Integrazione di Duo SAML SSO con Anyconnect Secure Remote Access mediante ISE Posture

Sommario

Introduzione

Questo documento descrive un esempio di configurazione per l'integrazione di Duo SAML SSO con Adaptive Security Appliance (ASA) e l'accesso Cisco AnyConnect Secure Mobility Client che sfrutta Cisco ISE per una valutazione dettagliata della postura. Duo SAML SSO viene implementato utilizzando Duo Access Gateway (DAG) che comunica con Active Directory per l'autenticazione iniziale dell'utente e quindi comunica con Duo Security (Cloud) per l'autenticazione a più fattori. Cisco ISE viene usato come server di autorizzazione per fornire la verifica dell'endpoint con la valutazione della postura.

Contributo di Dinesh Moudgil e Pulkit Saxena, Cisco HTTS Engineer.

Prerequisiti

Requisiti

In questo documento si presume che l'ASA sia completamente operativa e configurata per consentire a Cisco Adaptive Security Device Manager (ASDM) o all'interfaccia della riga di

comando (CLI) di apportare modifiche alla configurazione.

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Concetti fondamentali di Duo Access Gateway e Duo Security
- Conoscenze base della configurazione VPN di accesso remoto sull'appliance ASA
- Conoscenze base di ISE e servizi di postura

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

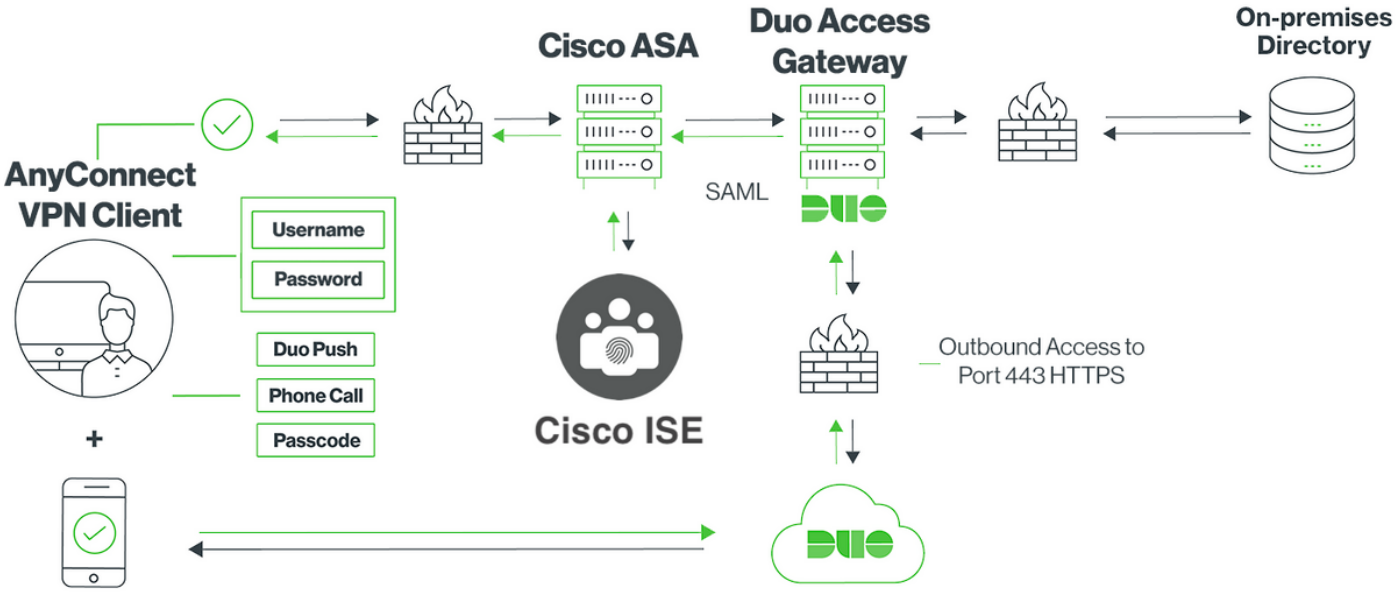
- Software Cisco Adaptive Security Appliance versione 9.12(3)12
- Duo Access Gateway
- Duo Security
- Cisco Identity Services Engine versione 2.6 e successive
- Microsoft Windows 10 con AnyConnect versione 4.8.03052

Nota: il software Anyconnect Embedded Browser, usato in questa implementazione, richiede un'appliance ASA versione 9.7(1)24, 9.8(2)28, 9.9(2)1 o successive di ciascuna versione e AnyConnect versione 4.6 o successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Flusso traffico

1. Il client Anyconnect avvia una connessione VPN SSL a Cisco ASA
2. Cisco ASA, configurato per l'autenticazione primaria con Duo Access Gateway (DAG), reindirizza il browser incorporato nel client Anyconnect al DAG per l'autenticazione SAML
3. Il client Anyconnect viene reindirizzato a Duo Access Gateway
4. Dopo che il client AnyConnect ha immesso le credenziali, viene creata una richiesta di autenticazione SAML che viene rilasciata da Cisco ASA a Duo Access Gateway
5. Duo Access Gateway sfrutta l'integrazione con Active Directory in loco per eseguire l'autenticazione primaria per il client Anyconnect
6. Una volta completata l'autenticazione primaria, Duo Access Gateway invia una richiesta a Duo Security tramite la porta TCP 443 per iniziare l'autenticazione a due fattori
7. Il client AnyConnect si è presentato con il "Duo Interactive Prompt" e l'utente completa l'autenticazione a due fattori Duo utilizzando il metodo preferito (push o passcode)
8. Duo Security riceve una risposta di autenticazione e restituisce le informazioni al Duo Access Gateway
9. In base alla risposta di autenticazione, Duo Access Gateway crea una risposta di autenticazione SAML che contiene un'asserzione SAML e risponde al client Anyconnect
10. Il client Anyconnect esegue l'autenticazione per la connessione VPN SSL con Cisco ASA
11. Quando l'autenticazione ha esito positivo, Cisco ASA invia una richiesta di autorizzazione a Cisco ISE

Nota: Cisco ISE è configurato solo per l'autorizzazione poiché Duo Access Gateway fornisce l'autenticazione necessaria

12. Cisco ISE elabora la richiesta di autorizzazione e, poiché lo stato della postura del client è Unknown, restituisce Posture redirect con accesso limitato al client Anyconnect tramite Cisco ASA

13. Se il client Anyconnect non ha un modulo di conformità, gli viene chiesto di scaricarlo per procedere più avanti con la valutazione della postura

14. Se il client Anyconnect ha un modulo di conformità, stabilisce una connessione TLS con Cisco ASA e il flusso di postura si avvia

15. A seconda delle condizioni di postura configurate su ISE, vengono eseguiti i controlli di postura e i dettagli vengono inviati dal client Anyconnect a Cisco ISE

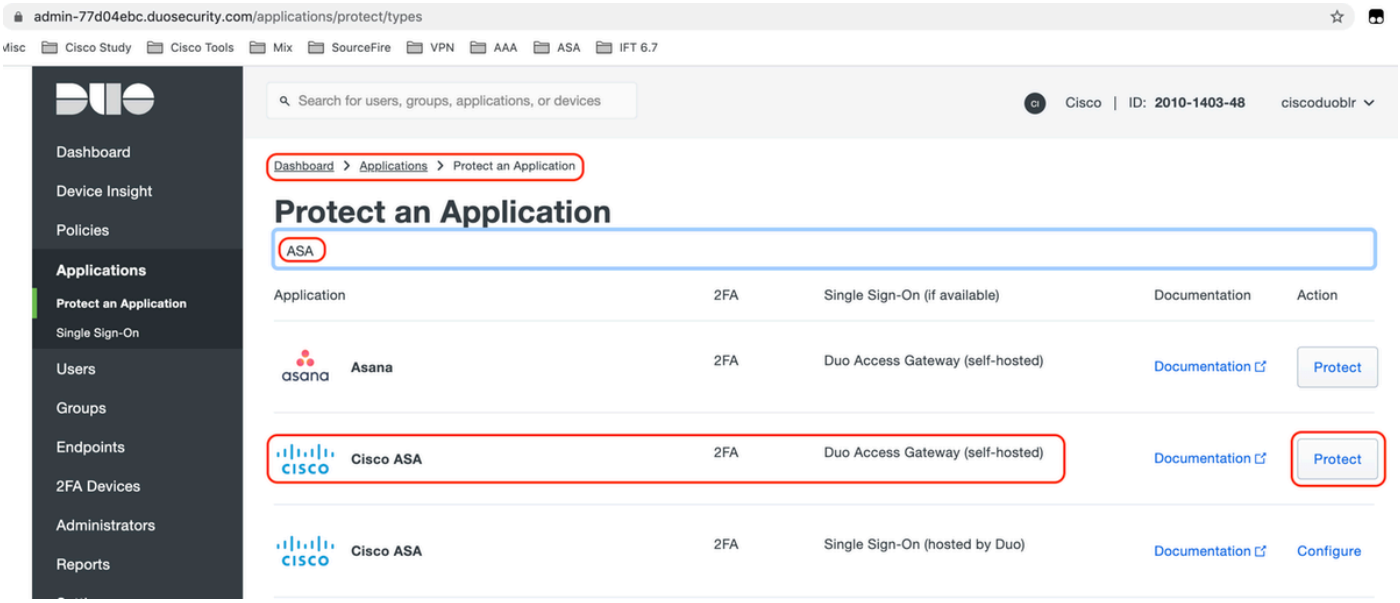
16. Se lo stato della postura del client cambia da Sconosciuto a Conforme, la richiesta di modifica dell'autorizzazione (CoA) viene inviata da Cisco ISE a Cisco ASA per concedere l'accesso completo al client e la VPN è completamente stabilita

Configurazioni

- Configurazione del portale di amministrazione Duo

In questa sezione, configurare l'applicazione ASA sul portale di amministrazione Duo.

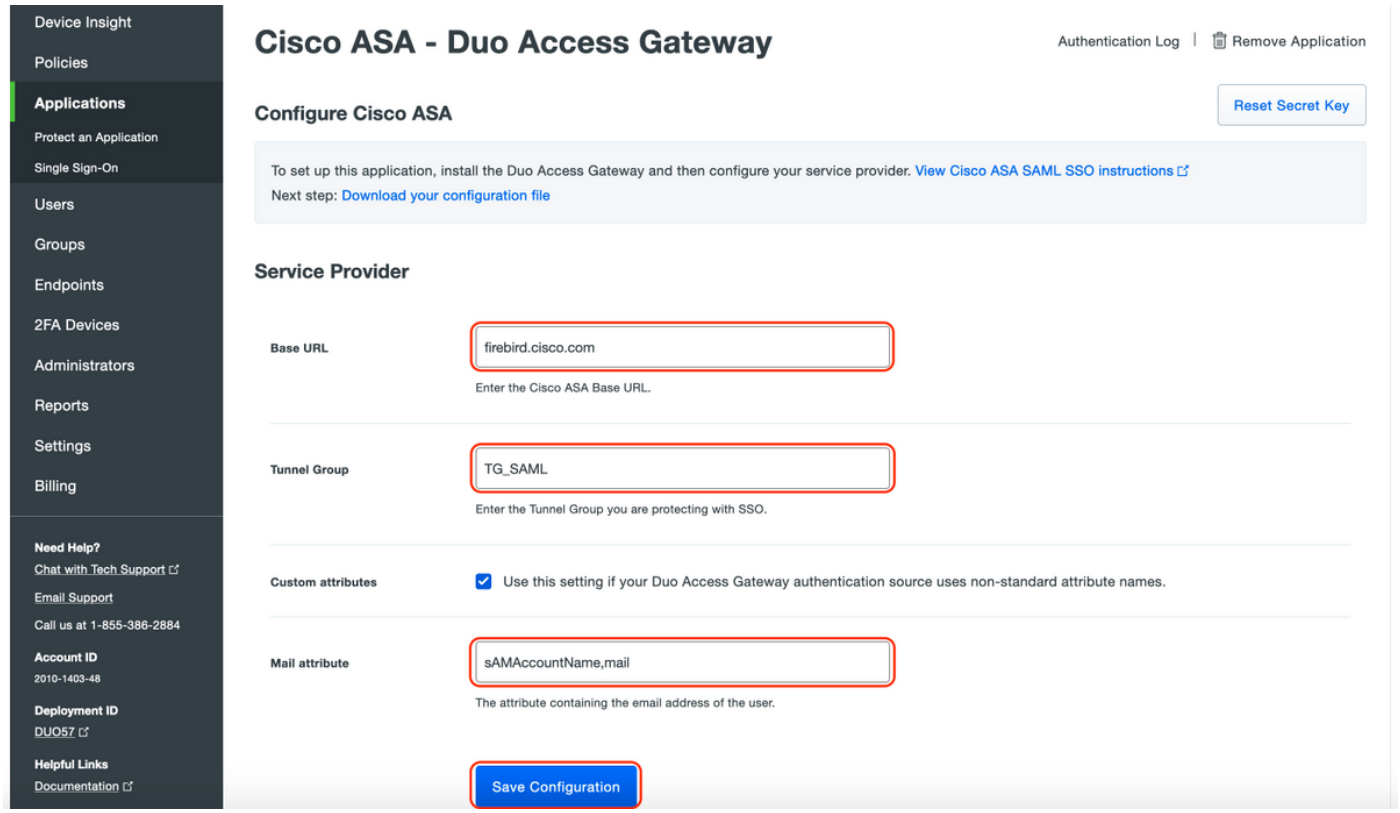
1. Accedere a "Duo Admin Portal" e selezionare "Applications > Protect an Application" (Applicazioni > Proteggi un'applicazione), quindi cercare "ASA" con tipo di protezione "2FA con Duo Access Gateway, con hosting automatico". Fare clic su "Protect" (Proteggi) all'estrema destra per configurare l'appliance Cisco ASA.



