

# 使用ISE终端安全评估将Duo SAML SSO与Anyconnect安全远程访问集成

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[流量传输](#)

[配置](#)

[- Duo管理员门户配置](#)

[- Duo接入网关\(DAG\)配置](#)

[-ASA 配置](#)

[-ISE 配置](#)

[验证](#)

[用户体验](#)

[故障排除](#)

[相关信息](#)

---

## 简介

本文档介绍将Duo SAML SSO与利用思科ISE进行详细状态评估的自适应安全设备(ASA)Cisco AnyConnect安全移动客户端访问相集成的配置示例。双核SAML SSO使用双核接入网关(DAG)实施，该网关与Active Directory通信以进行初始用户身份验证，然后与双核安全（云）通信以进行多重身份验证。思科ISE用作授权服务器，使用状况评估提供终端验证。

作者：Dinesh Moudgil和Pulkit Saxena，Cisco HTTS工程师。

## 先决条件

### 要求

本文档假设ASA完全运行且配置为允许思科自适应安全设备管理器(ASDM)或命令行界面(CLI)进行配置更改。


Cisco 建议您了解以下主题：

- Duo接入网关和Duo安全基础知识
- ASA上远程访问VPN配置的基本知识
- ISE和状态服务基础知识

## 使用的组件

本文档中的信息基于以下软件版本：

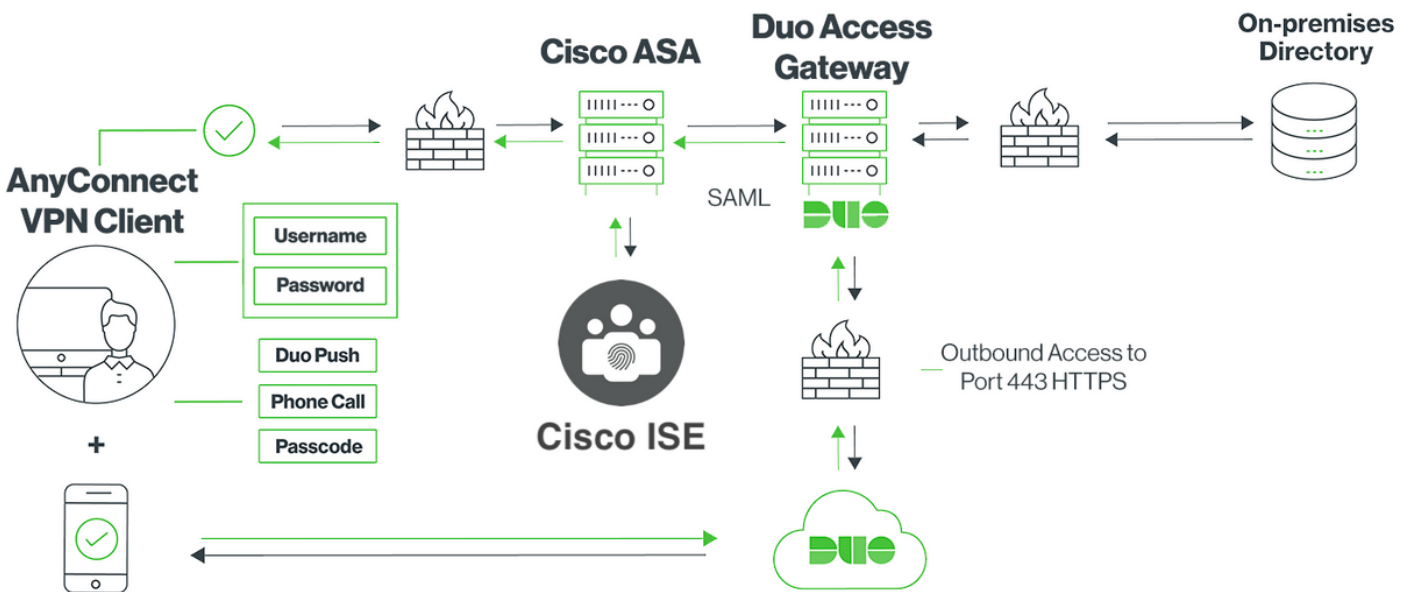
- 思科自适应安全设备软件版本9.12(3)12
- Duo接入网关
- Duo安全
- 思科身份服务引擎2.6版及更高版本
- Microsoft Windows 10与AnyConnect版本4.8.03052

 注意：此实施中使用的Anyconnect嵌入式浏览器要求每个版本的9.7(1)24、9.8(2)28、9.9(2)1或更高版本以及AnyConnect版本4.6或更高版本ASA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

### 网络图



### 流量传输

1. Anyconnect客户端发起到Cisco ASA的SSL VPN连接
2. Cisco ASA配置为使用双协议访问网关(DAG)进行主要身份验证，将Anyconnect客户端中的嵌入式浏览器重定向到DAG进行SAML身份验证
3. Anyconnect客户端被重定向到Duo接入网关
4. AnyConnect客户端输入凭证后，会建立SAML身份验证请求，并从Cisco ASA发送到Duo访问网关
5. Duo接入网关利用与现场Active Directory的集成来执行Anyconnect客户端的主要身份验证
6. 主身份验证成功后，Duo接入网关向Duo Security over TCP端口443发送请求以开始双因素身份验证
7. AnyConnect客户端已显示“Duo Interactive Prompt”，用户使用其首选方法（推送或密码）完成双因素身份验证
8. Duo Security收到身份验证响应并将信息返回到Duo接入网关
9. Duo接入网关根据身份验证响应构建SAML身份验证响应，其中包含SAML断言并响应Anyconnect客户端
10. Anyconnect客户端成功通过与Cisco ASA的SSL VPN连接的身份验证
11. 身份验证成功后，Cisco ASA向Cisco ISE发送授权请求



注意：Cisco ISE仅为授权配置，因为Duo Access Gateway提供必需的身份验证

---

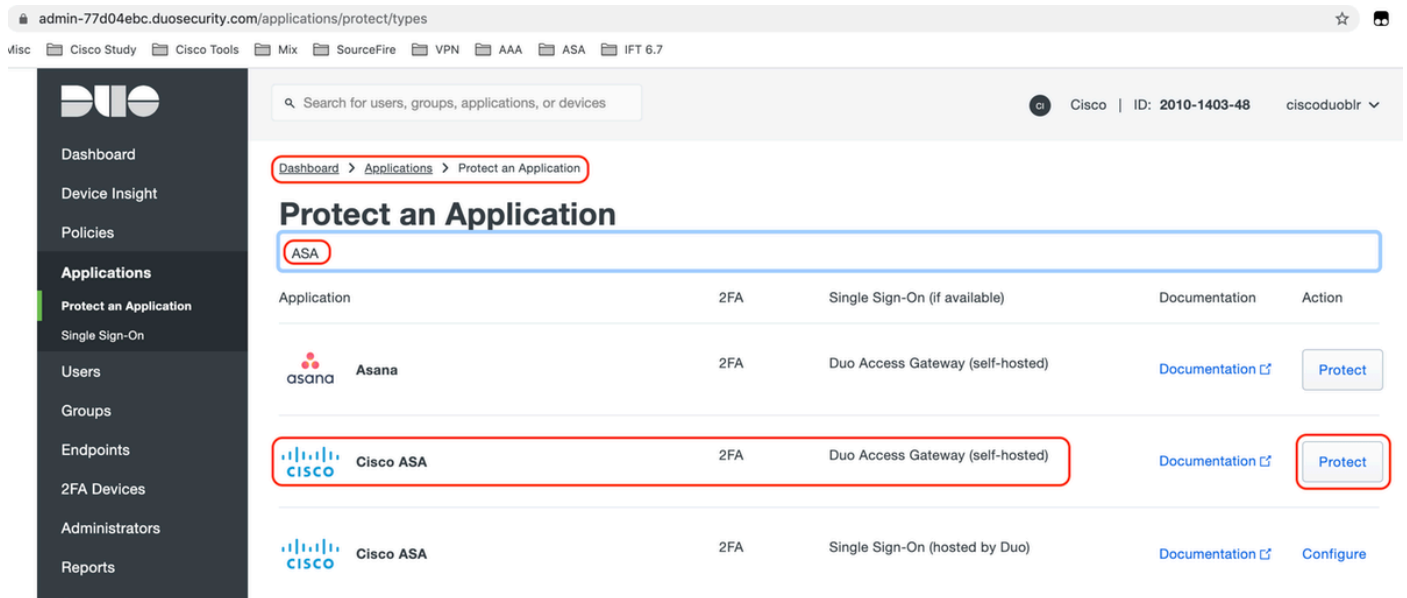
12. 思科ISE处理授权请求，并且由于客户端状态未知，通过思科ASA有限访问Anyconnect客户端返回状态重定向
13. 如果Anyconnect客户端没有合规性模块，系统会提示其下载以进行进一步的安全状态评估
14. 如果Anyconnect客户端具有合规性模块，则会与Cisco ASA建立TLS连接，并启动安全评估流程
15. 根据ISE上配置的终端安全评估条件，完成终端安全评估检查，并将详细信息从Anyconnect客户端发送到思科ISE
16. 如果客户端状态从Unknown更改为Compliant，则授权更改(CoA)请求从Cisco ISE发送到Cisco ASA以授予客户端完全访问权限和VPN完全建立

## 配置

## - Duo管理员门户配置

在本节中，在Duo Admin Portal上配置ASA应用。

1.登录“Duo Admin Portal”并导航至“Applications > Protect an Application”，搜索保护类型为“2FA with Duo Access Gateway， self-hosted”的“ASA”。点击最右边的“保护”以配置Cisco ASA



2.为受保护的应用ASA在“服务提供商”下配置以下属性

基本URL	firebird.cisco.com
隧道组	TG_SAML
邮件属性	sAMAccountName , mail

点击页面底部的“保存”

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

## Configure Cisco ASA

Reset Secret Key

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

在本文档中，其余配置使用默认参数，但可以根据客户要求进行调整。

此时可以为新SAML应用调整其他设置，例如从默认值更改应用的名称、启用自助服务或分配组策略。

3.单击“下载配置文件”链接获取Cisco ASA应用设置（作为JSON文件）。此文件将在后续步骤中上传到Duo接入网关

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

## Configure Cisco ASA

Reset Secret Key

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.

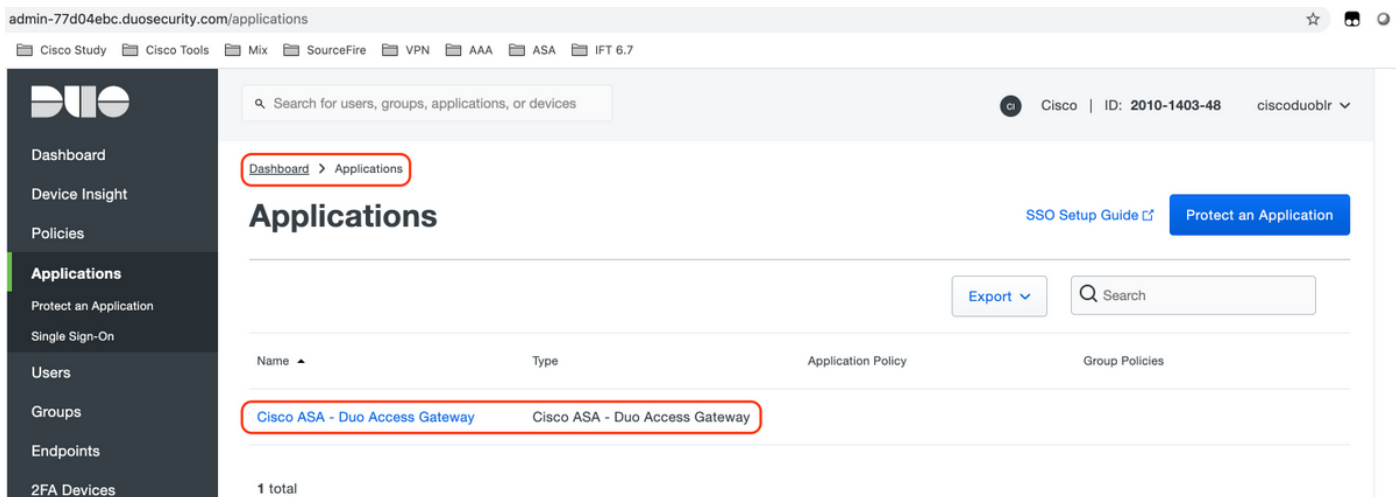
Custom attributes  Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute

The attribute containing the email address of the user.

