documentation	Protect
 Cisco ASA	2FA	Single Sign-On (hosted by Duo)	Documentation	Configure

2. 「サービスプロバイダー」の下で、保護されるアプリケーションであるASAに対して次の属性を設定します

ベースURL	firebird.cisco.com
トンネルグループ	TG_SAML
メール属性	sAMAccountName,mail

ページの下部にある「保存」をクリックします

The screenshot shows the Cisco Duo Admin Center interface for configuring a Cisco ASA application. The left sidebar contains navigation options like 'Device Insight', 'Policies', 'Applications', 'Users', 'Groups', 'Endpoints', '2FA Devices', 'Administrators', 'Reports', 'Settings', 'Billing', 'Need Help?', 'Account ID', 'Deployment ID', and 'Helpful Links'. The main content area is titled 'Cisco ASA - Duo Access Gateway' and includes an 'Authentication Log' and 'Remove Application' link. Below the title is a 'Configure Cisco ASA' section with a 'Reset Secret Key' button. A message box states: 'To set up this application, install the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions. Next step: Download your configuration file.' The 'Service Provider' configuration form has the following fields: 'Base URL' (firebird.cisco.com), 'Tunnel Group' (TG_SAML), 'Custom attributes' (checked), and 'Mail attribute' (sAMAccountName,mail). A 'Save Configuration' button is at the bottom.

このドキュメントの残りの設定ではデフォルトのパラメータを使用しますが、お客様の要件に基づいて設定できます。

この時点で、アプリケーションの名前をデフォルト値から変更したり、セルフサービスを有効にしたり、グループポリシーを割り当てたりするなど、新しいSAMLアプリケーションの追加設定を調整できます。

3. [構成ファイルのダウンロード]リンクをクリックして、Cisco ASAアプリケーションの設定を取得します (JSONファイルとして)。このファイルは、後の手順でDuo Access Gatewayにアップロードされます

Device Insight

Policies

Applications

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Administrators

Reports

Settings

Billing

Need Help?

Chat with Tech Support

Email Support

Call us at 1-855-386-2884

Account ID

2010-1403-48

Deployment ID

DU057

Helpful Links

Documentation

Cisco ASA - Duo Access Gateway

[Authentication Log](#) | [Remove Application](#)

[Reset Secret Key](#)

Configure Cisco ASA

To set up this application, install the Duo Access Gateway and then configure your service provider. [View Cisco ASA SAML SSO instructions](#)

Next step: [Download your configuration file](#)

Service Provider

Base URL

Enter the Cisco ASA Base URL.

Tunnel Group

Enter the Tunnel Group you are protecting with SSO.

Custom attributes Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute

The attribute containing the email address of the user.

[Save Configuration](#)

4. 「Dashboard > Applications」の下に、新しく作成されたASAアプリケーションが次の図のように表示されます。

admin-77d04ebc.duosecurity.com/applications

Cisco Study | Cisco Tools | Mix | SourceFire | VPN | AAA | ASA | IFT 6.7

DUO

Dashboard

Device Insight

Policies

Applications

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscoduobr

[Dashboard](#) > [Applications](#)

Applications

[SSO Setup Guide](#) | [Protect an Application](#)

[Export](#) |

Name	Type	Application Policy	Group Policies
Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway		

1 total

5. 図に示すように、「Users > Add User」に移動します。

Anyconnectリモートアクセス認証に使用する「duouser」という名前のユーザを作成し、エンドユーザデバイスでDuo Mobileをアクティブにします

Dashboard

Device Insight

Policies

Applications

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

Endpoints

Search for users, groups, applications, or devices

Dashboard > Users > Add User

Add User

Adding Users

Most applications allow users to enroll themselves after they complete primary authentication.

[Learn more about adding users](#)

Username:

Should match the primary authentication username.

図に示すように電話番号を追加するには、「電話を追加」オプションを選択します。

Dashboard

Device Insight

Policies

Applications

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

Endpoints

2FA Devices

Search for users, groups, applications, or devices

Dashboard > Users > duouser > Add Phone

Add Phone

[Learn more about Activating Duo Mobile](#)

Type: Phone Tablet

Phone number: [Show extension field](#)

Optional. Example: "+91 91234 56789"

特定のユーザーの「Duo Mobile」をアクティブにします

Device Info

[Learn more about Activating Duo Mobile](#)



Not using Duo Mobile

[Activate Duo Mobile](#)




Model

Unknown

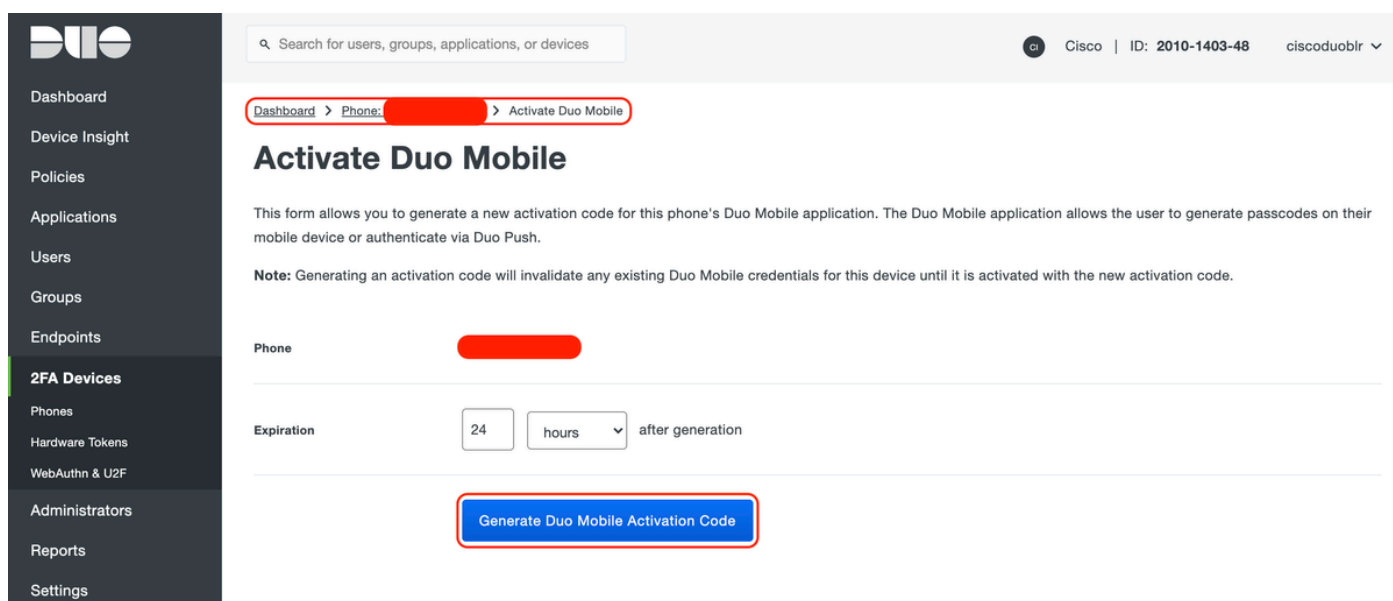


OS

Generic Smartphone

 注：エンドユーザデバイスには「Duo Mobile」をインストールしてください。
[IOSデバイス用Duoアプリケーションの手動インストール](#)
[Androidデバイス向けDuoアプリケーションの手動インストール](#)

図に示すように、「Duo Mobileアクティベーションコードを生成」を選択します。



Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscoduobl

Dashboard > Phone: [redacted] > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: [redacted]

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

次の図に示すように、「SMSで指示を送信」を選択します。

- Dashboard
- Device Insight
- Policies
- Applications
- Users
- Groups
- Endpoints
- 2FA Devices**
- Phones
- Hardware Tokens
- WebAuthn & U2F
- Administrators
- Reports
- Settings
- Billing
- Need Help?
- [Chat with Tech Support](#)
- [Email Support](#)
- Call us at 1-855-386-2884

[Dashboard](#) > [Phone: +91 \[redacted\]](#) > [Activate Duo Mobile](#)

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. activation instructions to the user by SMS.