2. Configurare gli attributi seguenti in "Service Provider" per l'applicazione protetta, ASA

URL di base	firebird.cisco.com
Gruppo di tunnel	TG_SAML
Attributo Mail	sAMAccountName,posta

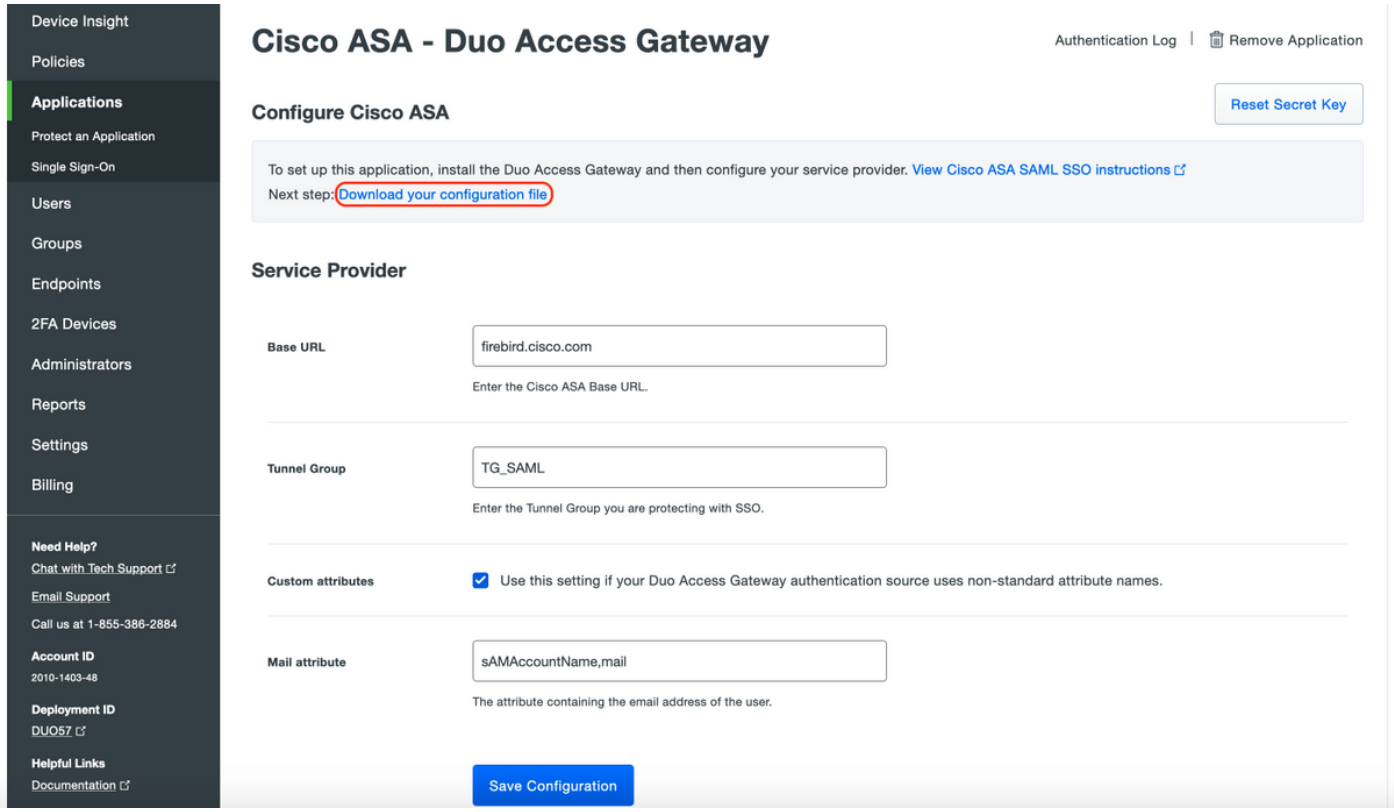
Fare clic su "Salva" in fondo alla pagina



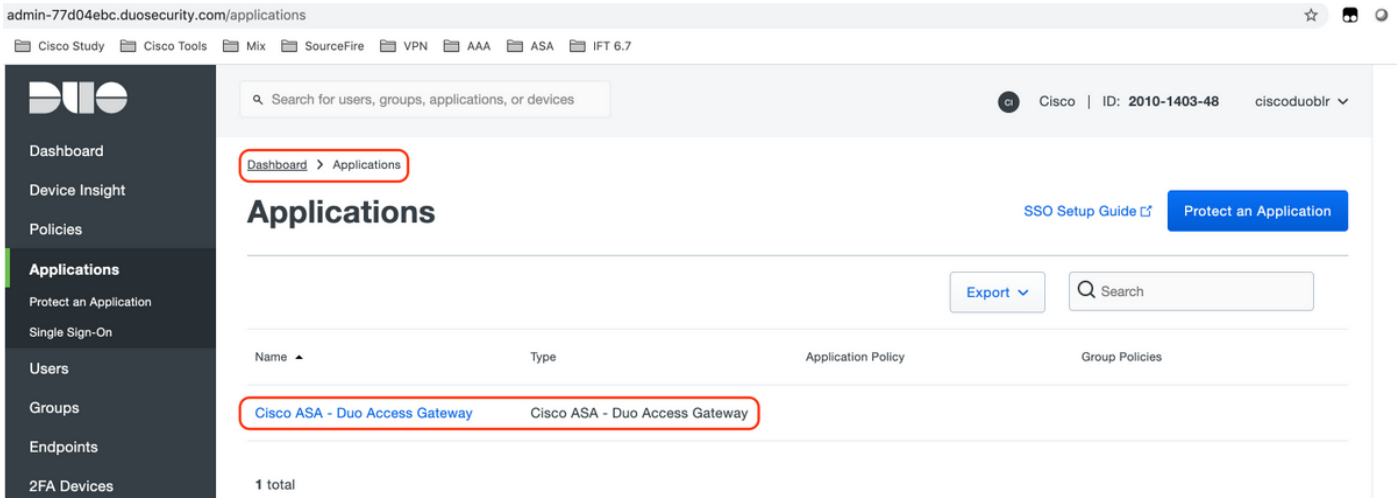
In questo documento, il resto della configurazione utilizza parametri predefiniti ma è possibile

impostarli in base ai requisiti del cliente.
In questo momento è possibile modificare ulteriori impostazioni per la nuova applicazione SAML, ad esempio modificare il nome dell'applicazione dal valore predefinito, attivare la modalità self-service o assegnare un criterio di gruppo.

3. Fare clic sul collegamento "Download your configuration file" per ottenere le impostazioni dell'applicazione Cisco ASA (come file JSON). Questo file viene caricato su Duo Access Gateway nei passaggi successivi