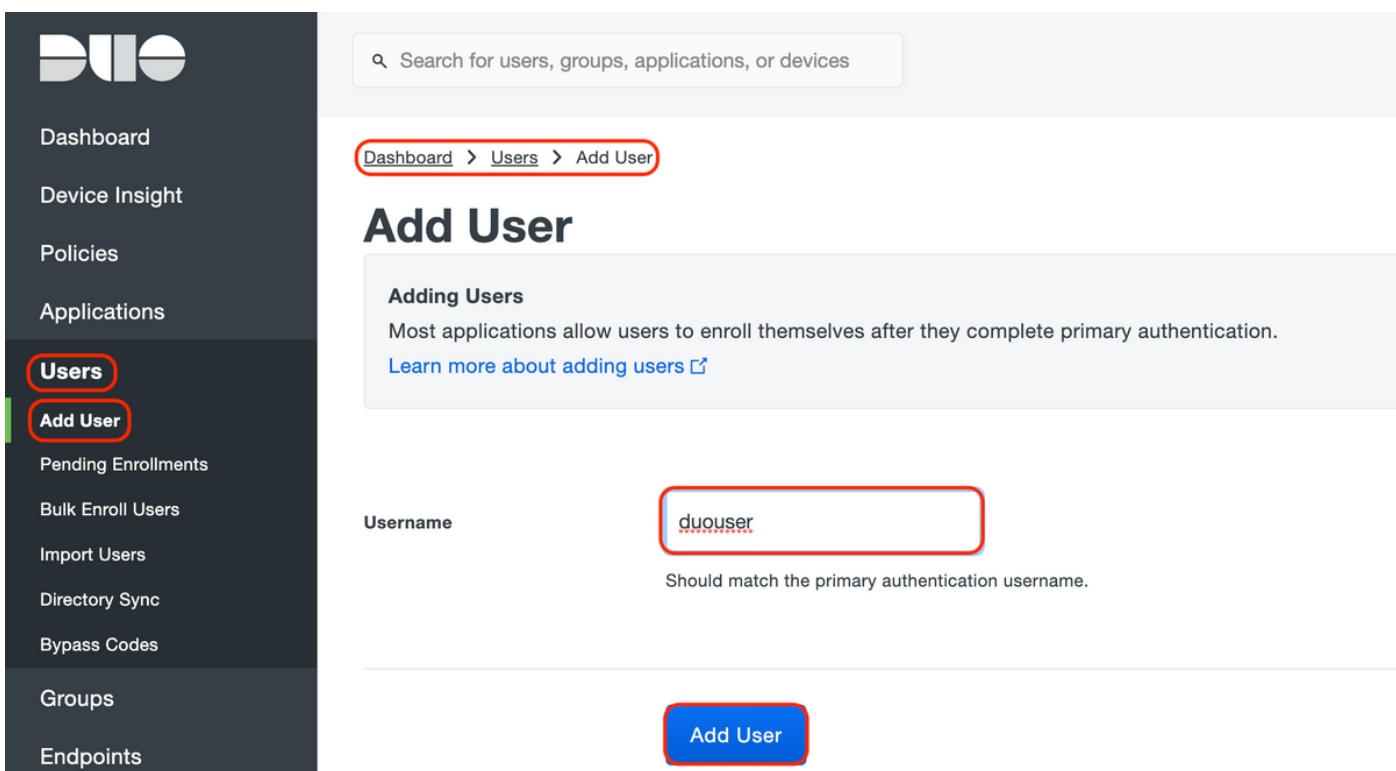
Save Configuration

4.在Dashboard > Applications下，新创建的ASA应用如下图所示：



5.导航至“用户>添加用户”，如图所示：

创建名为“duouser”的用户以用于Anyconnect远程访问身份验证，并在最终用户设备上激活Duo Mobile



要添加图中所示的电话号码，请选择“添加电话”选项。

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"

[Add Phone](#)

为特定用户激活“Duo Mobile”

### Device Info

[Learn more about Activating Duo Mobile](#)



Not using Duo Mobile  
[Activate Duo Mobile](#)



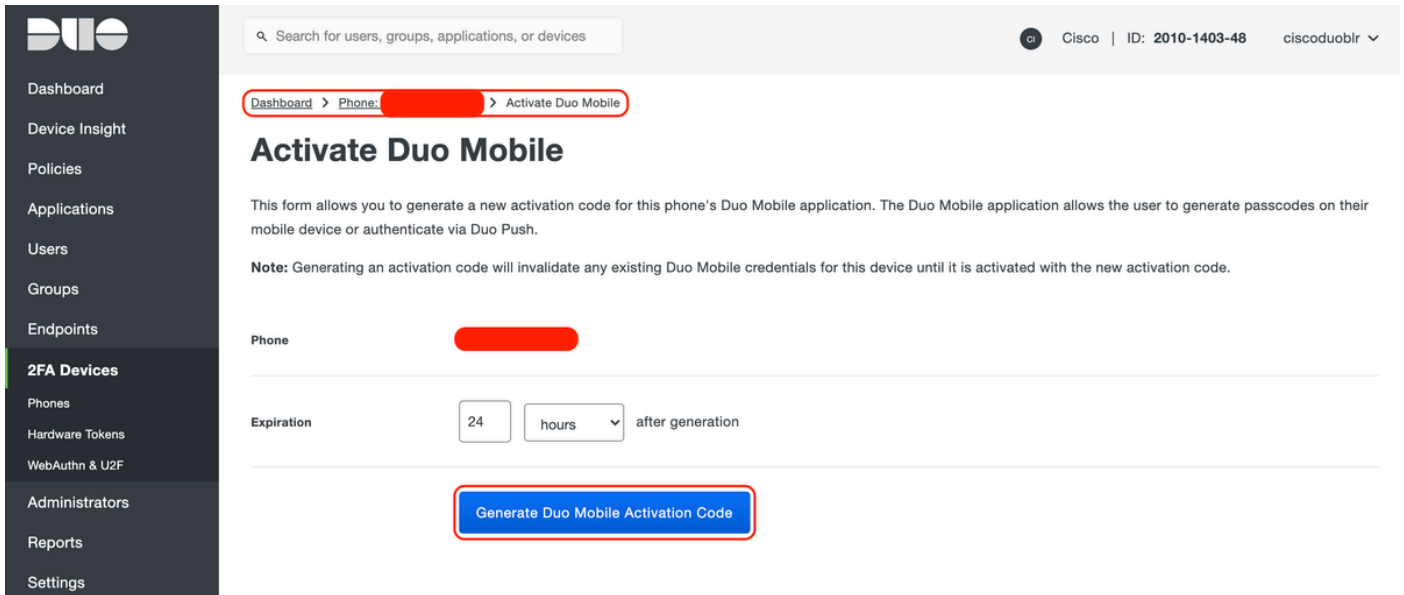
Model  
Unknown



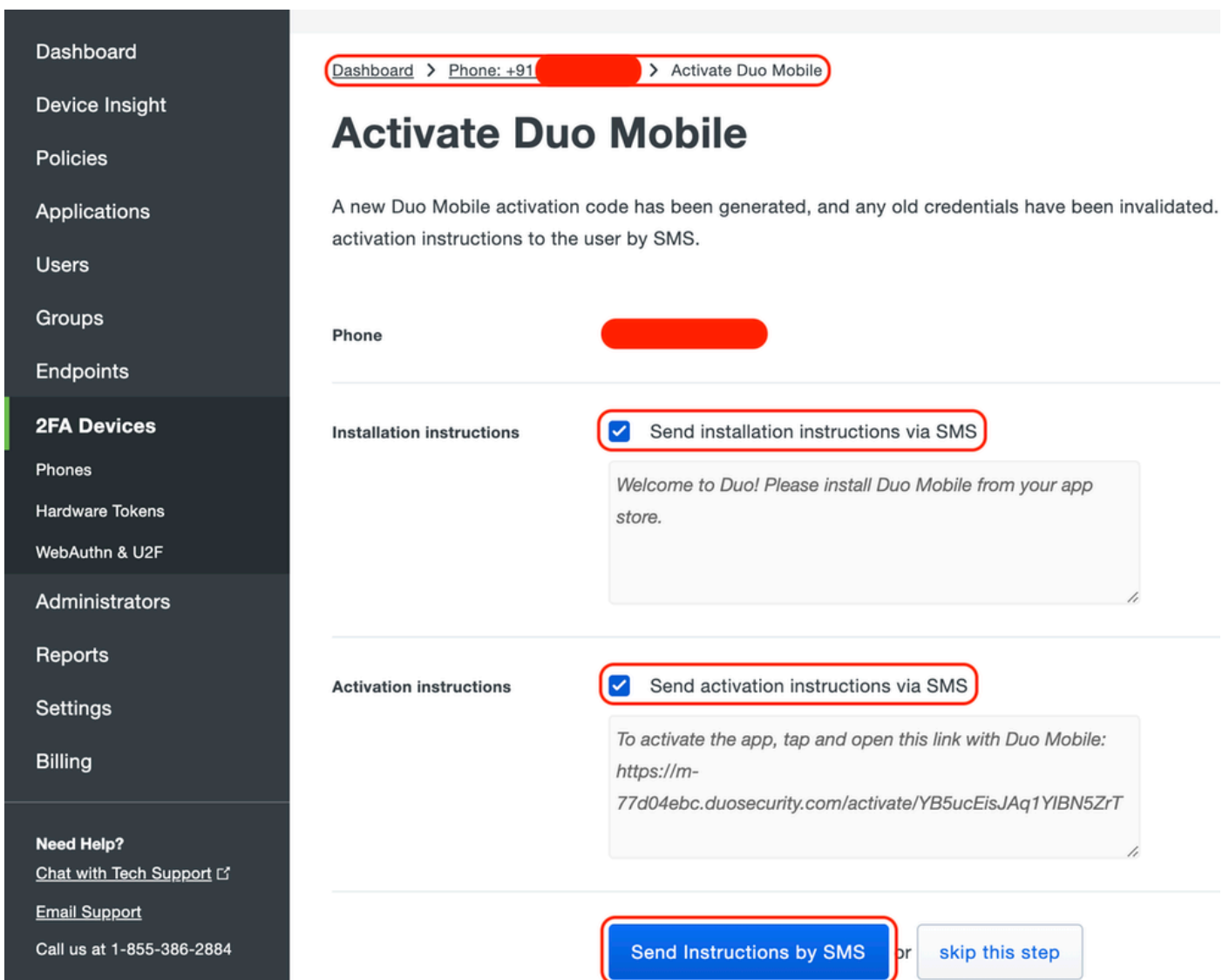
OS  
Generic Smartphone

- 注：确保在最终用户设备上安装“Duo Mobile”。
  - [手动安装IOS设备Duo应用程序](#)
  - [手动安装适用于Android设备的Duo应用程序](#)

选择“Generate Duo Mobile Activation Code”，如图所示：



选择“Send Instructions by SMS”（通过SMS发送说明），如图所示：



点击SMS中的链接，Duo应用将链接到“设备信息”部分中的用户帐户，如图所示：



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

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48

Duo Mobile instructions SMS'ed to +91 [REDACTED]

Dashboard > Phones > Phone: +91 [REDACTED]

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

**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接入网关(DAG)配置

### 1. 在网络中的服务器上部署Duo访问网关(DAG)

 注意：请遵循以下文档进行部署：

用于Linux的双核接入网关

<https://duo.com/docs/dag-linux>

用于Windows的双核接入网关

<https://duo.com/docs/dag-windows>

### 2. 在Duo Access Gateway主页上，导航至“Authentication Source”

### 3. 在“Configure Sources”下，输入您的Active Directory的以下属性，然后单击“Save Settings”

## 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:	<span>✔ LDAP Bind Succeeded</span> <span>✔ ldap://10.197.243.110</span>
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. 在“Set Active Source”下，选择源类型为“Active Directory”，然后单击“Set Active Source”

### Set Active Source

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

Source type

5. 导航至“Applications”，在“Add Application”子菜单下上传从“Configuration file”部分的Duo Admin Console下载的.json文件。相应的.json文件已在步骤3的Duo Admin Portal Configuration下下载

## Applications


### Add Application

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

Configuration file

6. 成功添加应用后，它将显示在“应用”(Applications)子菜单下

### Applications

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

7. 在“元数据”(Metadata)子菜单下，下载XML元数据和IdP证书，并记下随后在ASA上配置的以下URL

1. SSO URL
2. 注销URL
3. 实体Id
4. 错误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	<a href="https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
Logout URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer">https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer</a>
Entity ID	<a href="https://explorer.cisco.com/dag/saml2/idp/metadata.php">https://explorer.cisco.com/dag/saml2/idp/metadata.php</a>
Error URL	<a href="https://explorer.cisco.com/dag/module.php/duosecurity/du">https://explorer.cisco.com/dag/module.php/duosecurity/du</a>