Phone [redacted]

Installation instructions Send installation instructions via SMS

Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions Send activation instructions via SMS

*To activate the app, tap and open this link with Duo Mobile:
https://m-77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT*

[Send Instructions by SMS](#) or [skip this step](#)

SMSのリンクをクリックすると、Duoアプリがデバイス情報セクションのユーザアカウントにリンクされます (図を参照)。

Dashboard > Phones > Phone: +91 [redacted]

+91 [redacted] Send SMS Passcodes... | [redacted]

Shared phone
This phone is attached to multiple users.

duouser +91 [redacted] **testing 123** +91 [redacted] [Attach a user](#)

Authentication devices can share multiple users

Device Info
[Learn more about Activating Duo Mobile](#)

Using Duo Mobile [Reactivate Duo Mobile](#) **Model** Unknown **OS** Generic Smartphone

- Duo Access Gateway(DAG)の設定

1. Duo Access Gateway(DAG)をネットワーク内のサーバに導入

注：導入に関しては、次の文書に従ってください。

Linux用Duo Access Gateway
<https://duo.com/docs/dag-linux>

Windows用Duo Access Gateway
<https://duo.com/docs/dag-windows>

2. Duo Access Gatewayホームページで、「Authentication Source」に移動します。

3. [ソースの構成]で、Active Directoryの次の属性を入力し、[設定の保存]をクリックします

Configure Sources

Configure authentication source settings below. Changes made to non-active authentication sources will take effect when made active.

Source type	<input type="text" value="Active Directory"/> Specify the authentication source to configure.
Status:	✔ LDAP Bind Succeeded ✔ ldap://10.197.243.110
Server	<input type="text" value="10.197"/> <input type="text" value="389"/> Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separated for failover functionality. For example: ad1.server.com,ad2.server.com,10.1.10.150
Transport type	<input checked="" type="radio"/> CLEAR <input type="radio"/> LDAPS <input type="radio"/> STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.
Attributes	<input type="text" value="sAMAccountName,mail"/> Specify attributes to retrieve from the AD server. For example: sAMAccountName,mail.
Search base	<input type="text" value="CN=Users,DC=dmoudgil,DC=local"/> The DNs which will be used as a base for the search. Enter one per line. They will be searched in the order given.
Search attributes	<input type="text" value="sAMAccountName"/> Specify attributes the username should match against. For example: sAMAccountName,mail.
Search username	<input type="text" value="iseadmin"/> The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only access.
Search password	<input type="password" value="•••••"/> The password corresponding to the search username specified above.
<input type="button" value="Save Settings"/>	

4. [Set Active Source]で、ソース・タイプとして[Active Directory]を選択し、[Set Active Source]をクリックします

Set Active Source

Specify the source that end-users will use for primary authentication.

Source type

- 「Applications」に移動し、「Add Application」サブメニューの「Configuration file」セクションのDuo Admin Consoleからダウンロードした.jsonファイルをアップロードします。対応する.jsonファイルは、Duo Admin Portal Configurationのステップ3でダウンロードされました

Applications


Add Application

Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here.

Configuration file

- アプリケーションが正常に追加されると、「アプリケーション」サブメニューに表示されません

Applications

Name	Type	Logo	
<input type="text" value="Cisco ASA - Duo Access Gateway"/>	Cisco ASA		<input type="button" value="Delete"/>

- 「Metadata」サブメニューで、XMLメタデータとIdP証明書をダウンロードし、後でASAで設定する次のURLをメモします
 - SSOのURL
 - ログアウトURL
 - エンティティID
 - エラーURL

Metadata Recreate Certificate

Information for configuring applications with Duo Access Gateway. [Download XML metadata](#)

Certificate /C=US/ST=MI/L=Ann Arbor/O=Duo Security, Inc. [Download certificate](#)

Expiration 2030-04-30 18:57:14

SHA-1 Fingerprint [REDACTED]

SHA-256 Fingerprint [REDACTED]

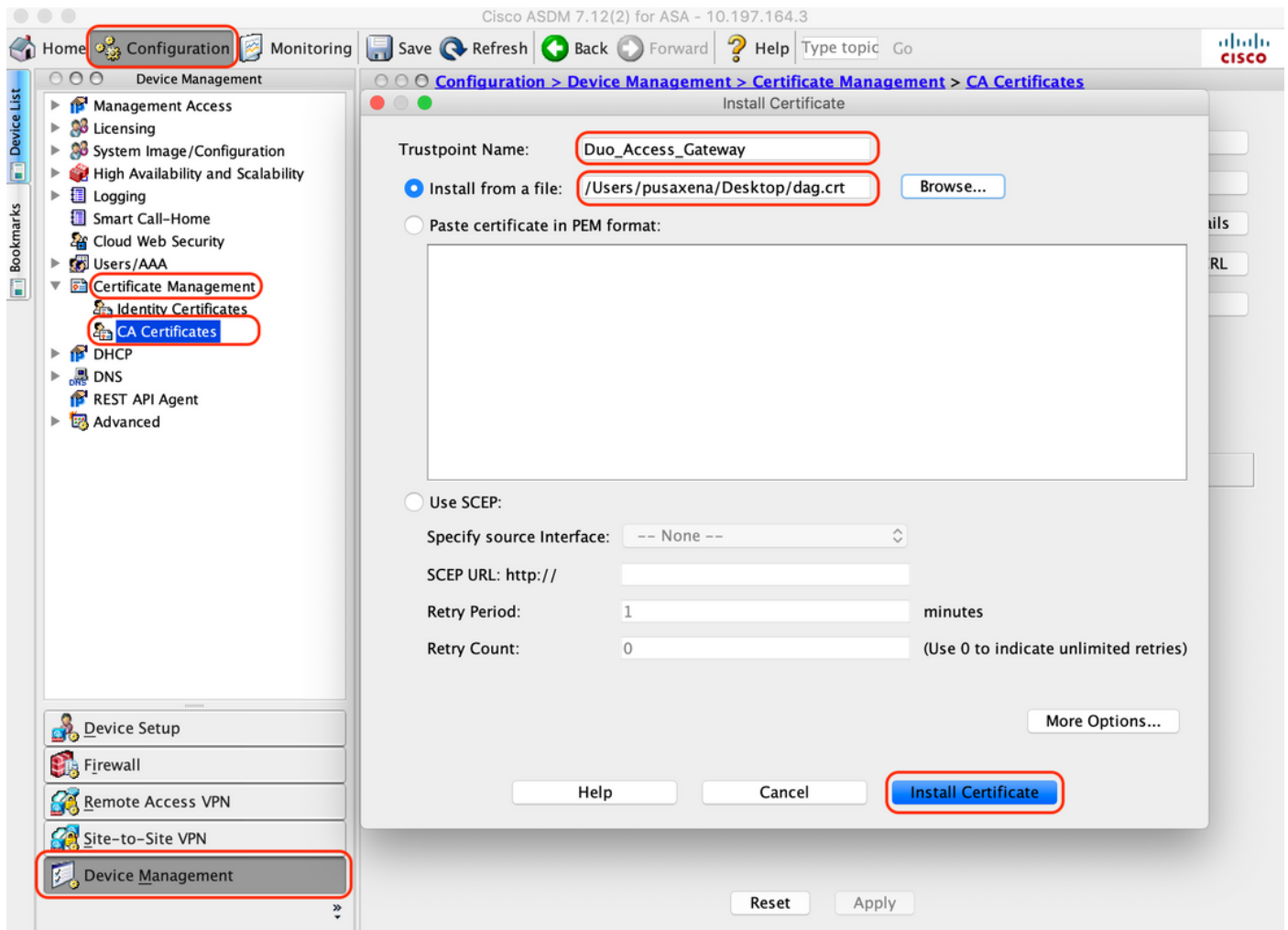
SSO URL	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
Logout URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer
Entity ID	https://explorer.cisco.com/dag/saml2/idp/metadata.php
Error URL	https://explorer.cisco.com/dag/module.php/duosecurity/du

-ASA の設定

このセクションでは、SAML IDP認証用のASAの設定と基本的なAnyConnect設定について説明します。このドキュメントでは、ASDMの設定手順とCLIの実行コンフィギュレーションについて概説します。