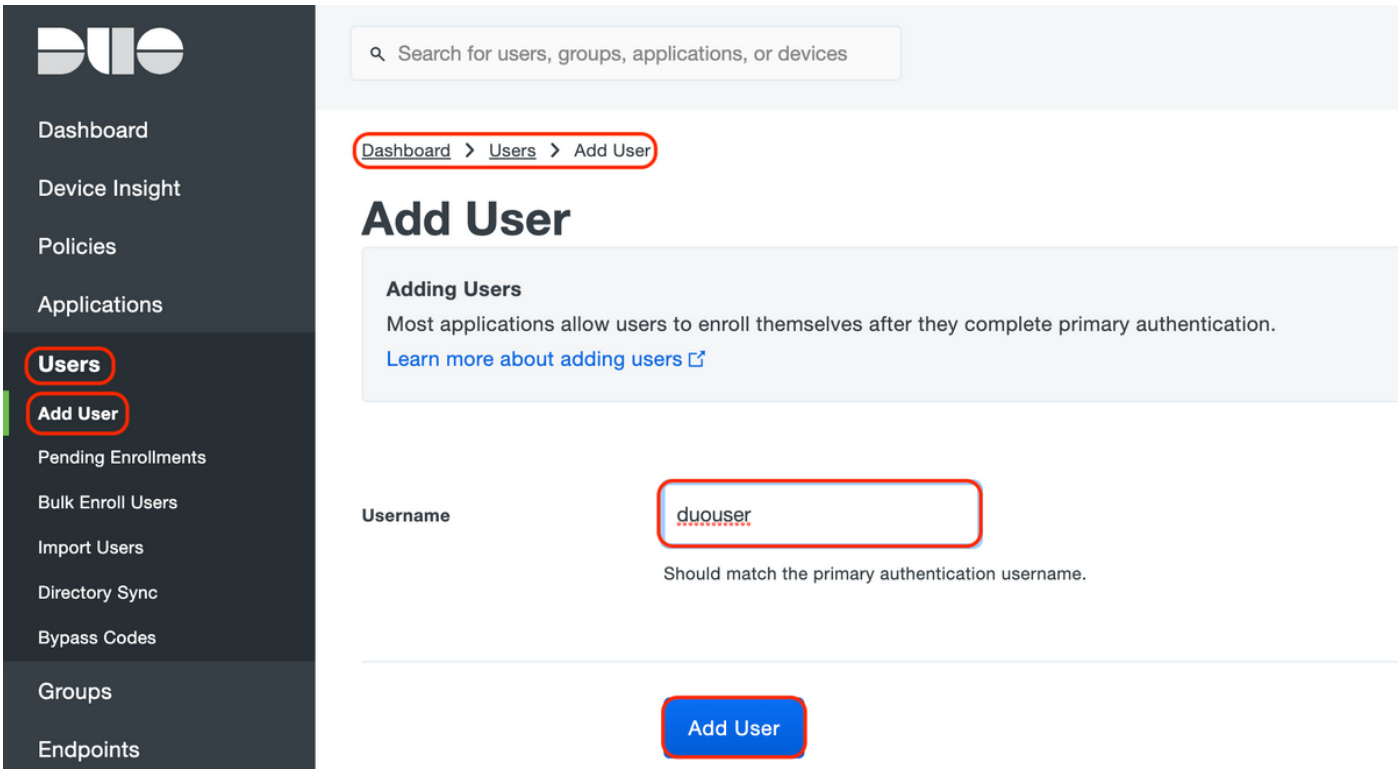


4. In "Dashboard > Applicazioni", l'applicazione ASA appena creata ha l'aspetto mostrato nell'immagine seguente:

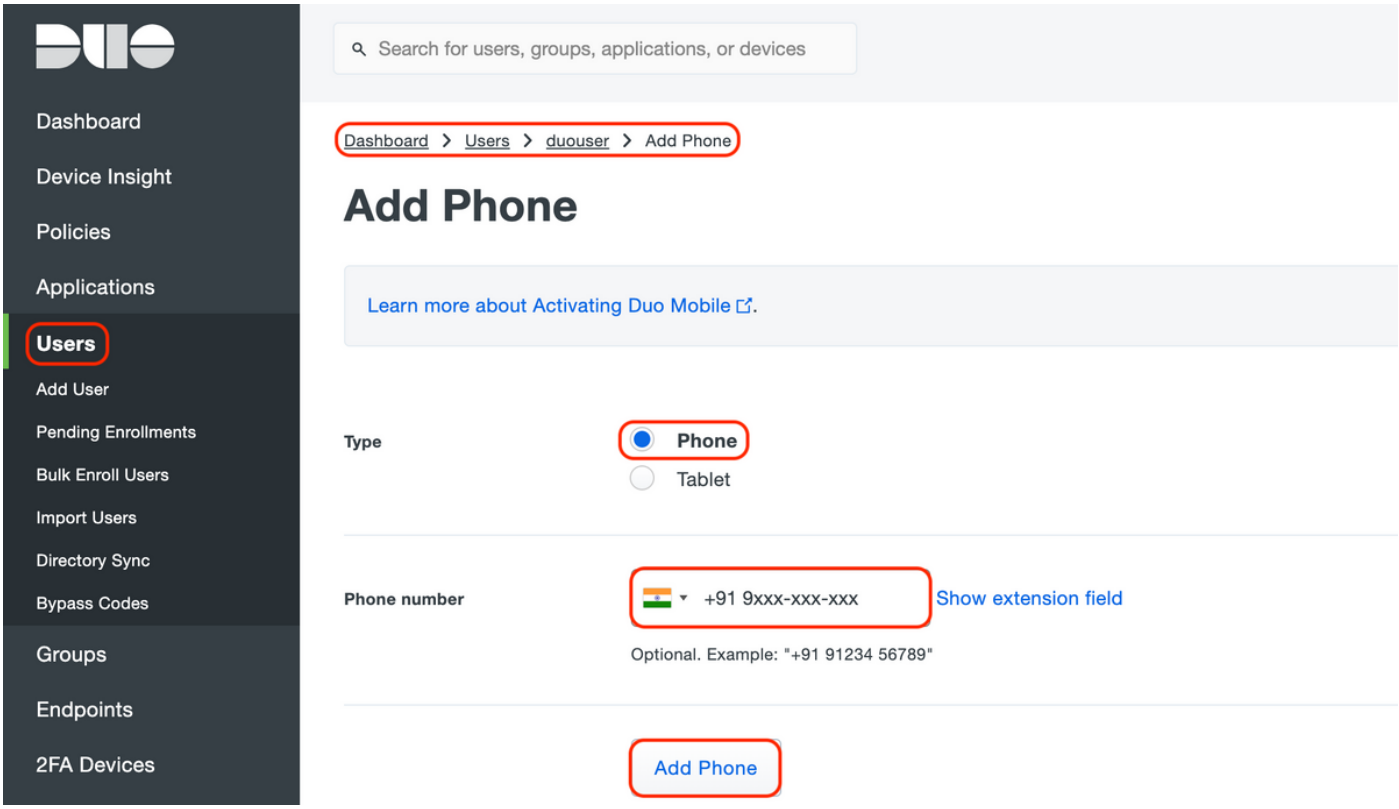


5. Passare a "Utenti > Aggiungi utente" come mostrato nell'immagine:

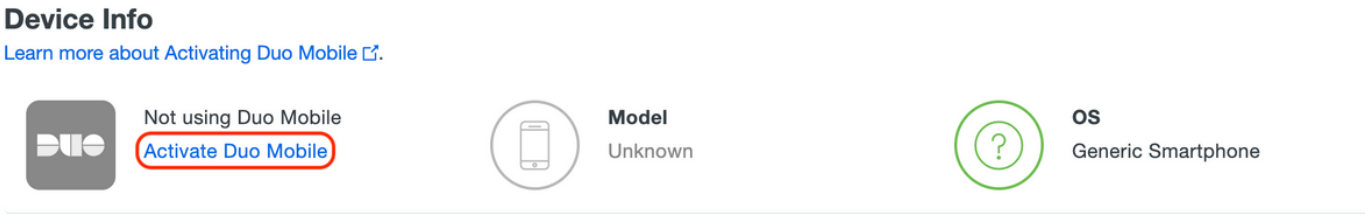
Creare un utente denominato "duouser" da utilizzare per l'autenticazione di Accesso remoto Anyconnect e attivare Duo Mobile sul dispositivo dell'utente finale



Per aggiungere il numero di telefono come mostrato nell'immagine, selezionare l'opzione "Add Phone" (Aggiungi telefono).

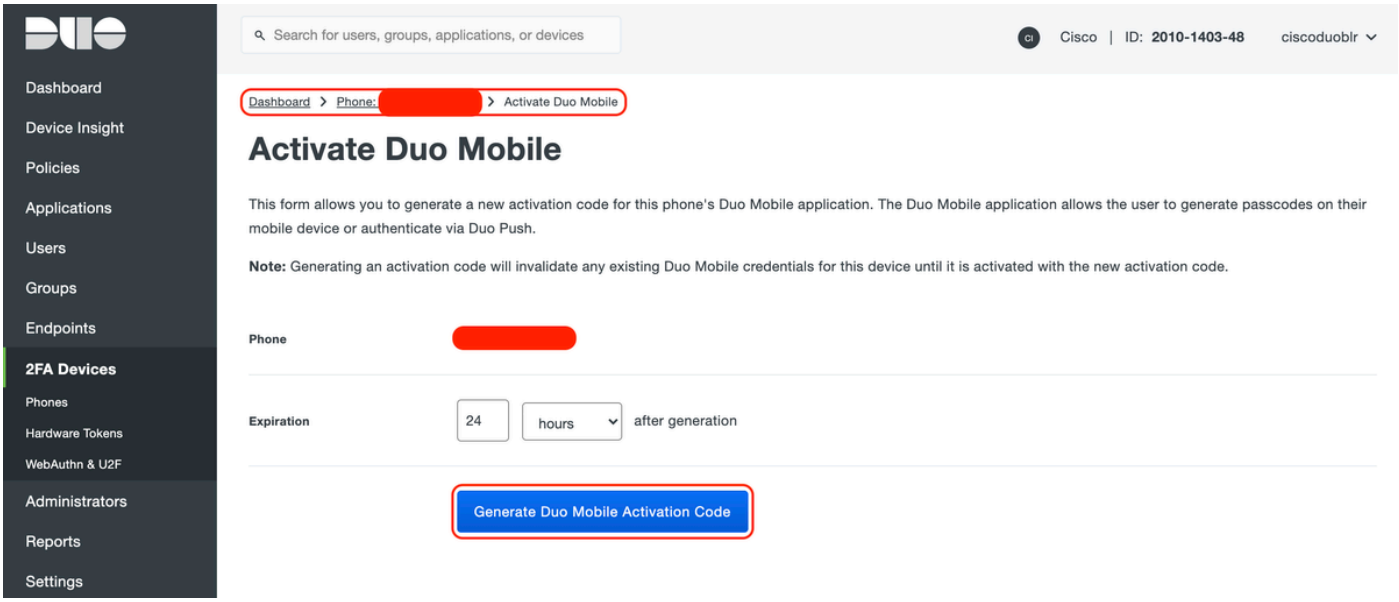


Attiva "Duo Mobile" per l'utente specifico

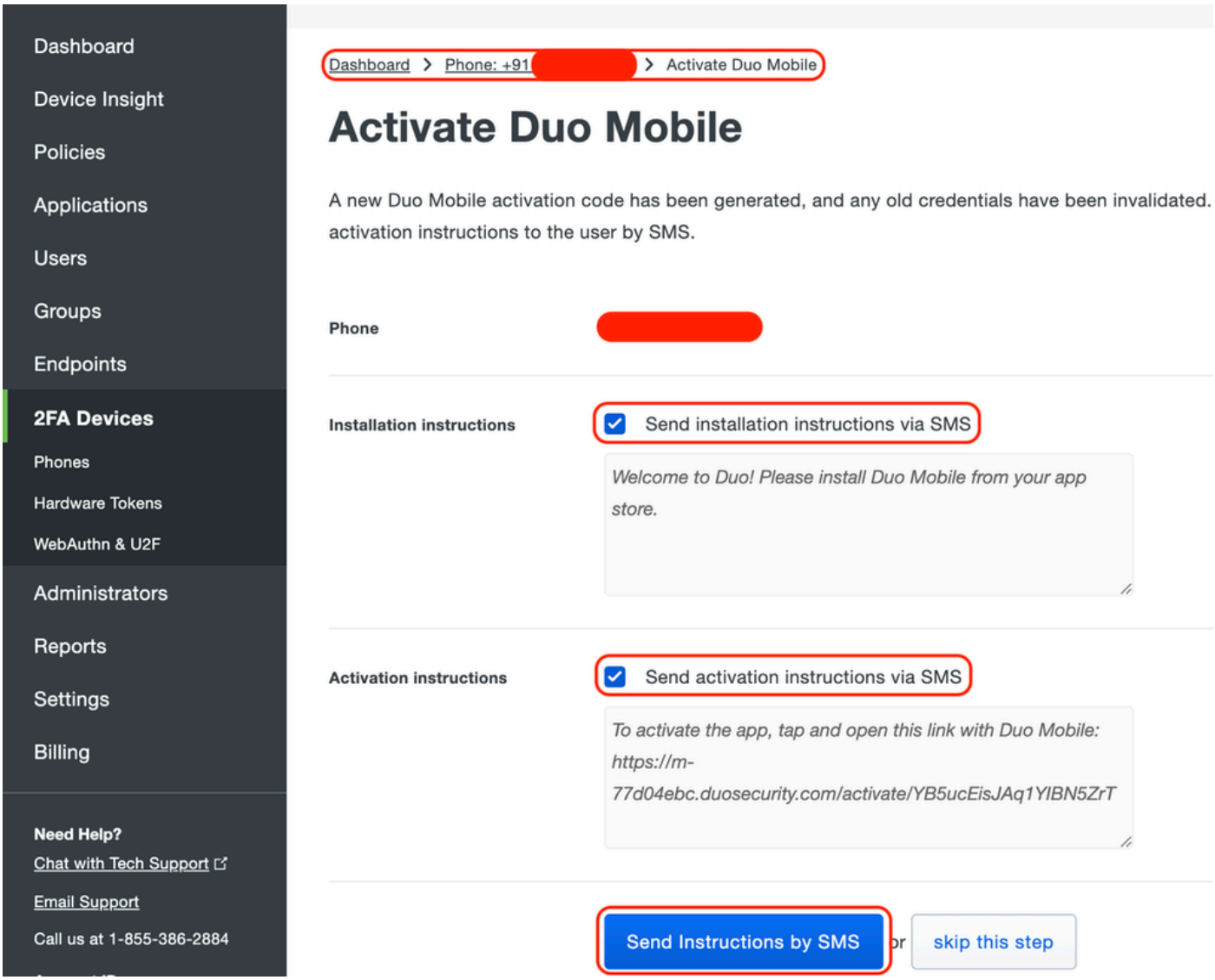


Nota: verificare che "Duo Mobile" sia installato sul dispositivo dell'utente finale.
[Installazione manuale dell'applicazione Duo per dispositivi IOS]
[Installazione manuale dell'applicazione Duo per dispositivi Android]

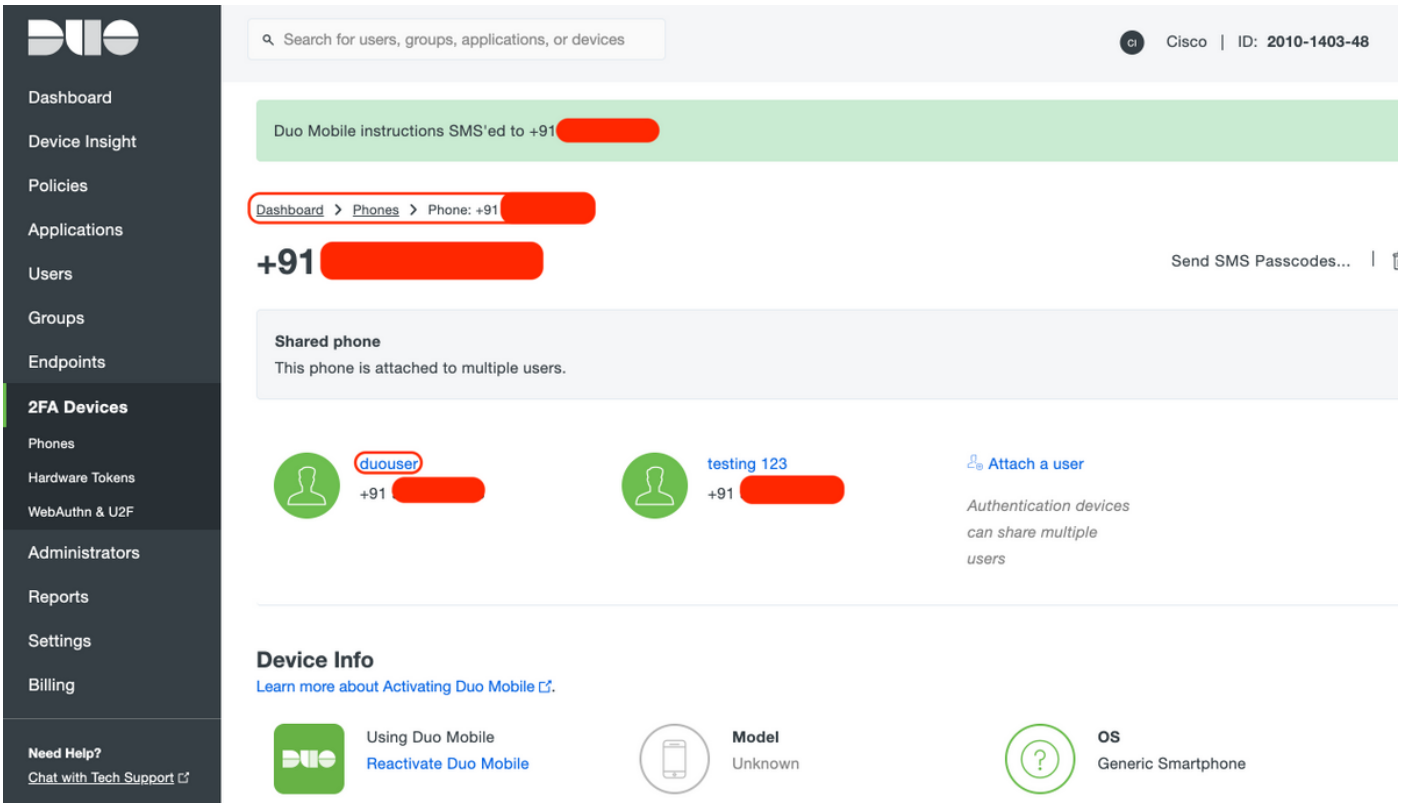
Selezionare "Generate Duo Mobile Activation Code" (Genera codice di attivazione mobile Duo) come illustrato nell'immagine:



Selezionare "Send Instructions by SMS" (Invia istruzioni tramite SMS) come mostrato nell'immagine:



Fare clic sul collegamento nell'SMS e l'app Duo viene collegata all'account utente nella sezione Informazioni sul dispositivo, come mostrato nell'immagine:



- Configurazione Duo Access Gateway (DAG)

1. Distribuire Duo Access Gateway (DAG) su un server nella rete

---

Nota: per la distribuzione, attenersi ai seguenti documenti:

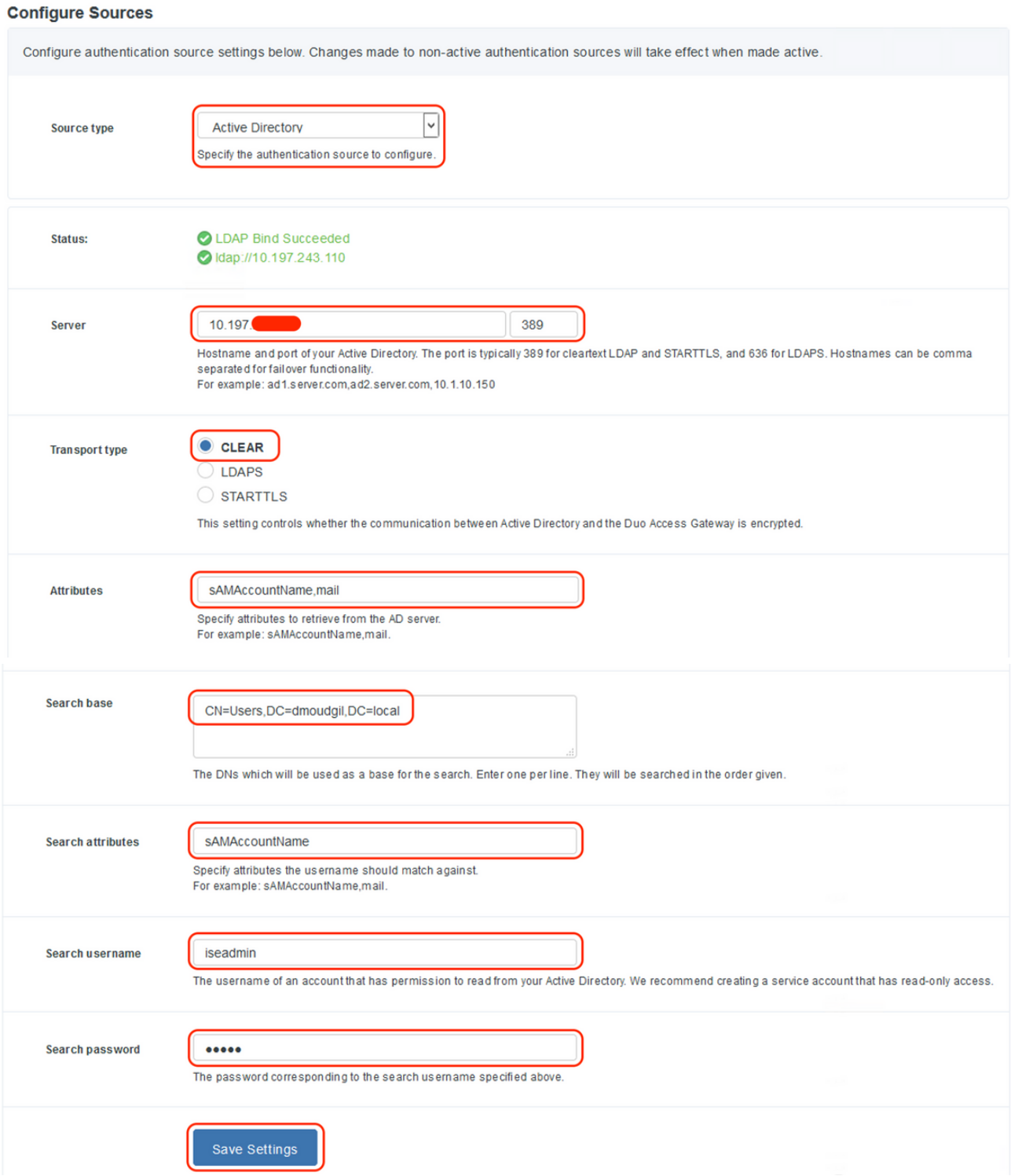
Duo Access Gateway per Linux
https://duo.com/docs/dag-linux

Duo Access Gateway per Windows
https://duo.com/docs/dag-windows

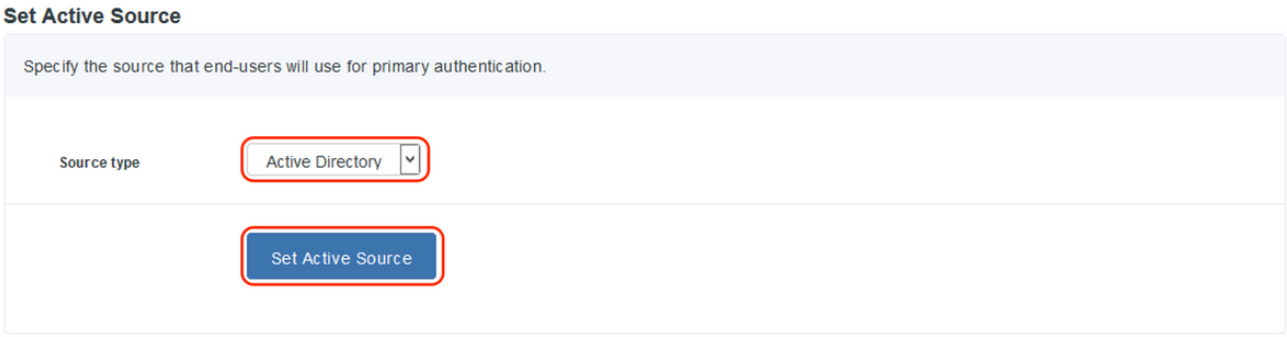
---

2. Nella home page di Duo Access Gateway, passare a "Authentication Source" (Origine autenticazione)

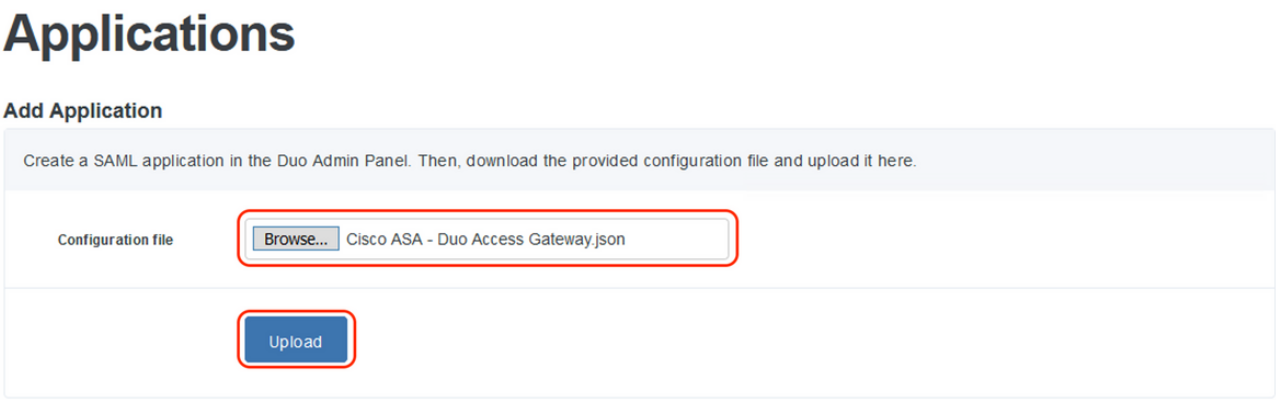
3. In "Configura origini", immettere gli attributi seguenti per Active Directory e fare clic su "Salva impostazioni"



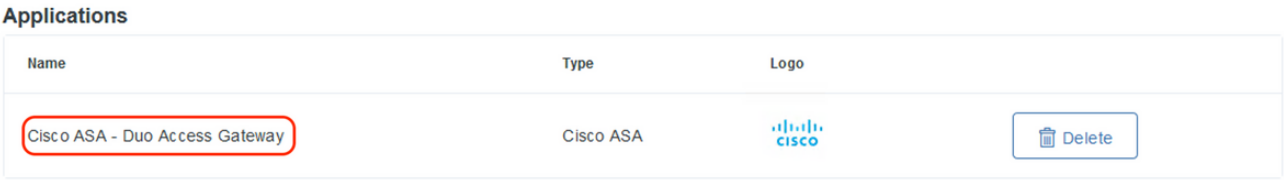
4. In "Imposta origine attiva" selezionare il tipo di origine "Active Directory" e fare clic su "Imposta origine attiva"



5. Passare a "Applications" (Applicazioni), nel sottomenu "Add Application" (Aggiungi applicazione), e caricare il file .json scaricato dalla Duo Admin Console nella sezione "Configuration file" (File di configurazione). Il file .json corrispondente è stato scaricato nel Passaggio 3 in Duo Admin Portal Configuration

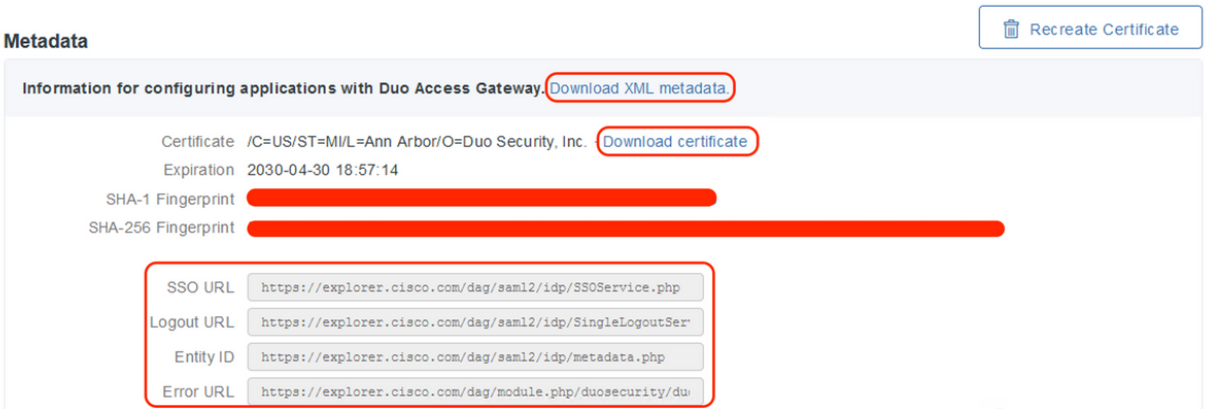


6. Una volta aggiunta l'applicazione, appare nel sottomenu "Applicazioni"



7. Nel sottomenu "Metadati", scaricare i metadati XML e il certificato IdP e annotare i seguenti URL, configurati successivamente sull'appliance ASA

    1. URL SSO
    2. URL di disconnessione
    3. ID entità
    4. URL errore



- Configurazione ASA

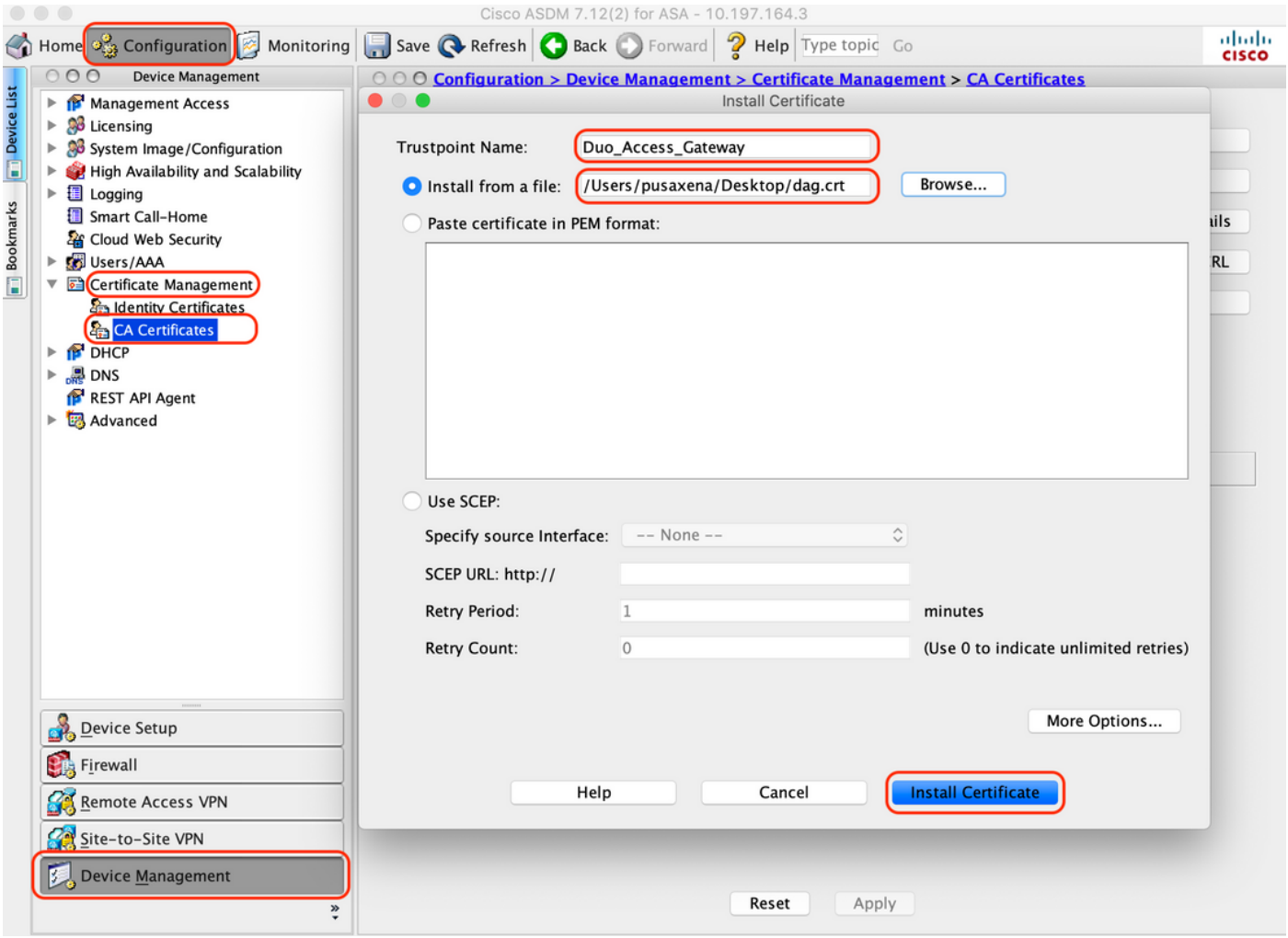
In questa sezione vengono fornite le informazioni per configurare l'ASA per l'autenticazione IDP SAML e la configurazione base di AnyConnect. Nel documento vengono illustrati i passaggi della configurazione ASDM e la configurazione di esecuzione CLI per una panoramica.

