Integre o SSO SAML Duo com o Acesso Remoto Seguro do Anyconnect usando a Postura do ISE

Contents

Introdução

Este documento descreve um exemplo de configuração para integração do SSO SAML Duo com o acesso do Cisco AnyConnect Secure Mobility Client do Adaptive Security Appliance (ASA) que aproveita o Cisco ISE para uma avaliação de postura detalhada. O SSO SAML Duo é implementado usando o Gateway de Acesso Duo (DAG), que se comunica com o Ative Diretory para autenticação inicial do usuário e, em seguida, se comunica com o Duo Security (Cloud) para autenticação multifator. O Cisco ISE é usado como um servidor de autorização para fornecer verificação de endpoint usando avaliação de postura.

Contribuição de Dinesh Moudgil e Pulkit Saxena, Engenheiro HTTS da Cisco.

Pré-requisitos

Requisitos

Este documento pressupõe que o ASA esteja totalmente operacional e configurado para permitir que o Cisco Adaptive Security Device Manager (ASDM) ou a Interface de Linha de Comando

(CLI) faça alterações na configuração.

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fundamentos do Gateway de Acesso Duo e Segurança Duo
- Conhecimento básico da configuração da VPN de acesso remoto no ASA
- Conhecimento básico de ISE e serviços de postura

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

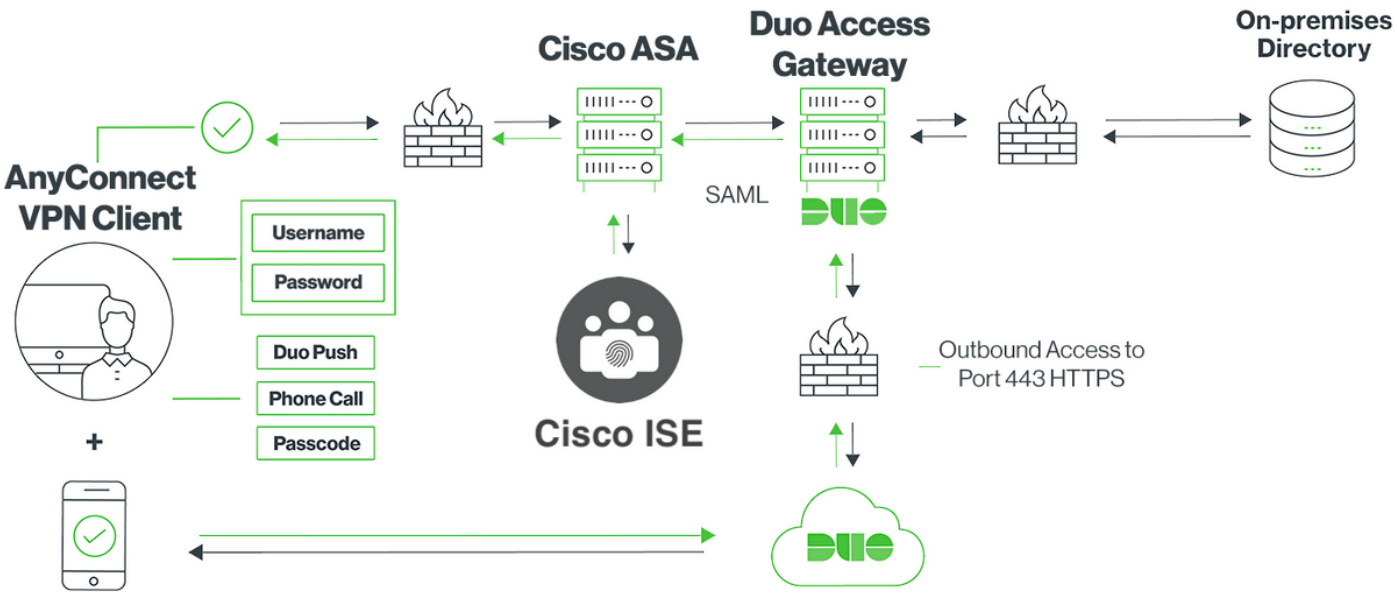
- Software Cisco Adaptive Security Appliance Versão 9.12(3)12
- Gateway de acesso Duo
- Segurança Duo
- Cisco Identity Services Engine versão 2.6 e posterior
- Microsoft Windows 10 com AnyConnect versão 4.8.03052

Observação: o Anyconnect Embedded Browser, usado nesta implementação, requer o ASA na versão 9.7(1)24, 9.8(2)28, 9.9(2)1 ou superior de cada versão, e o AnyConnect versão 4.6 ou posterior.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Fluxo de tráfico

1. O Anyconnect Client inicia uma conexão VPN SSL com o Cisco ASA

2. O Cisco ASA, configurado para autenticação primária com o Gateway de Acesso Duo (DAG), redireciona o navegador incorporado no cliente Anyconnect para a autenticação SAML

3. O cliente Anyconnect é redirecionado para o Gateway de Acesso Duo

4. Depois que o cliente AnyConnect insere as credenciais, uma solicitação de autenticação SAML é criada e emitida do Cisco ASA para o Gateway de Acesso Duo

5. O Gateway de acesso Duo aproveita a integração com o Ative Diretory no local para executar a autenticação primária para o cliente Anyconnect

6. Assim que a autenticação primária for bem-sucedida, o Gateway de Acesso Duo envia uma solicitação ao Duo Security pela porta TCP 443 para iniciar a autenticação de dois fatores

7. O cliente AnyConnect apresentou "Duo Interative Prompt" e o usuário conclui a autenticação de dois fatores do Duo usando seu método preferido (push ou senha)

8. A Segurança Duo recebe uma resposta de autenticação e retorna as informações ao Gateway de Acesso Duo

9. Com base na resposta de autenticação, o Gateway de Acesso Duo cria uma resposta de autenticação SAML que contém a asserção SAML e responde ao cliente Anyconnect

10. O cliente Anyconnect autentica com êxito a conexão VPN SSL com o Cisco ASA

11. Quando a autenticação for bem-sucedida, o Cisco ASA enviará uma solicitação de

autorização ao Cisco ISE

> Observação: o Cisco ISE é configurado apenas para autorização, já que o Gateway de Acesso Duo fornece a autenticação necessária

12. O Cisco ISE processa a solicitação de autorização e, como o status da postura do cliente é Desconhecido, retorna o redirecionamento de postura com acesso limitado ao cliente Anyconnect por meio do Cisco ASA

13. Se o Anyconnect client não tiver um módulo de conformidade, será solicitado que ele faça o download para prosseguir com a avaliação de postura

14. Se o Anyconnect client tiver um módulo de conformidade, ele estabelecerá uma conexão TLS com o Cisco ASA e o fluxo de postura será iniciado

15. Dependendo das condições de postura configuradas no ISE, as verificações de postura são feitas e os detalhes são enviados do cliente Anyconnect para o Cisco ISE

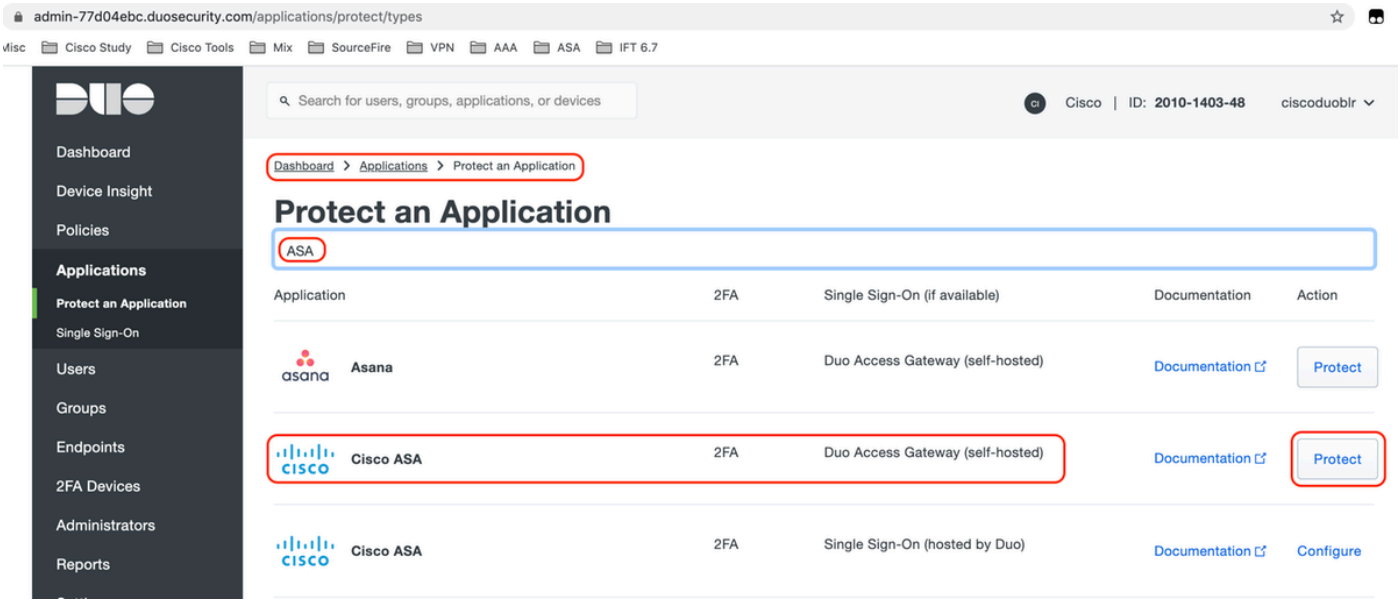
16. Se o status da postura do cliente mudar de Desconhecido para Compatível, a solicitação de alteração de autorização (CoA) é enviada do Cisco ISE para o Cisco ASA para conceder acesso total ao cliente e a VPN é totalmente estabelecida

Configurações

- Configuração do Portal de Administração Duo

Nesta seção, configure o aplicativo ASA no Portal de administração do Duo.

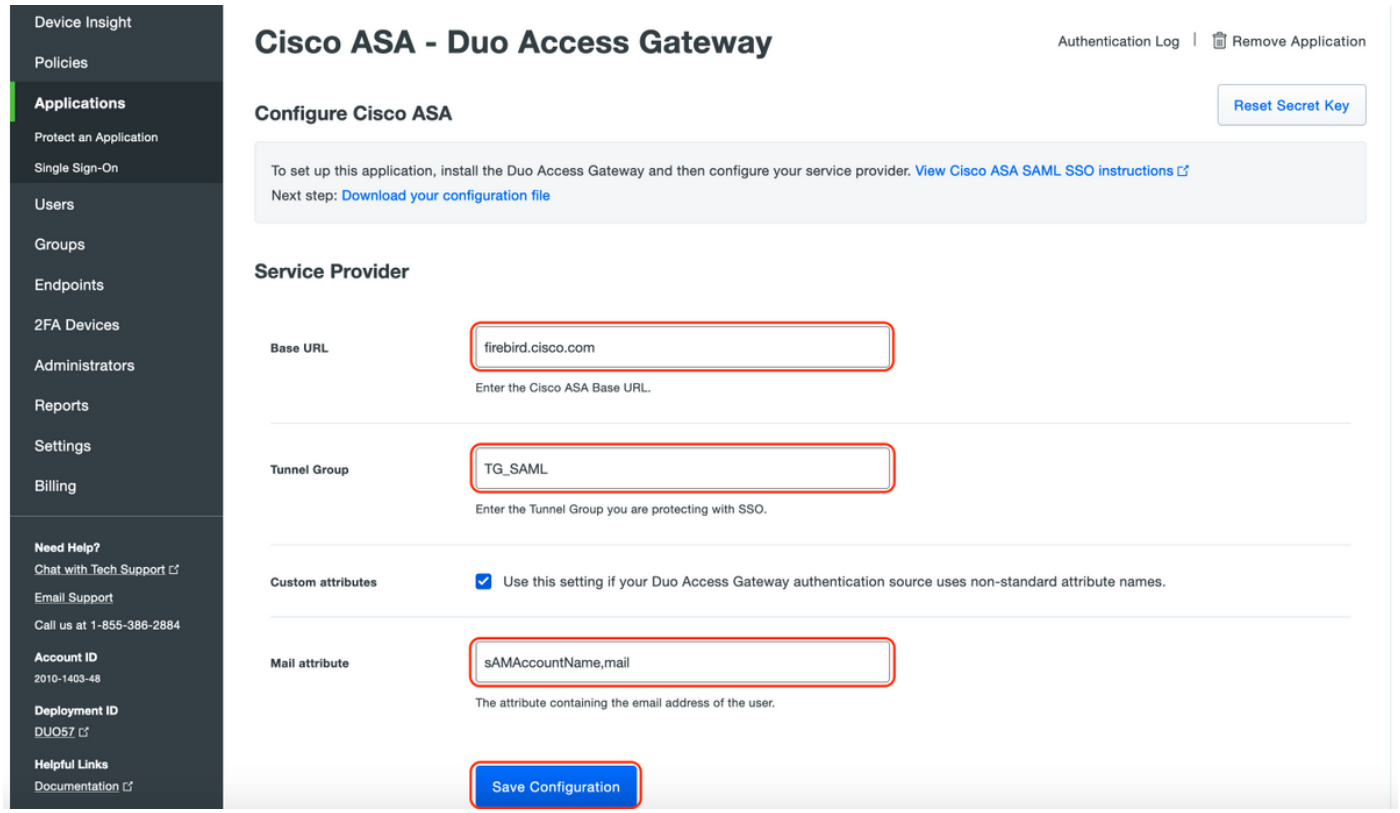
1. Faça login no "Duo Admin Portal" e navegue até "Applications > Protect an Application", e procure "ASA" com o tipo de proteção "2FA with Duo Access Gateway, self-hosted". Clique em "Proteger" à direita para configurar o Cisco ASA



2. Configure os seguintes atributos em "Provedor de serviços" para o aplicativo protegido, ASA

URL base	firebird.cisco.com
Grupo de Túneis	TG_SAML
Atributo de e-mail	sAMAccountName,mail

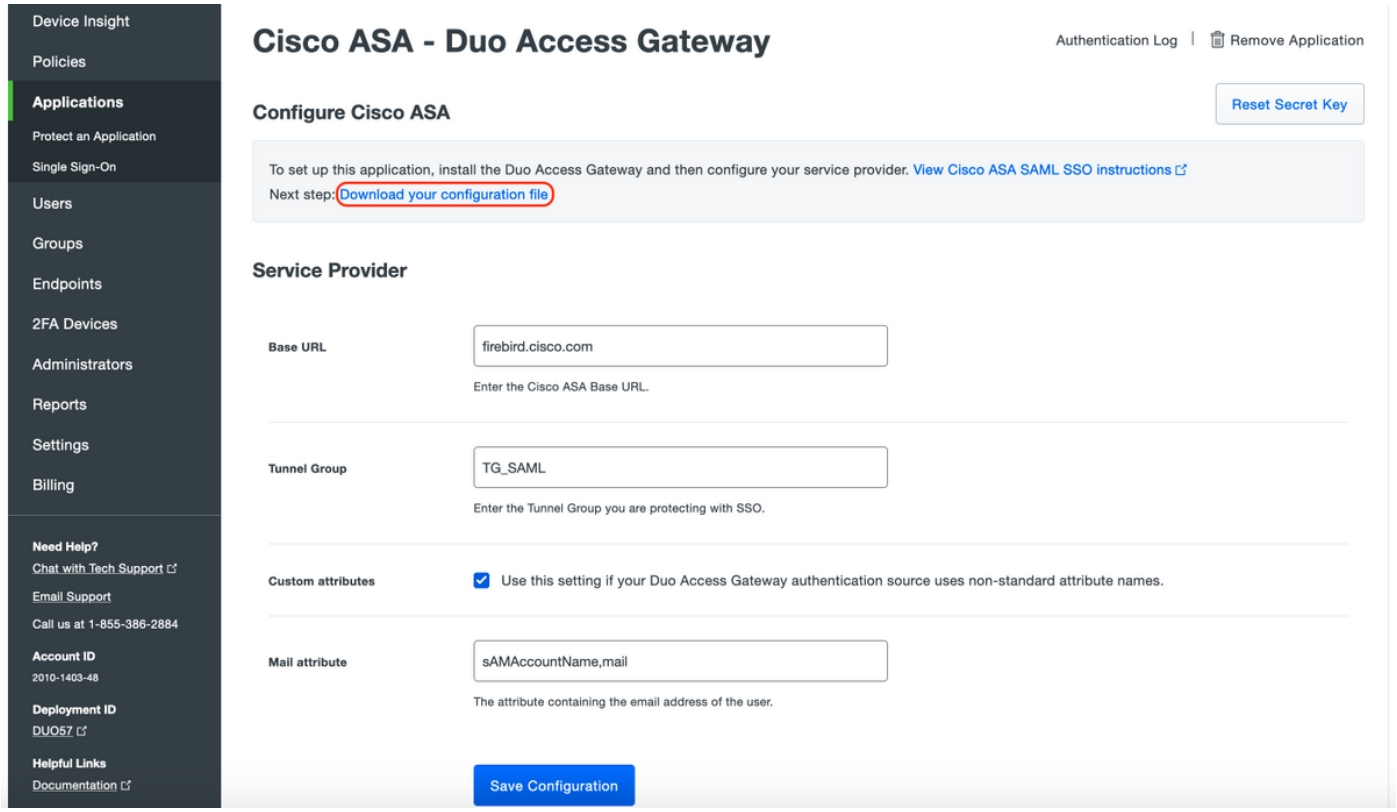
Clique em "Salvar" na parte inferior da página



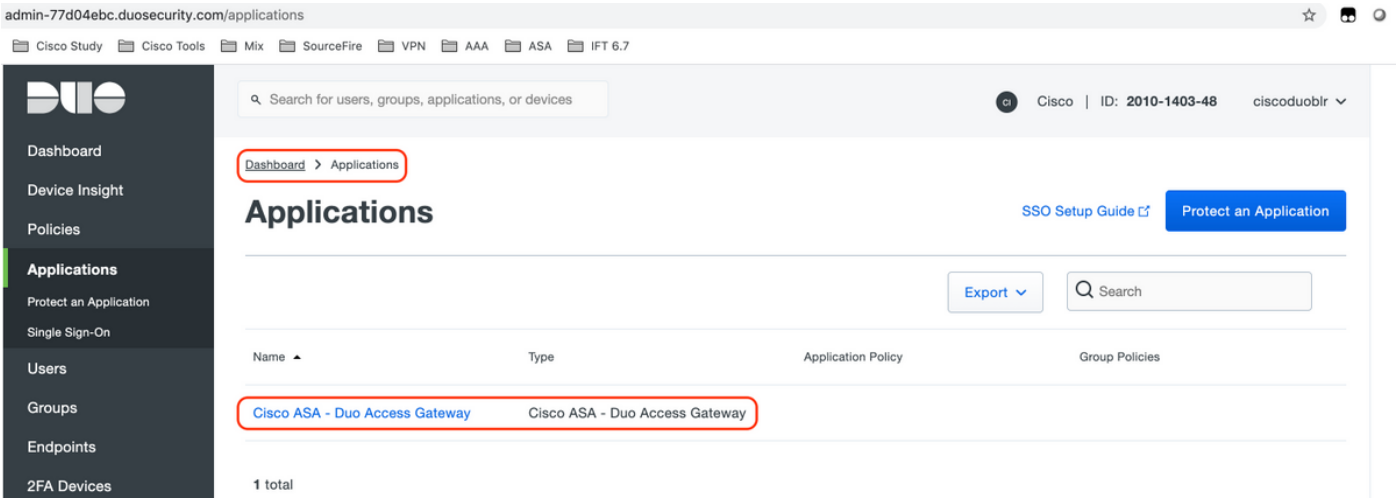
Neste documento, o restante da configuração usa parâmetros padrão, mas eles podem ser

definidos com base nos requisitos do cliente.
As configurações adicionais podem ser ajustadas para o novo aplicativo SAML neste momento, como alterar o nome do aplicativo do valor padrão, ativar o autoatendimento ou atribuir uma política de grupo.