## -ASA 配置

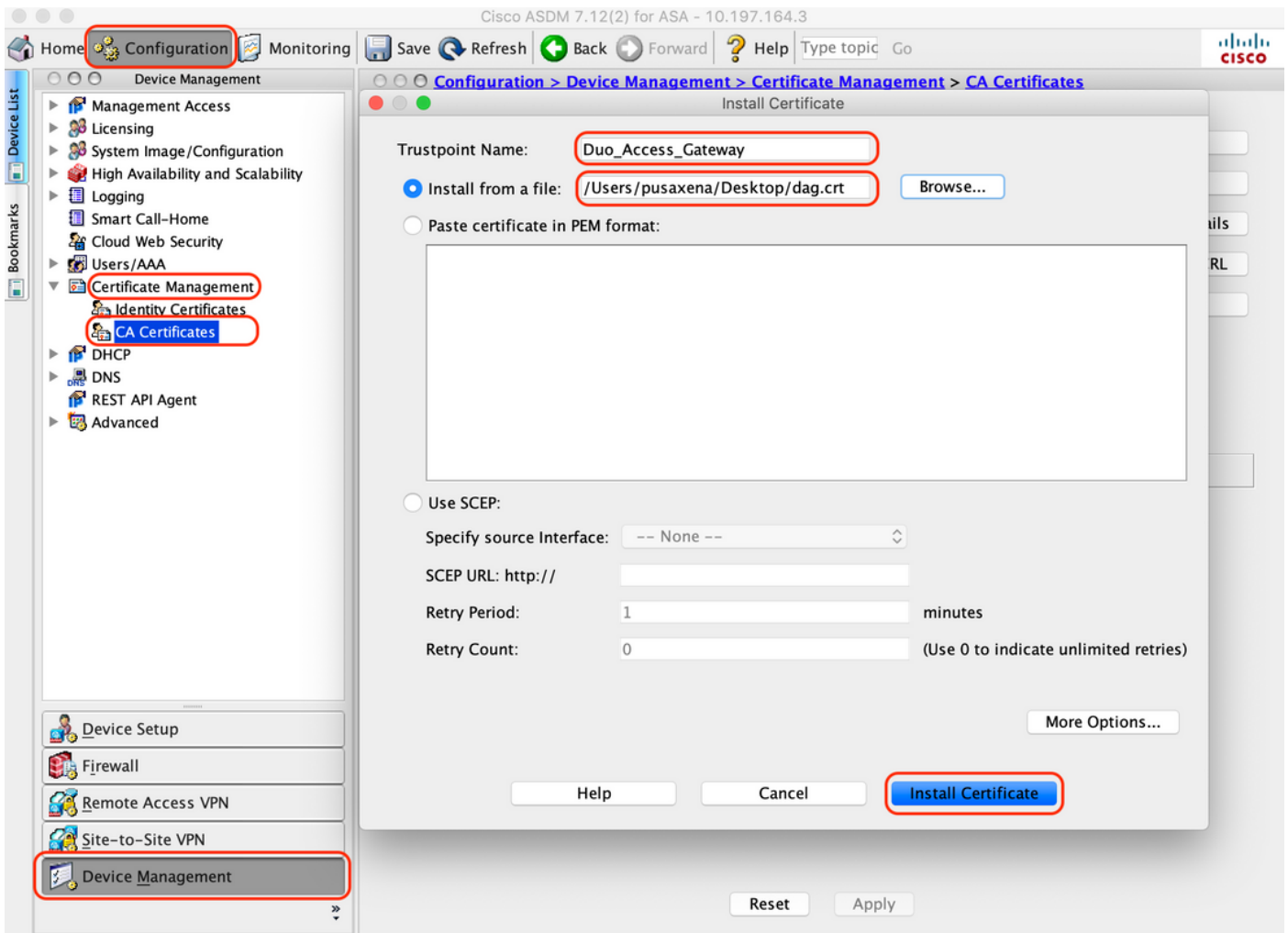
本节提供有关为SAML IDP身份验证和基本AnyConnect配置配置ASA的信息。本文档提供概述的ASDM配置步骤和CLI运行配置。

### 1.上传Duo接入网关证书

A.导航到“Configuration > Device Management > Certificate Management > CA Certificates”，然后单击“Add”

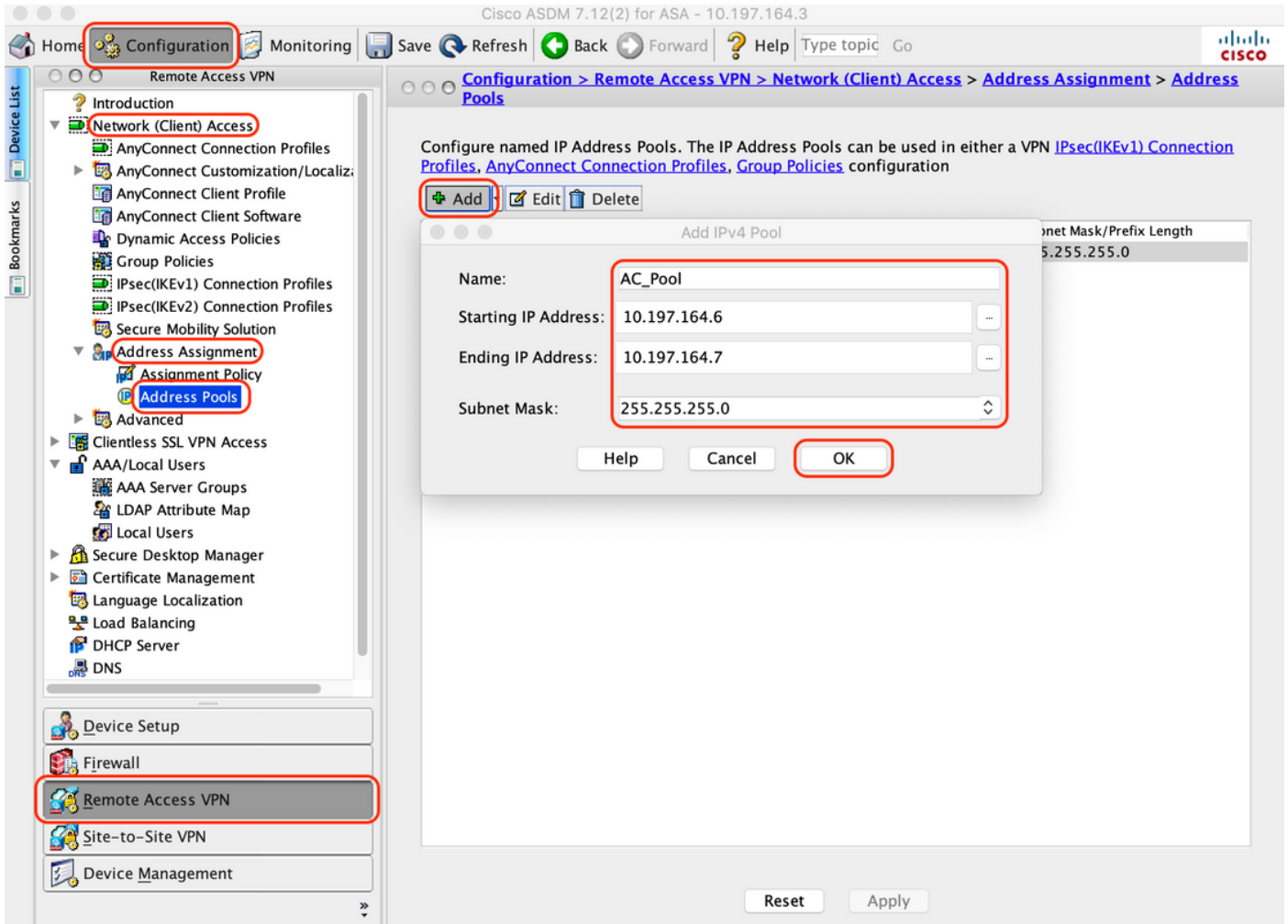
B.在“安装证书页面”上，配置信任点名称：Duo\_Access\_Gateway

C.单击“浏览”选择与DAG证书关联的路径，选择后，单击“安装证书”



## 2. 为AnyConnect用户创建IP本地池

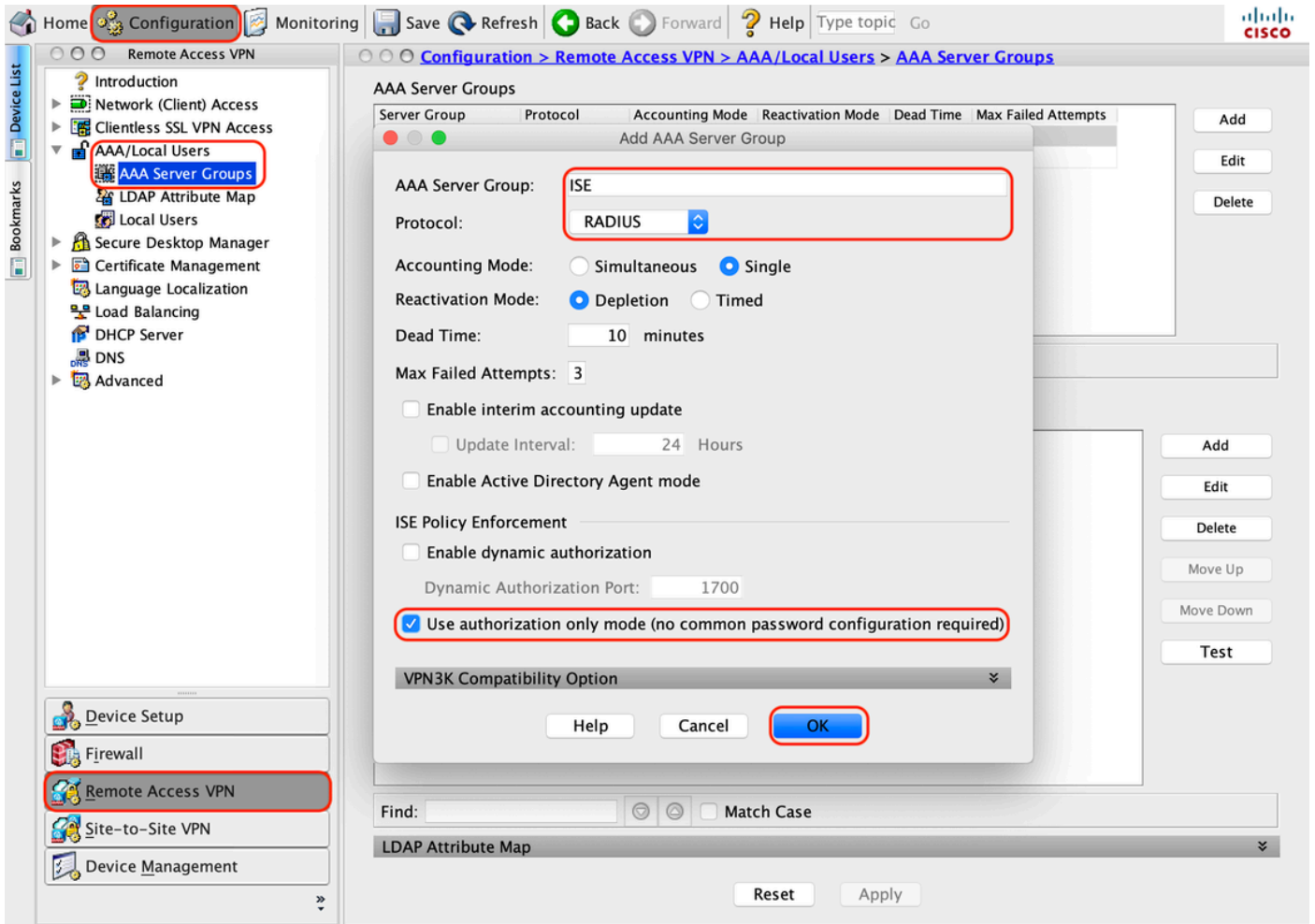
导航到“Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Address Pools”，单击“Add”