1. Carica certificato Duo Access Gateway

A. Selezionare "Configurazione > Gestione dispositivi > Gestione certificati > Certificati CA", quindi fare clic su "Aggiungi".

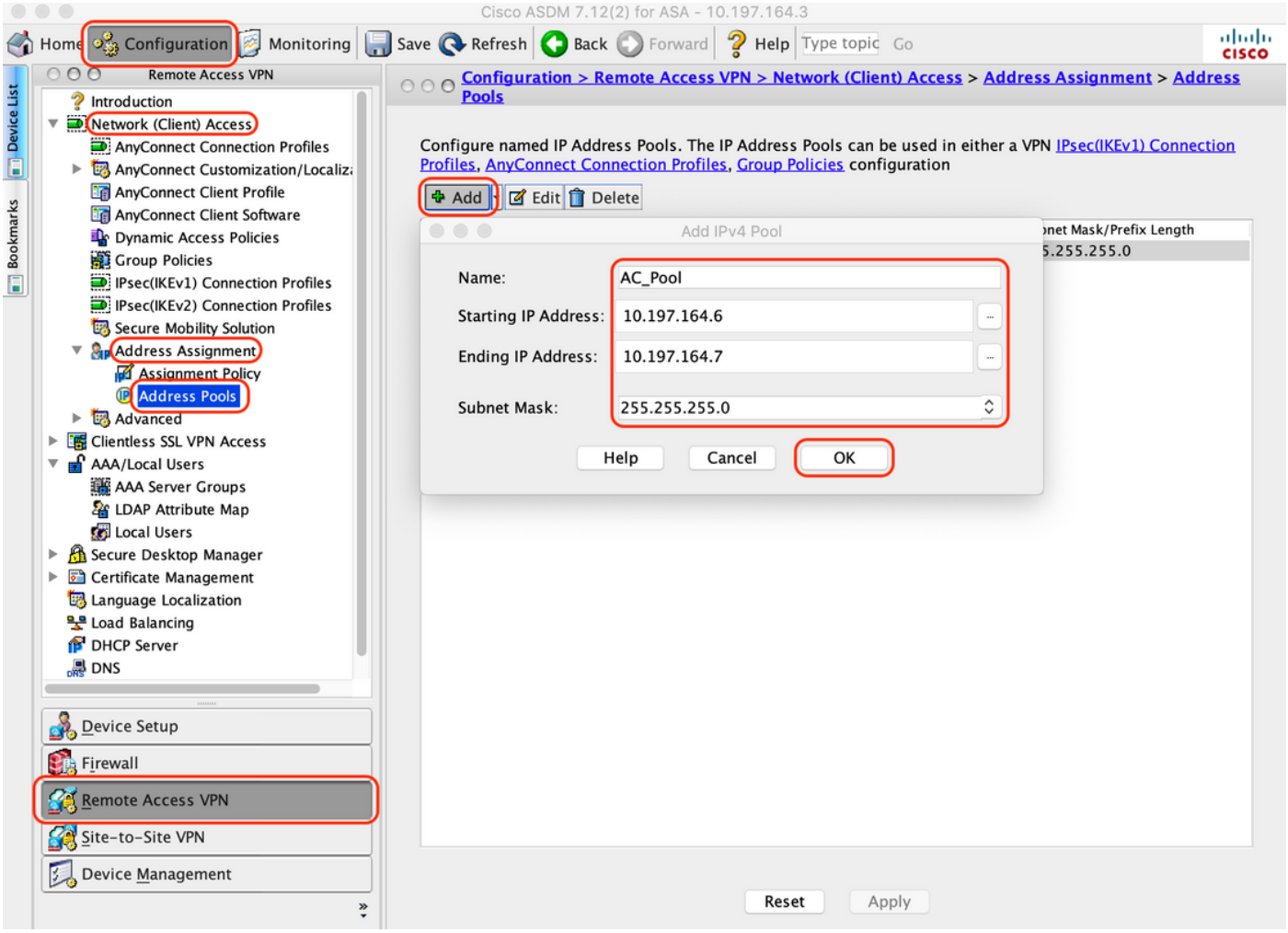
B. Nella pagina "Installa certificato", configurare il nome del punto di accesso: Duo_Access_Gateway

C. Fare clic su "Sfoglia" per selezionare il percorso associato al certificato del gruppo di disponibilità del database e, una volta selezionato, fare clic su "Installa certificato"



2. Creazione del pool locale IP per gli utenti AnyConnect

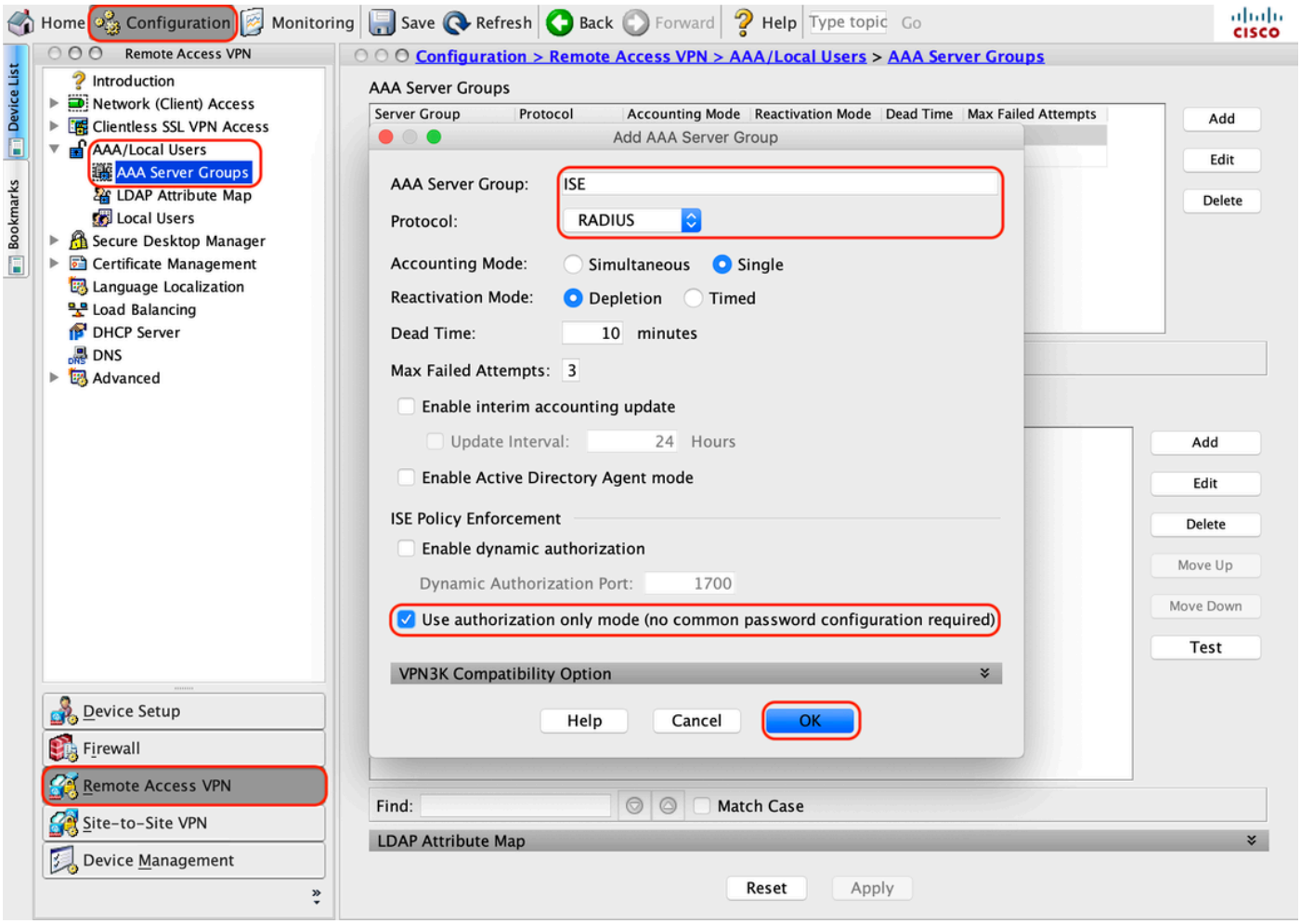
Selezionare "Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Assegnazione indirizzi > Pool di indirizzi", quindi fare clic su "Aggiungi".



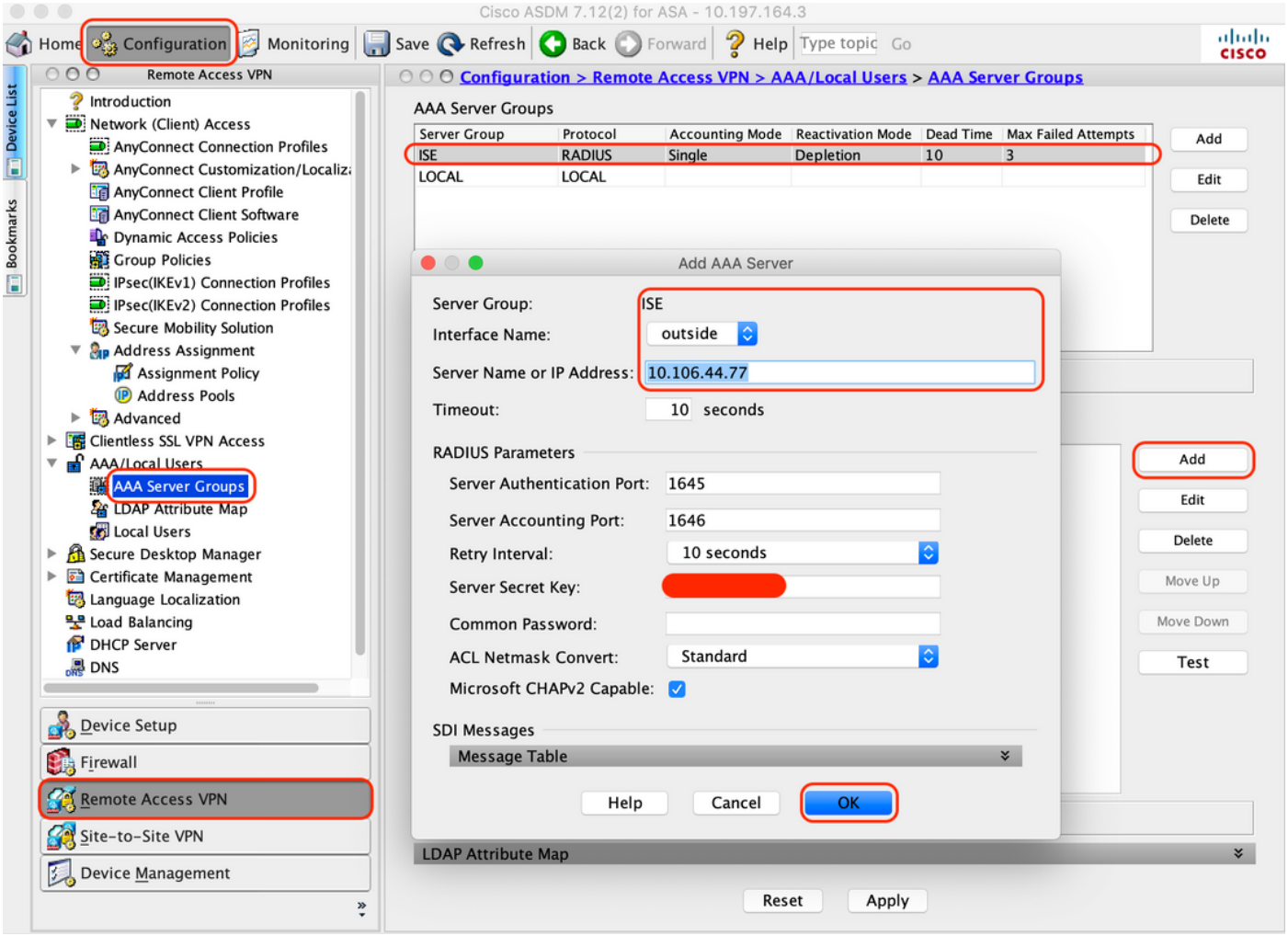
3. Configurare il gruppo di server AAA

A. In questa sezione configurare il gruppo di server AAA e fornire i dettagli del server AAA specifico che esegue l'autorizzazione.