3. Clique no link "Fazer download do arquivo de configuração" para obter as configurações do aplicativo Cisco ASA (como um arquivo JSON). Esse arquivo será carregado no Gateway de Acesso Duo em etapas posteriores

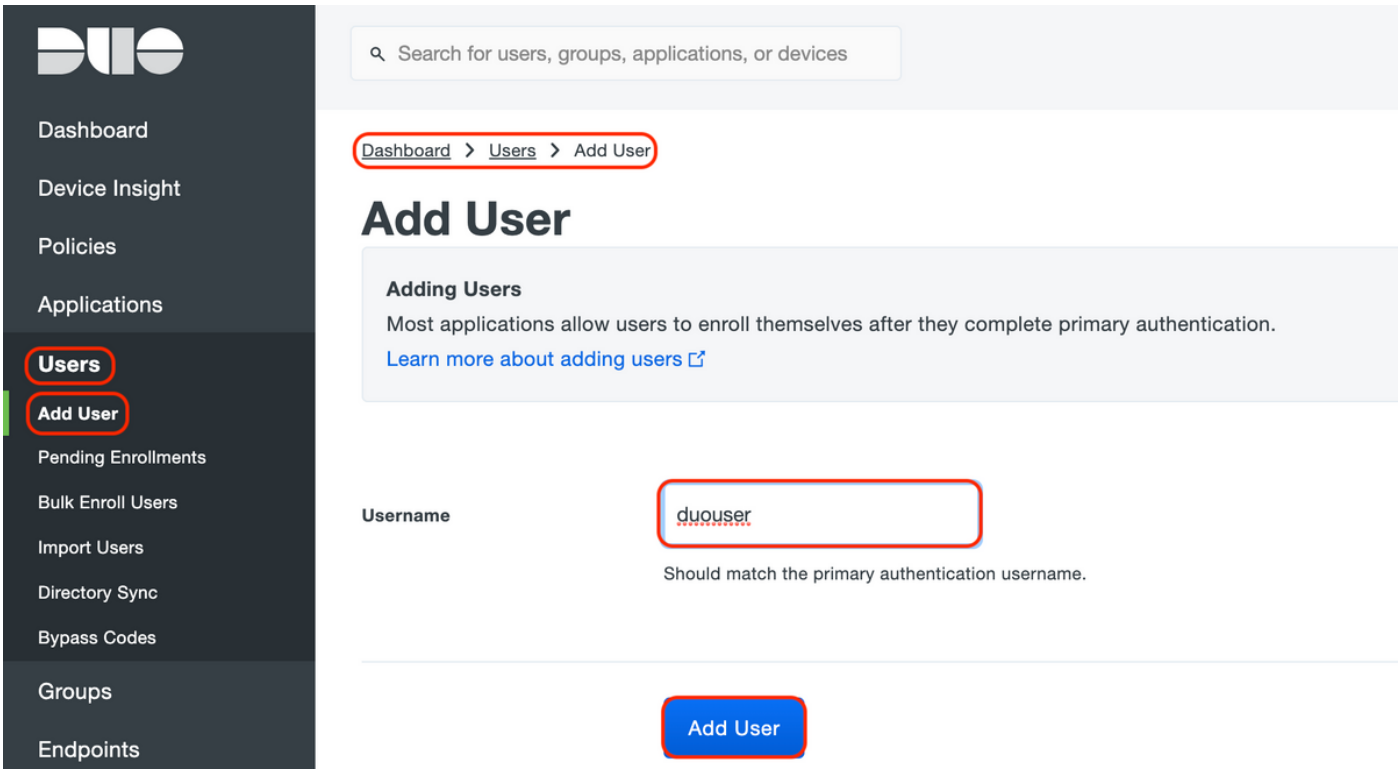


4. Em "Painel > Aplicativos", o aplicativo ASA recém-criado se parece com o mostrado na imagem abaixo:

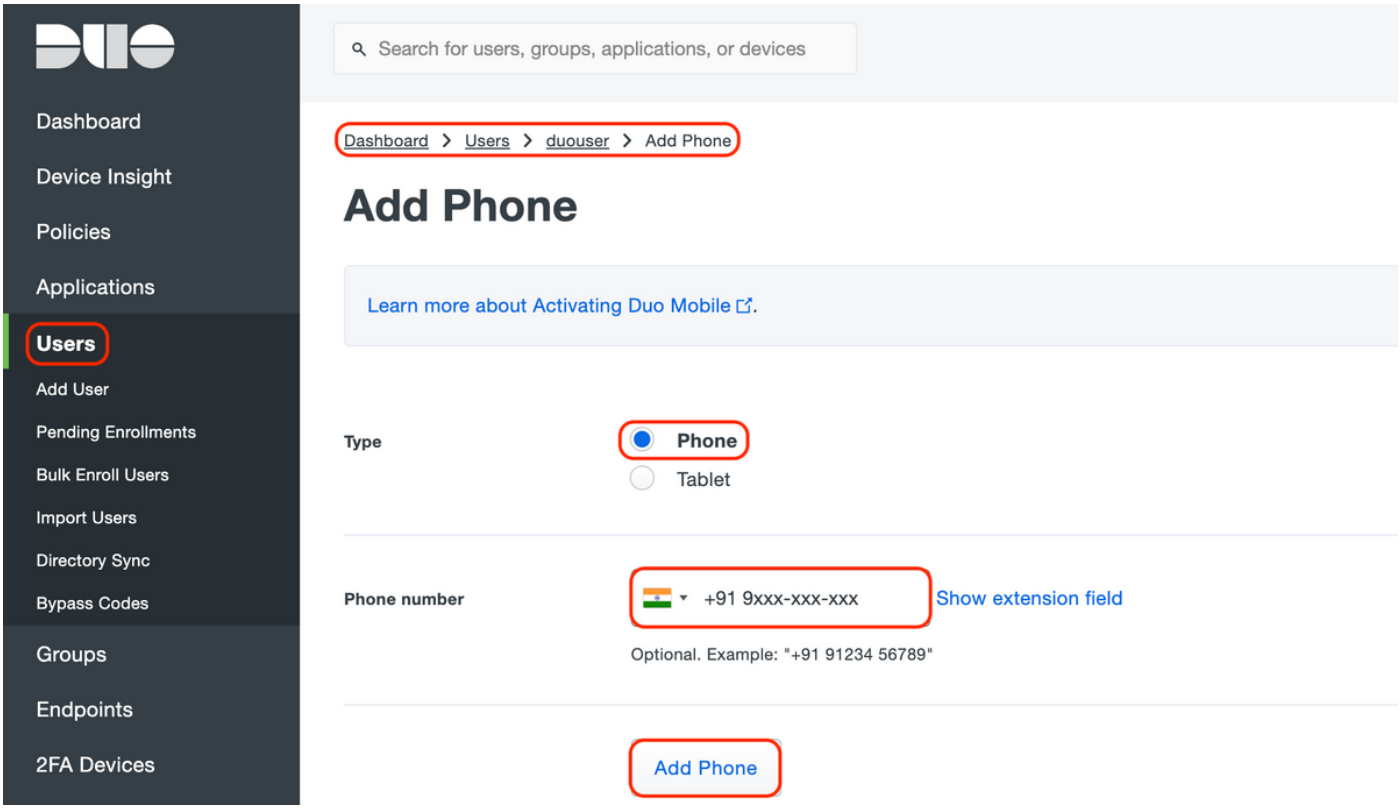


5. Navegue até "Usuários > Adicionar Usuário" conforme mostrado na imagem:

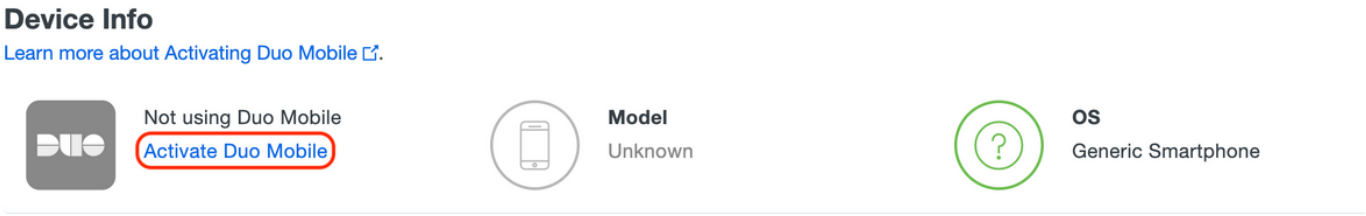
Crie um usuário chamado "duouser" para ser usado na autenticação do Acesso Remoto do Anyconnect e ative o Duo Mobile no dispositivo do usuário final



Para adicionar o número de telefone conforme mostrado na imagem, selecione a opção "Adicionar telefone".

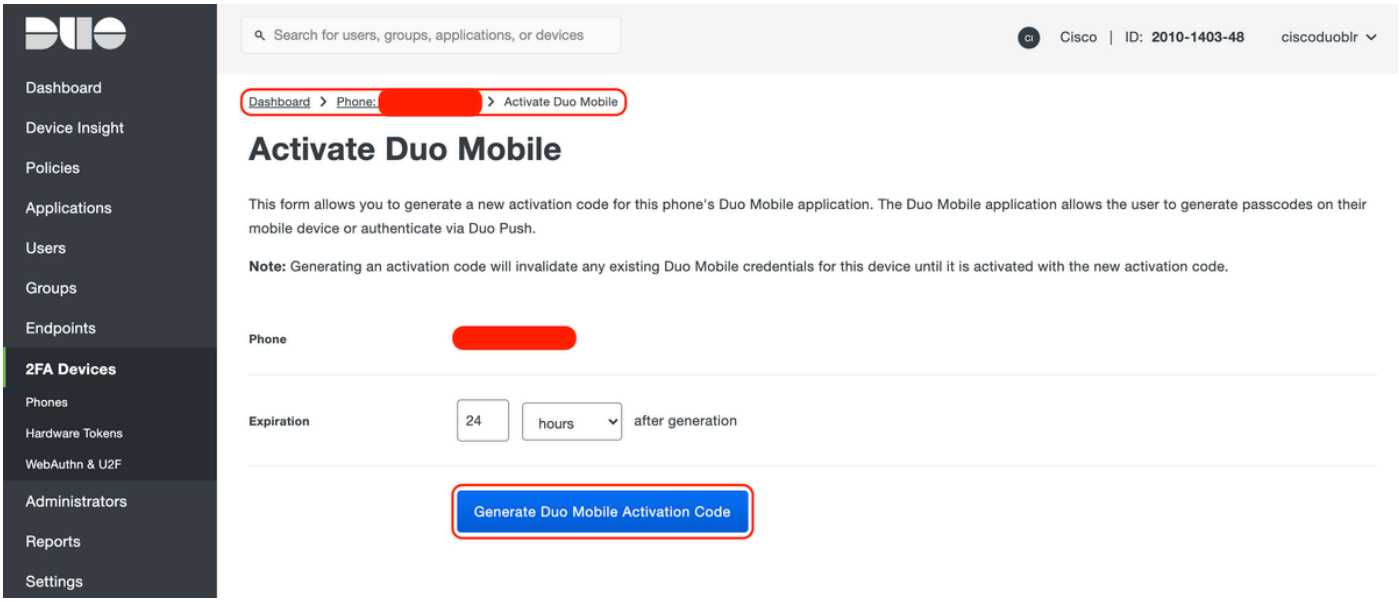


Ative "Duo móvel" para o usuário específico

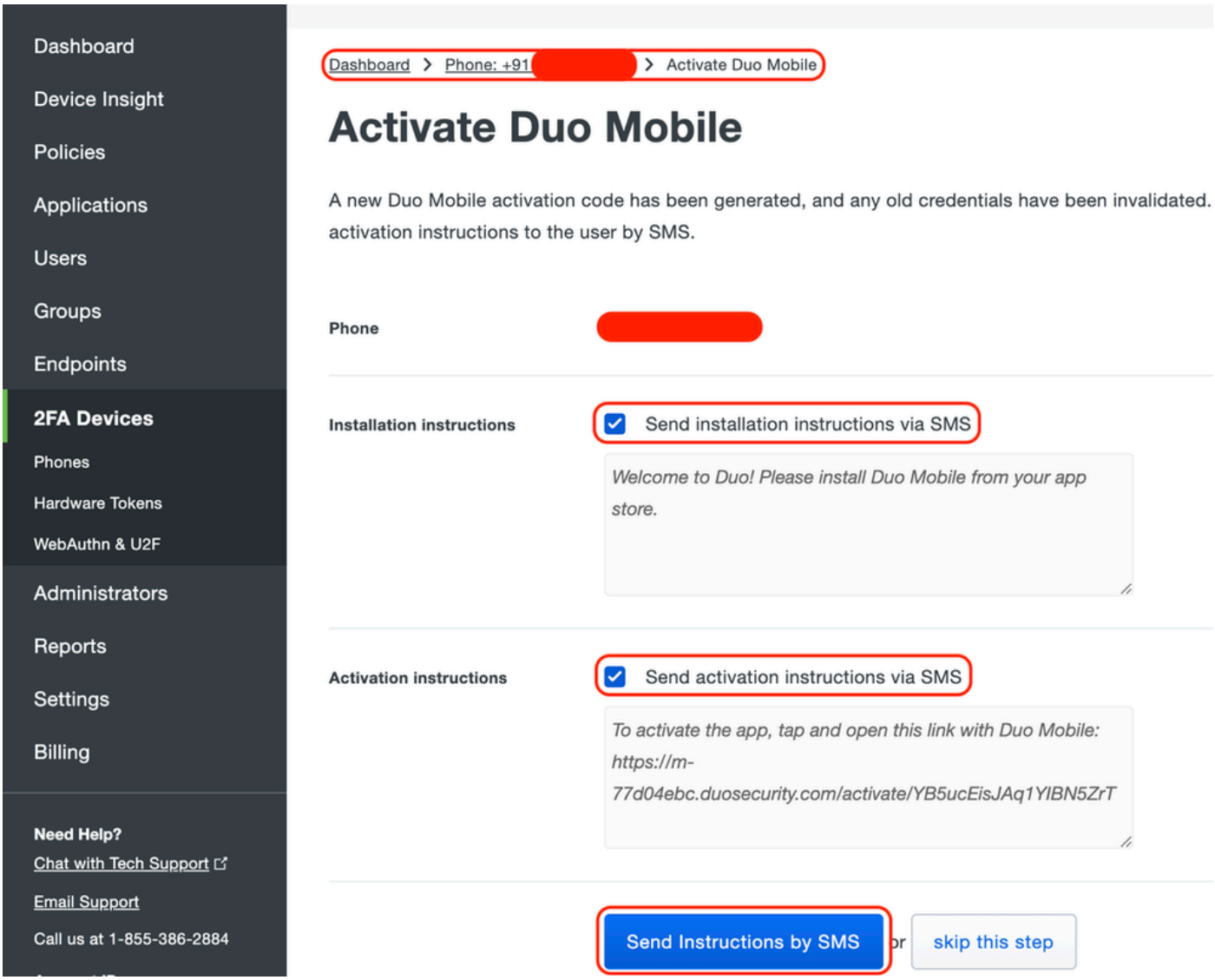


Observação: certifique-se de ter o "Duo Mobile" instalado no dispositivo do usuário final.
[Instalação manual do aplicativo Duo para dispositivos IOS]
[Instalação manual do aplicativo Duo para dispositivos android]

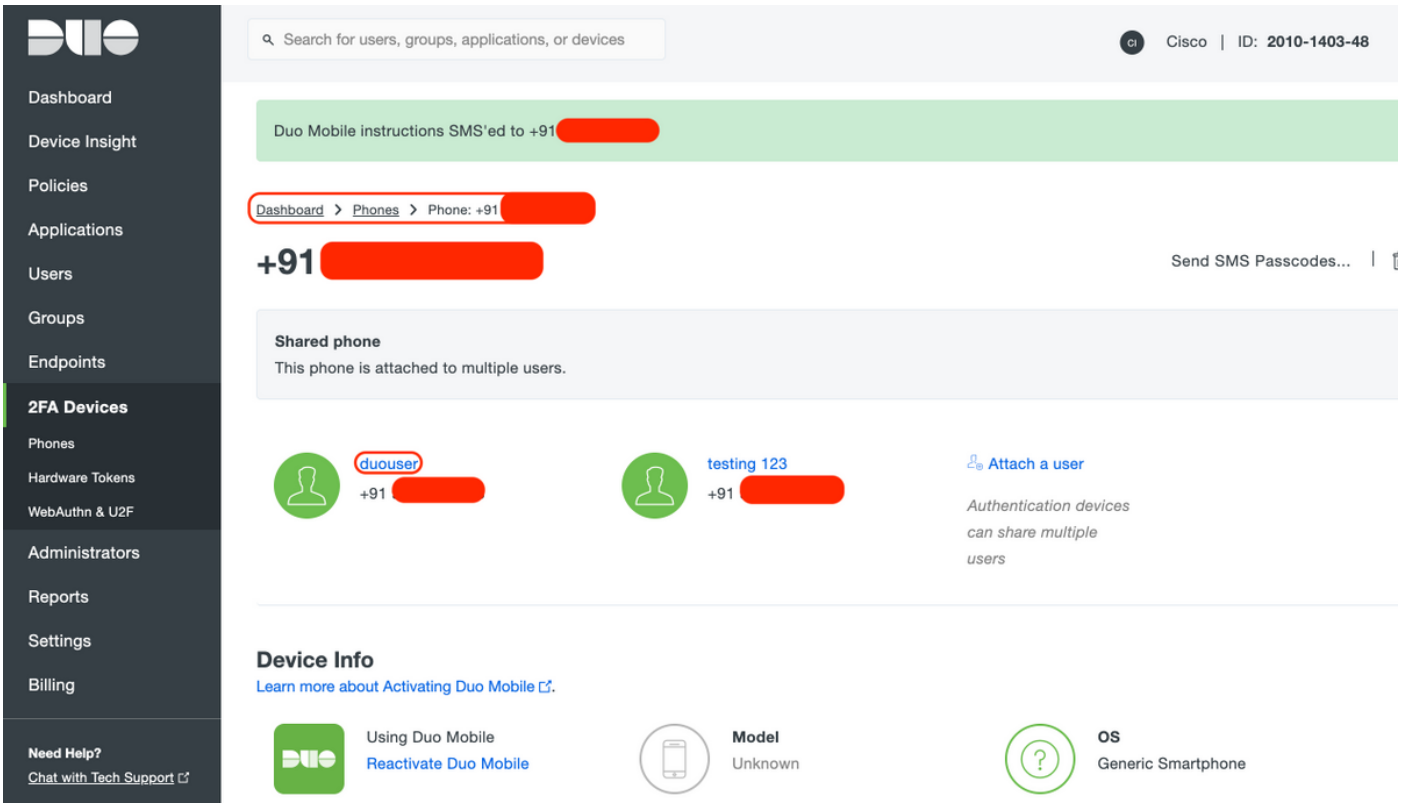
Selecione "Gerar código de ativação móvel duo" como mostrado na imagem:



Selecione "Send Instructions by SMS" (Enviar instruções por SMS), conforme mostrado na imagem:



Clique no link no aplicativo SMS e Duo que é vinculado à conta de usuário na seção Informações do dispositivo, como mostrado na imagem:



- Configuração do Gateway de Acesso Duo (DAG)

1. Implante o Gateway de Acesso Duo (DAG) em um servidor da sua rede

---

Nota: Siga os documentos abaixo para implantação:

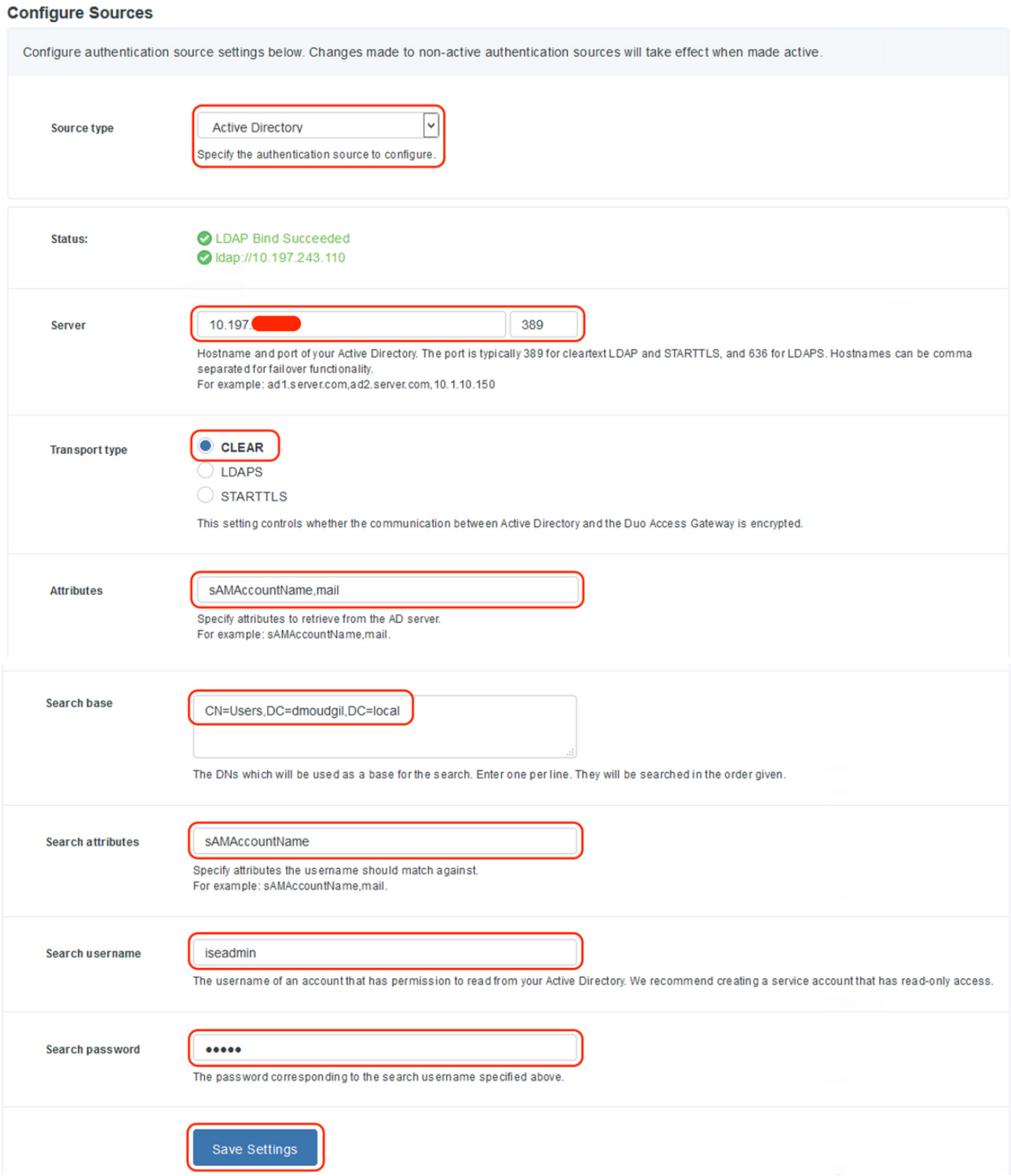
Gateway de acesso Duo para Linux
https://duo.com/docs/dag-linux

Gateway de acesso Duo para Windows
https://duo.com/docs/dag-windows

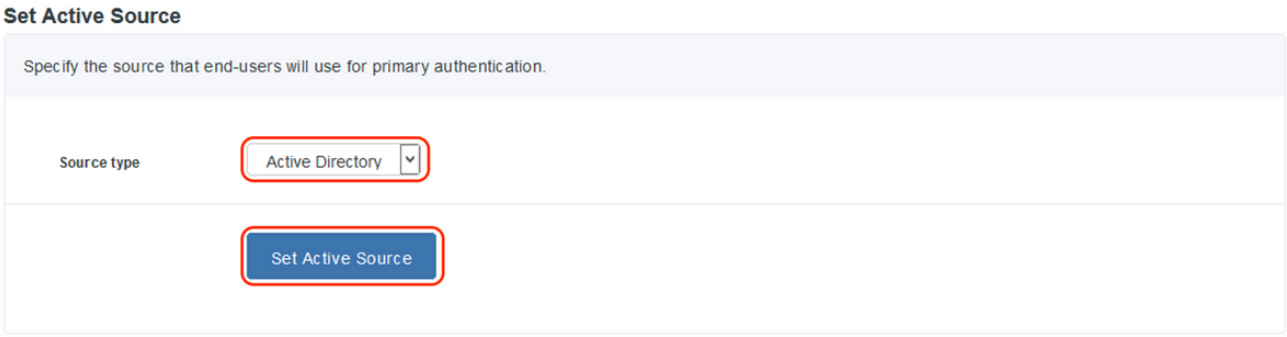
---

2. Na página inicial do Gateway de acesso Duo, navegue para "Origem da autenticação"

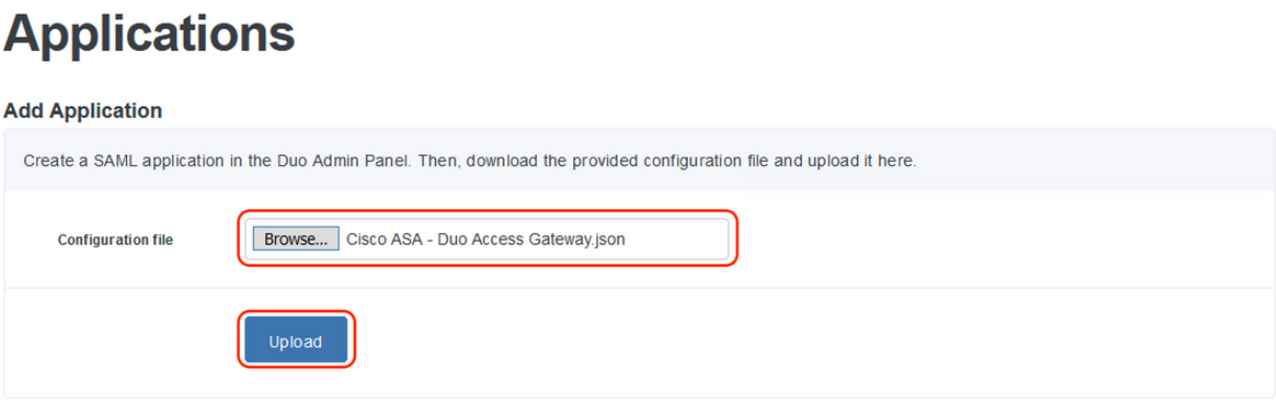
3. Em "Configurar fontes", insira os seguintes atributos para seu Ative Diretory e clique em "Salvar configurações"



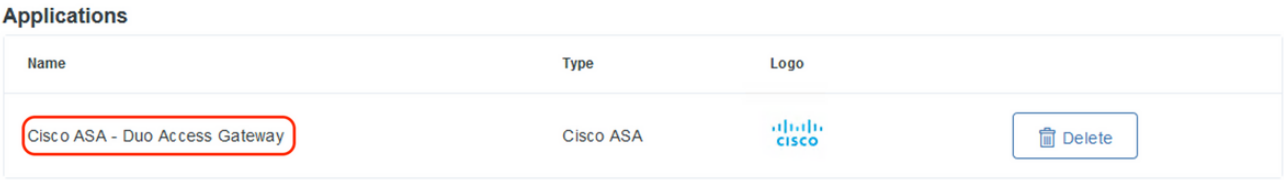
4. Em "Definir Origem Ativa", selecione o tipo de origem como "Ative Diretory" e clique em "Definir Origem Ativa"



5. Navegue até "Applications", no submenu "Add Application" faça o upload do arquivo .json baixado do Console Duo Admin na seção "Configuration file". O arquivo .json correspondente foi baixado na Etapa 3 na configuração do Portal de administração do Duo

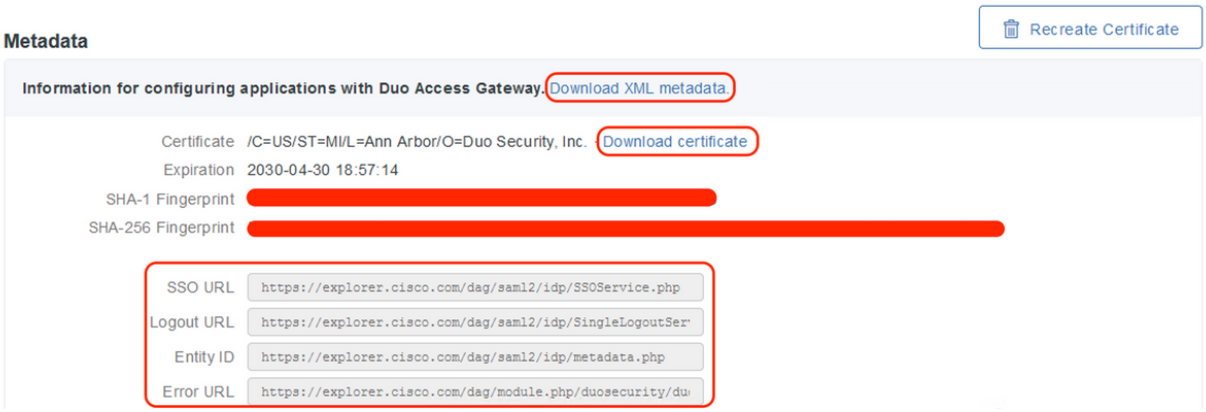


6. Quando o aplicativo for adicionado com êxito, ele aparecerá no submenu "Aplicativos"



7. No submenu "Metadados", faça o download dos metadados XML e do certificado IdP e anote os seguintes URLs que são configurados no ASA posteriormente

    1. URL SSO
    2. URL de logoff
    3. ID da entidade
    4. URL do Erro



-Configuração do ASA

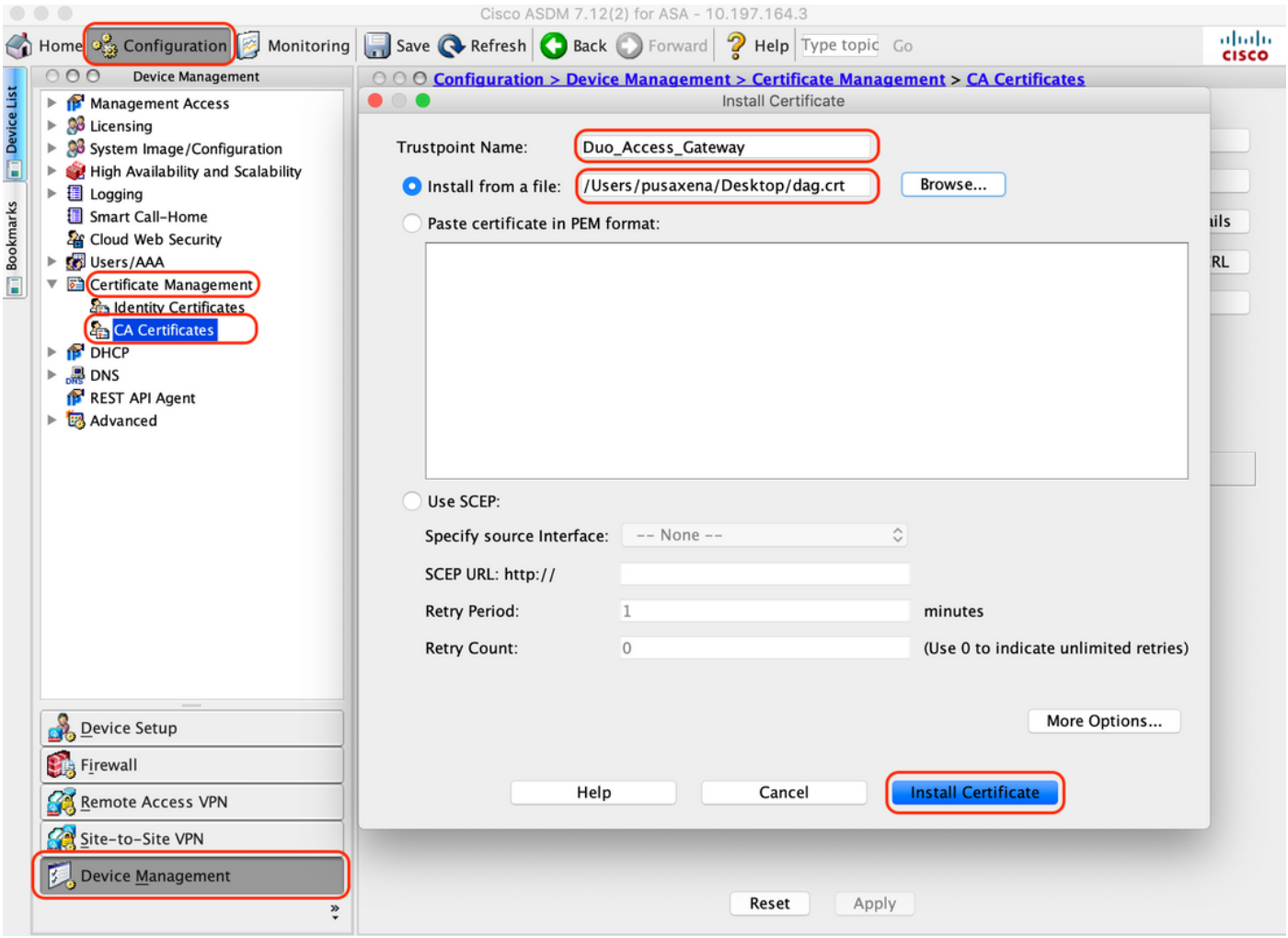
Esta seção fornece informações para configurar o ASA para autenticação IDP SAML e configuração básica do AnyConnect. O documento fornece as etapas de configuração do ASDM e a configuração de execução do CLI para a visão geral.

1. Carregar Certificado de Gateway de Acesso Duo

A. Navegue até "Configuration > Device Management > Certificate Management > CA Certificates", clique em "Add"

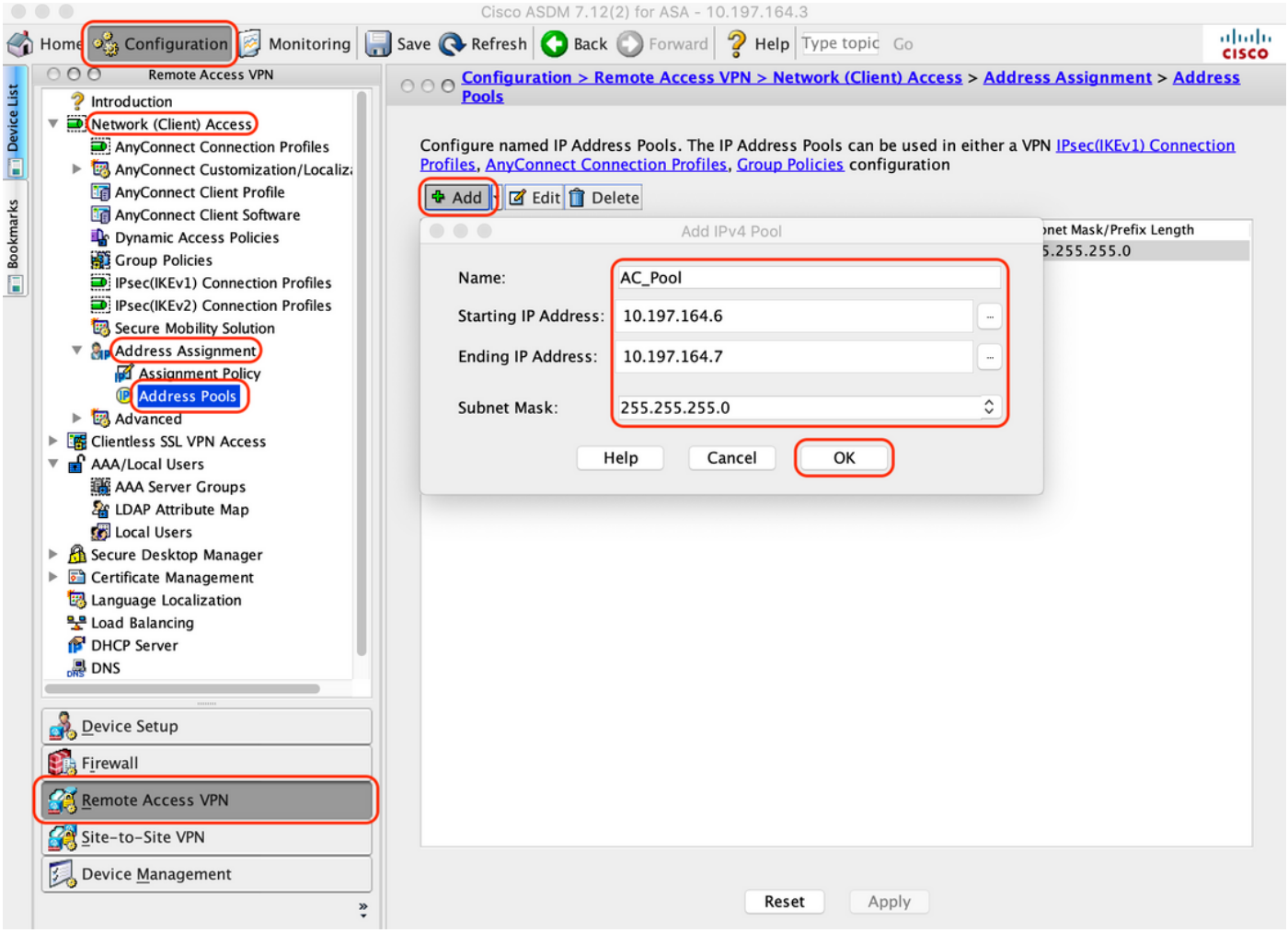
B. Na "Página Instalar Certificado", configure o Nome do ponto de confiança: Duo_Access_Gateway

C. Clique em "Procurar" para selecionar o caminho associado ao certificado DAG e, uma vez selecionado, clique em "Instalar certificado"