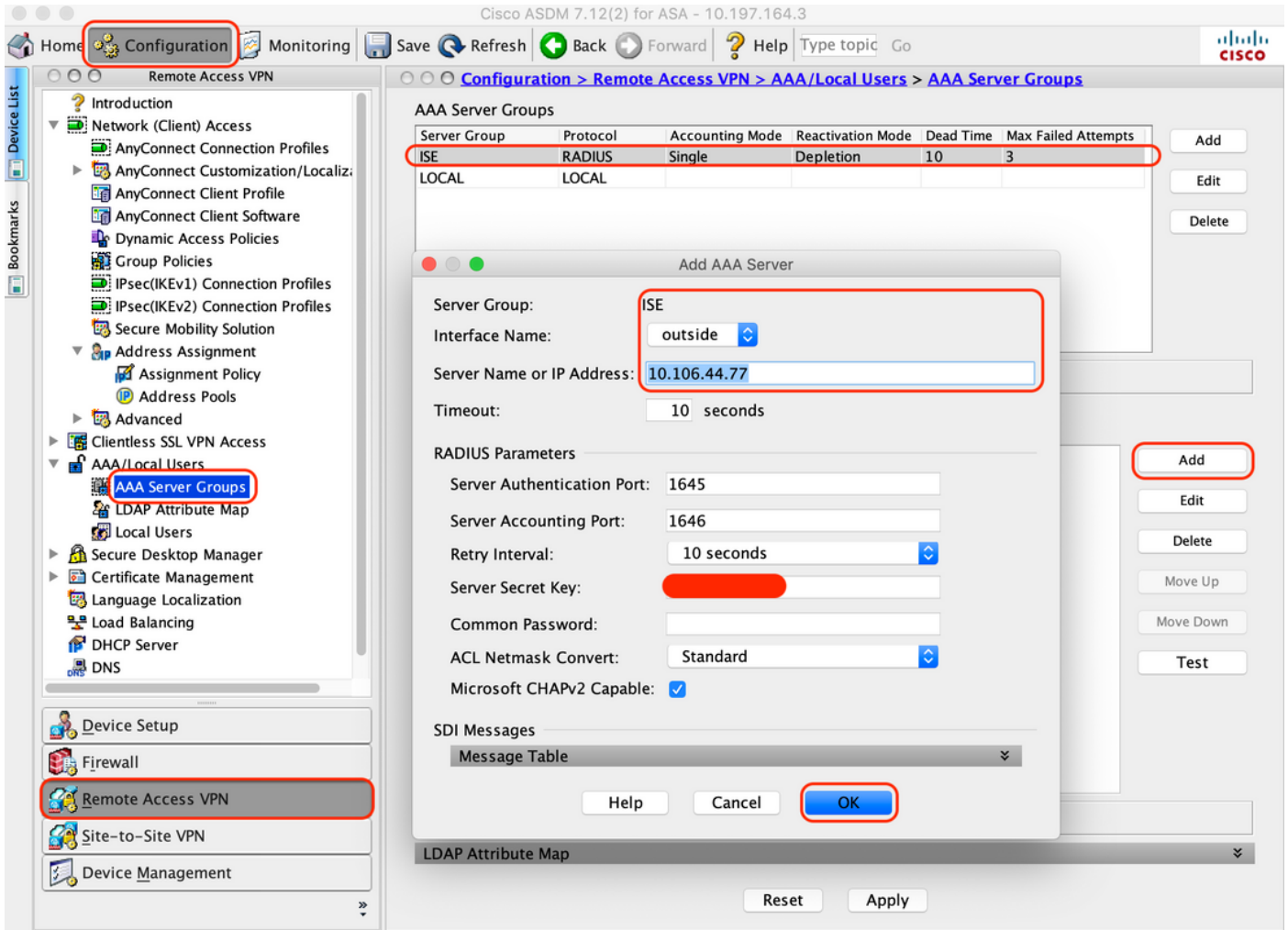
### 3. 配置AAA服务器组

A. 在本节中，配置AAA服务器组并提供执行授权的特定AAA服务器的详细信息

B. 导航到“Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups”，点击“Add”



C.在同一页的“Servers in the Selected group”部分下，点击“Add”并提供AAA服务器的IP地址详细信息

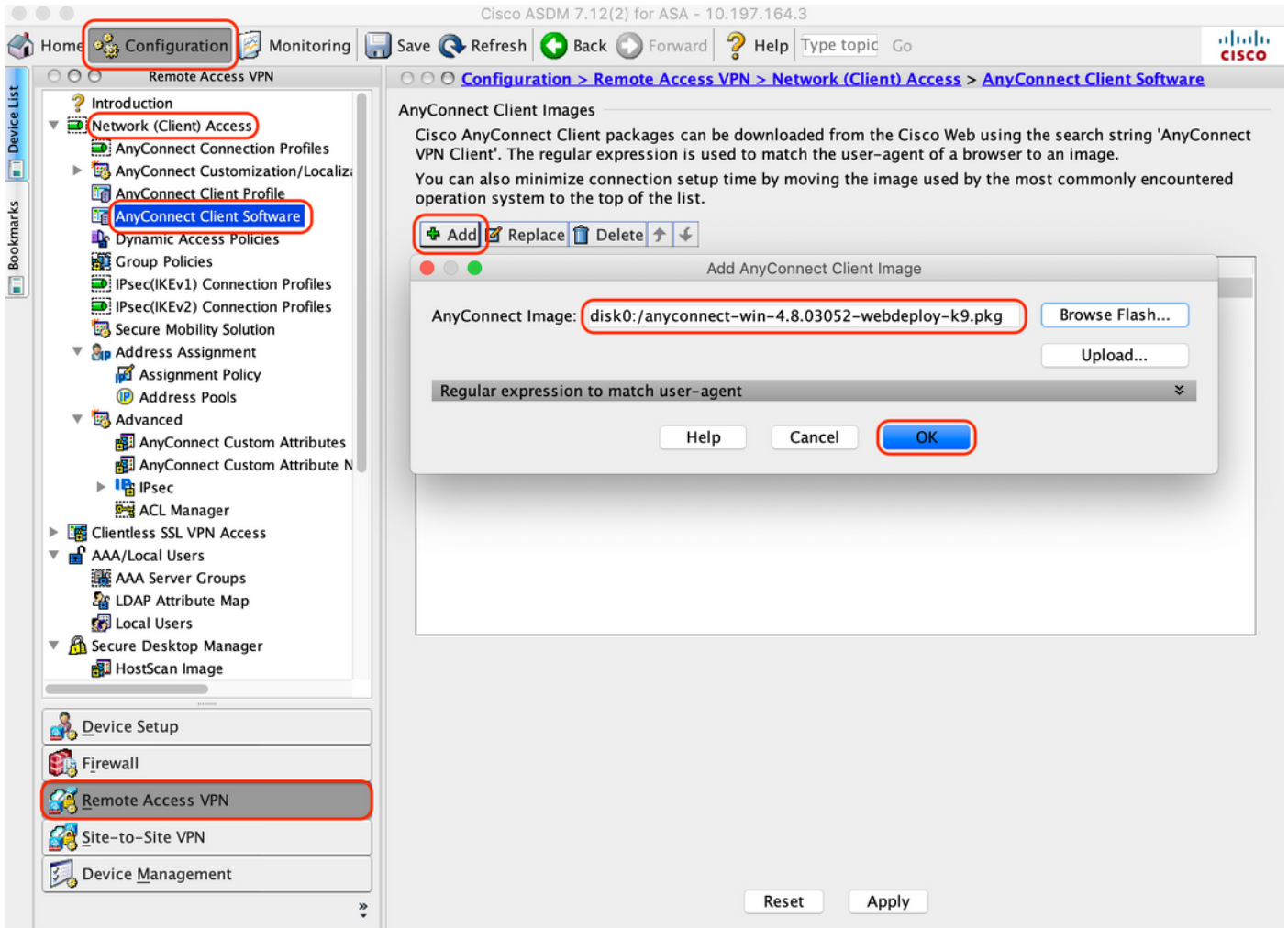


#### 4. 映射AnyConnect客户端软件

A. 映射用于WebVPN的Windows的AnyConnect客户端软件webdeploy映像4.8.03052

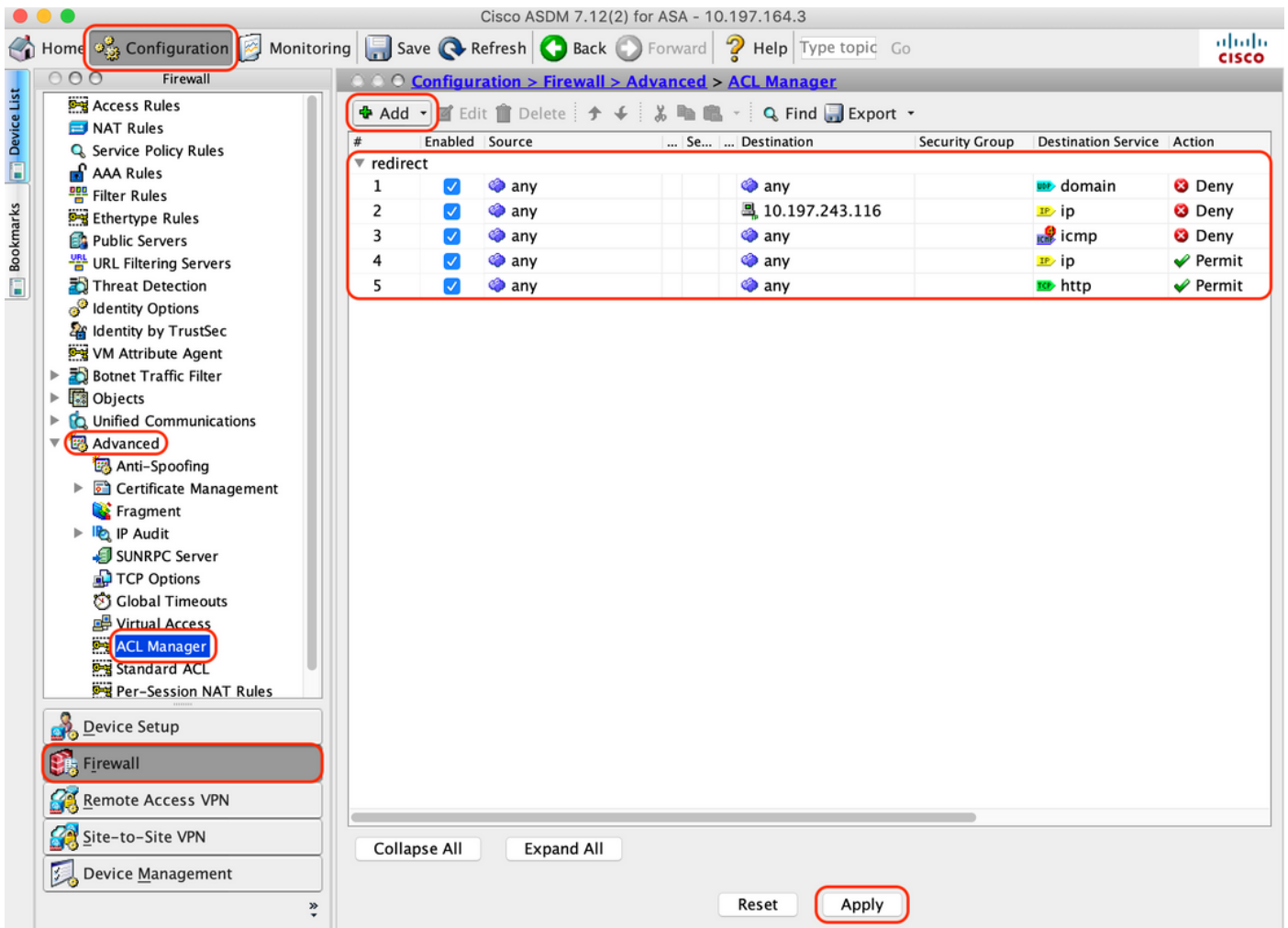
B. 导航到“Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Client Software”，点击“Add”