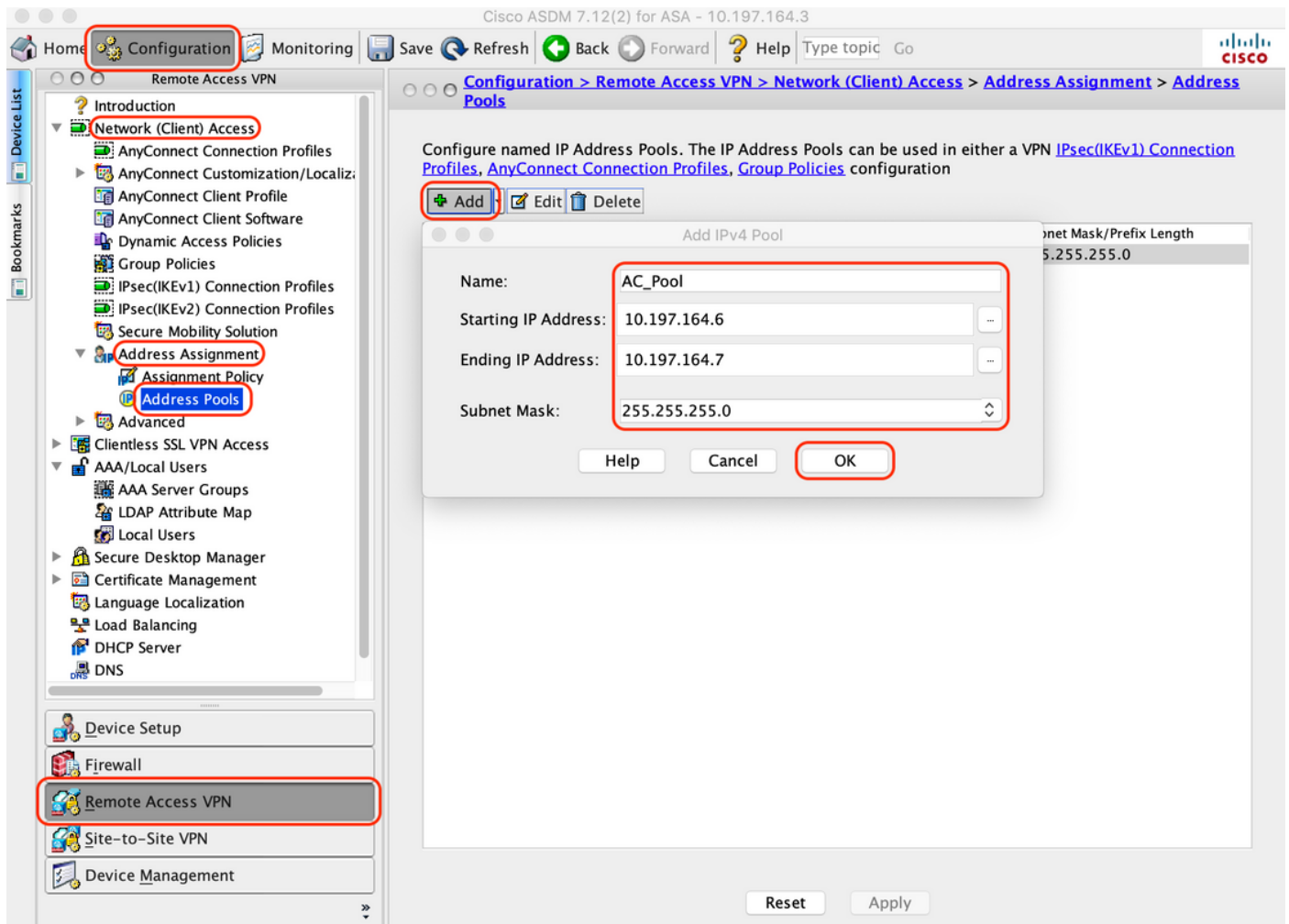
1. Duo Access Gateway証明書のアップロード

- A. 「Configuration > Device Management > Certificate Management > CA Certificates」に移動し、「Add」をクリックします。
- B. 「証明書のインストール」ページで、トラストポイント名Duo_Access_Gatewayを設定します。
- C. [参照]をクリックしてDAG証明書に関連付けられたパスを選択し、選択したら[証明書のインストール]をクリックします



2. AnyConnectユーザ用のIPローカルプールの作成

Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Poolsの順に選択し、Addをクリックします。



3. AAAサーバグループの設定

A. このセクションでは、AAAサーバグループを設定し、認可を実行する特定のAAAサーバの詳細を指定します

B. 「Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups」に移動し、「Add」をクリックします。

Home Configuration Monitoring Save Refresh Back Forward Help Type topic Go

Remote Access VPN

Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts

Add AAA Server Group

AAA Server Group: ISE

Protocol: RADIUS

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

Enable interim accounting update

Update Interval: 24 Hours

Enable Active Directory Agent mode

ISE Policy Enforcement

Enable dynamic authorization

Dynamic Authorization Port: 1700

Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

Help Cancel OK

Find: Match Case

LDAP Attribute Map

Reset Apply

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

C.同じページの「Servers in the Selected group」セクションで「Add」をクリックし、AAAサーバのIPアドレスの詳細を入力します

Cisco ASDM 7.12(2) for ASA - 10.197.164.3

Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ISE	RADIUS	Single	Depletion	10	3
LOCAL	LOCAL				

Add AAA Server

Server Group: ISE
Interface Name: outside
Server Name or IP Address: 10.106.44.77
Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645
Server Accounting Port: 1646
Retry Interval: 10 seconds
Server Secret Key:
Common Password:
ACL Netmask Convert: Standard
Microsoft CHAPv2 Capable:

SDI Messages
Message Table

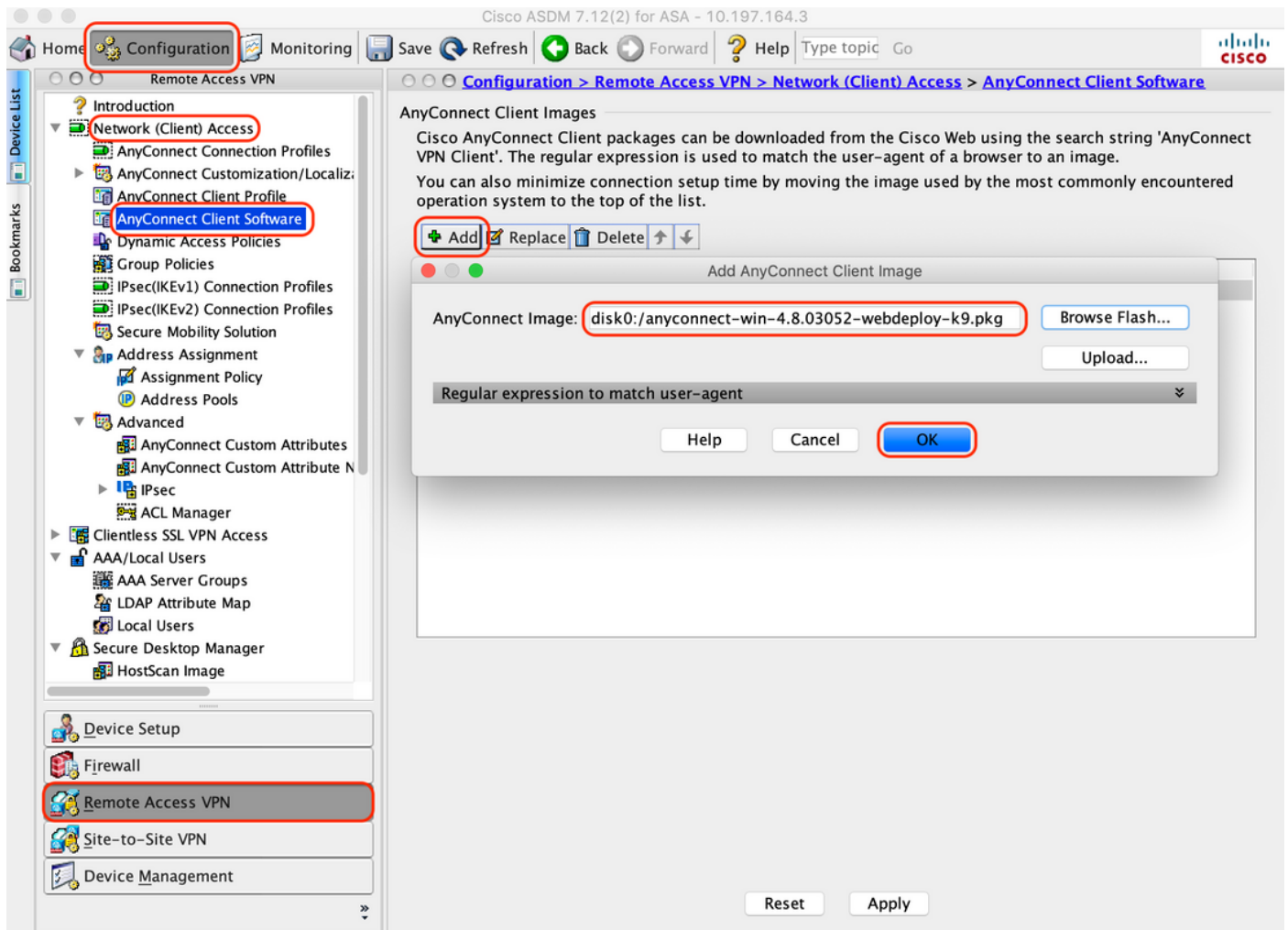
Help Cancel OK

Reset Apply

4. AnyConnectクライアントソフトウェアのマッピング

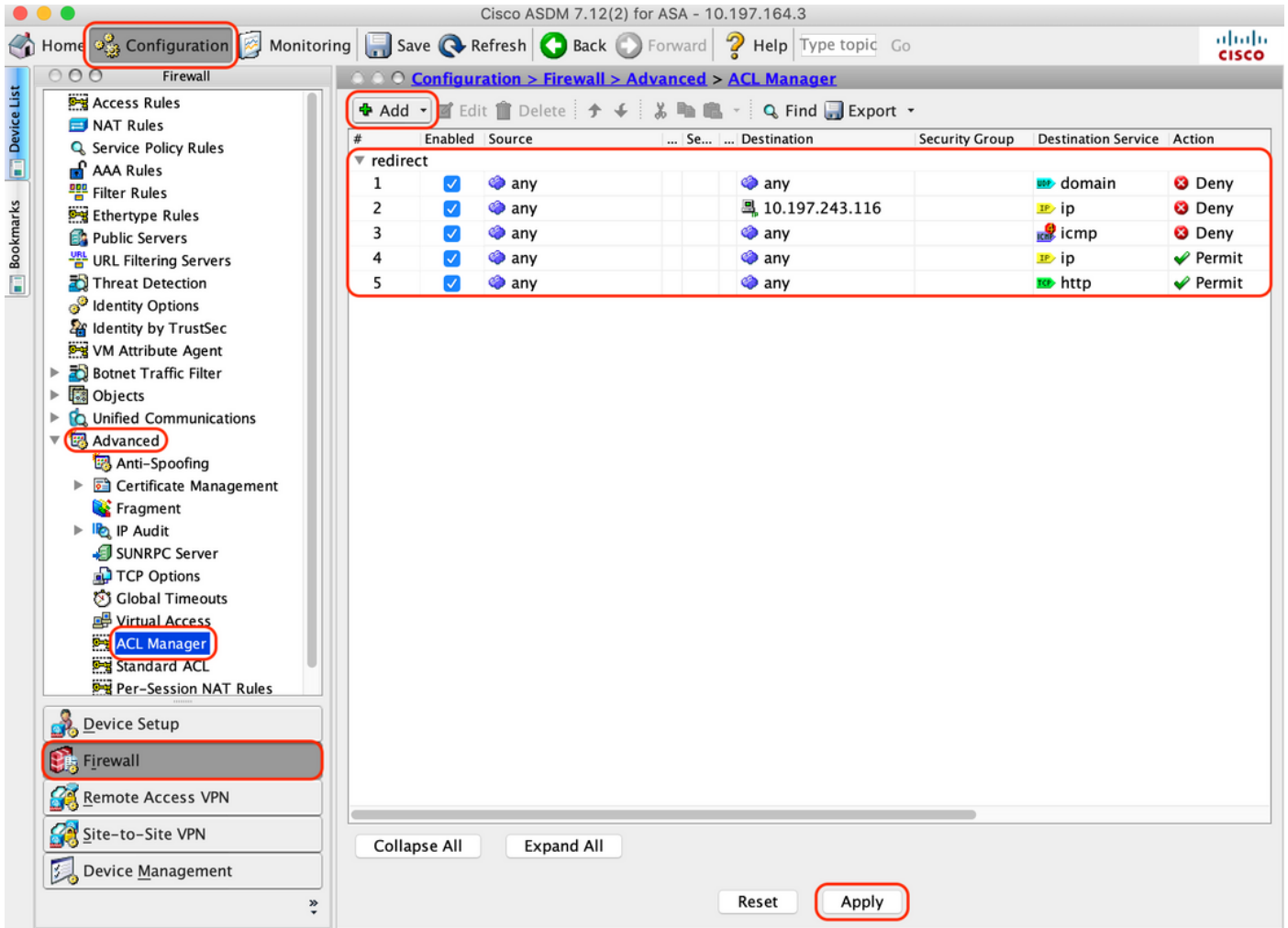
A. WebVPNに使用するAnyConnectクライアントソフトウェアwebdeployイメージ4.8.03052 for windowsをマッピングします

B. 「Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software」に移動し、「Add」をクリックします。



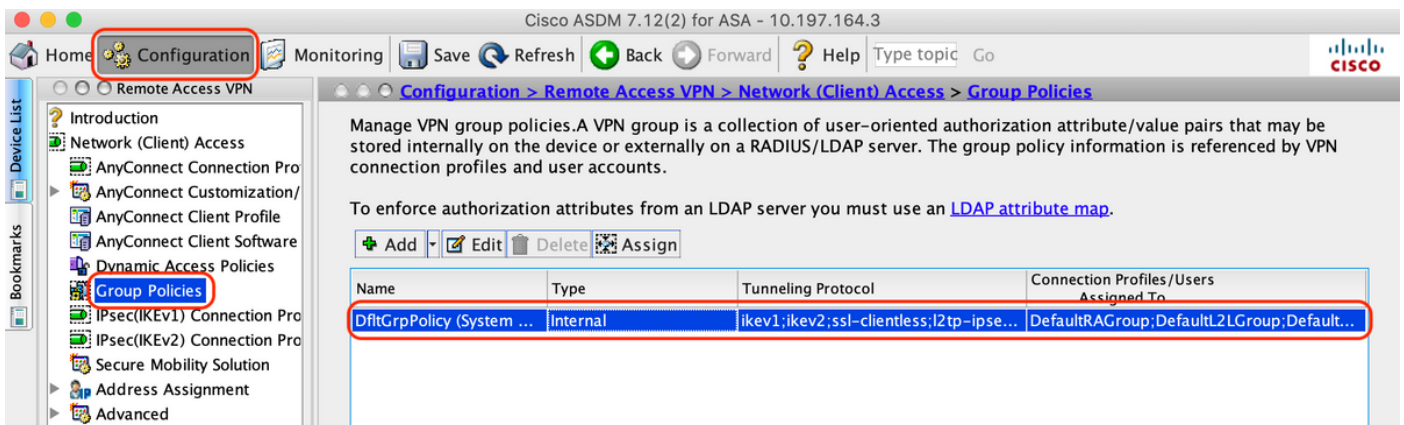
5. ISEからプッシュされるリダイレクトACLの設定

A. 「Configuration > Firewall > Advanced > ACL Manager」に移動し、AddをクリックしてリダイレクトACLを追加します。設定されたエントリは次のようになります。



6. 既存のグループポリシーの検証

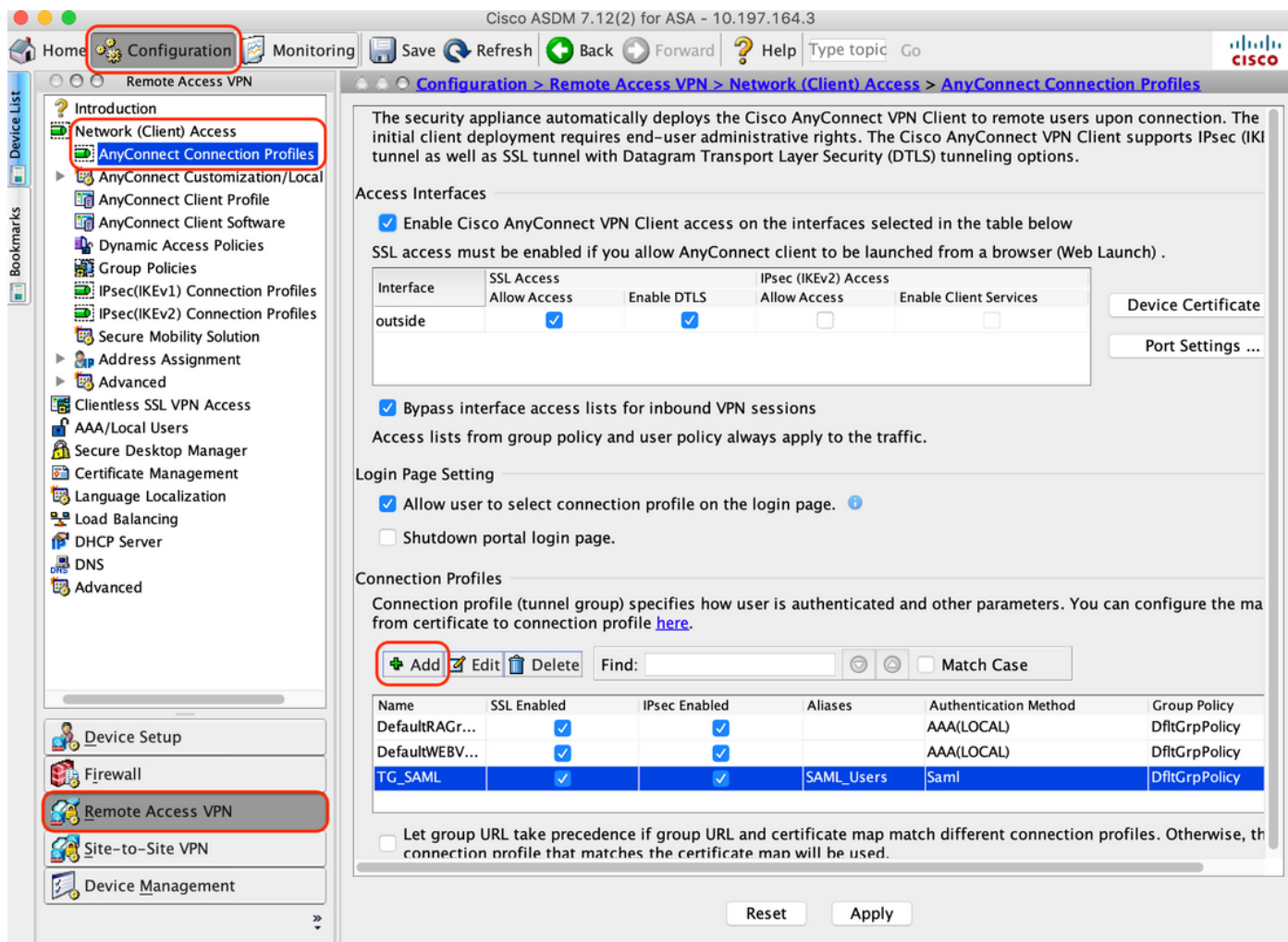
A. この設定はデフォルトのグループポリシーを使用します。これは、「Configuration > Remote Access VPN > Network (Client) Access > Group Policies」で確認できます。