2. Criar pool local de IP para usuários do AnyConnect

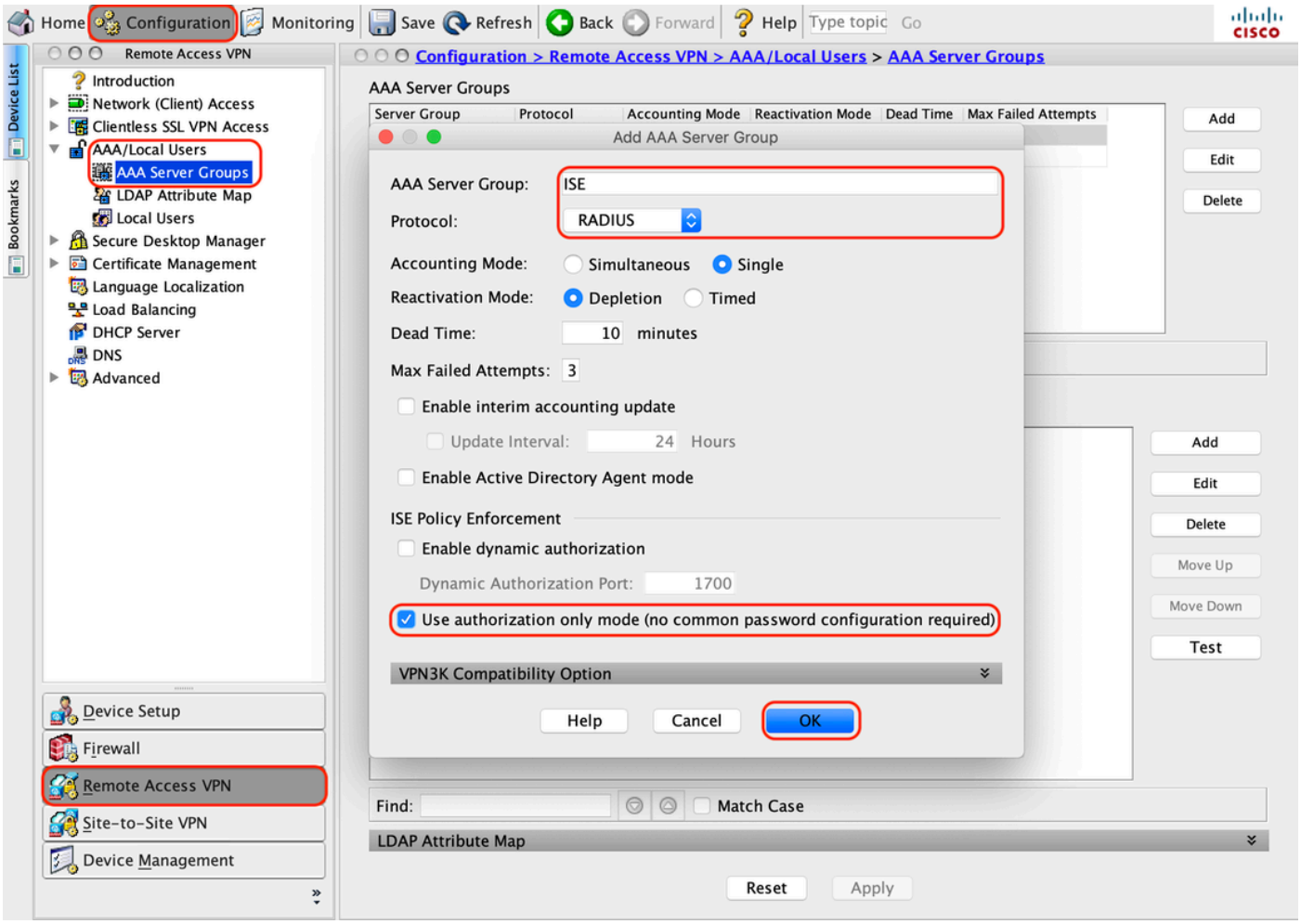
Navegue para "Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools" e clique em "Add"



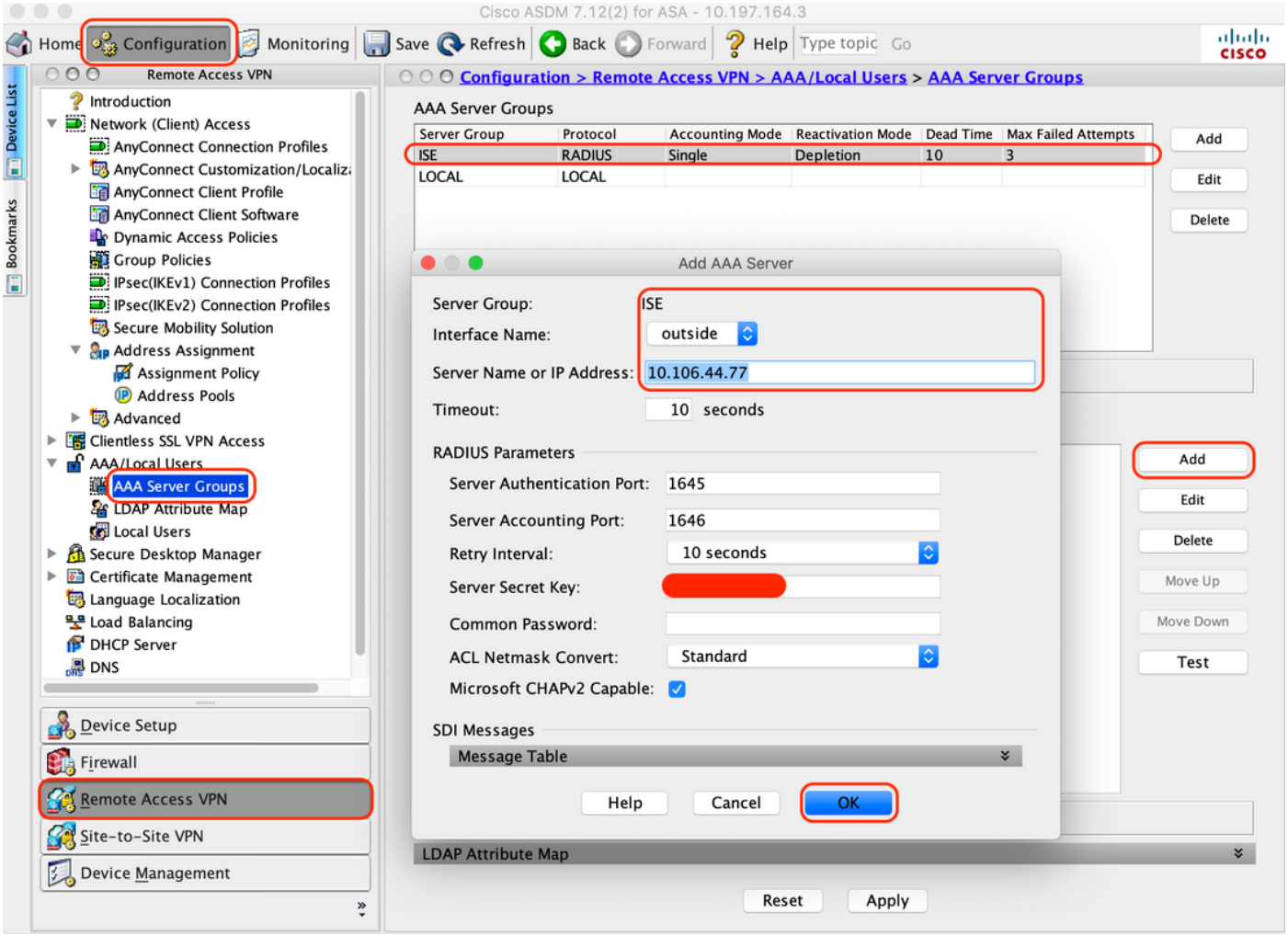
3. Configurar o Grupo de Servidores AAA

A. Nesta seção, configure o grupo de servidores AAA e forneça detalhes do servidor AAA específico que executa a autorização

B. Navegue para "Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups", clique em "Add"



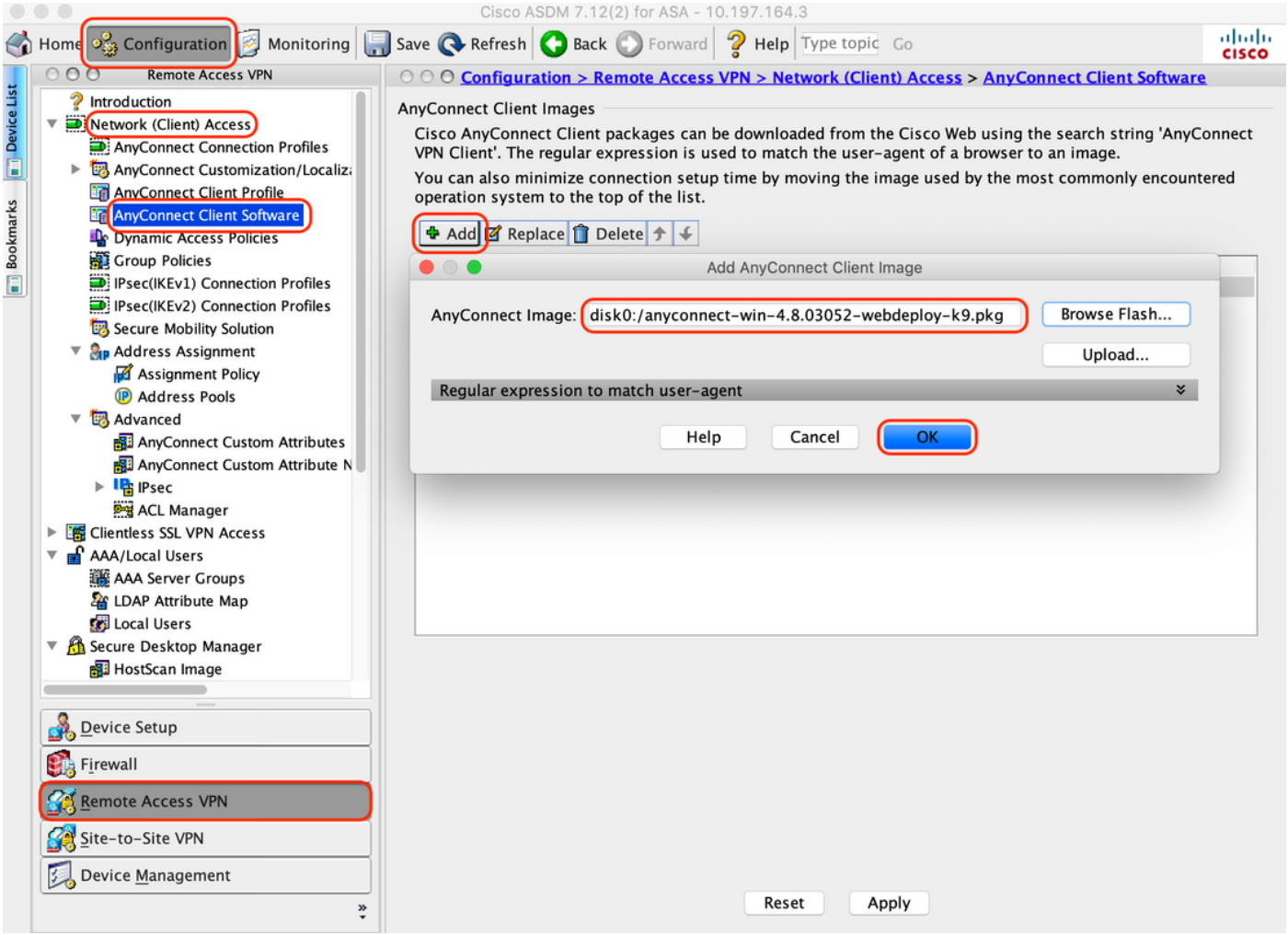
C. Na mesma página, na seção "Servidores no grupo Selecionado", clique em "Adicionar" e forneça os detalhes do endereço IP do servidor AAA



4. Mapear o software cliente do AnyConnect

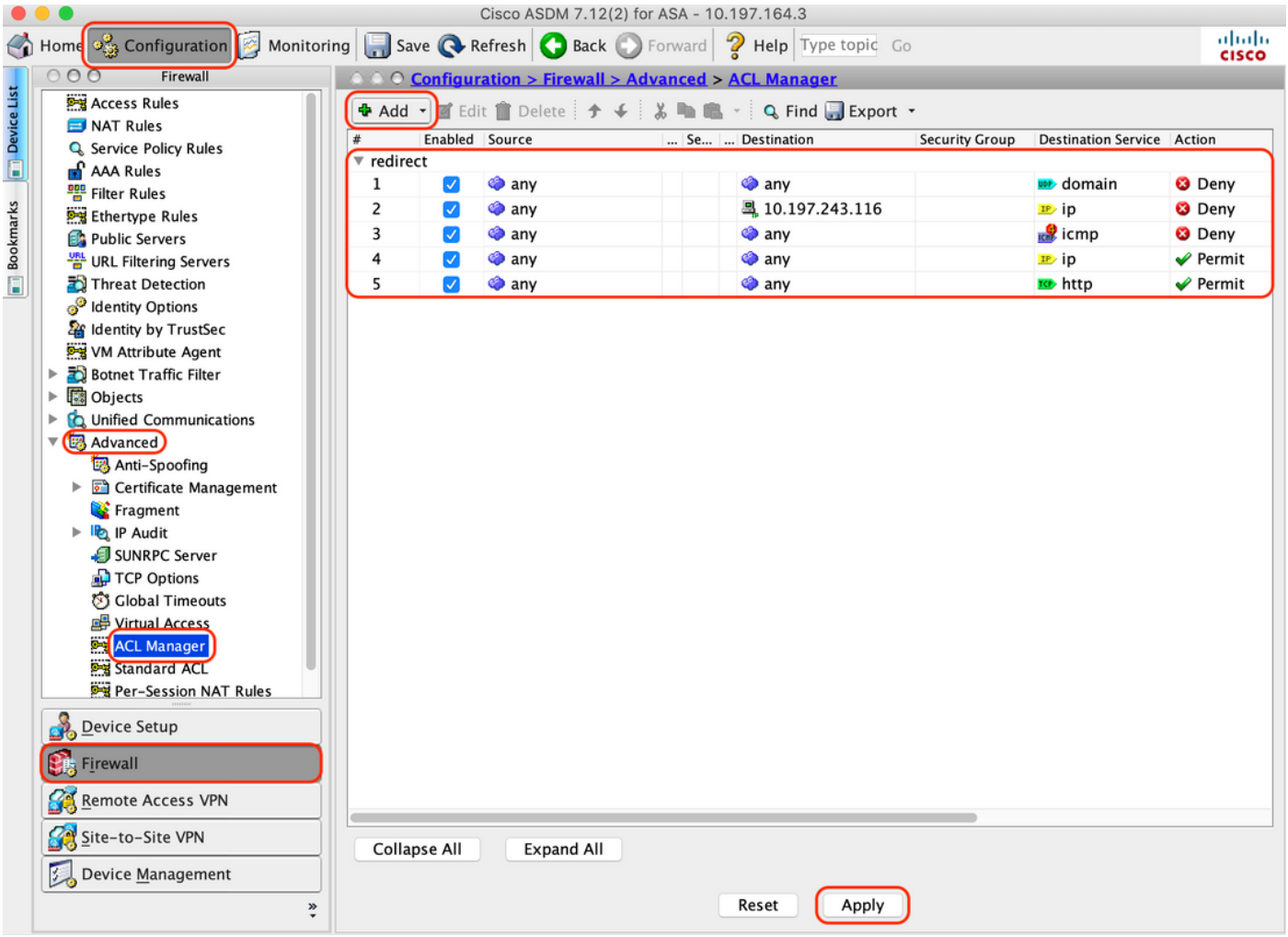
A. Mapeie a imagem 4.8.03052 do software cliente do AnyConnect para que as janelas sejam usadas para WebVPN

B. Navegue para "Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software", clique em "Add"



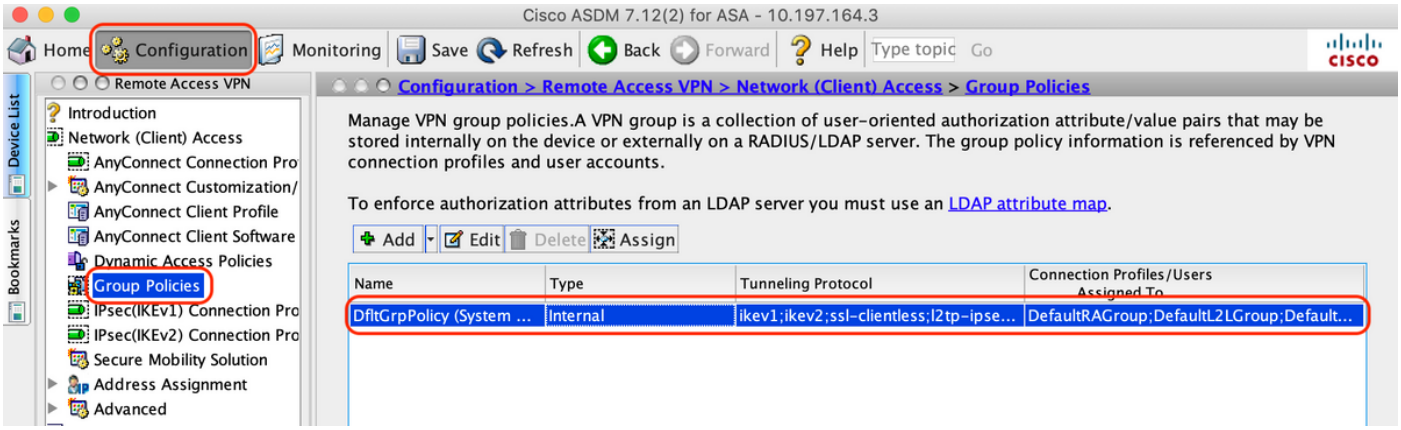
5. Configure a ACL de redirecionamento que é enviada como resultado do ISE

R. Navegue até "Configuration > Firewall > Advanced > ACL Manager" (Configuração > Firewall > Avançado > Gerenciador ACL), clique em Add (Adicionar) para adicionar a ACL de redirecionamento. As entradas, depois de configuradas, são como as mostradas abaixo:



6. Validar Diretiva de Grupo existente

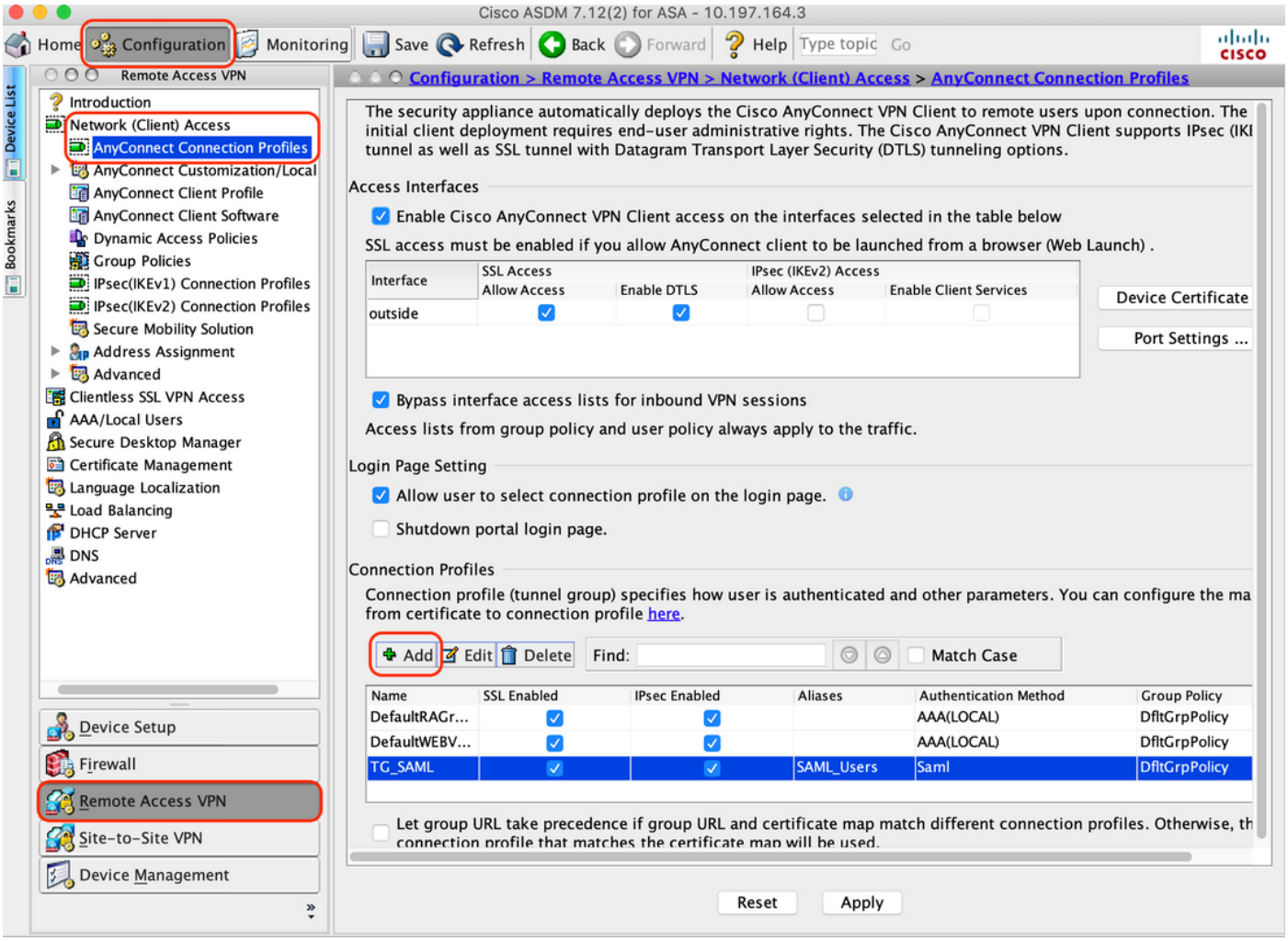
R. Esta configuração usa a política de grupo padrão e que pode ser visualizada em: "Configuration > Remote Access VPN > Network (Client) Access > Group Policies"



7. Configurar Perfil de Conexão

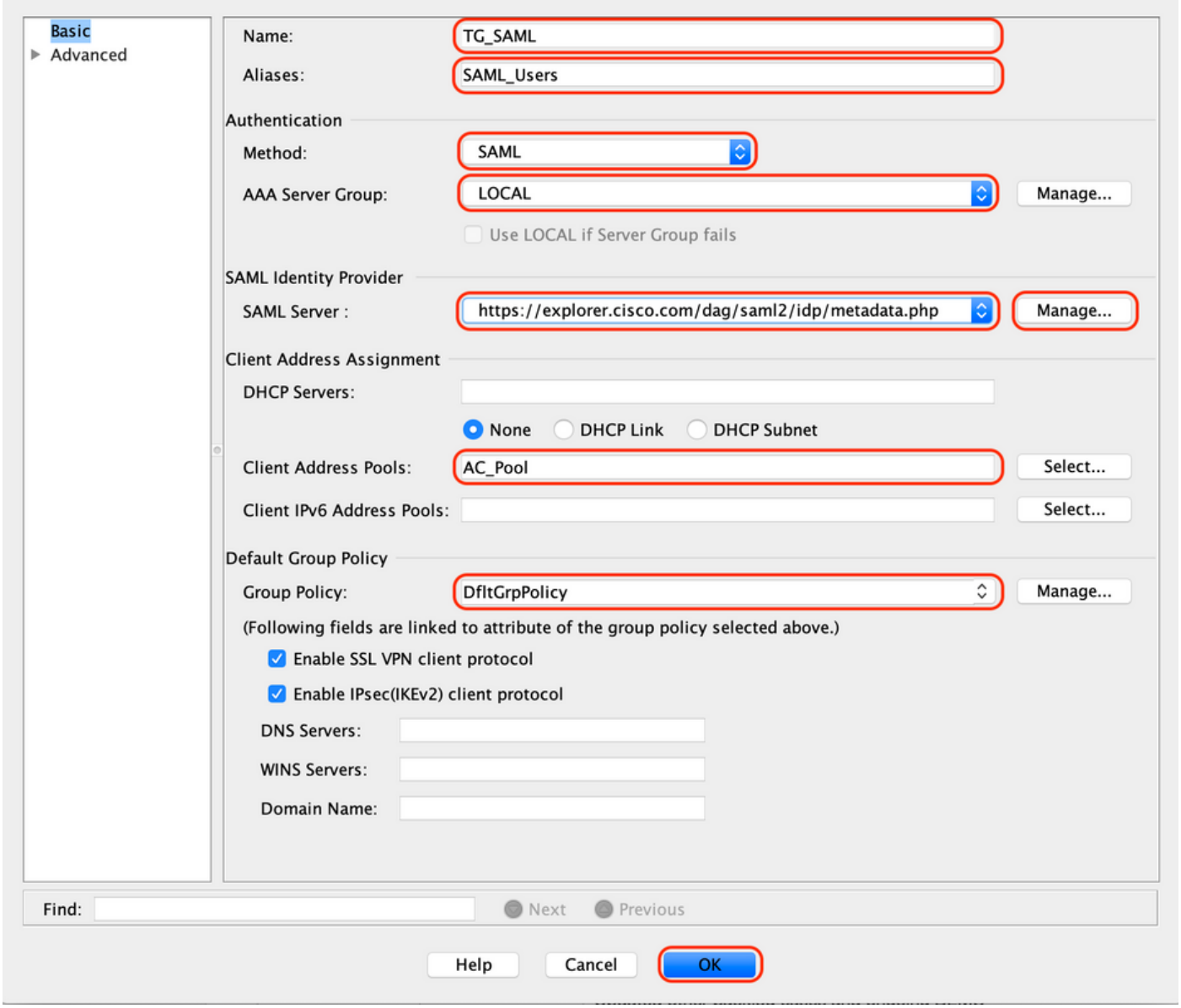
A. Crie um novo perfil de conexão ao qual os usuários do AnyConnect se conectam

B. Navegue para "Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles", clique em "Add"



C. Configure os detalhes abaixo associados ao perfil de conexão:

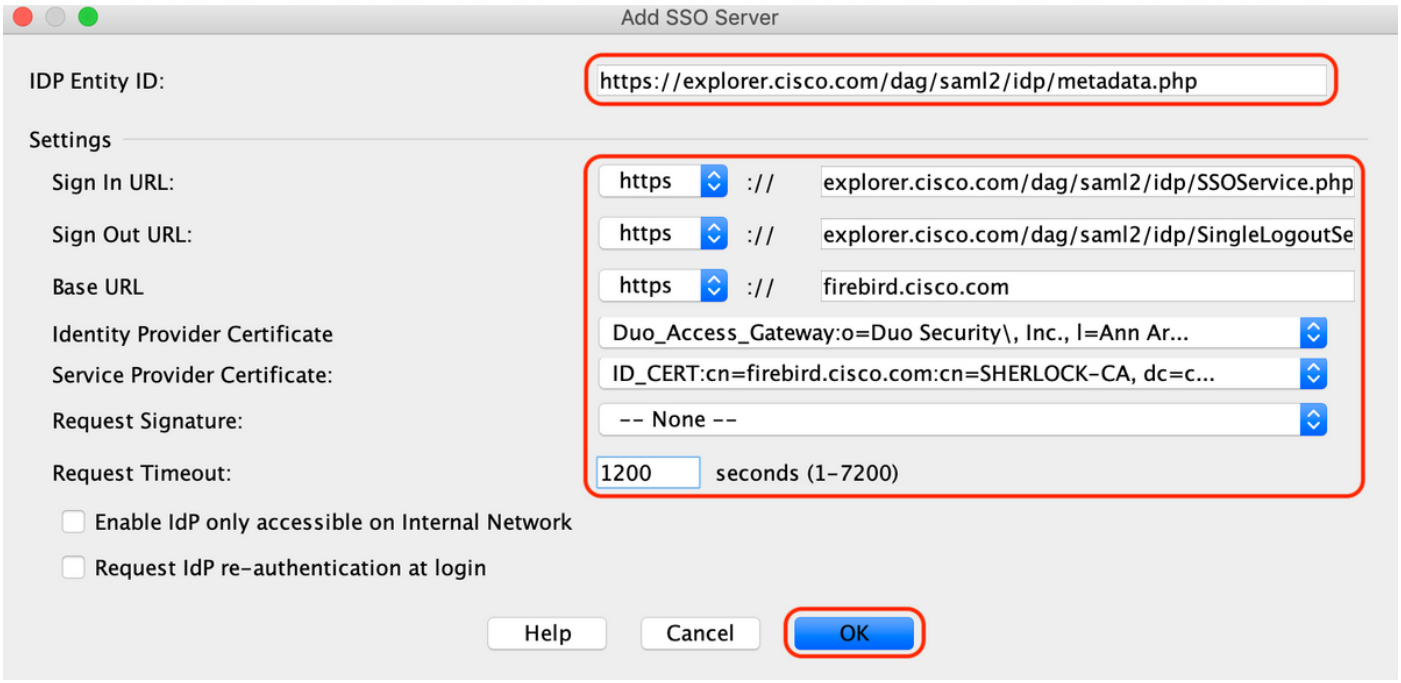
Nome	TG_SAML
Apelidos	SAML_Users
Método	SAML
Grupo de servidores AAA	Local
Pools de Endereços de Clientes	AC_Pool
Política de grupo	DfltGrpPolicy



D. Na mesma página, configure os detalhes do provedor de Identidade SAML, que serão exibidos abaixo:

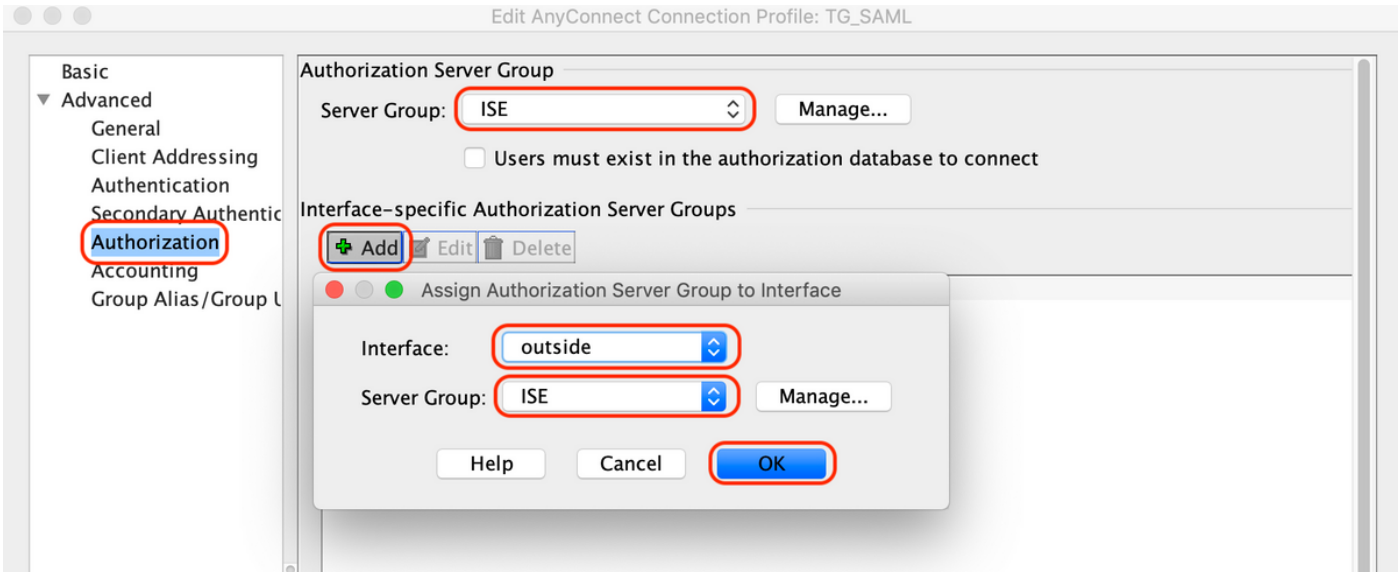
ID da entidade IDP	https://explorer.cisco.com/dag/saml2/idp/metadata.php
URL de Entrada	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
URL de Saída	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.ci
URL base	https://firebird.cisco.com

E. Clique em "Manage > Add" (Gerenciar > Adicionar).



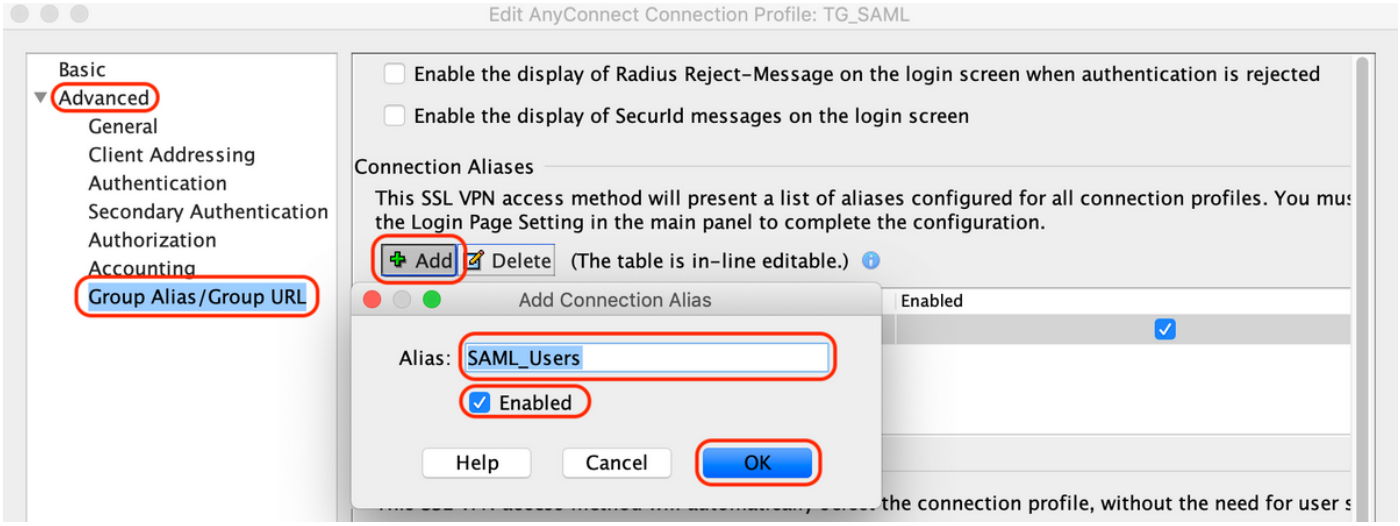
F. Na seção Advanced do perfil de conexão, defina o servidor AAA para autorização

Navegue para "Avançado > Autorização" e clique em "Adicionar"



G. Em Group Alias, defina o alias da conexão

Navegue para "Avançado > Apelido do grupo/URL do grupo" e clique em "Adicionar"



H. Isso conclui a configuração do ASA, o mesmo se parece com o abaixo na interface de linha de comando (CLI)

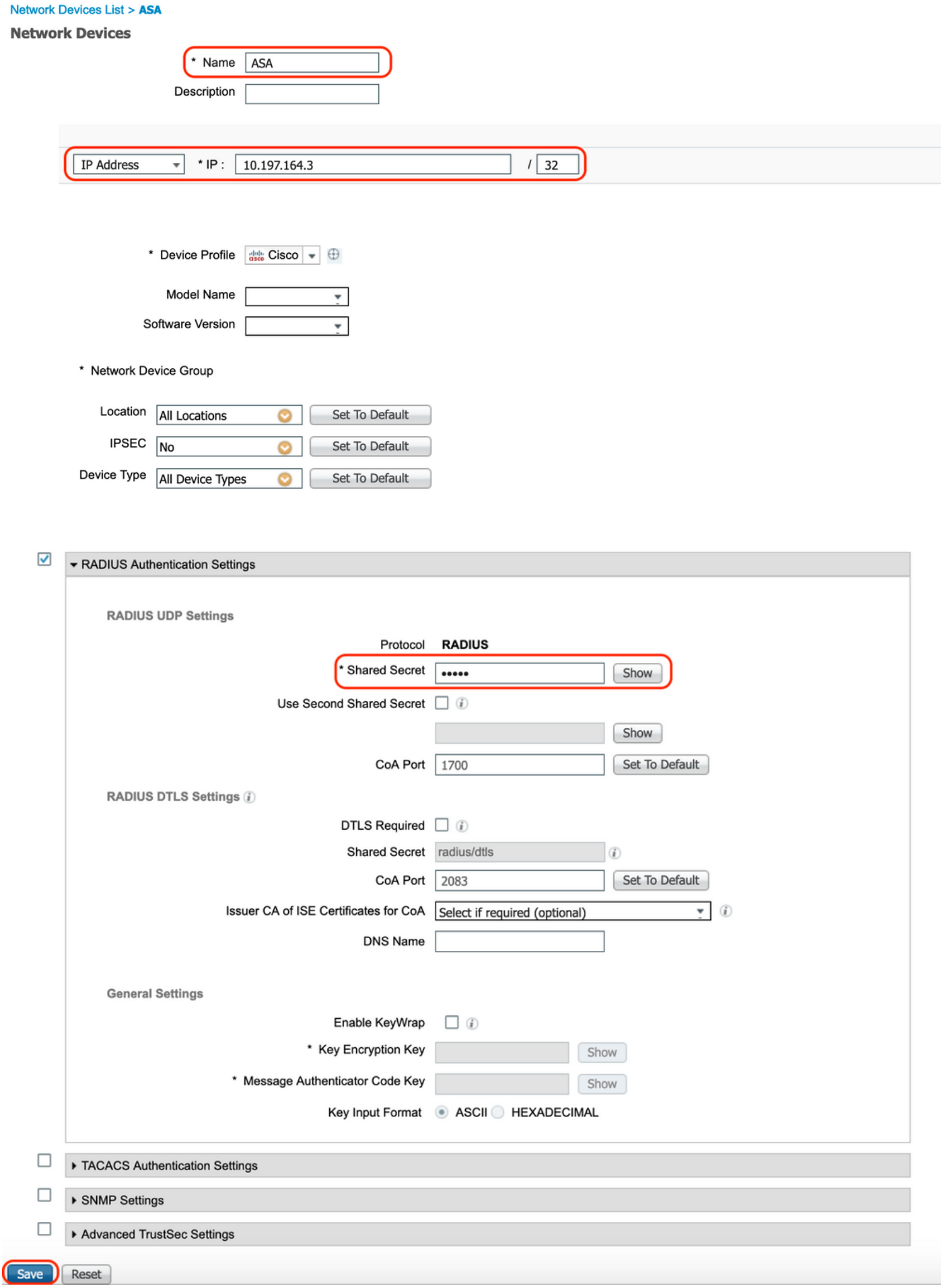
```
!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!--------------------Client pool configuration--------------------
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!--------------------Redirect Access-list-------------------------
!
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
 crl 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
!
```