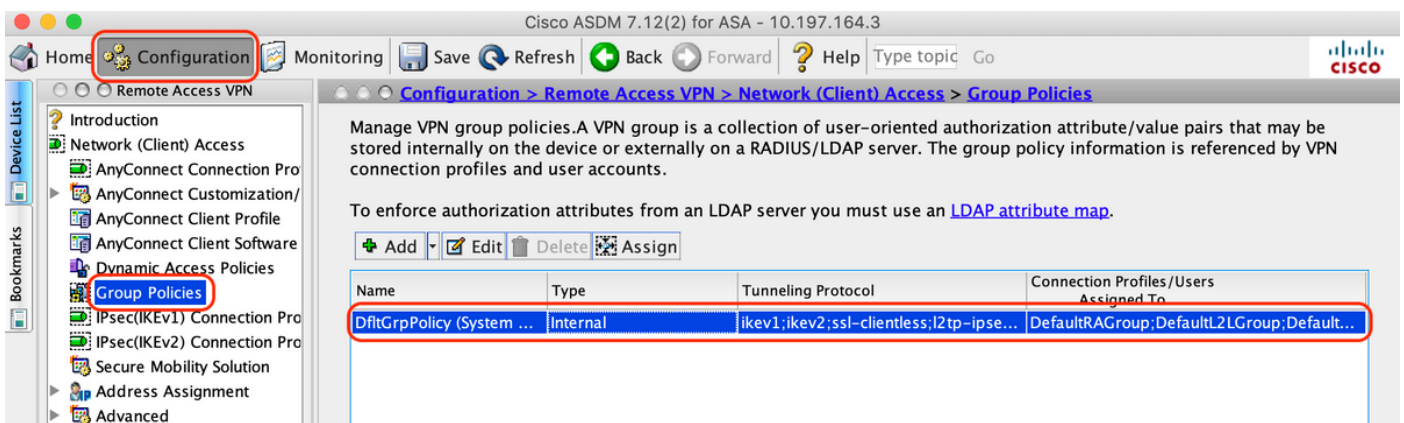
## 5. 配置由ISE推送的重定向ACL

A. 导航到“Configuration > Firewall > Advanced > ACL Manager”，点击Add以添加重定向ACL。配置后，条目如下所示：



## 6. 验证现有组策略

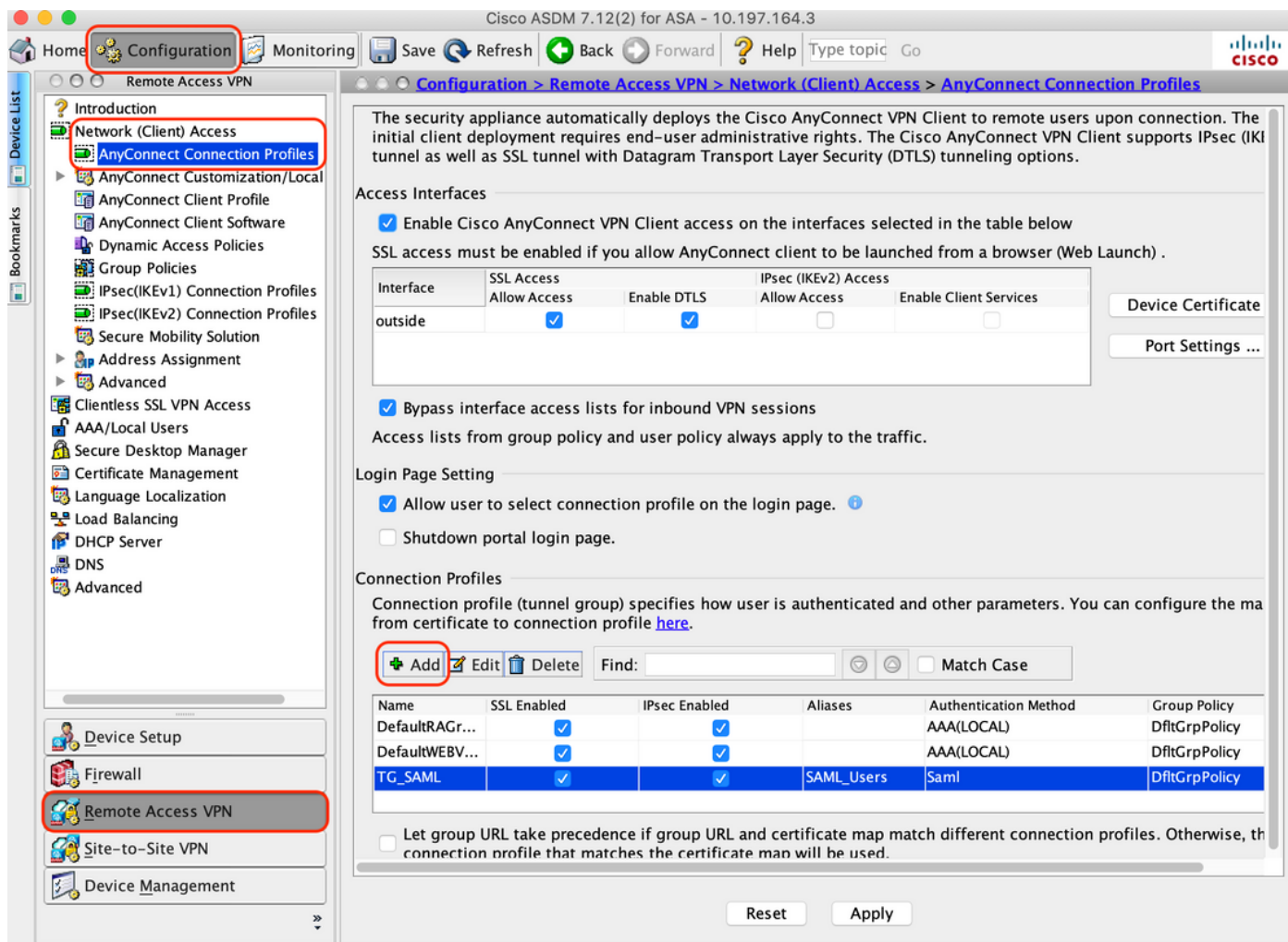
A. 此设置使用默认组策略，可以在以下位置查看：“Configuration > Remote Access VPN > Network(Client)Access > Group Policies”



## 7. 配置连接配置文件

A. 创建AnyConnect用户连接的新连接配置文件

B. 导航到“Configuration > Remote Access VPN > Network(Client)Access > Anyconnect Connection Profiles”，然后单击“Add”



C. 配置以下与连接配置文件相关的详细信息：

名称	TG_SAML
别名	SAML用户
方法	SAML
AAA 服务器组	本地
客户端地址池	AC_Pool
组策略	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:

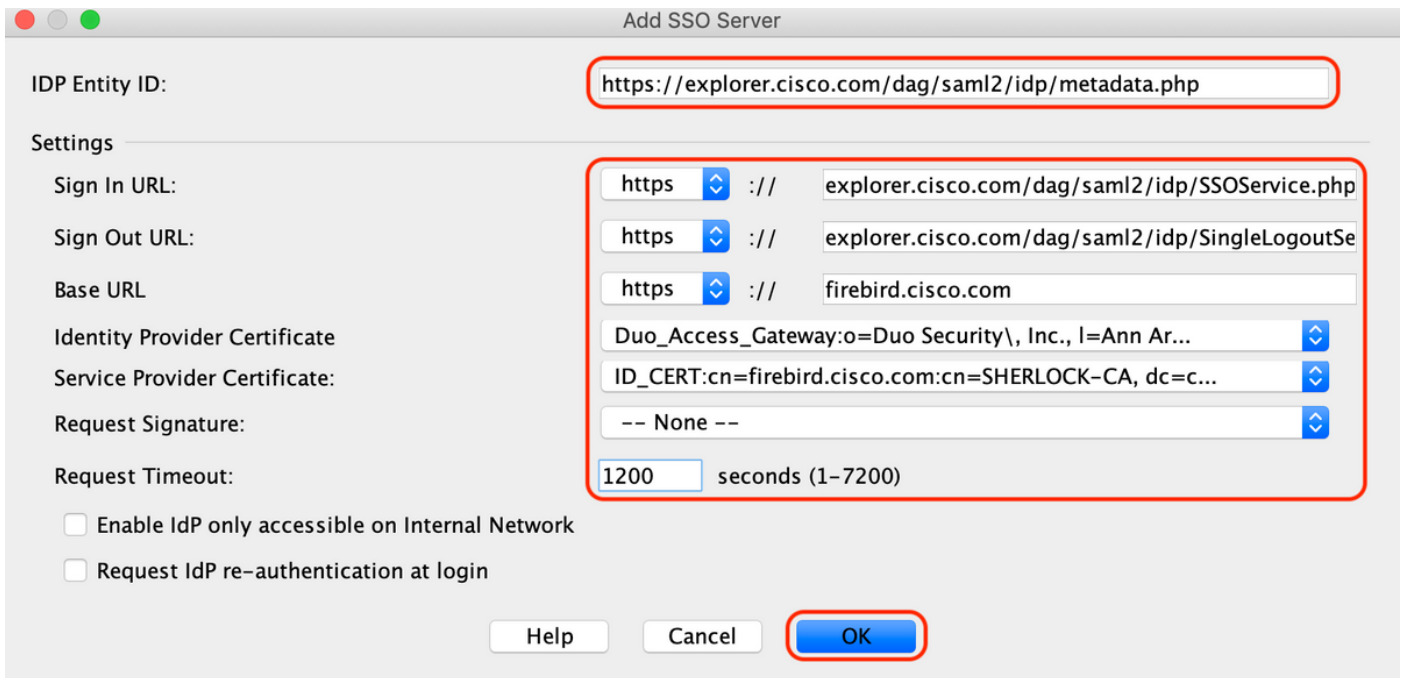
Find: Next Previous

Help Cancel OK

d.在同一页面上，配置SAML身份提供程序详细信息，如下所示：

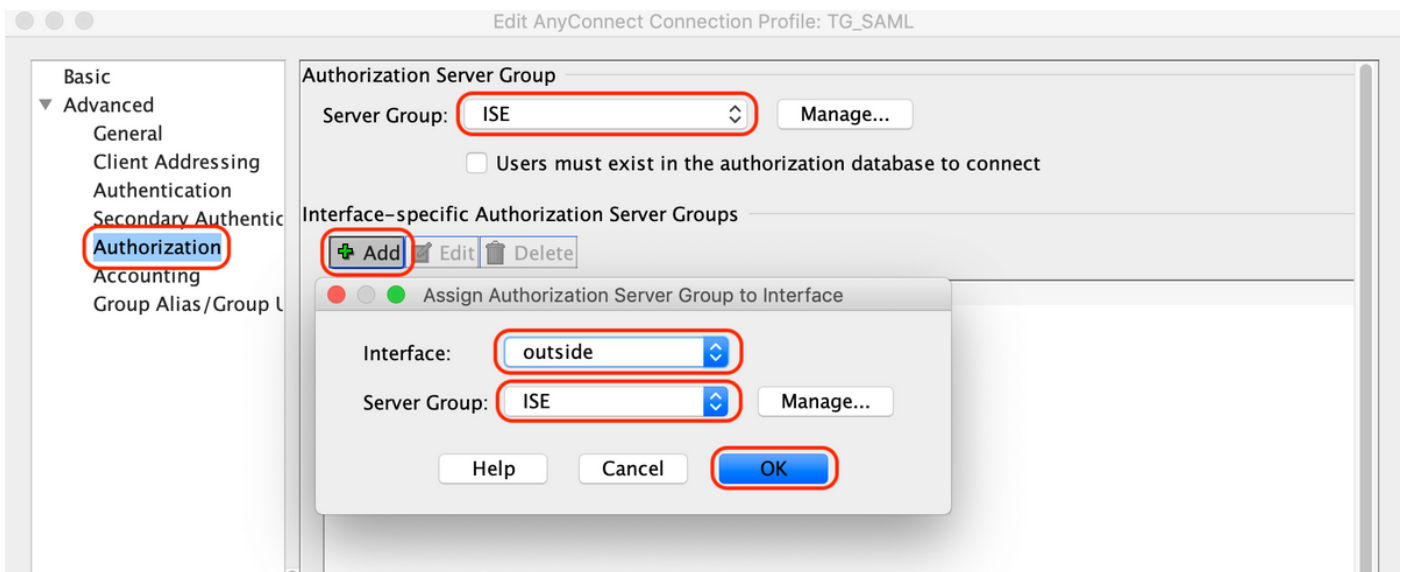
IDP实体Id	<a href="https://explorer.cisco.com/dag/saml2/idp/metadata.php">https://explorer.cisco.com/dag/saml2/idp/metadata.php</a>
登录URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
注销URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com">https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com</a>
基本URL	<a href="https://firebird.cisco.com">https://firebird.cisco.com</a>

E.点击“管理>添加”



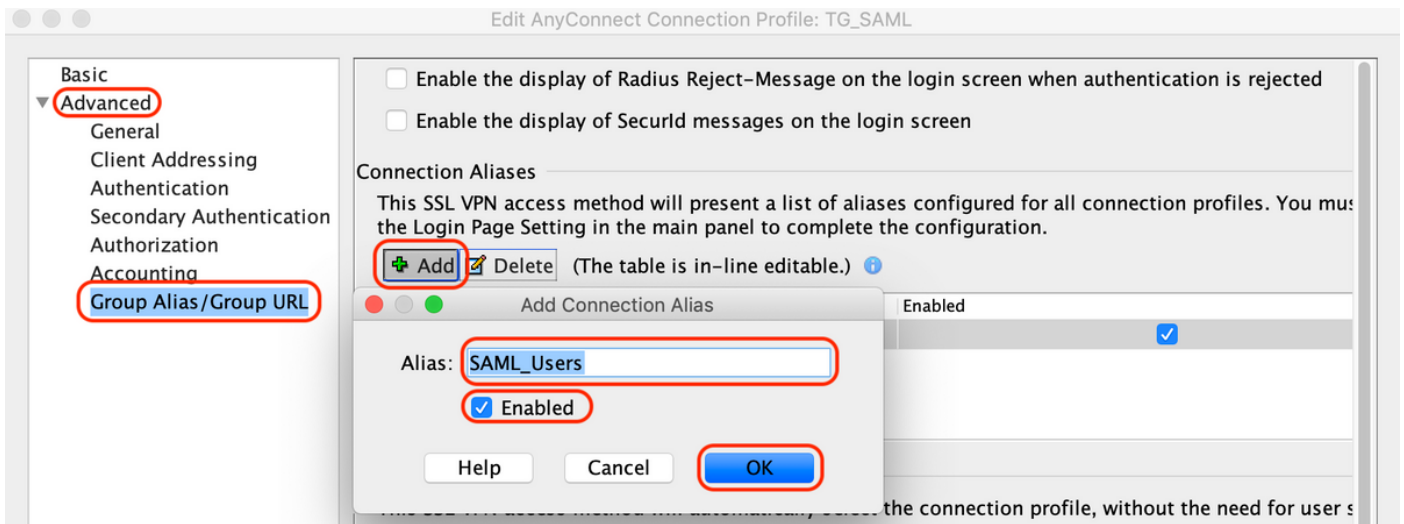
F.在连接配置文件的Advanced部分下，定义用于授权的AAA服务器

导航到“Advanced > Authorization”，然后单击“Add”



G.在“组别名”下，定义连接别名

导航到“Advanced > Group Alias/Group URL”，然后单击“Add”



H.这样，ASA配置即完成，如下面的命令行界面(CLI)所示

```

!
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 sam1
group-alias SAML_Users enable
saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
!