7. 接続プロファイルの設定

A. AnyConnectユーザが接続する新しい接続プロファイルを作成します

B. 「Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles」に移動し、「Add」をクリックします。



C. 接続プロファイルに関連付けられた次の詳細を設定します。

[名前(Name)]	TG_SAML
エイリアス	SAML_Users
メソッド	SAML
AAAサーバグループ	Local
クライアントアドレスプール	AC_プール
グループ ポリシー	DfltGrpPolicy

Basic
▶ Advanced

Name: TG_SAML

Aliases: SAML_Users

Authentication

Method: SAML

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : <https://explorer.cisco.com/dag/saml2/idp/metadata.php> Manage...

Client Address Assignment

DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: AC_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: DfltGrpPolicy Manage...

(Following fields are linked to attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

Find: Next Previous

Help Cancel OK

D.同じページで、次に示すようにSAML IDプロバイダーの詳細を設定します。

IDP インテ イテ イID	https://explorer.cisco.com/dag/saml2/idp/metadata.php
サイ ン イン URL	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
サイ ン アウト URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SSOService.php
ベー ス URL	https://firebird.cisco.com

E. 「Manage > Add」 をクリックします。

Add SSO Server

IDP Entity ID:

Settings

Sign In URL:

Sign Out URL:

Base URL:

Identity Provider Certificate:

Service Provider Certificate:

Request Signature:

Request Timeout: seconds (1-7200)

Enable IdP only accessible on Internal Network

Request IdP re-authentication at login

F. 接続プロファイルのAdvancedセクションで、認可用のAAAサーバを定義します

「Advanced > Authorization」に移動し、「Add」をクリックします。

Edit AnyConnect Connection Profile: TG_SAML

Basic

Advanced

General

Client Addressing

Authentication

Secondary Authentication

Authorization

Accounting

Group Alias/Group URL

Authorization Server Group

Server Group:

Users must exist in the authorization database to connect

Interface-specific Authorization Server Groups

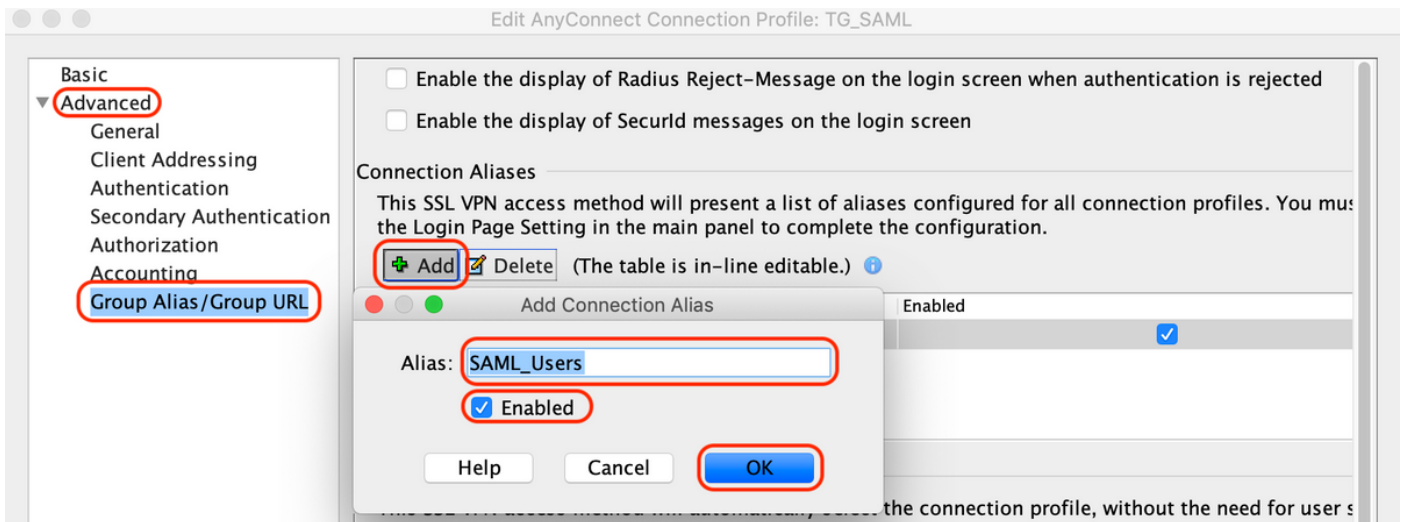
Assign Authorization Server Group to Interface

Interface:

Server Group:

G. Group Aliasで、接続エイリアスを定義します

「Advanced > Group Alias/Group URL」に移動し、「Add」をクリックします。



H.これでASAの設定は完了です。コマンドラインインターフェイス(CLI)でも同じことが次のように表示されます

```

!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!-----Client pool configuration-----
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!-----Redirect Access-list-----
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
!
!-----AAA server configuration-----
!
aaa-server ISE protocol radius
  authorize-only
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
  key *****
!
!-----Configure Trustpoint for Duo Access Gateway Certificate-----
!
crypto ca trustpoint Duo_Access_Gateway
  enrollment terminal
  crl configure
!
!-----Configure Trustpoint for ASA Identity Certificate-----
!
crypto ca trustpoint ID_CERT
  enrollment terminal
  fqdn firebird.cisco.com

```

```

subject-name CN=firebird.cisco.com
ip-address 10.197.164.3
keypair ID_RSA_KEYS
no ca-check
cr1 configure
!
!-----Enable AnyConnect and configuring SAML authentication-----
!
webvpn
enable outside
hsts
enable
max-age 31536000
include-sub-domains
no preload
anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
anyconnect enable
saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
url sign-in https://explorer.cisco.com/dag/saml2/idp/SSOService.php
url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
base-url https://firebird.cisco.com
trustpoint idp Duo_Access_Gateway
trustpoint sp ID_CERT
no signature
no force re-authentication
timeout assertion 1200
tunnel-group-list enable
cache
disable
error-recovery disable
!
!-----Group Policy configuration-----
!
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
!
!-----Tunnel-Group (Connection Profile) Configuraiton-----
!
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
address-pool AC_Pool
authorization-server-group ISE
accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
authentication saml
group-alias SAML_Users enable
saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
!