-Configuração do ISE

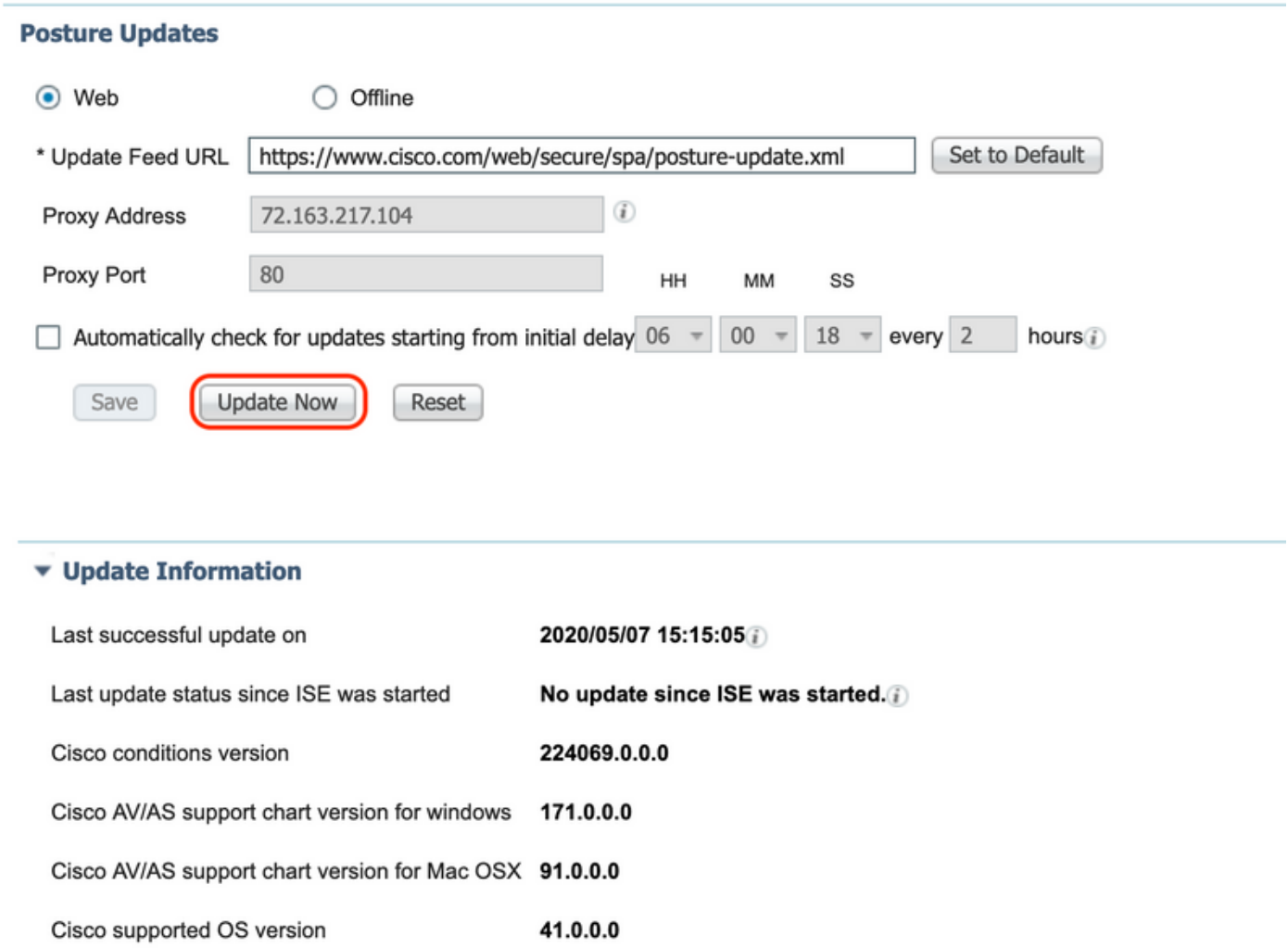
1. Adicione o Cisco ASA como dispositivo de rede

Em "Administração > Recursos de rede > Dispositivos de rede", clique em "Adicionar". Configure o nome do dispositivo de rede, o endereço IP associado e em "Radius Authentication Settings", configure o "Shared Secret" e clique em "Save"


Network Devices List > ASA
Network Devices
* Name
ASA
Description
IP Address
* IP :
10.197.164.3
/ 32
* Device Profile
Cisco
Model Name
Software Version
* Network Device Group
Location
All Locations
Set To Default
IPSEC
No
Set To Default
Device Type
All Device Types
Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
* Shared Secret
Show
Use Second Shared Secret
Show
CoA Port
1700
Set To Default
RADIUS DTLS Settings
DTLS Required
Shared Secret
radius/dtls
CoA Port
2083
Set To Default
Issuer CA of ISE Certificates for CoA
Select if required (optional)
DNS Name
General Settings
Enable KeyWrap
* Key Encryption Key
Show
* Message Authenticator Code Key
Show
Key Input Format
ASCII
HEXADECIMAL
TACACS Authentication Settings
SNMP Settings
Advanced TrustSec Settings
Save
Reset

2. Instalar as atualizações de postura mais recentes

Navegue para "Administração > Sistema > Configurações > Postura > Atualizações" e clique em "Atualizar agora"



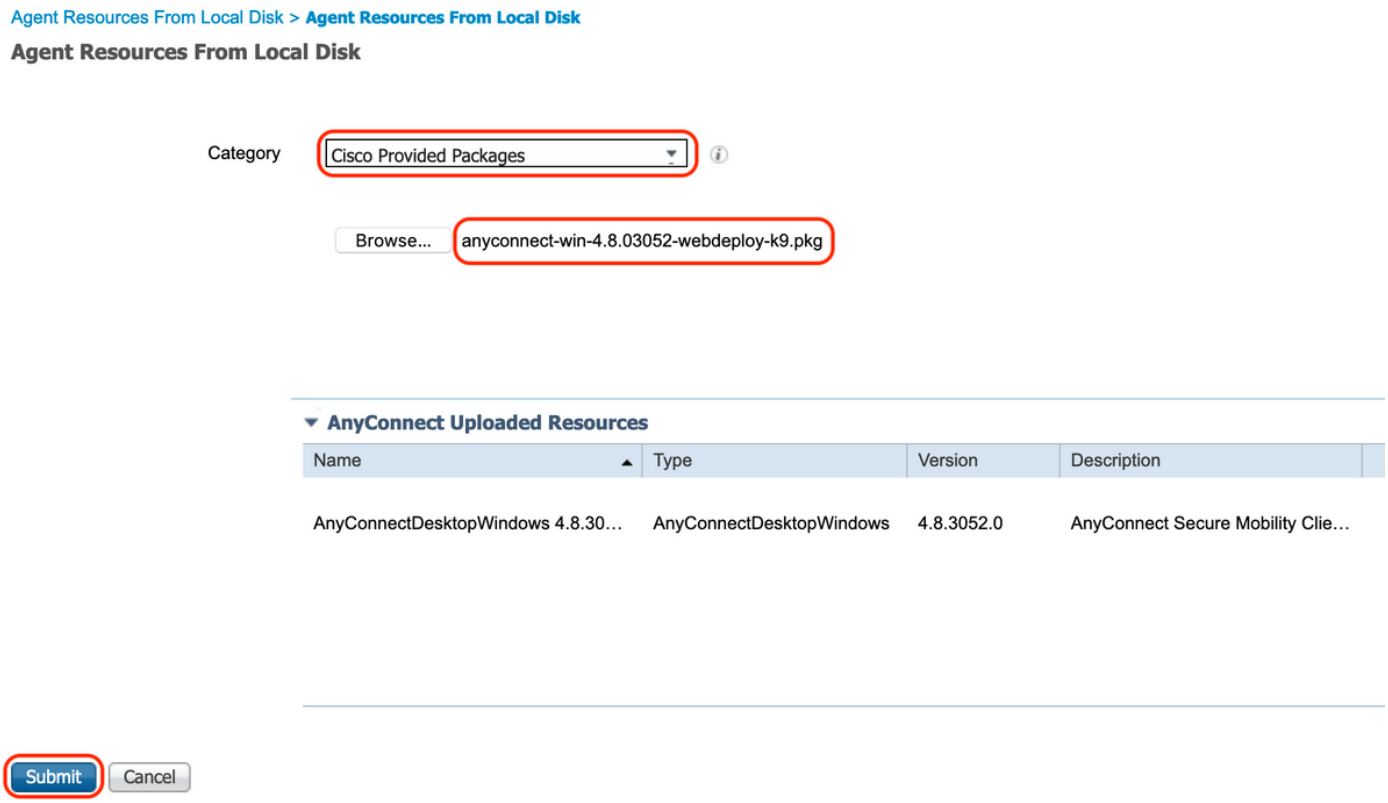
3. Carregar o módulo de conformidade e o pacote de implantação do headend do AnyConnect no ISE

Navegue para "Política > Elementos de política > Resultados > Provisionamento de cliente > Recursos". Clique em "Adicionar" e selecione "Recursos do agente do disco local" ou "Recursos do agente do site da Cisco" com base na busca dos arquivos na estação de trabalho local ou no site da Cisco.

Nesse caso, para carregar arquivos da estação de trabalho local em Categoria, selecione "Pacotes fornecidos pela Cisco", clique em "Procurar", selecione os pacotes necessários e clique em "Enviar".

Este documento usa "anyconnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg" como

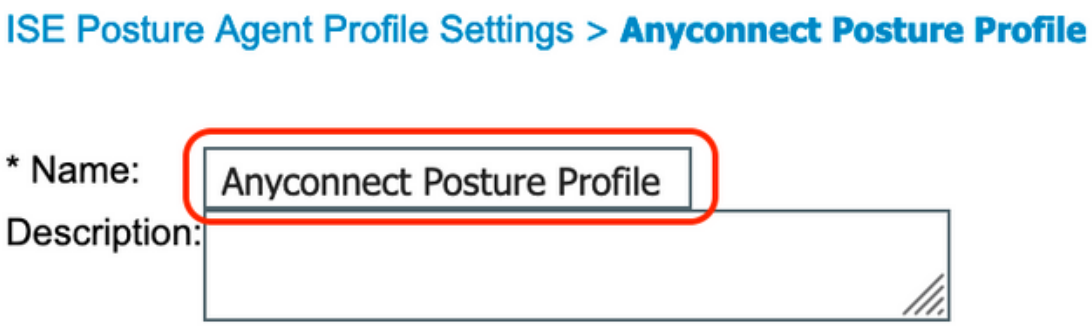
módulo de conformidade e "anyconnect-win-4.8.03052-webdeploy-k9.pkg" como Pacote de implantação do headend do AnyConnect.



4. Criar um perfil de postura do AnyConnect

A. Navegue até "Policy > Policy Elements > Results > Client Provisioning > Resources" (Política > Elementos de política > Resultados > Provisionamento de cliente > Recursos). Clique em "Adicionar" e selecione "Perfil de postura do AnyConnect"

B. Insira o nome do perfil de postura do Anyconnect, configure o nome do servidor como "*" nas regras de nome do servidor e clique em "Salvar"



Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
* Server name rules	*	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		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	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

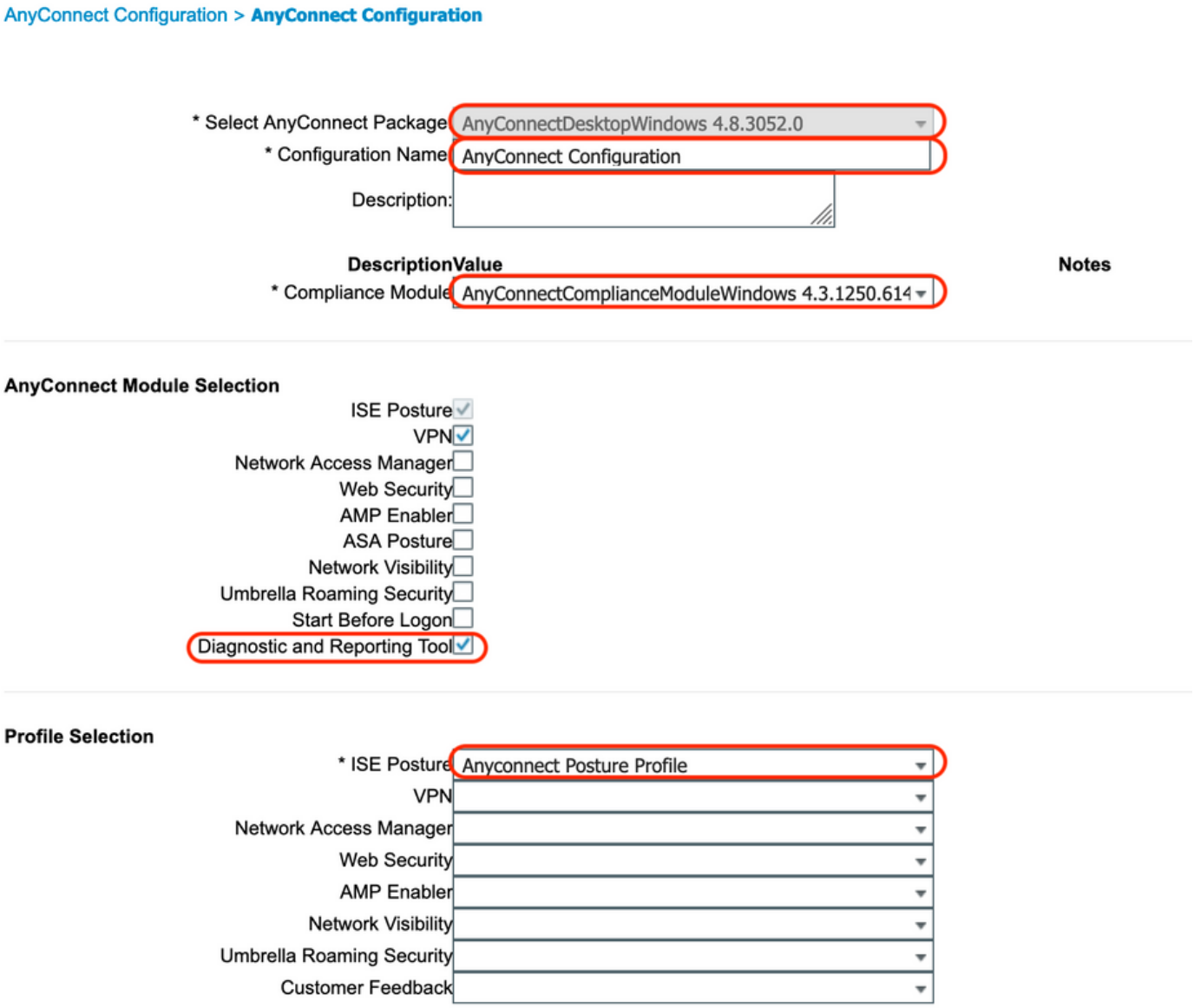
5. Criar Configuração Do Anyconnect

A. Navegue até "Policy > Policy Elements > Results > Client Provisioning > Resources" (Política > Elementos de política > Resultados > Provisionamento de cliente > Recursos). Clique em "Adicionar" e selecione "Configuração do AnyConnect"

B. Selecione o pacote AnyConnect, insira o nome da configuração, selecione o módulo de conformidade necessário

C. Em "AnyConnect Module Selection" (Seleção de módulo do AnyConnect), marque "Diagnostic and Reporting Tool" (Ferramenta de diagnóstico e geração de relatórios)

D. Em "Seleção de perfil", selecione Perfil de postura e clique em "Salvar"

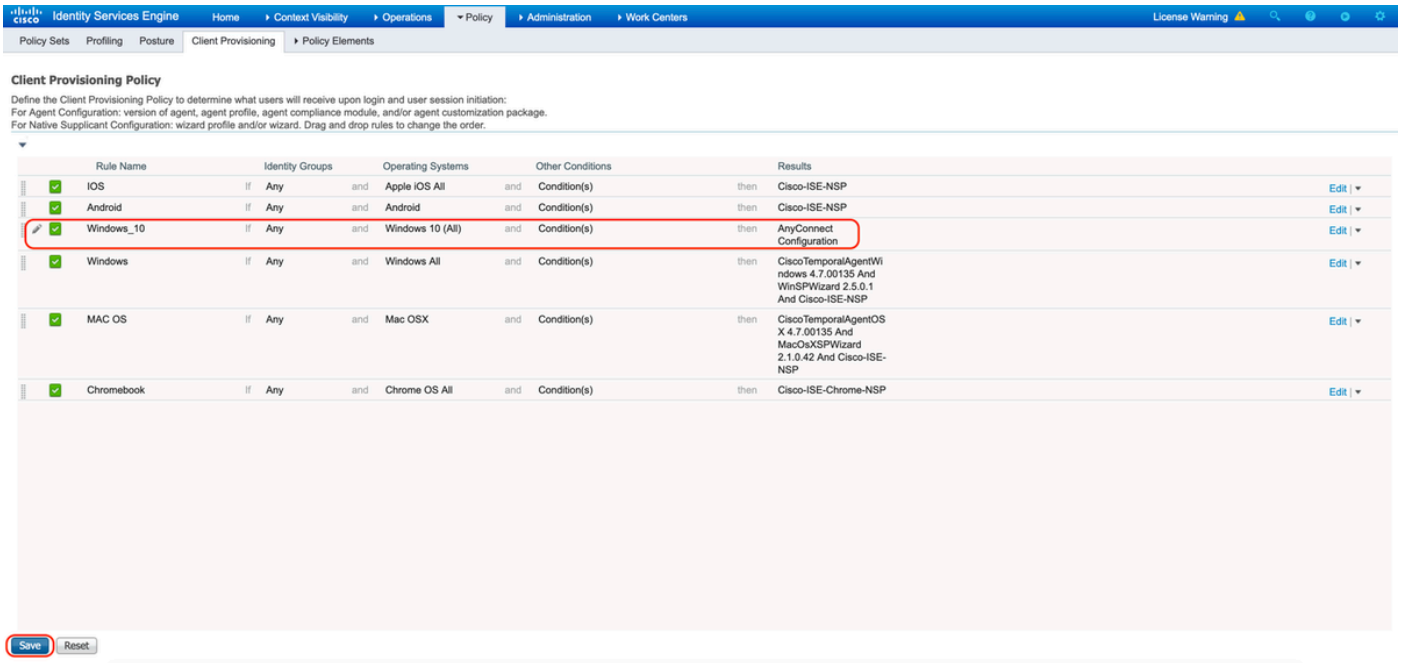


6. Criar Política de Provisionamento de Cliente

A. Navegue até "Política > Provisionamento de clientes"

B. Clique em "Editar" e selecione "Inserir Regra Acima"

C. Insira o Nome da regra, selecione o Sistema operacional necessário e, em Resultados (em "Agente" > "Configuração do agente"), selecione "Configuração do AnyConnect" que foi criada na Etapa 5 e clique em "Salvar"