B. Selezionare "Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups" (Configurazione > VPN ad accesso remoto > Utenti locali AAA > Gruppi di server AAA), quindi fare clic su "Add" (Aggiungi).



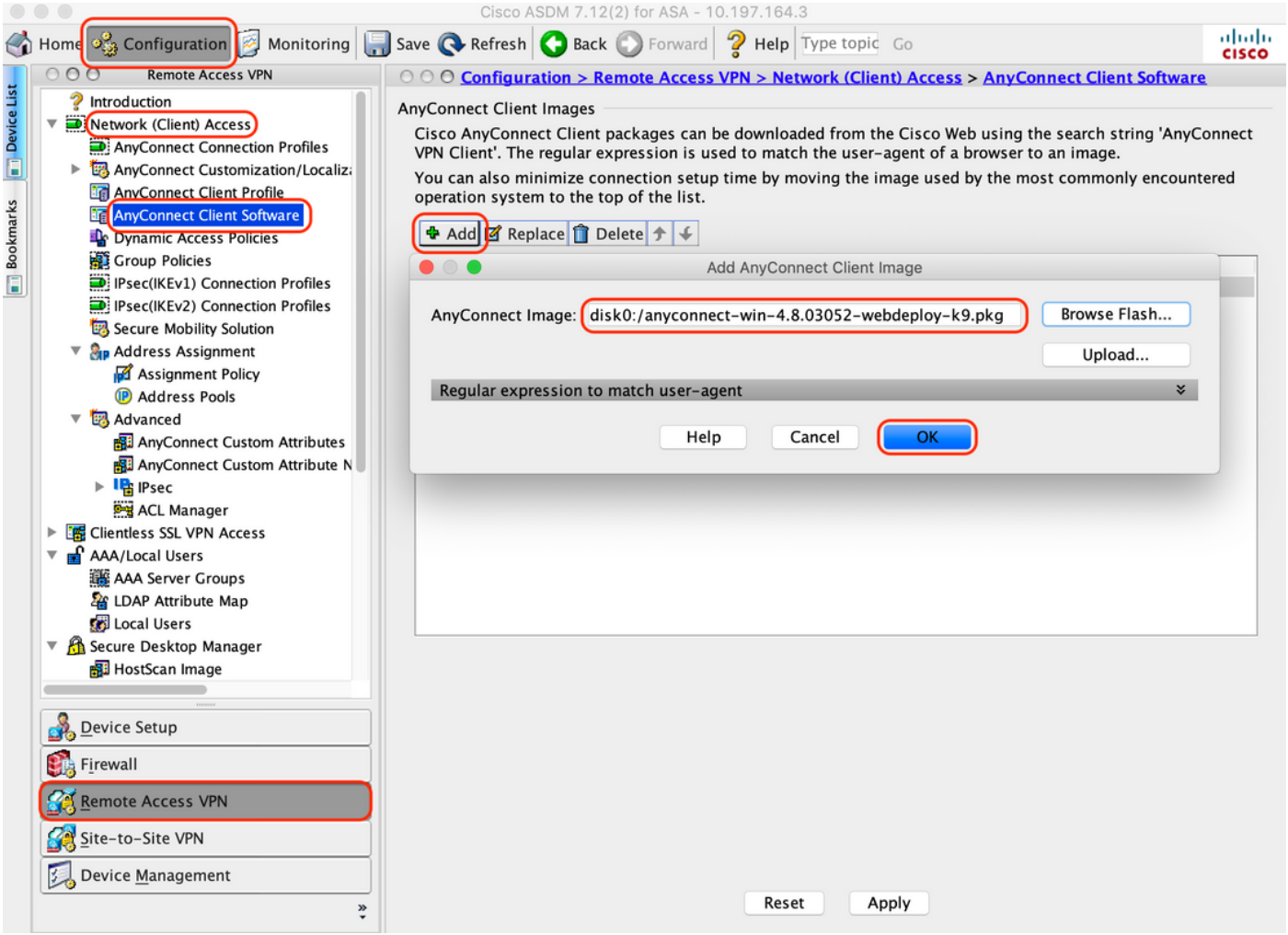
C. Nella stessa pagina, nella sezione "Server nel gruppo selezionato", fare clic su "Aggiungi" e fornire i dettagli dell'indirizzo IP del server AAA



4. Mappa il software client AnyConnect

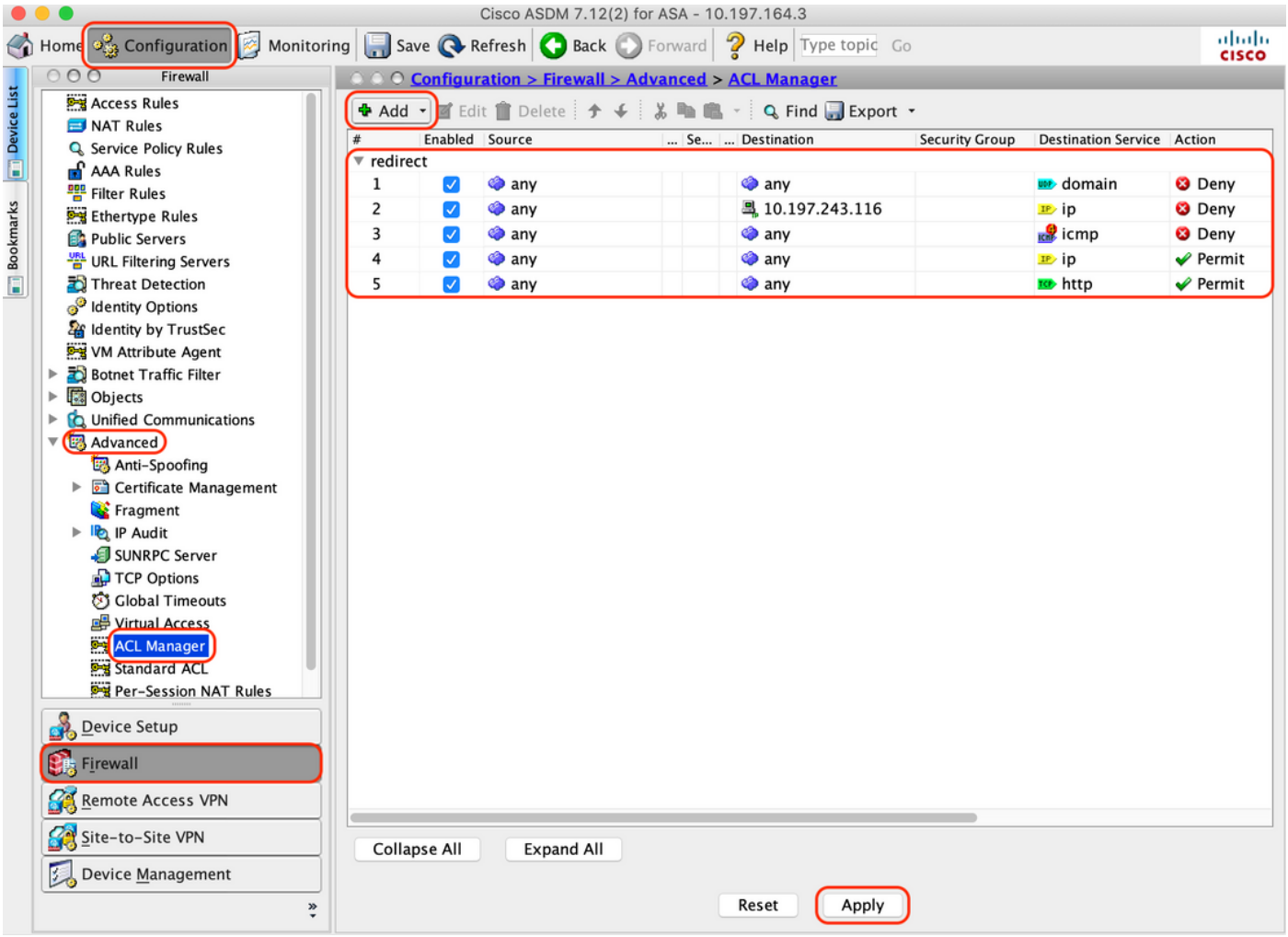
A. Mappare l'immagine WebDeployment del software client AnyConnect 4.8.03052 per usare Windows per WebVPN

B. Selezionare "Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software", quindi fare clic su "Add"



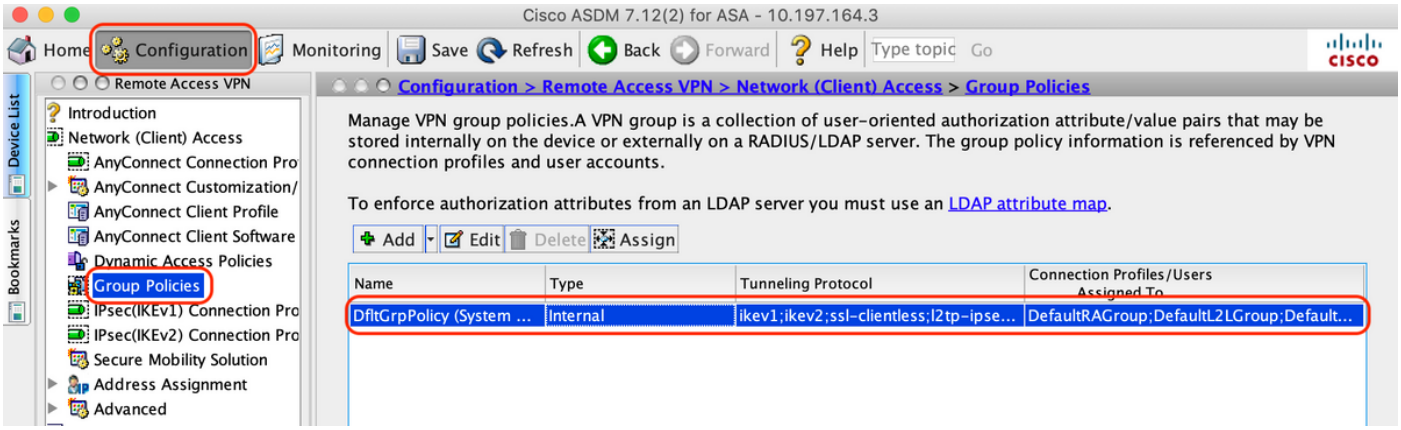
5. Configurare l'ACL di reindirizzamento su cui viene eseguito il push come risultato di ISE

A. Selezionare "Configuration > Firewall > Advanced > ACL Manager", quindi fare clic su Add per aggiungere l'ACL di reindirizzamento. Le voci, una volta configurate, vengono visualizzate come illustrato di seguito:



6. Convalida Criteri di gruppo esistenti

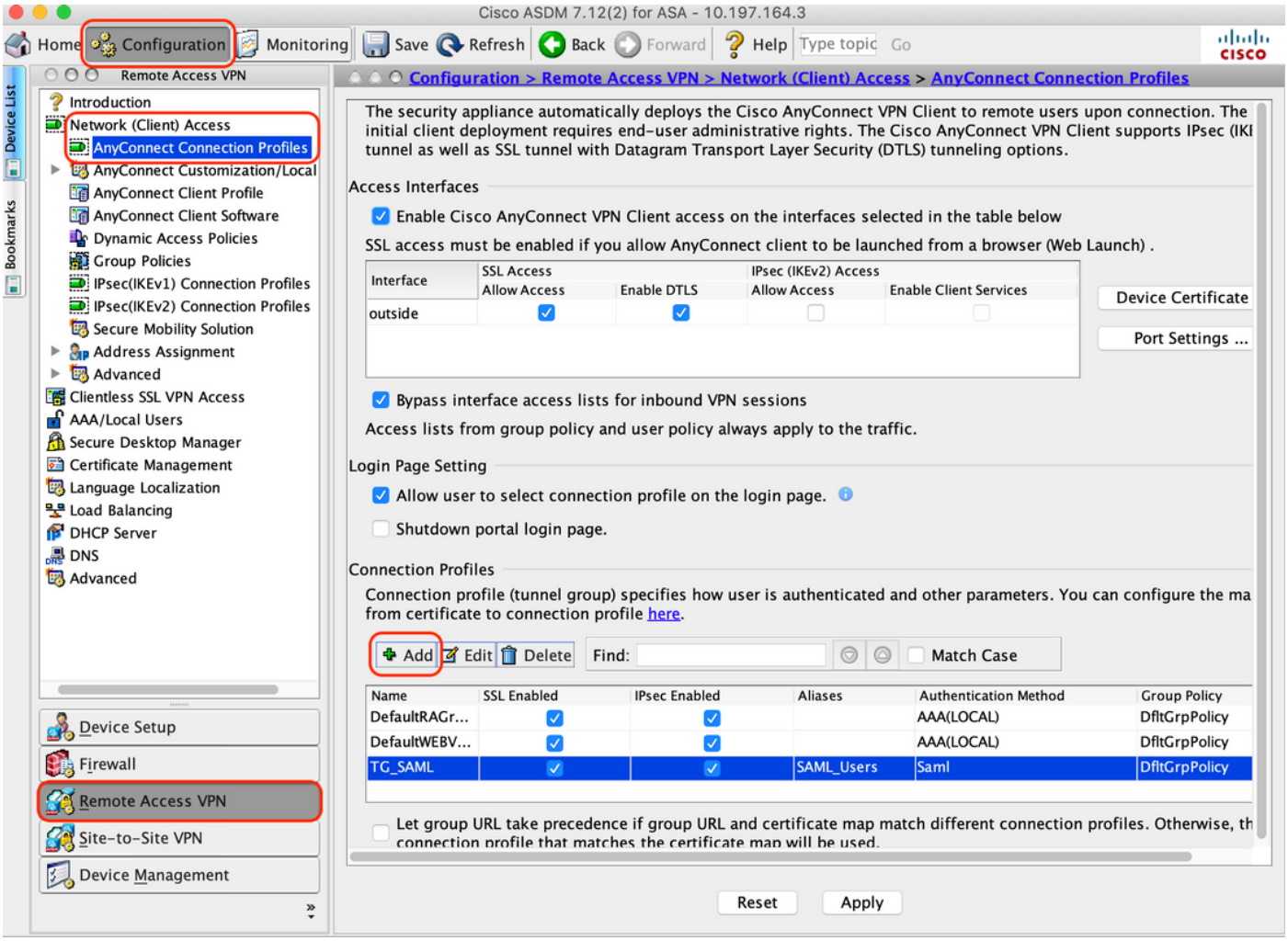
R. Questa impostazione utilizza i criteri di gruppo predefiniti e può essere visualizzata in: "Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo"