```

-ISE 設定

1.ネットワークデバイスとしてのCisco ASAの追加

[Administration] > [Network Resources] > [Network Devices]で、[Add]をクリックします。
ネットワークデバイスの名前、関連するIPアドレスを設定し、「Radius Authentication Settings」
で「Shared Secret」を設定して「Save」をクリックします。

Network Devices

* Name
Description

IP Address /

* Device Profile
Model Name
Software Version

* Network Device Group

Location
IPSEC
Device Type



▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**
* Shared Secret
Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required
Shared Secret
CoA Port
Issuer CA of ISE Certificates for CoA
DNS Name

General Settings

Enable KeyWrap
* Key Encryption Key
* Message Authenticator Code Key
Key Input Format ASCII HEXADECIMAL



▶ TACACS Authentication Settings



▶ SNMP Settings



▶ Advanced TrustSec Settings

2.最新のポスチャアップデートをインストールする

「Administration」 > 「System」 > 「Settings」 > 「Posture」 > 「Updates」 に移動し、「Update Now」 をクリックします。

Posture Updates

Web Offline

* Update Feed URL

Proxy Address ⓘ

Proxy Port HH MM SS

Automatically check for updates starting from initial delay every hours ⓘ

▼ Update Information

Last successful update on	2020/05/07 15:15:05 ⓘ
Last update status since ISE was started	No update since ISE was started. ⓘ
Cisco conditions version	224069.0.0.0
Cisco AV/AS support chart version for windows	171.0.0.0
Cisco AV/AS support chart version for Mac OSX	91.0.0.0
Cisco supported OS version	41.0.0.0

3. ISEでのコンプライアンスモジュールとAnyConnectヘッドエンド導入パッケージのアップロード

「Policy > Policy Elements > Results > Client Provisioning > Resources」の順に移動します。[追加]をクリックし、ファイルをローカルワークステーションからフェッチするか、シスコサイトからフェッチするかに基づいて、[ローカルディスクのエージェントリソース]または[シスコサイトのエージェントリソース]を選択します。

この場合、カテゴリの下のローカルワークステーションからファイルをアップロードするには、「Cisco Provided Packages」を選択し、「Browse」をクリックして必要なパッケージを選択し、「Submit」をクリックします。

このドキュメントでは、コンプライアンスモジュールとして「anyconnect-win-4.3.1012.6145-

isecompliance-webdeploy-k9.pkg」を、AnyConnectヘッドエンド導入パッケージとして「anyconnect-win-4.8.03052-webdeploy-k9.pkg」を使用しています。

[Agent Resources From Local Disk](#) > [Agent Resources From Local Disk](#)

Agent Resources From Local Disk

Category ⓘ

Browse...

▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.8.30...	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie...

4. AnyConnectポスチャプロファイルの作成

A. 「Policy > Policy Elements > Results > Client Provisioning > Resources」の順に選択します。
[Add]をクリックし、[AnyConnect Posture Profile]を選択します。

B. Anyconnectポスチャプロファイルの名前を入力し、サーバ名ルールでサーバ名を「*」に設定して、「保存」をクリックします。

ISE Posture Agent Profile Settings > Anyconnect Posture Profile

* Name:

Description:

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	<input type="text" value="60"/> secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	<input type="text" value="4"/>	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host	<input type="text"/>	IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
* Server name rules	<input type="text" value="*"/>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com*
Call Home List	<input type="text"/>	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPAddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

5. Anyconnect設定の作成

A. 「Policy > Policy Elements > Results > Client Provisioning > Resources」の順に選択します。
[Add]をクリックし、[AnyConnect Configuration]を選択します。

B. AnyConnectパッケージを選択し、構成名を入力し、必要なコンプライアンスモジュールを選択します。

C. 「AnyConnect Module Selection」で、「Diagnostic and Reporting Tool」にチェックマークを付けます。

D. 「プロファイルの選択」で「ポスチャプロファイル」を選択し、「保存」をクリックします。

* Select AnyConnect Package

* Configuration Name

Description:

DescriptionValue

* Compliance Module

Notes

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

Network Visibility

Umbrella Roaming Security

Customer Feedback

6. クライアントプロビジョニングポリシーの作成

A. Policy > Client Provisioningの順に移動します

B. 「編集」をクリックし、「上にルールを挿入」を選択します

C. ルール名を入力し、必要なオペレーティングシステムを選択し、結果（「エージェント」>「エージェント構成」内）で、ステップ5で作成した「AnyConnect構成」を選択し、「保存」をクリックします

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Client Provisioning Policy
 Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows_10	If Any	and Windows 10 (All)	and Condition(s)	then AnyConnect Configuration
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOS X 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

Save Reset

7. ポスチャ条件の作成

A. “Policy > Policy Elements > Conditions > Posture > File Condition”に移動します。

B. [追加]をクリックし、条件名を「VPN_Posture_File_Check」、必要なオペレーティングシステムを「Windows 10(All)」、ファイルタイプを「FileExistence」、ファイルパスを「ABSOLUTE_PATH」、フルパスとファイル名を「C:\custom.txt」に設定し、File Operatorを「Exists」に選択します。

C. この例では、C : ドライブに「custom.txt」という名前のファイルが存在することをファイル条件として使用します

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Dictionarys > Conditions > Results

Library Conditions
 Smart Conditions
 Time and Date
 Profiling
 > Posture
 Anti-Malware Condition
 Anti-Spyware Condition
 Anti-Virus Condition
 Application Condition
 Compound Condition
 Disk Encryption Condition
 File Condition

File Conditions List > VPN_Posture_File_Check

File Condition

* Name: VPN_Posture_File_Check

Description:

* Operating System: Windows 10 (All)

Compliance Module: Any version

* File Type: FileExistence

* File Path: ABSOLUTE_PATH

* File Operator: Exists

C:\custom.txt

Save Reset

8. ポスチャ修復アクションの作成

「Policy > Policy Elements > Results > Posture > Remediation Actions」に移動し、対応するファイル修復アクションを作成します。このドキュメントでは、次の手順で設定する修復操作として「メッセージテキストのみ」を使用します。

9. ポスチャ要件ルールの作成

A. 「Policy > Policy Elements > Results > Posture > Requirements」の順に移動します

B. 「編集」をクリックし、「新規要件を挿入」を選択します

C. 条件名を「VPN_Posture_Requirement」、必要なオペレーティングシステムを「Windows 10(All)」、コンプライアンスモジュールを「4.x以降」、ポスチャタイプを「Anyconnect」に設定

D. 「VPN_Posture_File_Check」(ステップ7で作成)の条件で、「Remediations Actions」の下の「Action」に「Message Text Only」を選択し、エージェントユーザのカスタムメッセージを入力します。

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
requirement_vpn					
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
USB_Block_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only
Any_AM_Installation_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win	then Select Remediations
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
VPN_Posture_Requirement	for Windows 10 (All)	using 4.x or later	using AnyConnect	met if VPN_Posture_File_Check	then Message Text Only

Note: Remediation Action is filtered based on the operating system and stealth mode selection. Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.

Save Reset

10. ポスチャポリシーの作成

A. 「Policies > Posture」に移動します。

B. ステップ9で設定したルール名を「VPN_Posture_Policy_Win」、必要なオペレーティングシステムを「Windows 10(All)」、コンプライアンスモジュールを「4.x以降」、ポスチャタイプを「

Anyconnect」、要件を「VPN_Posture_Requirement」に設定します

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
⊙	Policy Options	Default_AppVis_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_AppVis_Requirement_Win
⊙	Policy Options	Default_AppVis_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_AppVis_Requirement_Win_temporal
⊙	Policy Options	Default_Firewall_Policy_Mac	Any	Mac OSX	4.x or later	AnyConnect		Default_Firewall_Requirement_Mac
⊙	Policy Options	Default_Firewall_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_Firewall_Requirement_Mac_temporal
⊙	Policy Options	Default_Firewall_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_Firewall_Requirement_Win
⊙	Policy Options	Default_Firewall_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Firewall_Requirement_Win_temporal
⊙	Policy Options	Default_Hardware_Attributes_Policy_Mac	Any	Mac OSX	4.x or later	AnyConnect		Default_Hardware_Attributes_Requirement_Mac
⊙	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Mac_temporal
⊙	Policy Options	Default_Hardware_Attributes_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_Hardware_Attributes_Requirement_Win
⊙	Policy Options	Default_Hardware_Attributes_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Win_temporal
⊙	Policy Options	Default_USB_Block_Policy_Win	Any	Windows All	4.x or later	AnyConnect		USB_Block
⊙	Policy Options	Default_USB_Block_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		USB_Block_temporal
⊙	Policy Options	VPN_Posture_Policy_Win	Any	Windows 10 (All)	4.x or later	AnyConnect		VPN_Posture_Requirement

11. ダイナミックACL(DACL)の作成

「Policy > Policy Elements > Results > Authorization > Downloadable ACL」に移動し、異なるポスチャステータスのDACLを作成します。

このドキュメントでは、次のDACLを使用します。

A. ポスチャ不明 : DNS、PSN、HTTP、およびHTTPSトラフィックへのトラフィックを許可します

Downloadable ACL List > PostureUnknown

Downloadable ACL

* Name: PostureUnknown

Description:

IP version: IPv4 (selected), IPv6, Agnostic

* DACL Content:

```
1234567 permit udp any any eq domain
8910111 permit ip any host 10.106.44.77
2131415 permit tcp any any eq 80
1617181 permit tcp any any eq 443
9202122
2324252
6272829
3031323
3343536
```

Check DACL Syntax

Save (highlighted) Reset

B.ポスチャ非準拠：プライベートサブネットへのアクセスを拒否し、インターネットトラフィックのみを許可します。

The screenshot shows the configuration page for a Downloadable ACL in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Authorization' > 'Downloadable ACLs' selected. The main content area is titled 'Downloadable ACL List > PostureNonCompliant'. The configuration fields are: Name: 'PostureNonCompliant', Description: (empty), IP version: 'IPv4' (selected), and DACL Content: 'deny ip any 10.0.0.0 255.0.0.0', 'deny ip any 172.16.0.0 255.240.0.0', 'deny ip any 192.168.0.0 255.255.0.0', 'permit ip any any'. The 'Save' button is highlighted with a red box.