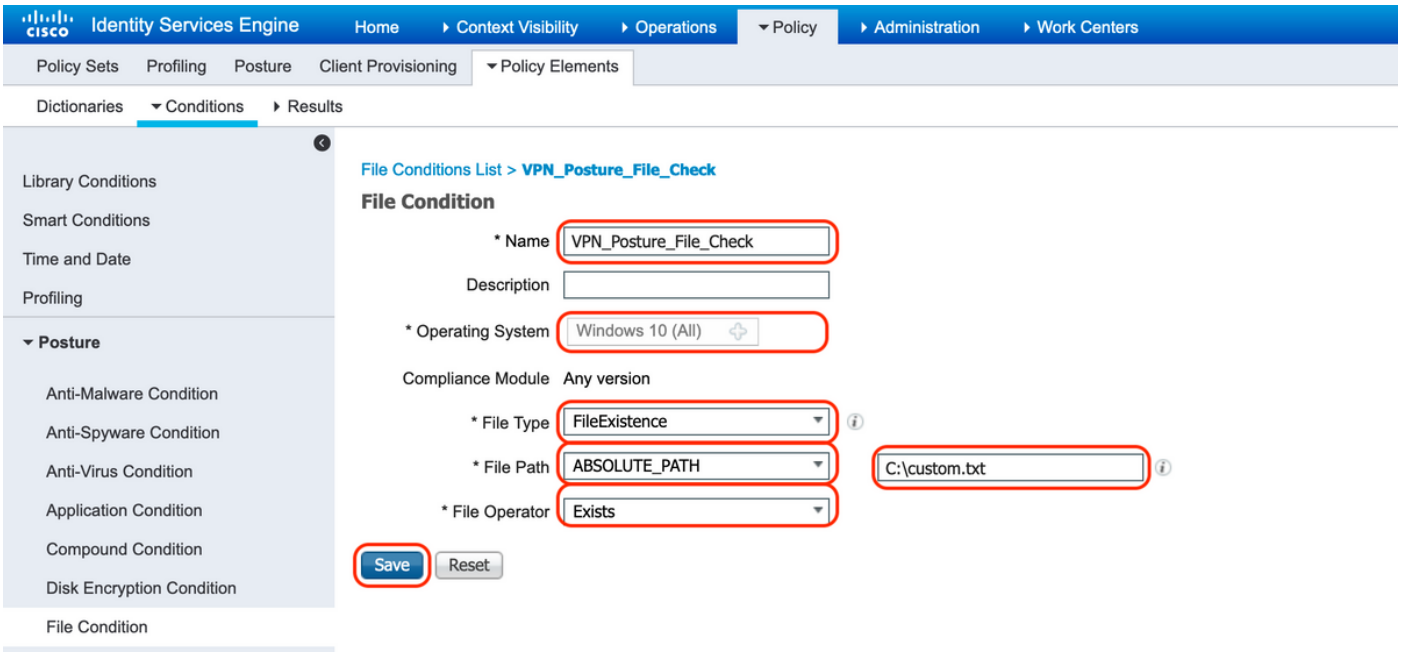


7. Criar uma Condição de Postura

A. Navegue até "Política > Elementos de política > Condições > Postura > Condição de arquivo"

B. Clique em "Adicionar" e configure o nome da condição "VPN_Posture_File_Check", o sistema operacional necessário como "Windows 10(All)", o tipo de arquivo como "FileExistence", o caminho do arquivo como "ABSOLUTE_PATH" e o caminho completo e o nome do arquivo como "C:\custom.txt", selecione o operador do arquivo como "Exists"

C. Este exemplo usa a presença de um arquivo chamado "custom.txt" em C: drive como a condição do arquivo



8. Criar Ação de Remediação de Postura

Navegue para "Política > Elementos de política > Resultados > Postura > Ações de correção" para criar a Ação de correção de arquivo correspondente. Este documento usa "Somente texto da mensagem" como ações de remediação que é configurado na próxima etapa.

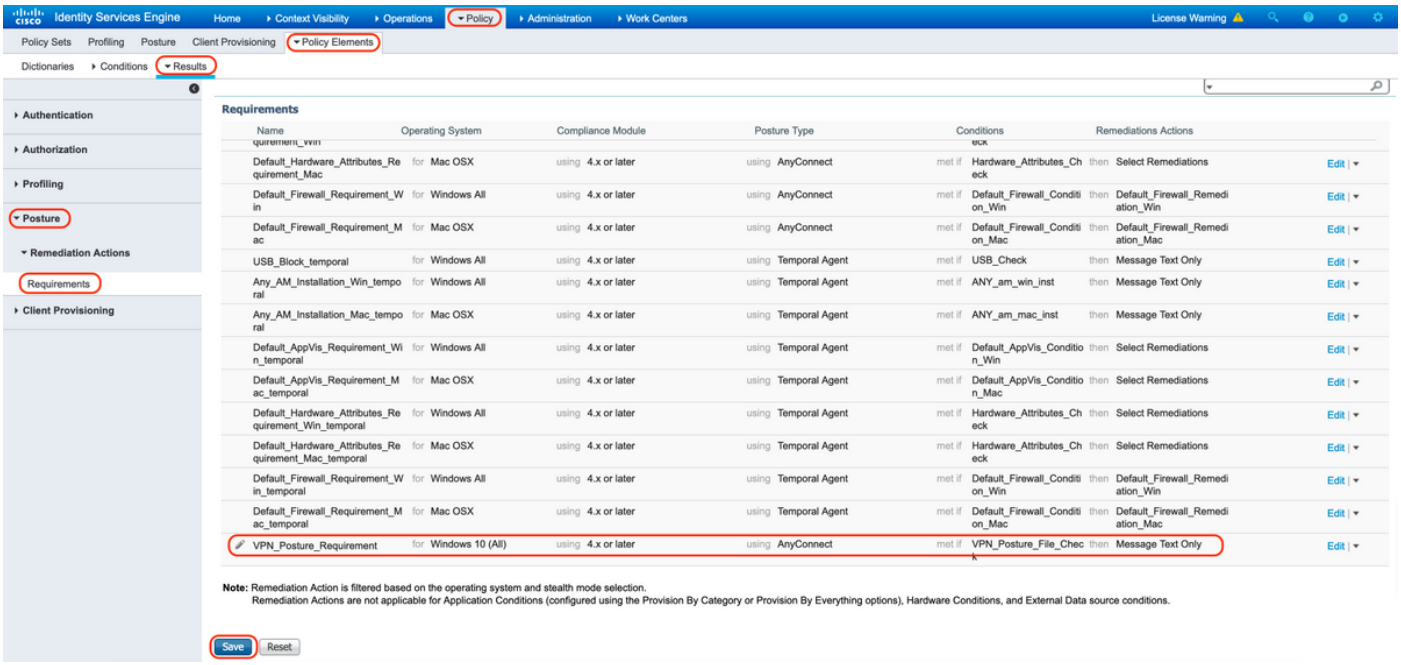
9. Criar regra de Requisito de Situação

A. Navegue até "Política > Elementos de política > Resultados > Postura > Requisitos"

B. Clique em "Editar" e selecione "Inserir novo requisito"

C. Configure o nome da condição "VPN_Posture_Requirement", o sistema operacional necessário como "Windows 10(All)", o módulo de conformidade como "4.x ou posterior", o tipo de postura como "Anyconnect"

D. Condições como "VPN_Posture_File_Check" (criado na Etapa 7) e em Ações de correções, selecione Ação como "Somente texto da mensagem" e insira a mensagem personalizada para o usuário do agente

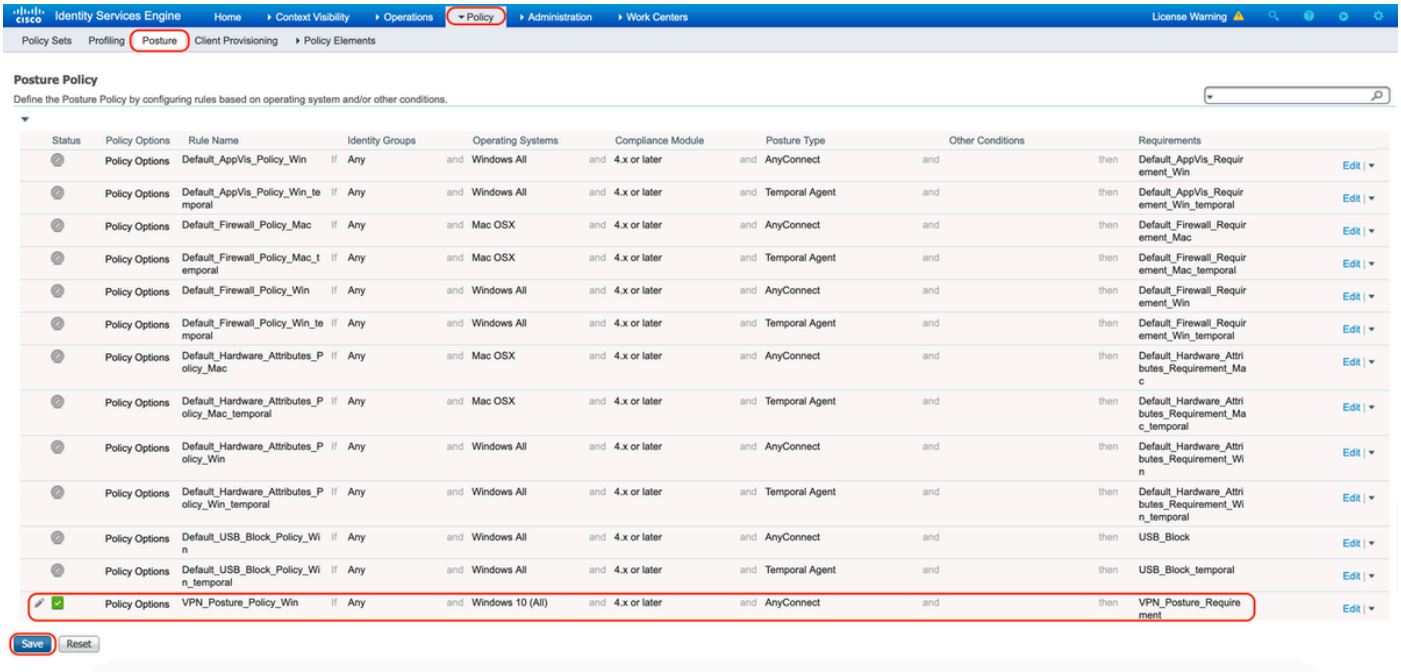


10. Criar uma Política de Postura

A. Navegue até "Policies > Posture"

B. Configure o nome da regra como "VPN_Posture_Policy_Win", o sistema operacional

necessário como "Windows 10(All)", o módulo de conformidade como "4.x ou posterior", o tipo de postura como "Anyconnect" e os requisitos como "VPN_Posture_Requirement", conforme configurado na Etapa 9

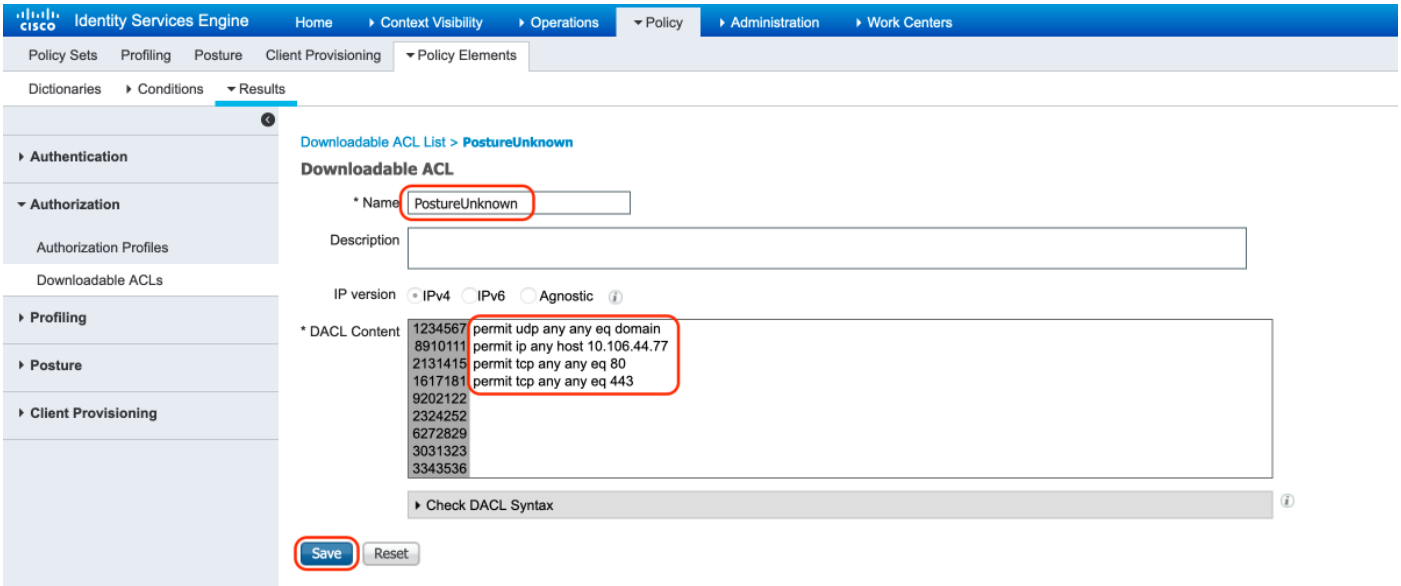


11. Criar ACLs Dinâmicas (DACLs)

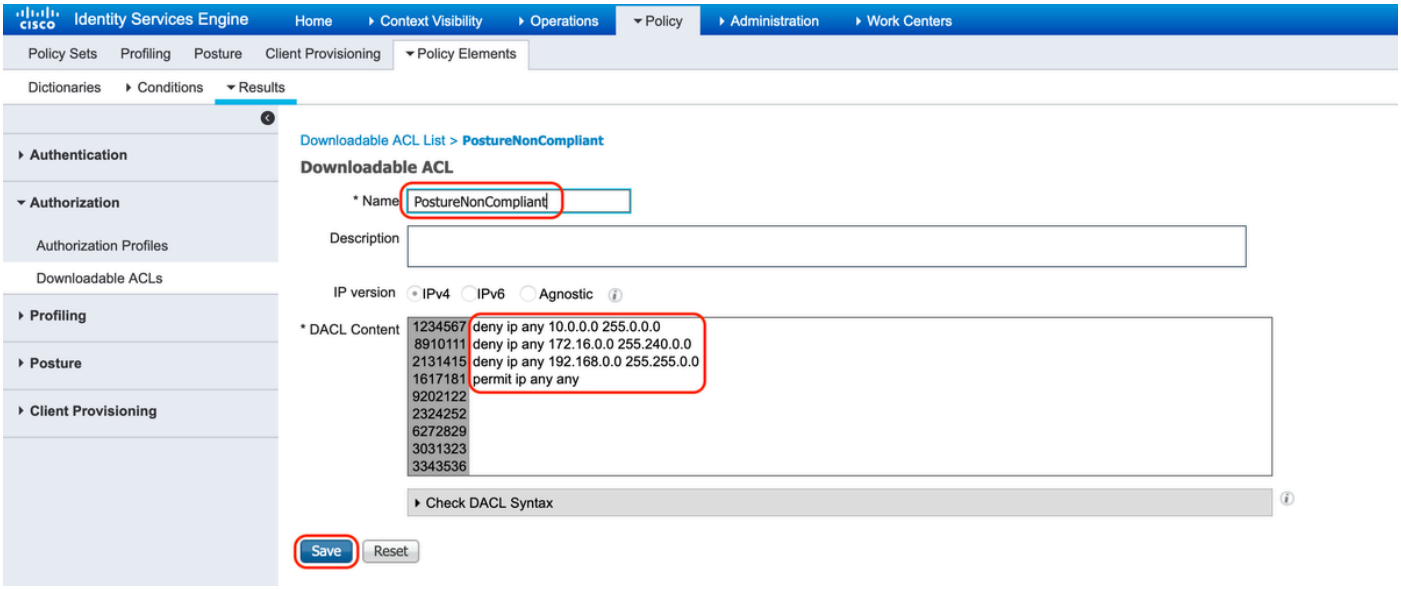
Navegue até "Policy > Policy Elements > Results > Authorization > Downlodable ACLS" e crie as DACLs para diferentes status de postura.

Este documento usa as seguintes DACLs.

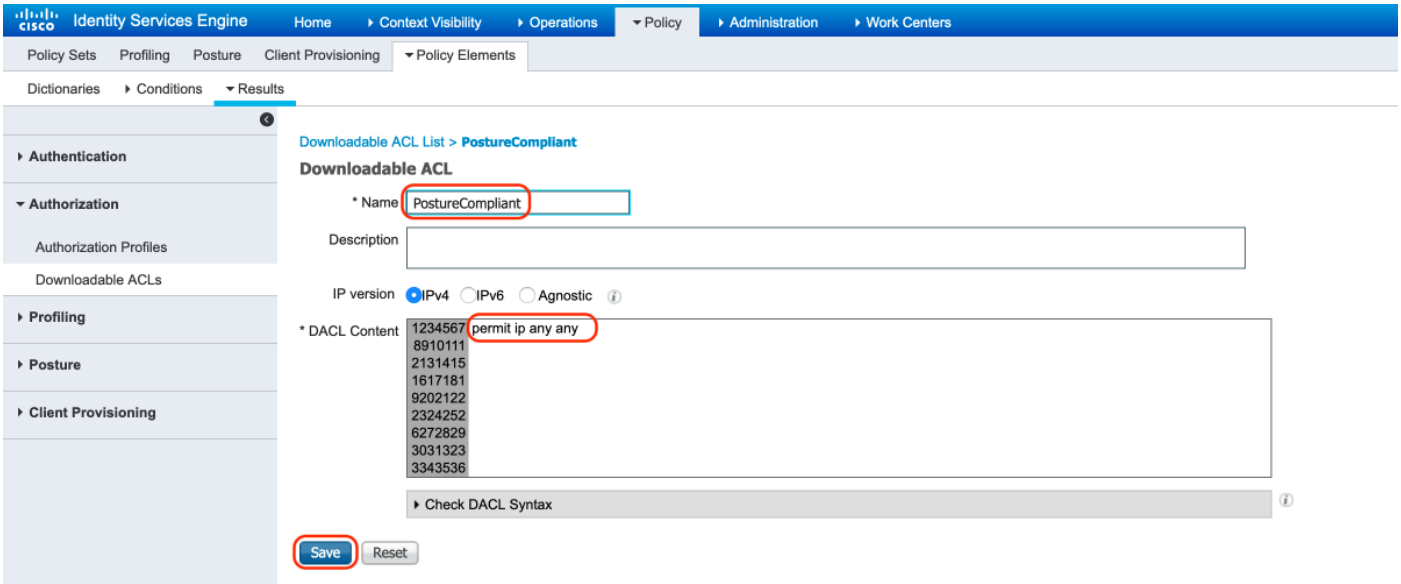
A. Postura desconhecida: permite o tráfego para DNS, PSN e HTTP, e tráfego HTTPS