7. Configurare il profilo di connessione

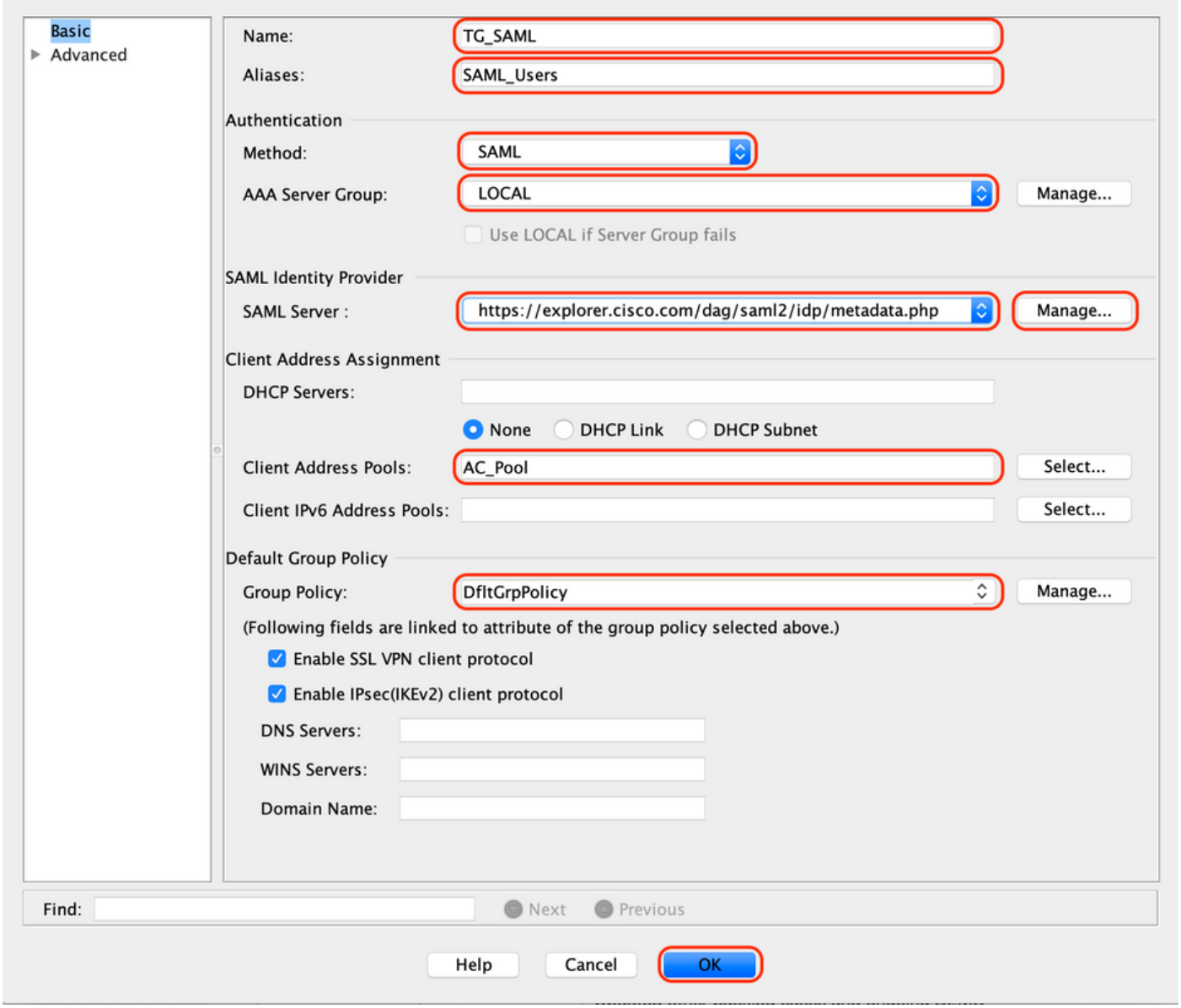
A. Creare un nuovo profilo di connessione a cui si connettono gli utenti AnyConnect

B. Selezionare "Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione Anyconnect", quindi fare clic su "Aggiungi".



C. Configurare i seguenti dettagli associati al profilo di connessione:

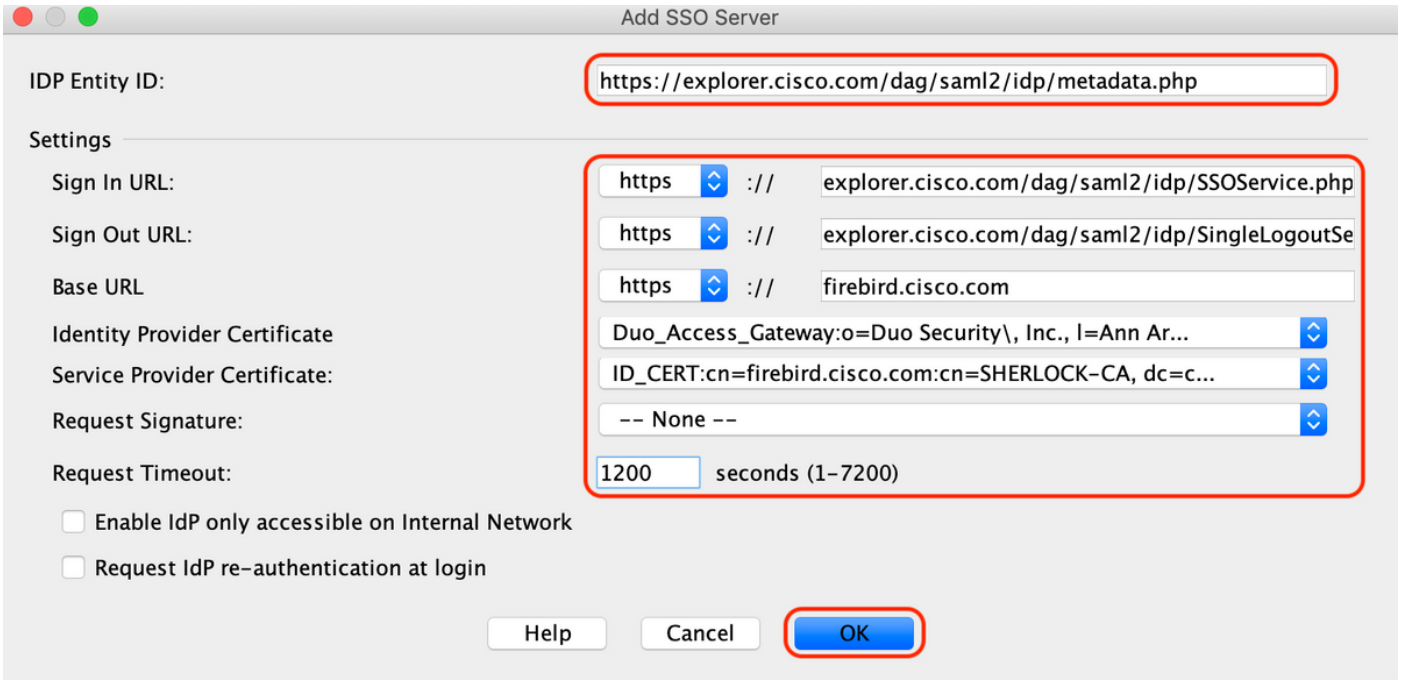
Nome	TG_SAML
Alias	Utenti_SAML
Metodo	SAML
Gruppo server AAA	Locale
Pool di indirizzi client	Pool_CA
Criteri di gruppo	CriterioGruppoDflt



D. Nella stessa pagina configurare i dettagli del provider di identità SAML, come illustrato di seguito:

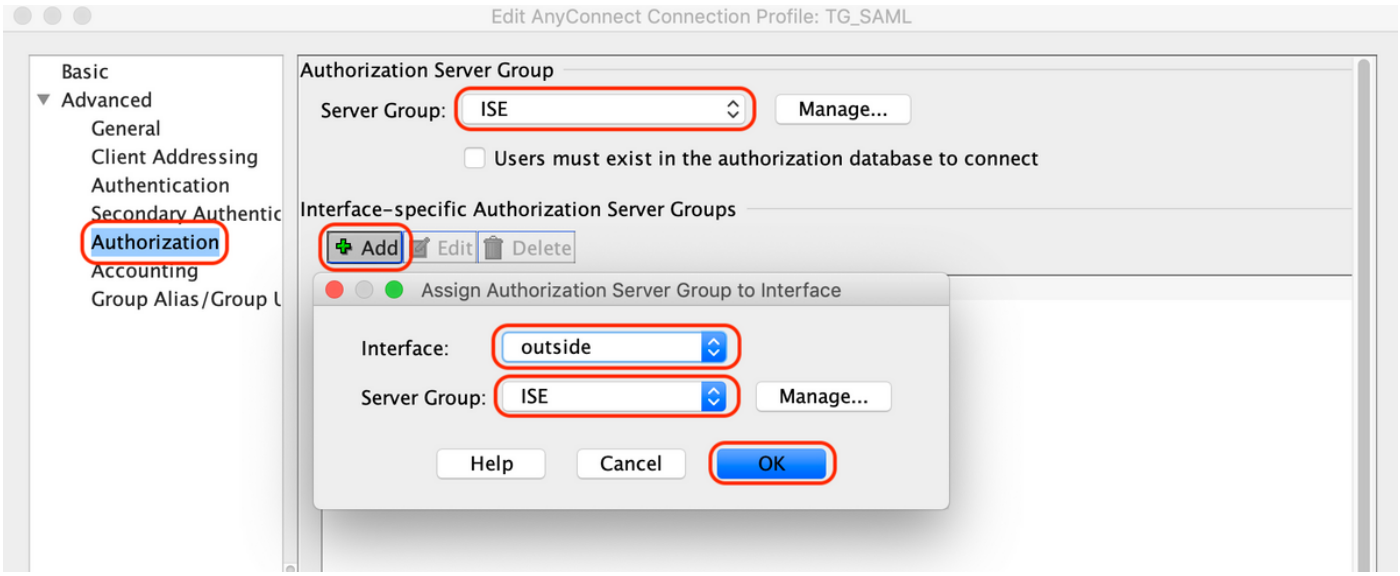
ID entità IDP	https://explorer.cisco.com/dag/saml2/idp/metadata.php
URL di accesso	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
URL di disconnessione	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://exp
URL di base	https://firebird.cisco.com

E. Fare clic su "Gestisci > Aggiungi"



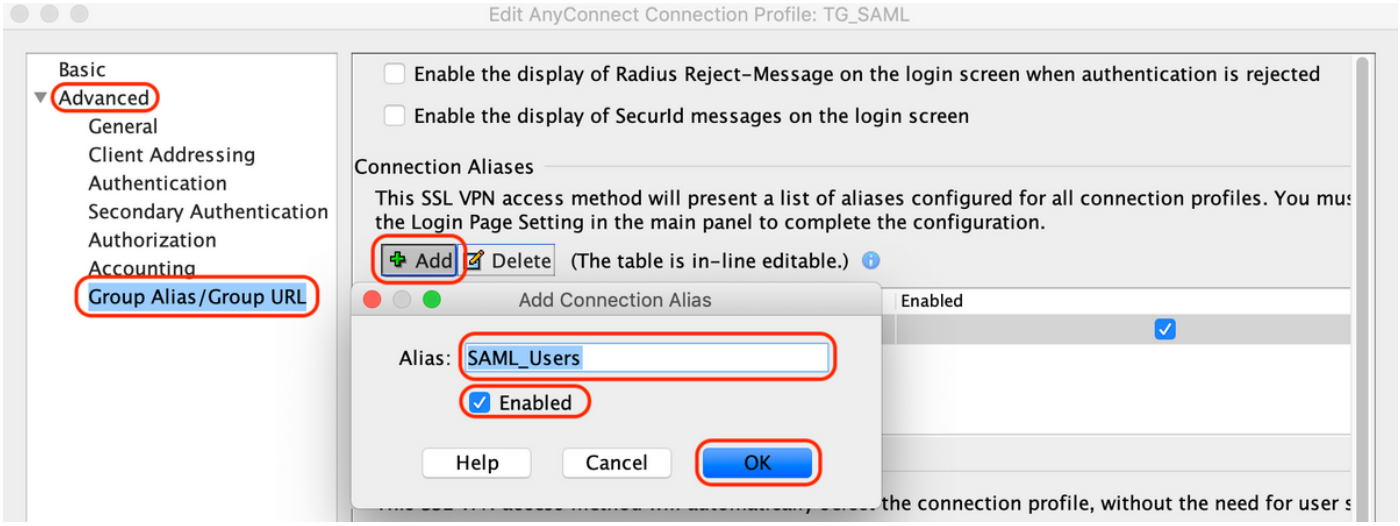
F. Nella sezione Avanzate del profilo di connessione, definire il server AAA per l'autorizzazione.