```

## -ISE 配置

### 1.添加Cisco ASA作为网络设备

在“Administration > Network Resources > Network Devices”下，单击“Add”。

配置网络设备的名称、关联的IP地址，并在“Radius身份验证设置”下配置“共享密钥”并单击“保存”

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. 安装最新的状态更新

导航至“管理>系统>设置>状态>更新”并单击“立即更新”

---

### 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. 上传ISE上的合规性模块和AnyConnect头端部署包

导航到“Policy > Policy Elements > Results > Client Provisioning > Resources”。点击“添加”，然后根据要从本地工作站还是思科站点获取文件，选择“从本地磁盘获取代理资源”或“从思科站点获取代理资源”。

在这种情况下，要从“类别”下的本地工作站上传文件，请选择“思科提供的软件包”，然后单击“浏览”，选择所需的软件包，然后单击“提交”。

本文档使用“anyconnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg”作为合规性模块，使用“anyconnect-win-4.8.03052-webdeploy-k9.pkg”作为AnyConnect头端部署包。

### 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. 创建AnyConnect状态配置文件

A. 导航到“策略>策略元素>结果>客户端调配>资源”。点击“Add”并选择“AnyConnect Posture Profile”

B. 输入Anyconnect终端安全评估配置文件的名称，并在服务器名称规则下将服务器名称配置为“\*”，然后点击“保存”

### 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. 创建Anyconnect配置

A. 导航到“策略>策略元素>结果>客户端调配>资源”。点击“添加”并选择“AnyConnect配置”

B. 选择AnyConnect软件包，输入配置名称，选择所需的合规性模块

C. 在“AnyConnect模块选择”下，选中“诊断和报告工具”

D. 在“Profile Selection”下，选择Posture Profile并单击“Save”

\* Select AnyConnect Package **AnyConnectDesktopWindows 4.8.3052.0** ▼

\* Configuration Name **AnyConnect Configuration**

Description:

**DescriptionValue**

\* Compliance Module **AnyConnectComplianceModuleWindows 4.3.1250.614** ▼

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 **Anyconnect Posture Profile** ▼

VPN ▼

Network Access Manager ▼

Web Security ▼

AMP Enabler ▼

Network Visibility ▼

Umbrella Roaming Security ▼

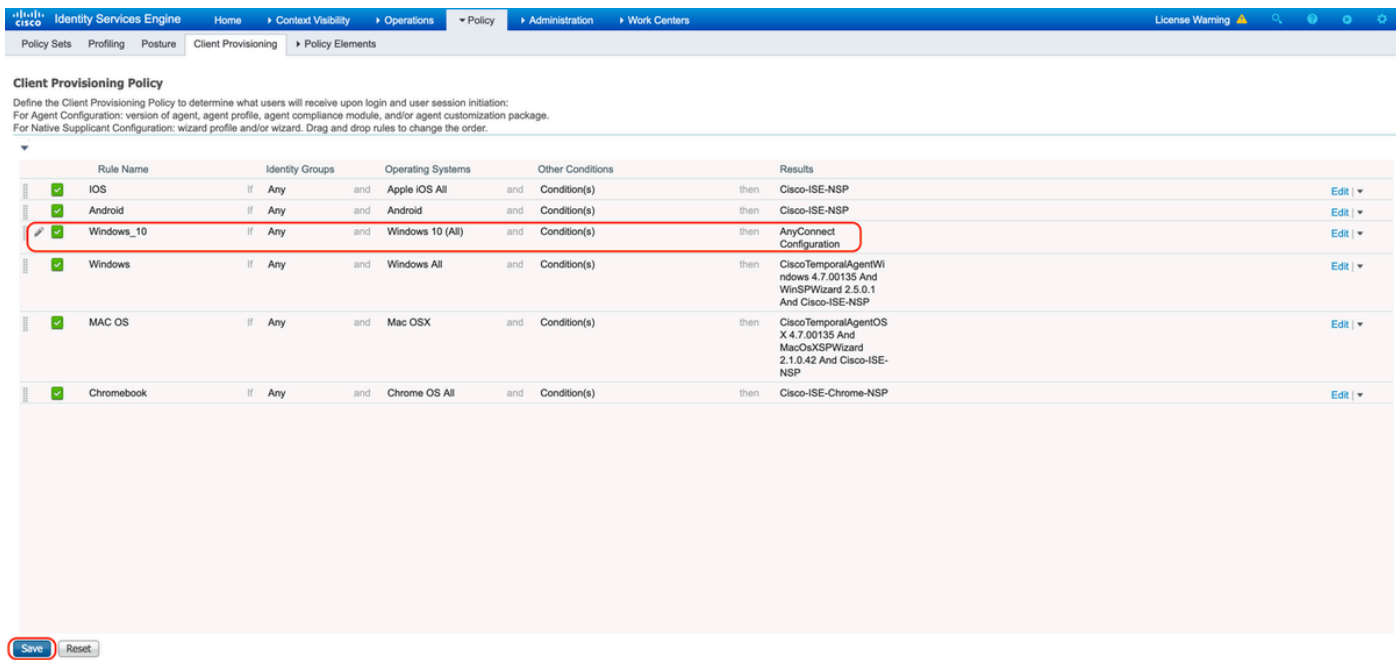
Customer Feedback ▼

## 6. 创建客户端调配策略

A. 导航到“策略>客户端调配”。

B. 点击“编辑”，然后选择“在上面插入规则”

C. 输入Rule Name，选择所需的操作系统，然后在Results（在"Agent" > "Agent Configuration"中）下，选择在第5步中创建的"AnyConnect Configuration"，然后单击"Save"

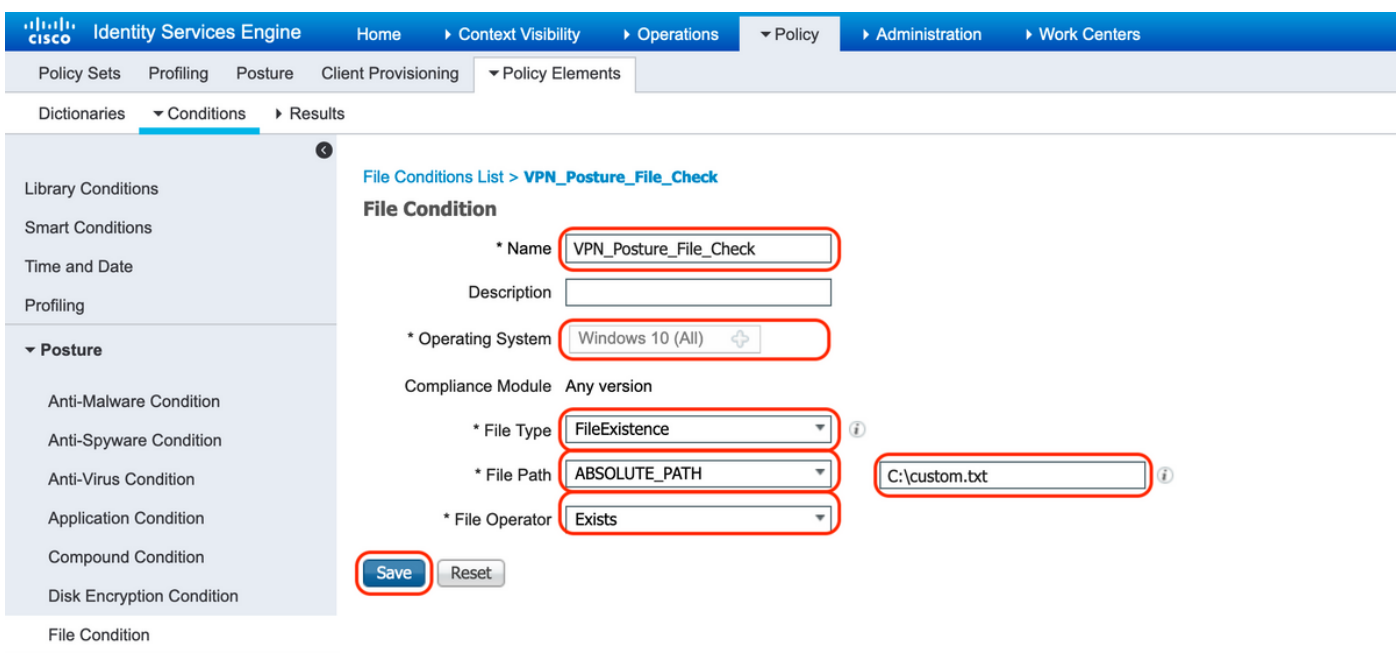


## 7. 创建安全评估条件

A. 导航至“策略>策略元素>条件>状态>文件条件”

B. 单击“添加”并将条件名称“VPN\_Posture\_File\_Check”、所需的操作系统为“Windows 10(All)”、文件类型为“FileExistence”、文件路径为“ABSOLUTE\_PATH”、完整路径和文件名配置为“C:\custom.txt”，选择文件操作符为“Exists”

C. 此示例使用C：驱动器下名为“custom.txt”的文件作为文件条件



## 8. 创建状况补救操作

导航到“Policy > Policy Elements > Results > Posture > Remediation Actions”以创建对应的File Remediation Action。本文档使用“仅消息文本”作为下一步中配置的补救操作。

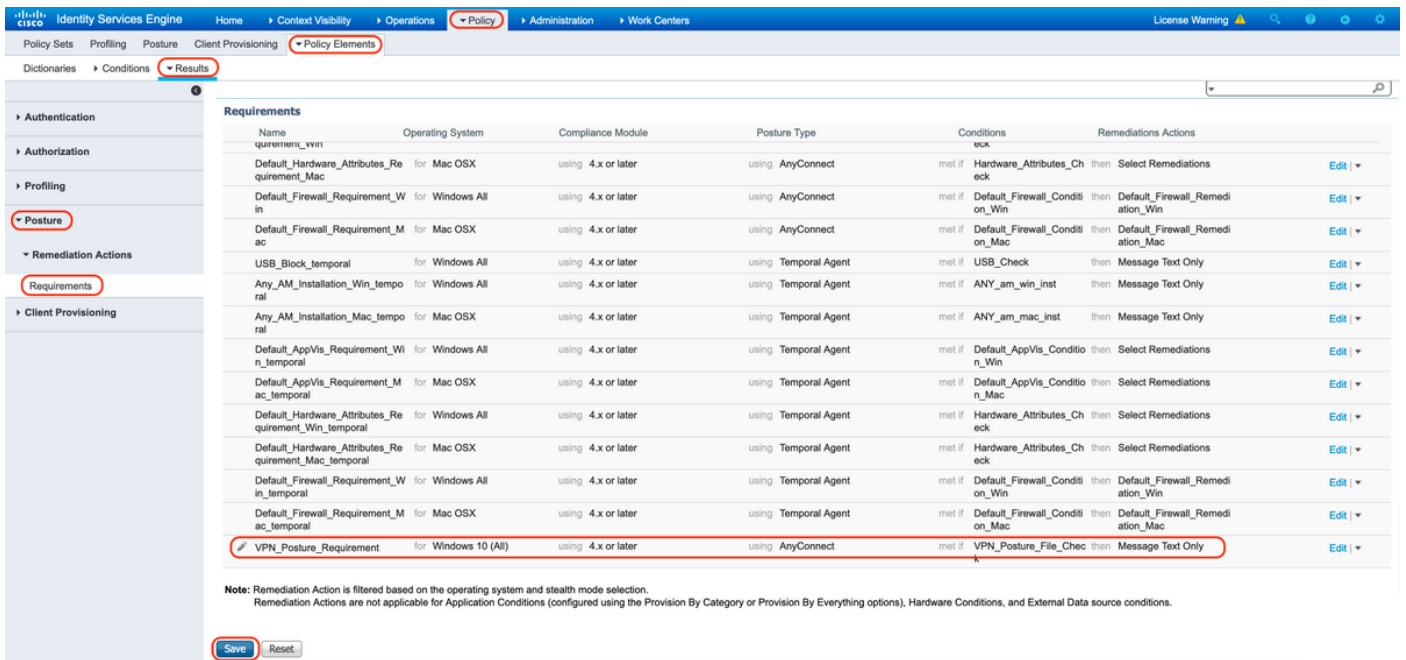
## 9. 创建状况要求规则

A. 导航至“策略>策略元素>结果>状态>要求”

B. 单击“编辑”，然后选择“插入新要求”

C. 将条件名称“VPN\_Posture\_Requirement”、所需的操作系统配置为“Windows 10(All)”、合规性模块配置为“4.x或更高版本”、安全评估类型配置为“Anyconnect”

D. 条件为“VPN\_Posture\_File\_Check”（在第7步中创建），在“Remediations Actions”下，选择“Action”作为“Message Text Only”，然后输入座席用户的自定义消息



## 10. 创建安全评估策略

A. 导航到“策略>状态”

B. 将规则名称配置为“VPN\_Posture\_Policy\_Win”，将所需的操作系统配置为“Windows 10(All)”，将合规性模块配置为“4.x或更高版本”，将状态类型配置为“Anyconnect”，将要求配置为“VPN\_Posture\_Requirement”（如步骤9中所配置）