C.ポスチャ準拠：ポスチャ準拠エンドユーザのすべてのトラフィックを許可します。

The screenshot shows the configuration page for a Downloadable ACL in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Authorization' > 'Downloadable ACLs' selected. The main content area is titled 'Downloadable ACL List > PostureCompliant'. The configuration fields are: Name: 'PostureCompliant', Description: (empty), IP version: 'IPv4' (selected), and DACL Content: 'permit ip any any'. The 'Save' button is highlighted with a red box.

12.許可プロファイルの作成

「Policy > Policy Elements > Results > Authorization > Authorization Profiles」に移動します。

A.不明なポスチャの許可プロファイル

DACL "PostureUnknown"を選択し、Web Redirectionをチェックし、Client Provisioning(Posture)を選択し、リダイレクトACL名"redirect" (ASAで設定) を設定し、クライアントプロビジョニングポータル (デフォルト) を選択します。

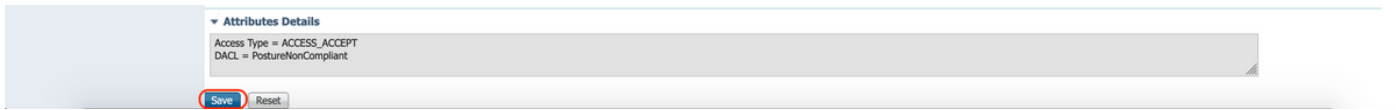
The screenshot shows the configuration page for an Authorization Profile named "Posture Redirect". The "Name" field is set to "Posture Redirect". The "Access Type" is set to "ACCESS_ACCEPT". The "Network Device Profile" is set to "Cisco". Under "Common Tasks", the "DACL Name" is set to "PostureUnknown". The "Web Redirection (CWA, MDM, NSP, CPP)" checkbox is checked. Under "Client Provisioning", the "Client Provisioning (Posture)" checkbox is checked, and the "ACL" is set to "redirect" and the "Value" is set to "Client Provisioning Portal (default)". The "Attributes Details" section shows the following configuration:

```
Access Type = ACCESS_ACCEPT
DACL = PostureUnknown
cisco-av-pair = uri-redirect-ac=redirect
cisco-av-pair = uri-redirect=https://ip:port/portal/gateway?sessionId=SessionId&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp
```

B. ポスチャ非準拠の認証プロファイル

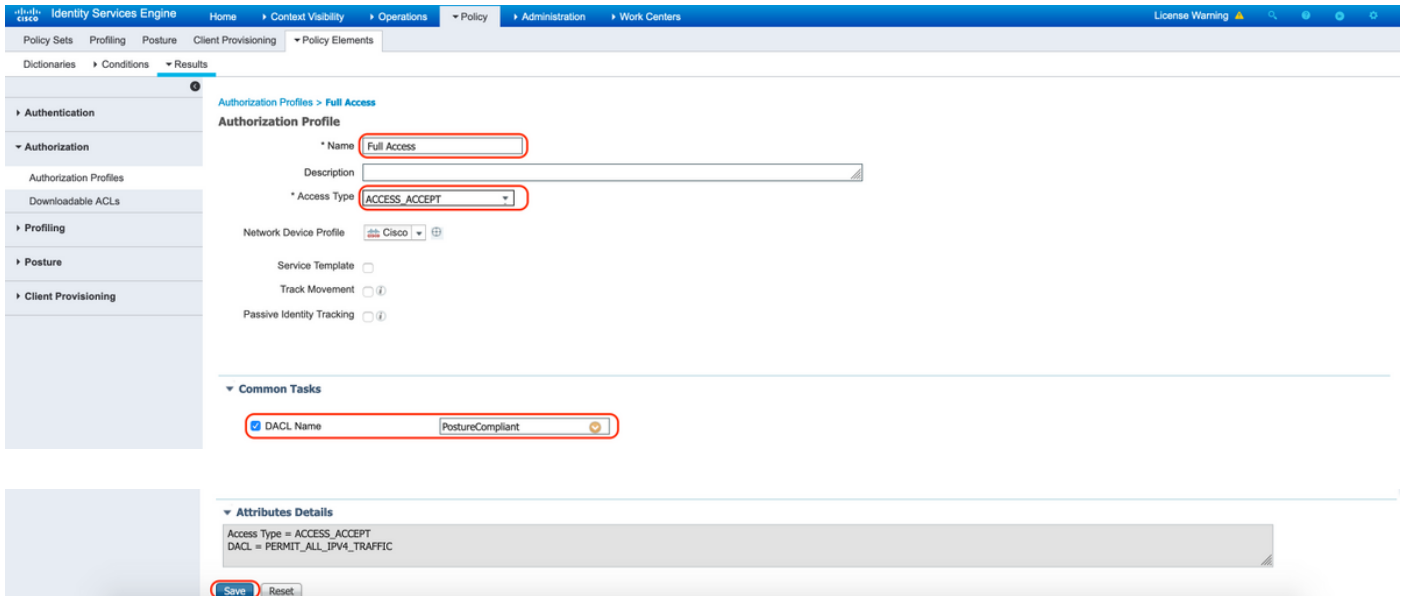
ネットワークへのアクセスを制限するには、DACL「PostureNonCompliant」を選択します

The screenshot shows the configuration page for an Authorization Profile named "Posture Non Compliant". The "Name" field is set to "Posture Non Compliant". The "Access Type" is set to "ACCESS_ACCEPT". The "Network Device Profile" is set to "Cisco". Under "Common Tasks", the "DACL Name" is set to "PostureNonCompliant".



C. ポスチャ準拠の認証プロファイル

ネットワークへのフルアクセスを許可するには、DACL「PostureCompliant」を選択します。



12. 許可ポリシーの設定

前の手順で設定した認可プロファイルを使用して、ポスチャ準拠、ポスチャ非準拠、ポスチャ不明の3つの認可ポリシーを設定します。

各ポリシーの結果を判断するために、共通の条件「セッション：ポスチャステータス」が使用されます。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Policy Sets → Default

Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Default	Default policy set		Default Network Access x +	49
> Authentication Policy (3) > Authorization Policy - Local Exceptions > Authorization Policy - Global Exceptions					

Authorization Policy (15)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
✔	Anyconnect Posture Compliant	Session PostureStatus EQUALS Compliant		Full Access +	Select from list +	6	⚙
✔	Anyconnect Posture Non Compliant	Session PostureStatus EQUALS NonCompliant		Posture Non Compliant +	Select from list +	0	⚙
✔	Anyconnect Posture Unknown	AND Network Access-Device IP Address EQUALS 10.197.164.3 Session PostureStatus EQUALS Unknown		Posture Redirect +	Select from list +	13	⚙

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ユーザが正常に認証されたかどうかを確認するには、ASAで次のコマンドを実行します。

```
<#root>
```

```
firebird(config)#
```

```
show vpn-sess detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : _585b5291f01484dfd16f394be7031d456d314e3e62
Index         : 125
Assigned IP   : explorer.cisco.com      Public IP    : 10.197.243.143
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx      : 16404                   Bytes Rx     : 381
Pkts Tx       : 16                       Pkts Rx     : 6
Pkts Tx Drop  : 0                         Pkts Rx Drop : 0
Group Policy  : DfltGrpPolicy              Tunnel Group :
```

```
TG_SAML
```

```
Login Time    : 07:05:45 UTC Sun Jun 14 2020
Duration      : 0h:00m:16s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                       VLAN         : none
```

Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 125.1
Public IP : 10.197.243.143
Encryption : none Hashing : none
TCP Src Port : 57244 TCP Dst Port : 443
Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 125.2
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 57248
TCP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PostureUnknown-5ee45b05

DTLS-Tunnel:

Tunnel ID : 125.3
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 49175
UDP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 458 Bytes Rx : 381
Pkts Tx : 4 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PostureUnknown-5ee45b05

ISE Posture:

Redirect URL : <https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&p>
Redirect ACL : redirect

ポスチャ評価が完了すると、「Filter Name」フィールドにプッシュされたDACLに示されるように、ユーザアクセスがフルアクセスに変更されます

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username : _585b5291f01484dfd16f394be7031d456d314e3e62
Index : 125
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 16404 Bytes Rx : 381
Pkts Tx : 16 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group :

TG_SAML

Login Time : 07:05:45 UTC Sun Jun 14 2020
Duration : 0h:00m:36s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 125.1
Public IP : 10.197.243.143
Encryption : none Hashing : none
TCP Src Port : 57244 TCP Dst Port : 443
Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 125.2
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384

Encapsulation: TLSv1.2 TCP Src Port : 57248
 TCP Dst Port : 443 Auth Mode : SAML
 Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
 Client OS : Windows
 Client Type : SSL VPN Client
 Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
 Bytes Tx : 7973 Bytes Rx : 0
 Pkts Tx : 6 Pkts Rx : 0
 Pkts Tx Drop : 0 Pkts Rx Drop : 0
 Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

DTLS-Tunnel:

Tunnel ID : 125.3
 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
 Encryption : AES-GCM-256 Hashing : SHA384
 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
 Encapsulation: DTLSv1.2 UDP Src Port : 49175
 UDP Dst Port : 443 Auth Mode : SAML
 Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
 Client OS : Windows
 Client Type : DTLS VPN Client
 Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
 Bytes Tx : 458 Bytes Rx : 381
 Pkts Tx : 4 Pkts Rx : 6
 Pkts Tx Drop : 0 Pkts Rx Drop : 0
 Filter Name :

#ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

ISEで認証が正常に実行されたかどうかを確認するには、「Operations」>「RADIUS」>「Live Logs」に移動します。

このセクションには、認証ユーザに関連する情報 (ID、認証プロファイル、認証ポリシー、ポストチャステータス) が表示されます。

Refresh Never Show Latest 20 records Within Last 24 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM			0	_585b5291f01484d1d1...	00:50:56:A0:D6:97	Windows10-...	Default	Anyconnect ...	Full Access	Compliant	10.197.164.7	ASA
Jun 14, 2020 07:44:59.975 AM				#ACSACL#-IP-PERMI...								ASA
Jun 14, 2020 07:44:34.963 AM				#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.958 AM				_585b5291f01484d1d1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA

注: ISEでの追加のポストチャ検証については、次のドキュメントを参照してください。
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-access.html#anc7>

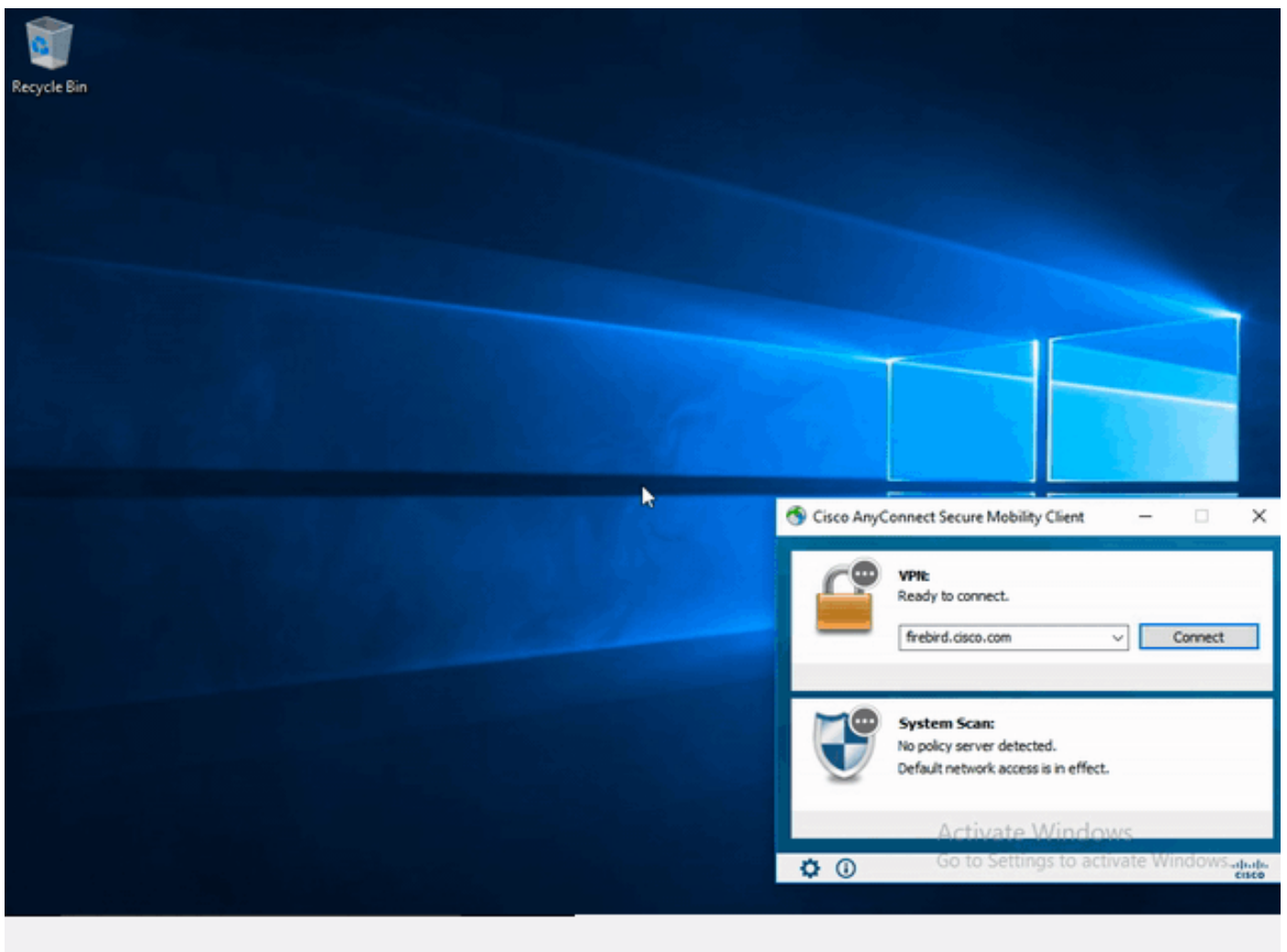
Duo Admin Portalの認証ステータスを確認するには、Admin Panelの左側にある認証ログを表示する「Reports」をクリックします。

詳細 : <https://duo.com/docs/administration#reports>

Duo Access Gatewayのデバッグロギングを表示するには、次のリンクを使用します。


https://help.duo.com/s/article/1623?language=en_US


ユーザ エクスペリエンス



トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

 注：debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

 注意:ASAでは、さまざまなデバッグレベルを設定できます。デフォルトでは、レベル1が使用されます。デバッグレベルを変更すると、デバッグの冗長性が高くなる場合があります。特に実稼働環境では、注意して実行してください。

ほとんどのSAMLのトラブルシューティングでは、SAML設定のチェックやデバッグの実行によって検出される設定の誤りが関係します。

「debug webvpn saml 255」は、ほとんどの問題のトラブルシューティングに使用できますが、このデバッグで有用な情報が得られないシナリオでは、追加のデバッグを実行できます。


```
debug webvpn 255
debug webvpn anyconnect 255
debug webvpn session 255
debug webvpn request 255
```

ASAの認証と認可の問題をトラブルシューティングするには、次のdebugコマンドを使用します

。

```
debug radius all
debug aaa authentication
debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to
```

```
posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)
```

 注：ポスチャフローの詳細とAnyConnectおよびISEのトラブルシューティングについては、次のリンクを参照してください。

[ISE ポスチャ スタイルの 2.2 前後の比較](#)

Duo Access Gatewayのデバッグログの解釈とトラブルシューティング

https://help.duo.com/s/article/5016?language=en_US

関連情報

<https://www.youtube.com/watch?v=W6bE2GTU0Is&>

<https://duo.com/docs/cisco#asa-ssl-vpn-using-saml>

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-access.html#anc0>

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。