B. Postura não compatível: nega o acesso a sub-redes privadas e permite apenas o tráfego da Internet



C. Compatível com postura: permite todo o tráfego para usuários finais em conformidade com postura

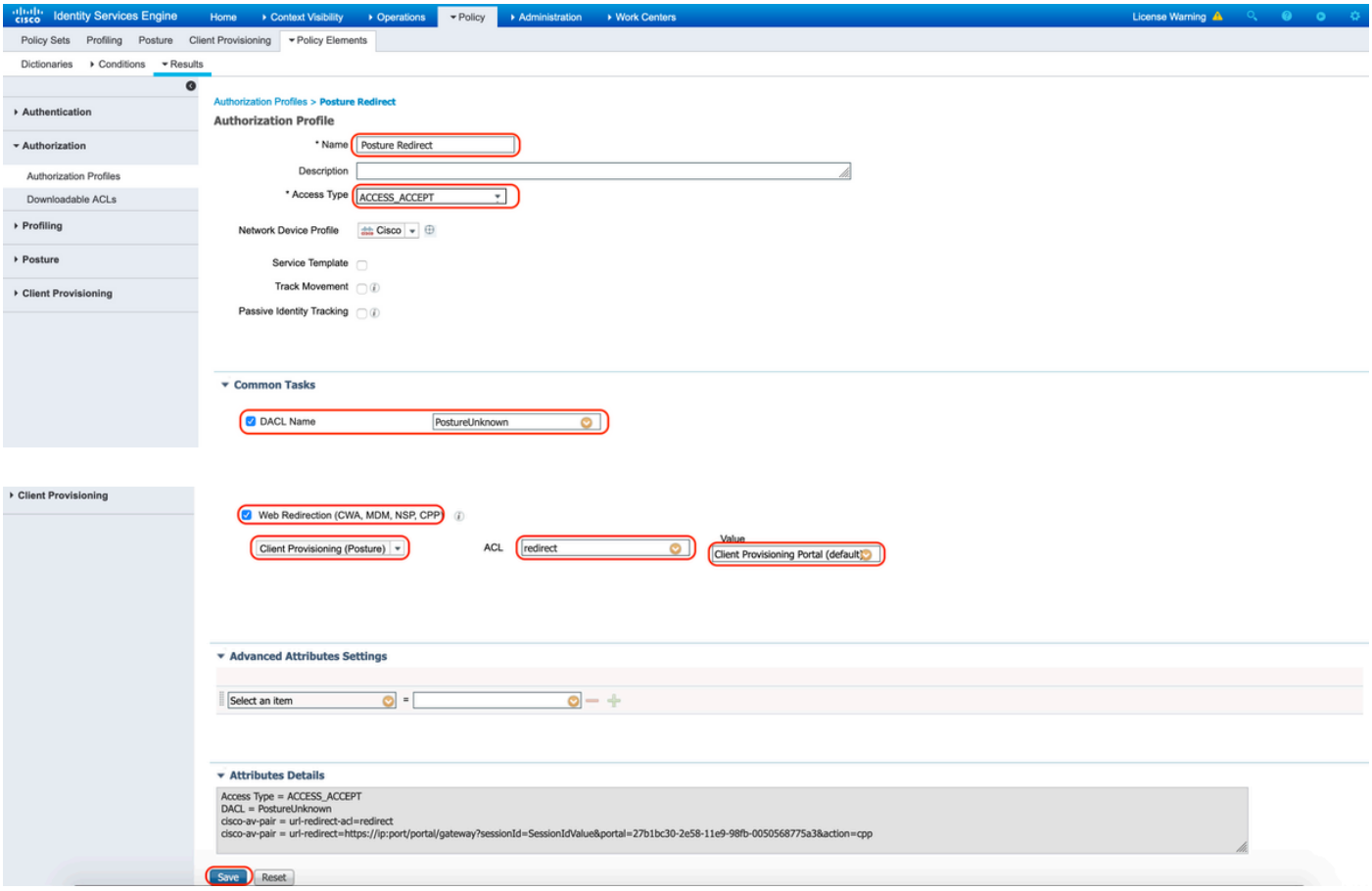


12. Criar Perfis de Autorização

Navegue para "Política > Elementos de política > Resultados > Autorização > Perfis de autorização".

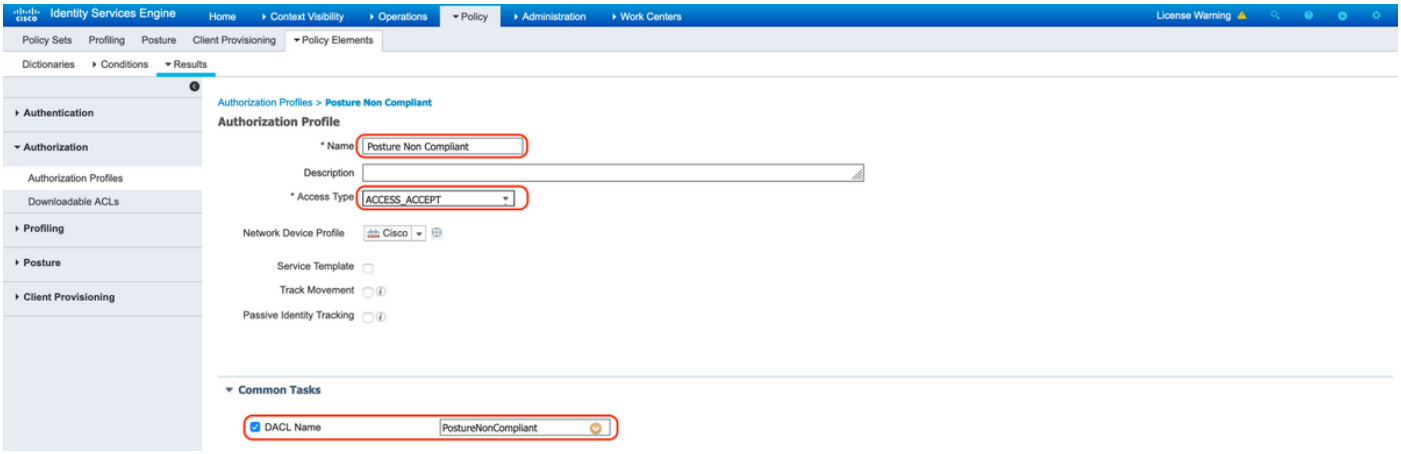
A. Perfil de autorização para postura desconhecida

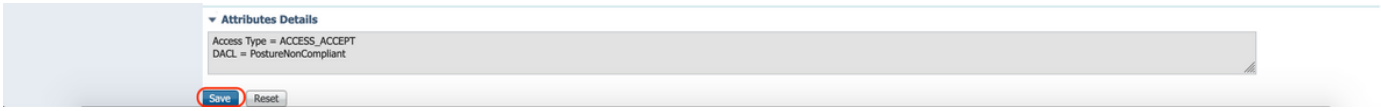
Selecione DACL "PostureUnknown", marque Web Redirection, selecione Client Provisioning(Posture), configure Redirect ACL name "redirect" (para ser configurado no ASA) e selecione o portal Client Provisioning (padrão)



B. Perfil de autorização para não conformidade com a postura

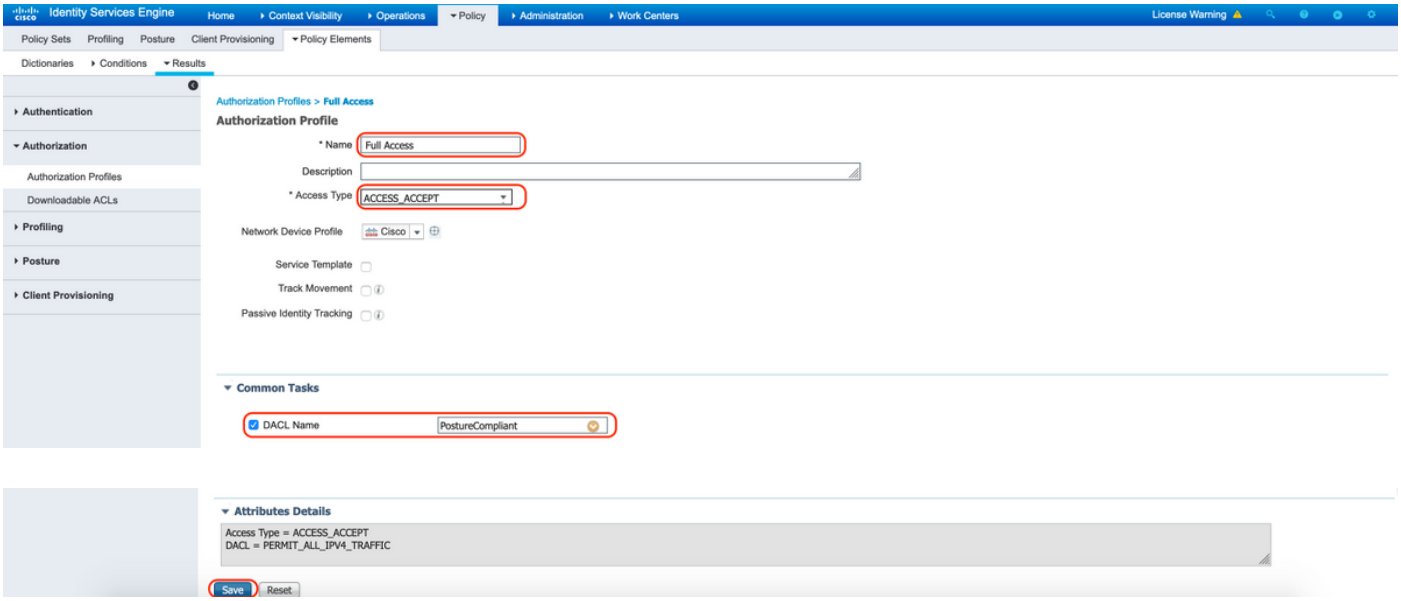
Selecione DACL "PostureNonCompliant" para limitar o acesso à rede





C. Perfil de Autorização para Conformidade com Posturas

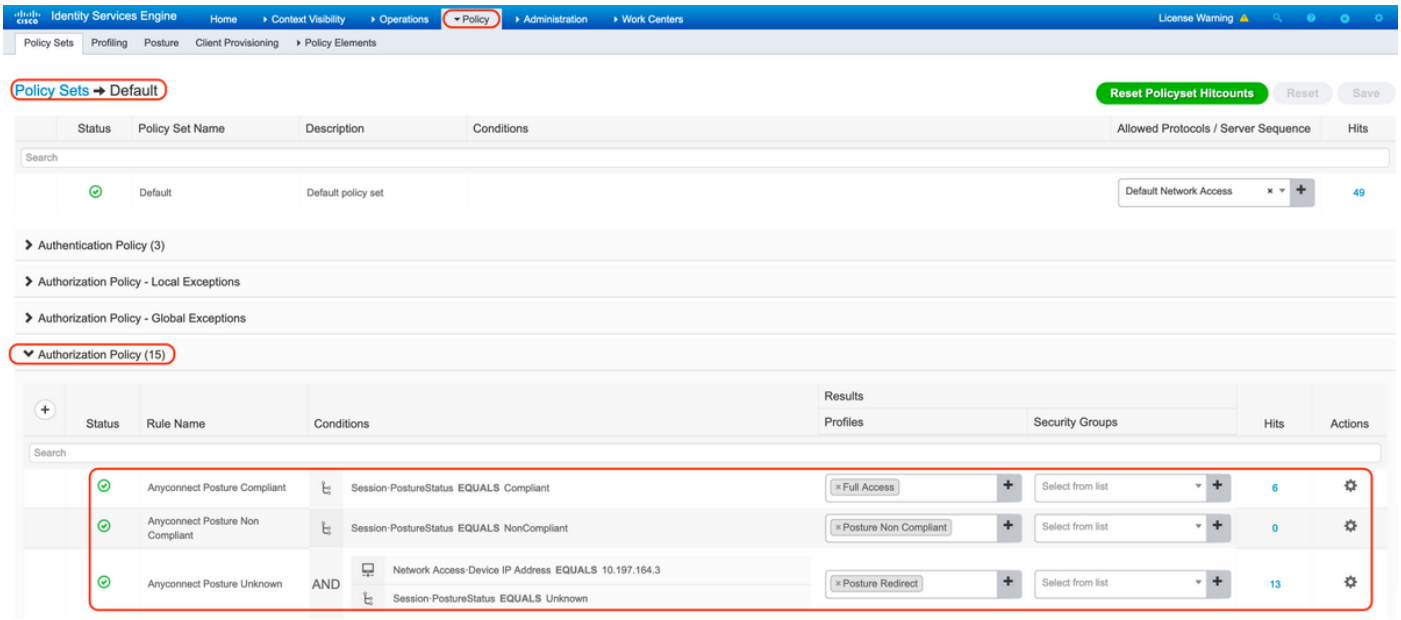
Selecione DACL "PostureCompliant" para permitir acesso total à rede



12. Configurar Políticas de Autorização

Use os perfis de autorização configurados na etapa anterior para configurar 3 políticas de autorização para Posture Compliant, Posture Non-Compliant e Posture Unknown.

Condição comum "Sessão: Status da Postura" é usada para determinar os resultados de cada política



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar se o usuário foi autenticado com êxito, execute o seguinte comando no ASA.

<#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&po
  Redirect ACL : redirect
```

Uma vez concluída a avaliação de postura, o acesso do usuário é alterado para acesso completo, conforme observado na DACL enviada no campo "Nome do filtro"

<#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
```

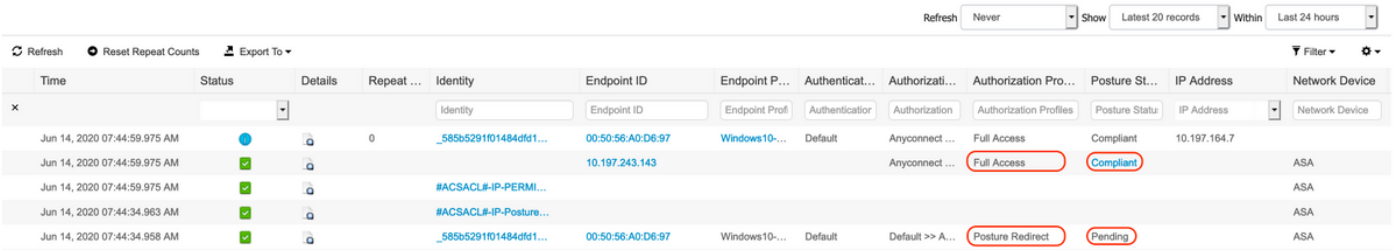
```
  Encapsulation: TLSv1.2               TCP Src Port : 57248
  TCP Dst Port : 443                   Auth Mode    : SAML
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 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
```

Para verificar se a autorização foi executada com êxito no ISE, navegue para "Operações > RADIUS > Registros ao vivo"

Esta seção exibe as informações relevantes associadas ao usuário autorizado, ou seja, identidade, perfil de autorização, política de autorização e status da postura.

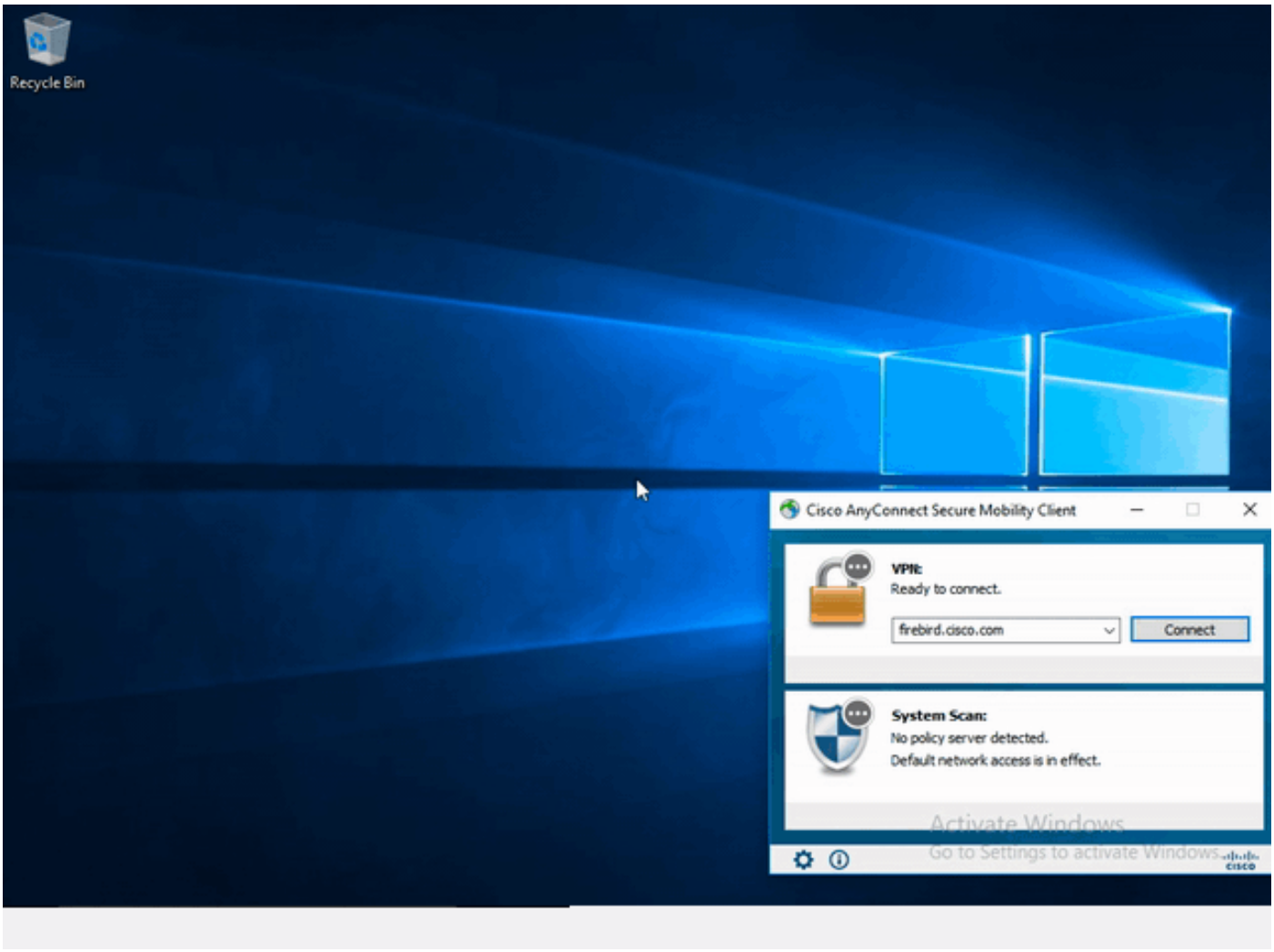


Observação: para validação de postura adicional no ISE, consulte a seguinte documentação: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc7

Para verificar o status da autenticação no Portal de administração Duo, clique em "Relatórios" no lado esquerdo do Painel de administração que mostra o Log de autenticação.
Mais detalhes: https://duo.com/docs/administration#reports

Para exibir o log de depuração do Gateway de Acesso Duo, use o seguinte link: https://help.duo.com/s/article/1623?language=en_US

Experiência do usuário



Troubleshooting

Esta seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

⚠ Cuidado: no ASA, você pode definir vários níveis de depuração; por padrão, o nível 1 é usado. Se você alterar o nível de depuração, o detalhamento das depurações poderá aumentar. Faça isso com cuidado, especialmente em ambientes de produção.

A maioria das soluções de problemas SAML envolverá uma configuração incorreta que pode ser encontrada através da verificação da configuração SAML ou da execução de depurações.

"debug webvpn saml 255" pode ser usado para solucionar a maioria dos problemas, no entanto, em cenários onde essa depuração não fornece informações úteis, depurações adicionais podem ser executadas:

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

Para solucionar problemas de autenticação e autorização no ASA, use os seguintes comandos de depuração:

```
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)
```

✎ Observação: para obter o fluxo de postura detalhado e a solução de problemas do AnyConnect e ISE, consulte o link a seguir:
[Comparação de estilo de postura do ISE para pré e pós 2.2]

Para interpretar e solucionar problemas de registros de depuração do Gateway de Acesso Duo

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

Informações Relacionadas

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-acces.html#anc0

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.