**Posture Policy**  
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

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

Save Reset

## 11. 创建动态ACL(DACL)

导航到 Policy > Policy Elements > Results > Authorization > Downloadable ACL，并为不同的安全评估状态创建DAACL。

本文档使用以下DAACL。

### A. 安全评估未知：允许流量到达DNS、PSN、HTTP和HTTPS流量

Downloadable ACL List > PostureUnknown

**Downloadable ACL**

\* Name: PostureUnknown

Description: [Empty]

IP version:  IPv4  IPv6  Agnostic

\* DAACL Content:

```

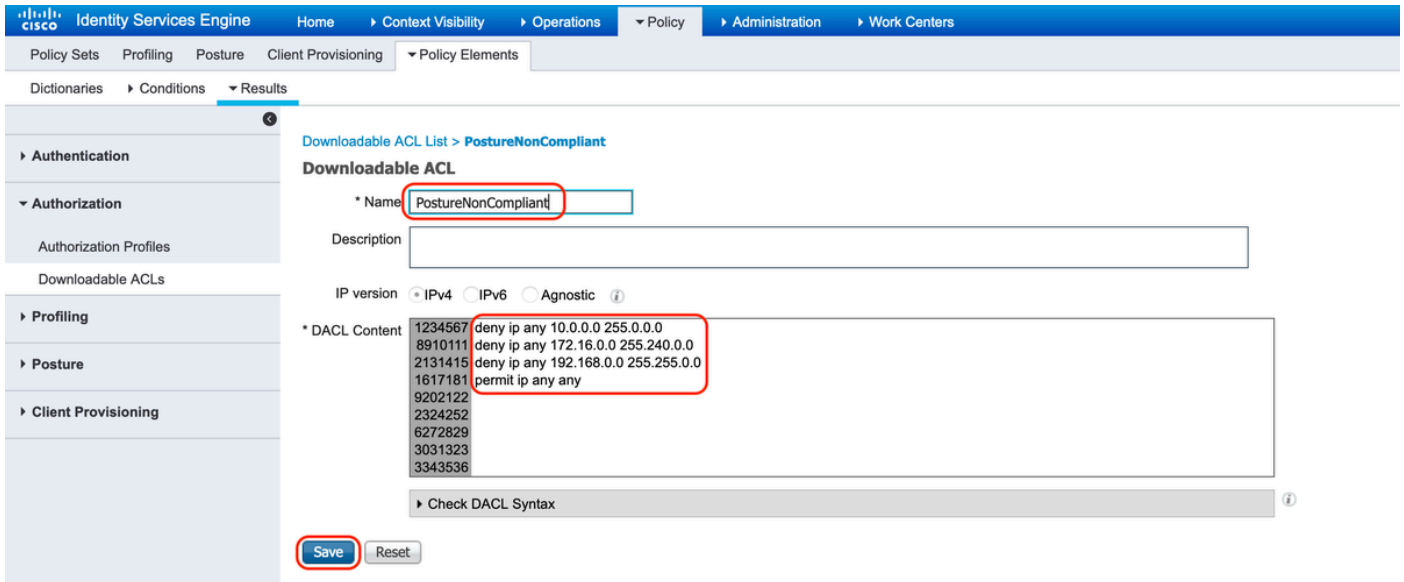
1234567 permit udp any any eq domain
8910111 permit ip any host 10.106.44.77
2131415 permit tcp any any eq 80
1617181 permit tcp any any eq 443
9202122
2324252
6272629
3031323
3343536

```

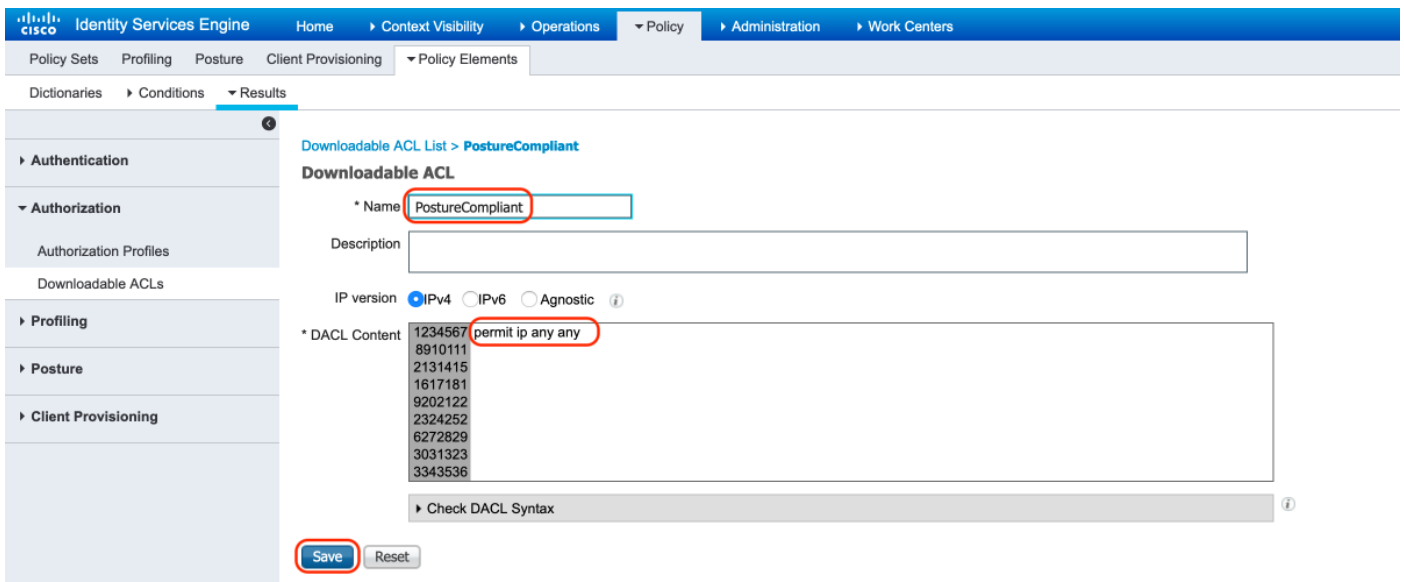
Check DAACL Syntax

Save Reset

### B. 状态不兼容：拒绝访问私有子网并仅允许互联网流量



### C.安全评估合规性：允许安全评估合规性最终用户的所有流量



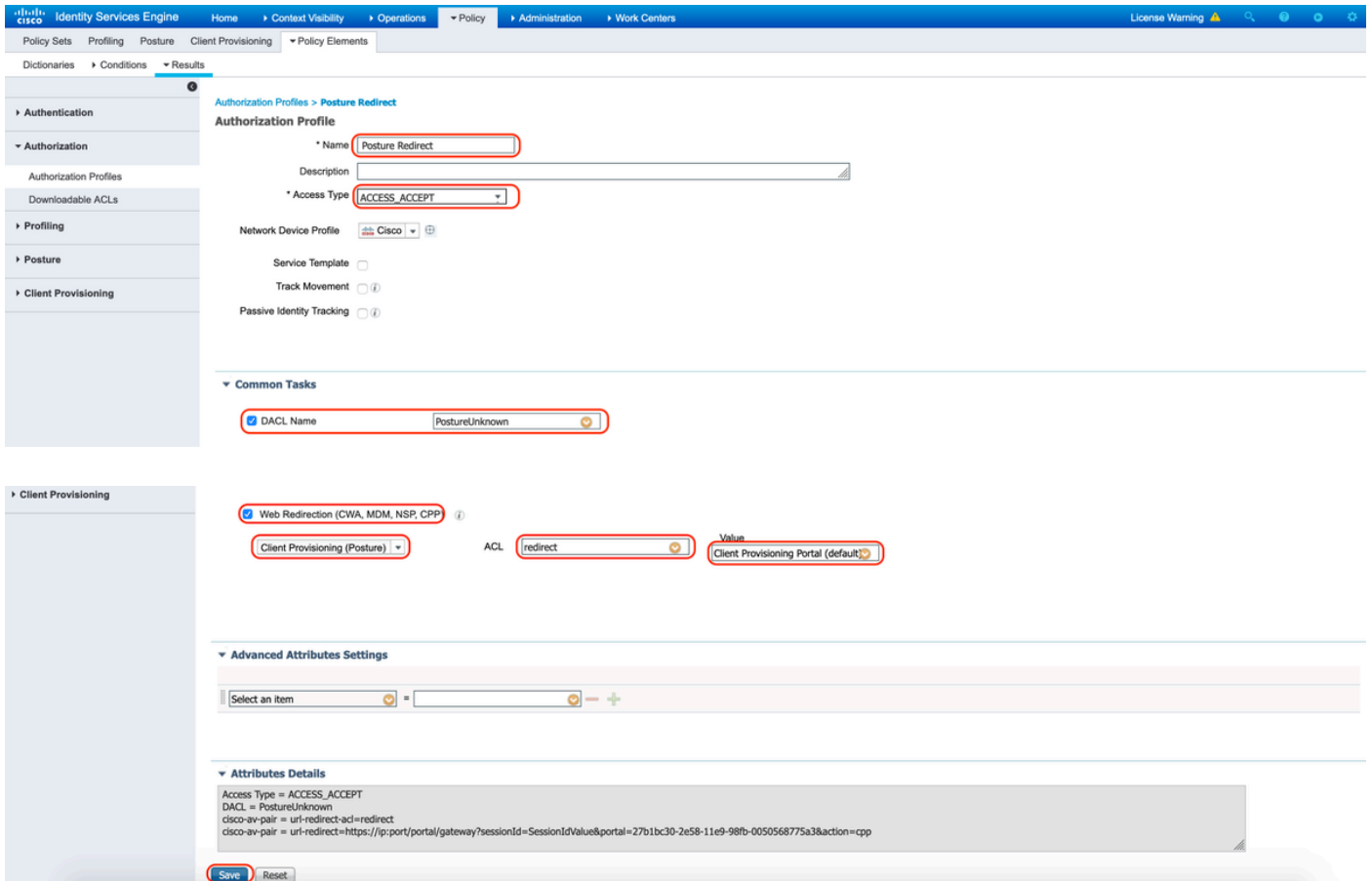
## 12.创建授权配置文件

导航至“Policy > Policy Elements > Results > Authorization > Authorization Profiles”。

### A.未知状态的授权配置文件

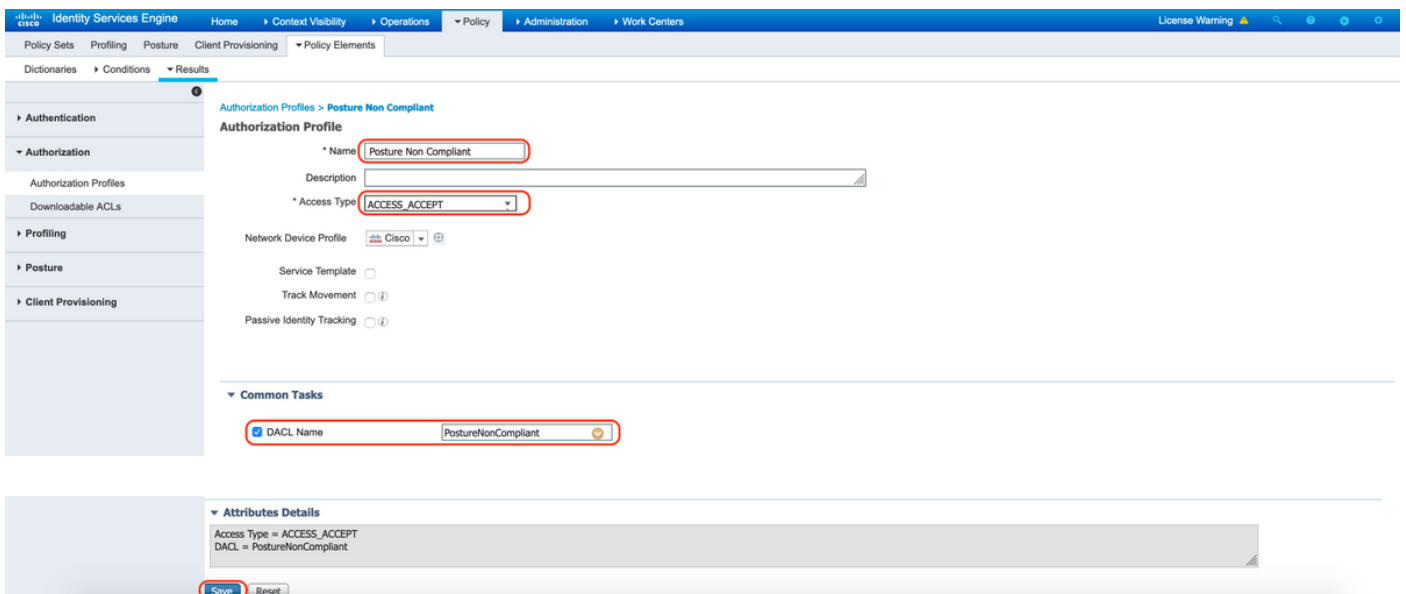
选择DACL“PostureUnknown”，选中Web Redirection，选择Client Provisioning(Posture)，配置 Redirect ACL名称“redirect”（要在ASA上配置），然后选择Client Provisioning门户（默认）





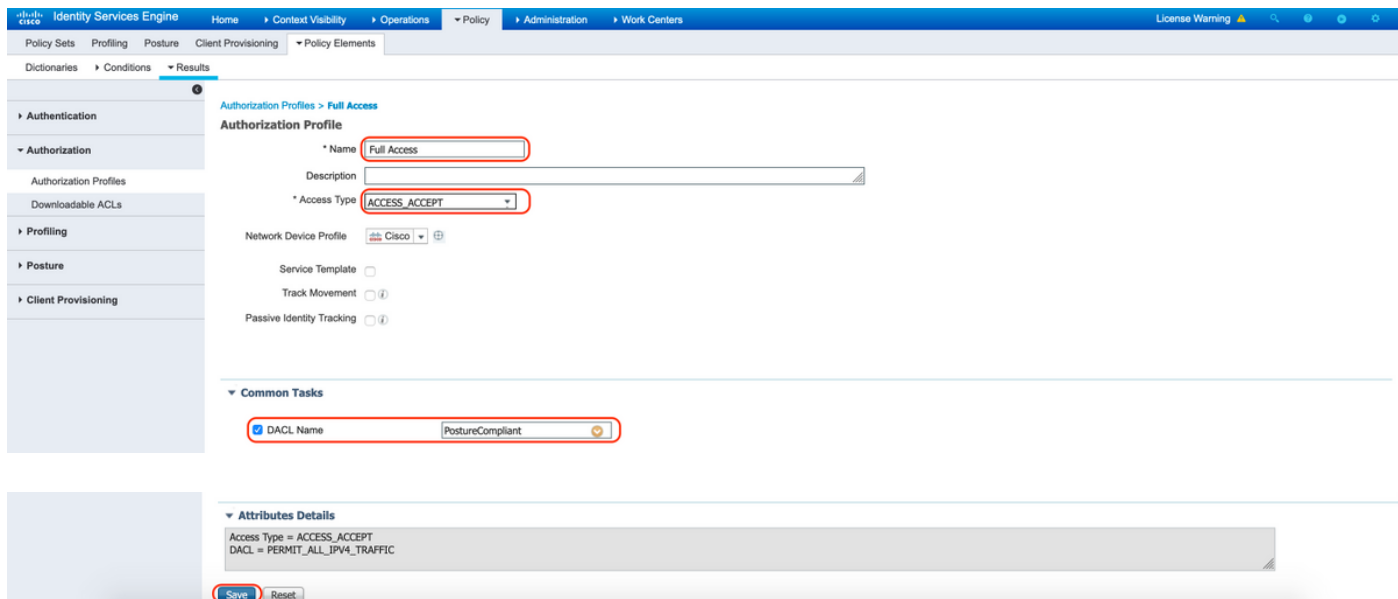
## B. 状态不合规的授权配置文件

选择DACL“PostureNonCompliant”以限制对网络的访问



## C. 安全评估合规性的授权配置文件

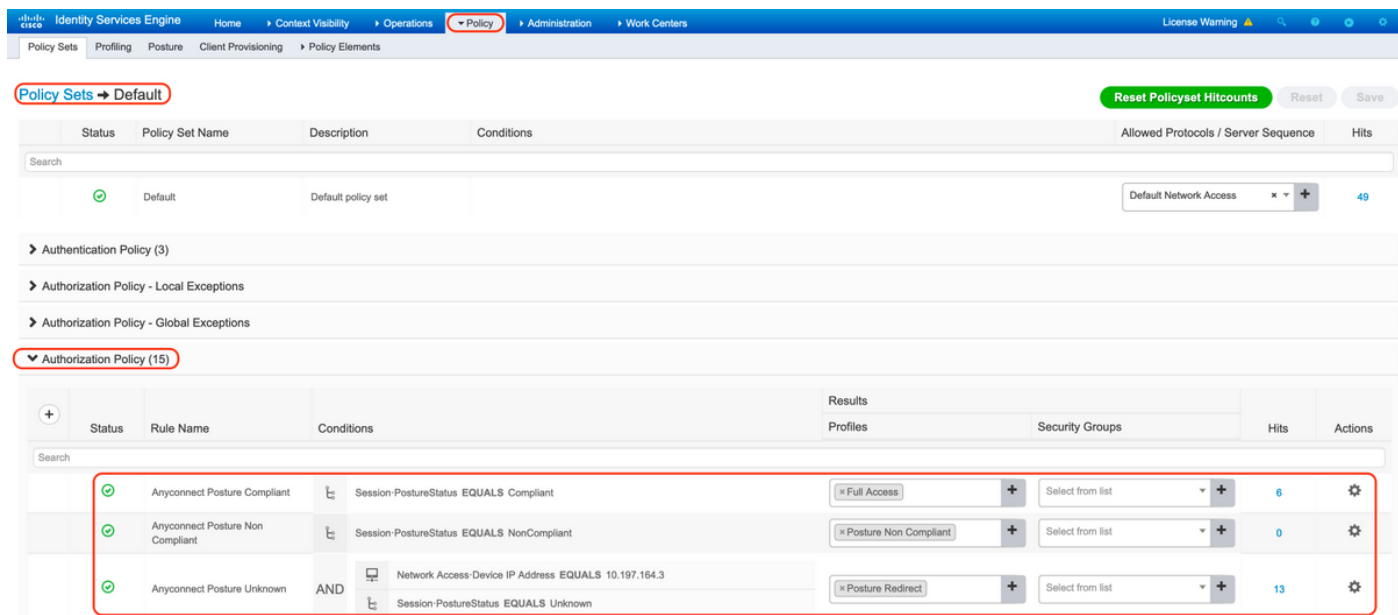
## 选择DACL“PostureCompliant”以允许对网络的完全访问



## 12. 配置授权策略

使用在上一步中配置的授权配置文件为安全评估合规性、安全评估不合规性和安全评估未知配置3个授权策略。

通用条件“会话：状态状态”用于确定每个策略的结果



## 验证

使用本部分可确认配置能否正常运行。

要验证用户是否成功通过身份验证，请在ASA上运行以下命令。

```
<#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

状态评估完成后，用户访问将更改为完全访问，如字段“Filter Name”中推送的DACL中所示

<#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-57E6b0d3

要验证是否在ISE上成功执行授权，请导航到“操作> RADIUS >实时日志”

此部分显示与授权用户相关的信息，例如身份、授权配置文件、授权策略和状态状态。

Refresh Never Show Latest 20 records Within Last 24 hours

Refresh Reset Repeat Counts Export To Filter

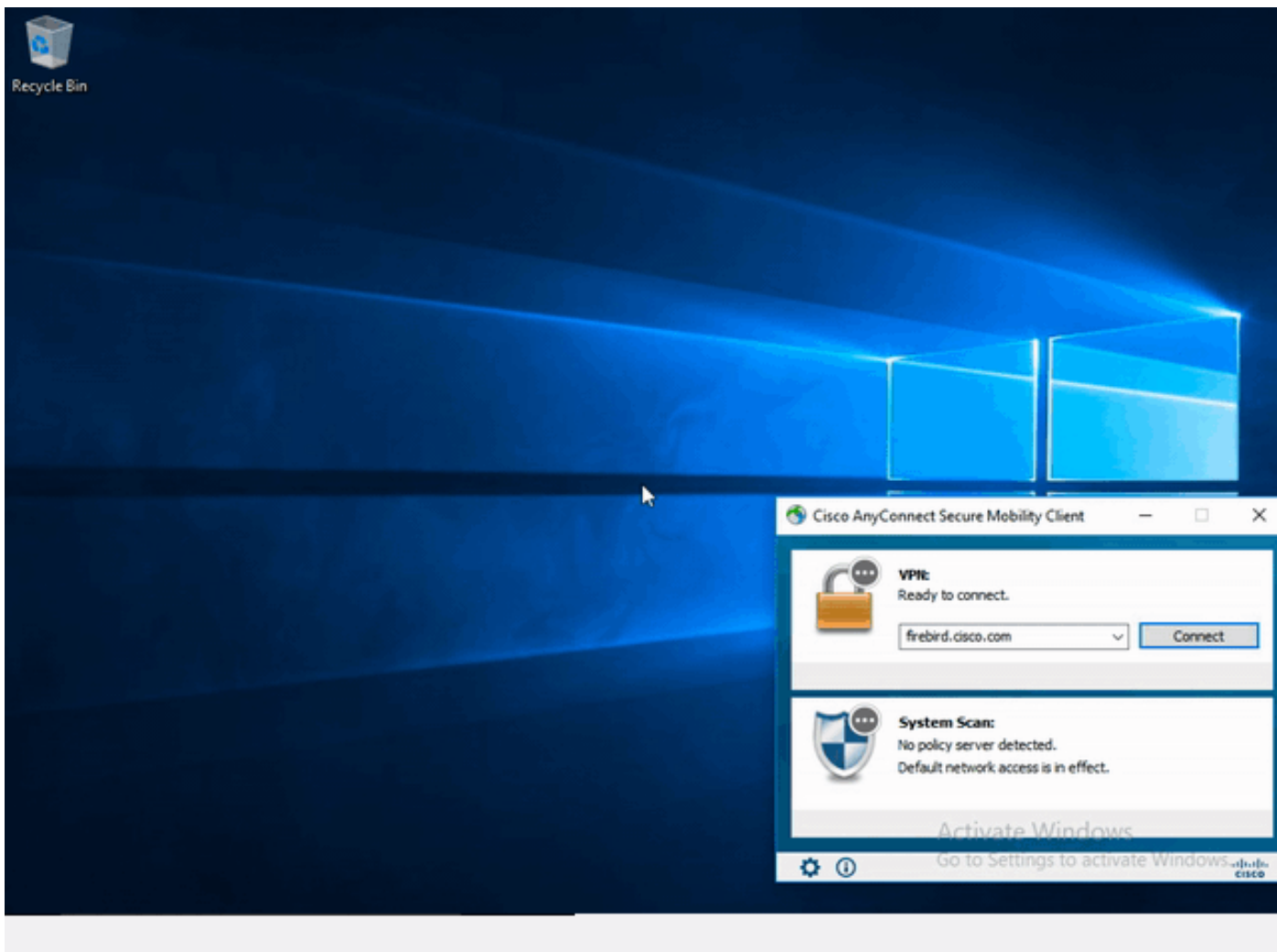
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM			0	_585b5291f01484df1...	00:50:56:A0:D6:97	Windows10-...	Default	Anyconnect ...	Full Access	Compliant	10.197.164.7	ASA
Jun 14, 2020 07:44:59.975 AM				#ACSACL#-IP-PERMI...	10.197.243.143			Anyconnect ...	Full Access	Compliant		ASA
Jun 14, 2020 07:44:34.963 AM				#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.958 AM				_585b5291f01484df1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA

注意：有关ISE上的其他状态验证，请参阅以下文档：  
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc7>

要验证Duo Admin Portal的身份验证状态，请点击Admin Panel左侧的“Reports”，Admin Panel将显示Authentication Log。  
更多详情：<https://duo.com/docs/administration#reports>


要查看Duo接入网关的调试日志记录，请使用以下链接：  
[https://help.duo.com/s/article/1623?language=en\\_US](https://help.duo.com/s/article/1623?language=en_US)


## 用户体验



## 故障排除

本节提供可用于对配置进行故障排除的信息。

 注意：使用[debug命令之前](#)，请参阅有关Debug命令的重要信息。

 注意：在ASA上，您可以设置各种调试级别；默认情况下，使用级别1。如果更改调试级别，调试的详细程度可能会增加。请谨慎执行此操作，尤其是在生产环境中。

大多数SAML故障排除都会涉及配置错误，通过检查SAML配置或运行调试可以发现该错误。

debug webvpn saml 255可用于排除大多数问题，但在此调试不提供有用信息的情况下，可以运行其他调试：

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

要排除ASA上的身份验证和授权问题，请使用以下debug命令：

```
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)
```



注意：有关详细的安全评估流程和AnyConnect和ISE故障排除，请参阅以下链接：

[高级版和高级版2.2的ISE终端安全评估样式比较](#)

解释Duo接入网关调试日志并排除其故障

[https://help.duo.com/s/article/5016?language=en\\_US](https://help.duo.com/s/article/5016?language=en_US)

---

## 相关信息

<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>



## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。