Selezionare "Avanzate > Autorizzazione" e fare clic su "Aggiungi".



G. In Alias gruppo definire l'alias della connessione.

Selezionare "Avanzate > URL gruppo/alias gruppo" e fare clic su "Aggiungi"



H. La configurazione dell'ASA è stata completata, come mostrato di seguito nell'interfaccia della riga di comando (CLI)

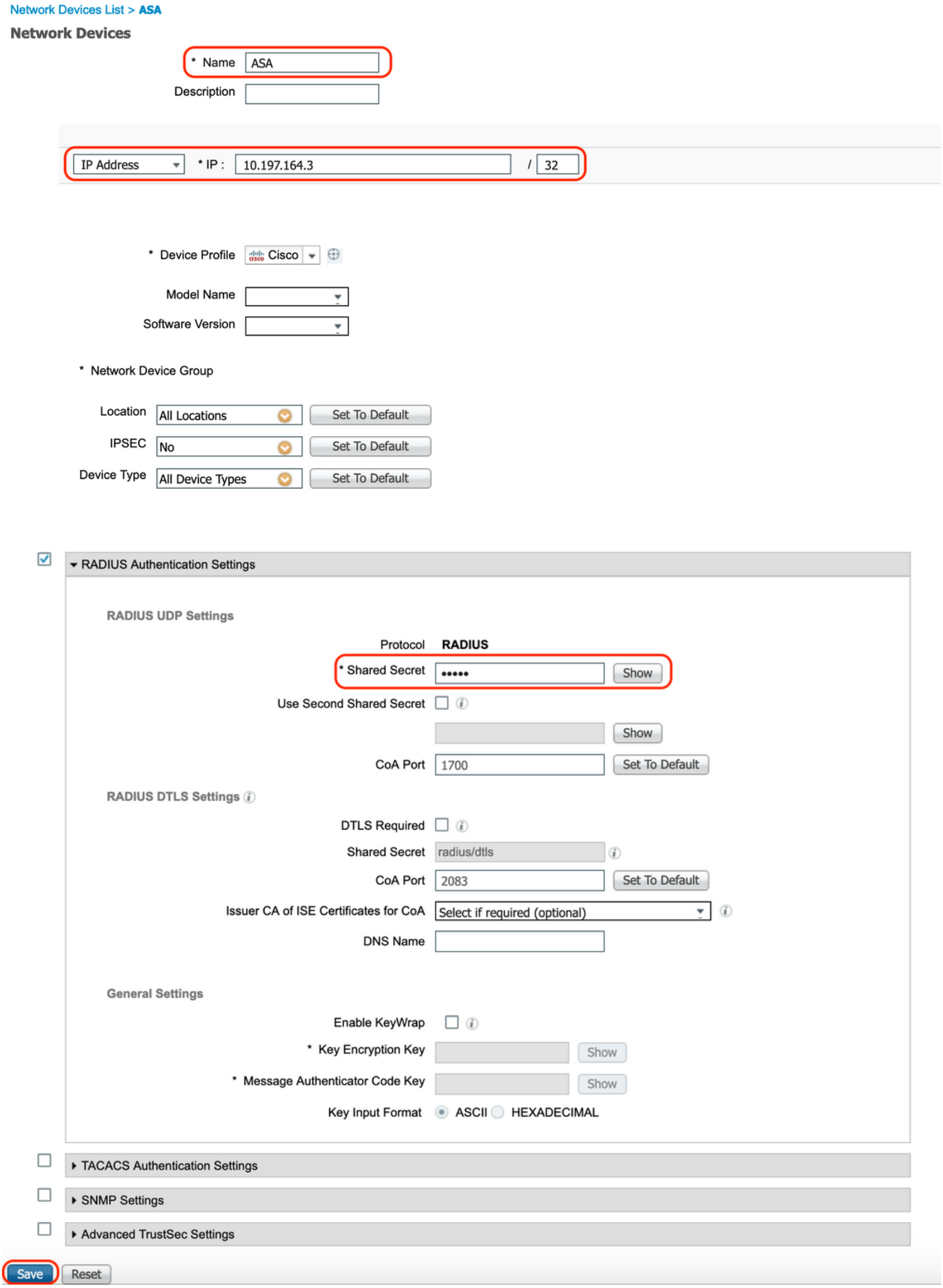
```
!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!--------------------Client pool configuration--------------------
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!--------------------Redirect Access-list-------------------------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

-Configurazione di ISE

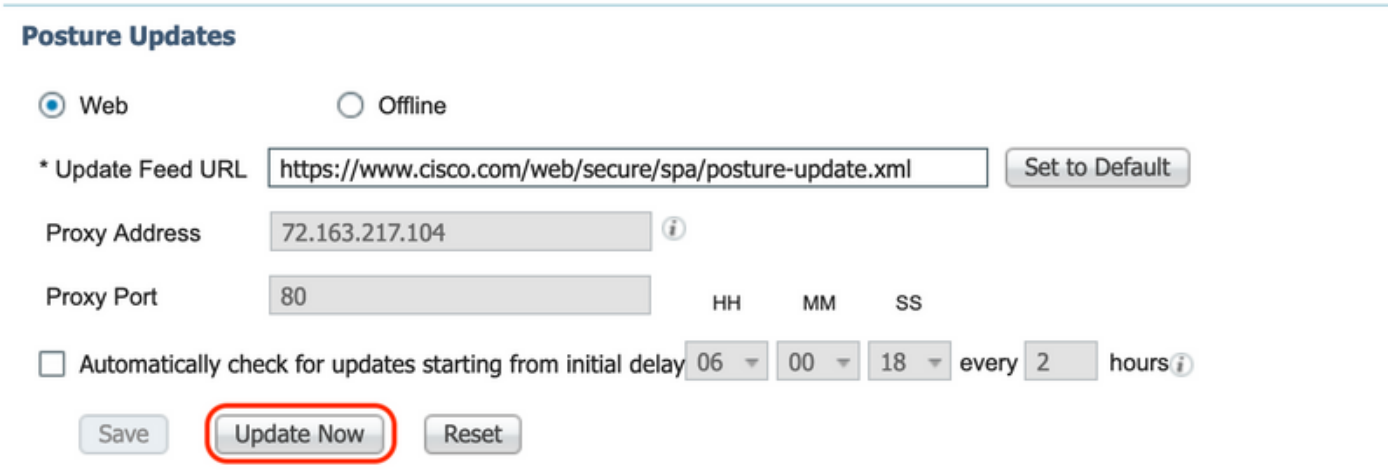
1. Aggiungere Cisco ASA come dispositivo di rete

In "Amministrazione > Risorse di rete > Dispositivi di rete", fare clic su "Aggiungi".
Configurare il nome del dispositivo di rete, l'indirizzo IP associato e in "Impostazioni autenticazione Radius" configurare "Segreto condiviso" e fare clic su "Salva"


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. Installare gli ultimi aggiornamenti della postura

Selezionare "Amministrazione > Sistema > Impostazioni > Postura > Aggiornamenti" e fare clic su "Aggiorna"



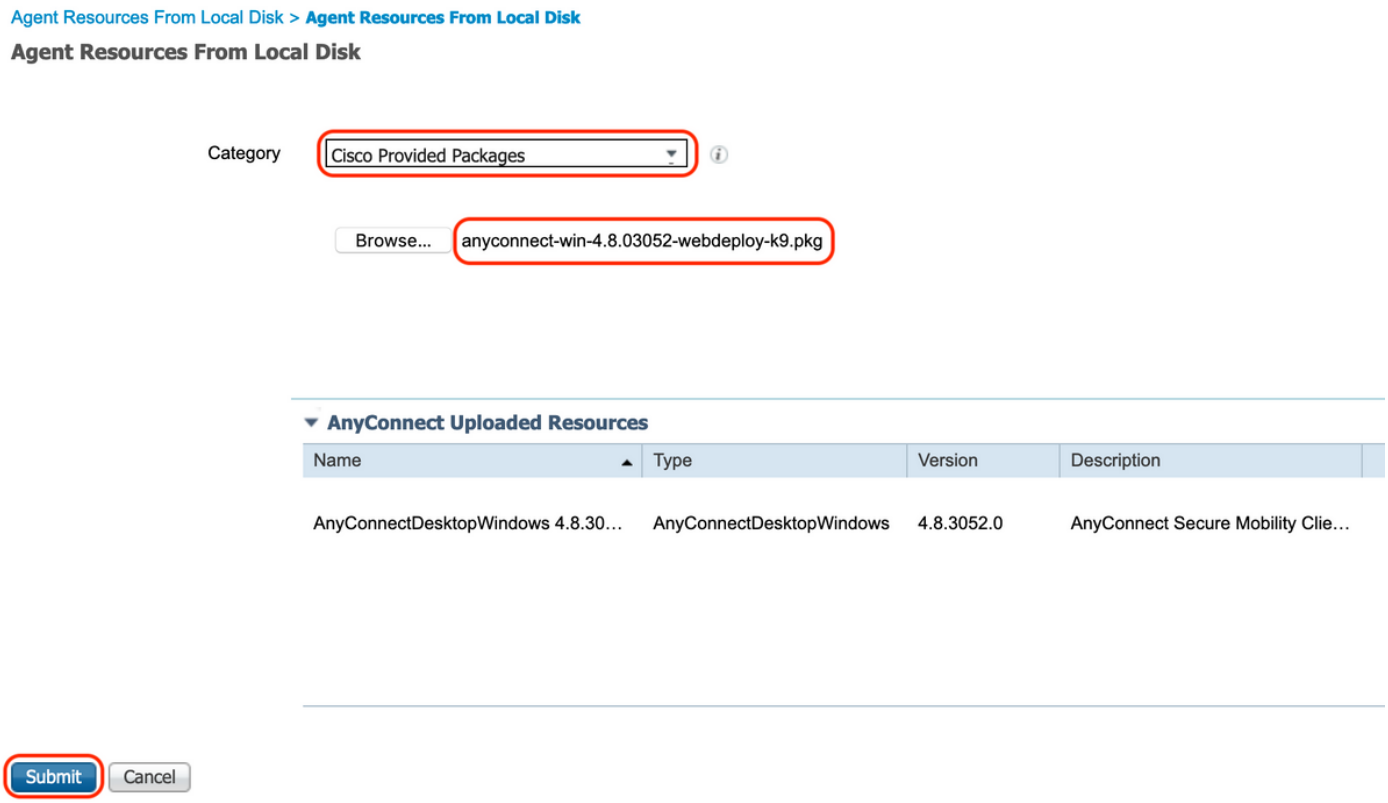
3. Caricare il modulo di conformità e il pacchetto di implementazione dell'headend AnyConnect su ISE

Passare a "Policy > Elementi criterio > Risultati > Provisioning client > Risorse". Fare clic su "Add" (Aggiungi) e selezionare "Agent resources from local disk" (Risorse agente da disco locale) o "Agent resources from Cisco site" (Risorse agente da sito Cisco) a seconda che i file debbano essere recuperati dalla workstation locale o dal sito Cisco.

In questo caso, per caricare i file dalla workstation locale in Categoria, selezionare "Cisco Provided Packages", fare clic su "Browse" (Sfoglia), selezionare i pacchetti richiesti e fare clic su "Submit" (Invia).

Questo documento utilizza "anyconnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg"

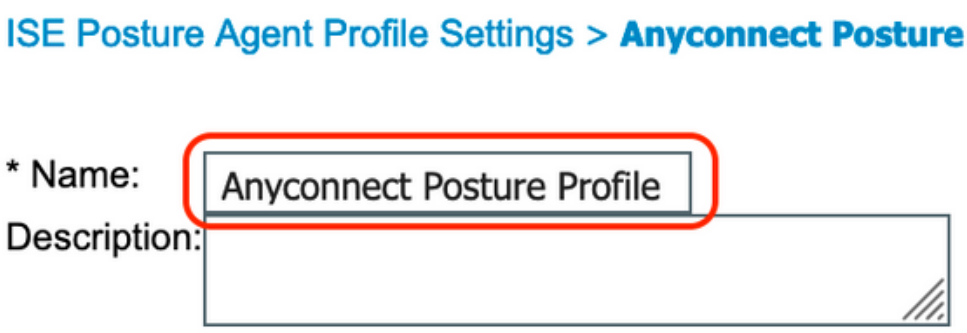
come modulo sulla conformità e "anyconnect-win-4.8.03052-webdeploy-k9.pkg" come pacchetto di distribuzione dell'headend AnyConnect.



4. Creazione di un profilo di postura di AnyConnect

A. Passare a "Policy > Elementi criteri > Risultati > Client Provisioning > Risorse". Fare clic su "Add" (Aggiungi) e selezionare "AnyConnect Posture Profile" (Profilo postura di AnyConnect)

B. Immettere il nome per il profilo di postura di Anyconnect e configurare il nome del server come "*" in Regole per il nome del server, quindi fare clic su "Salva"



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

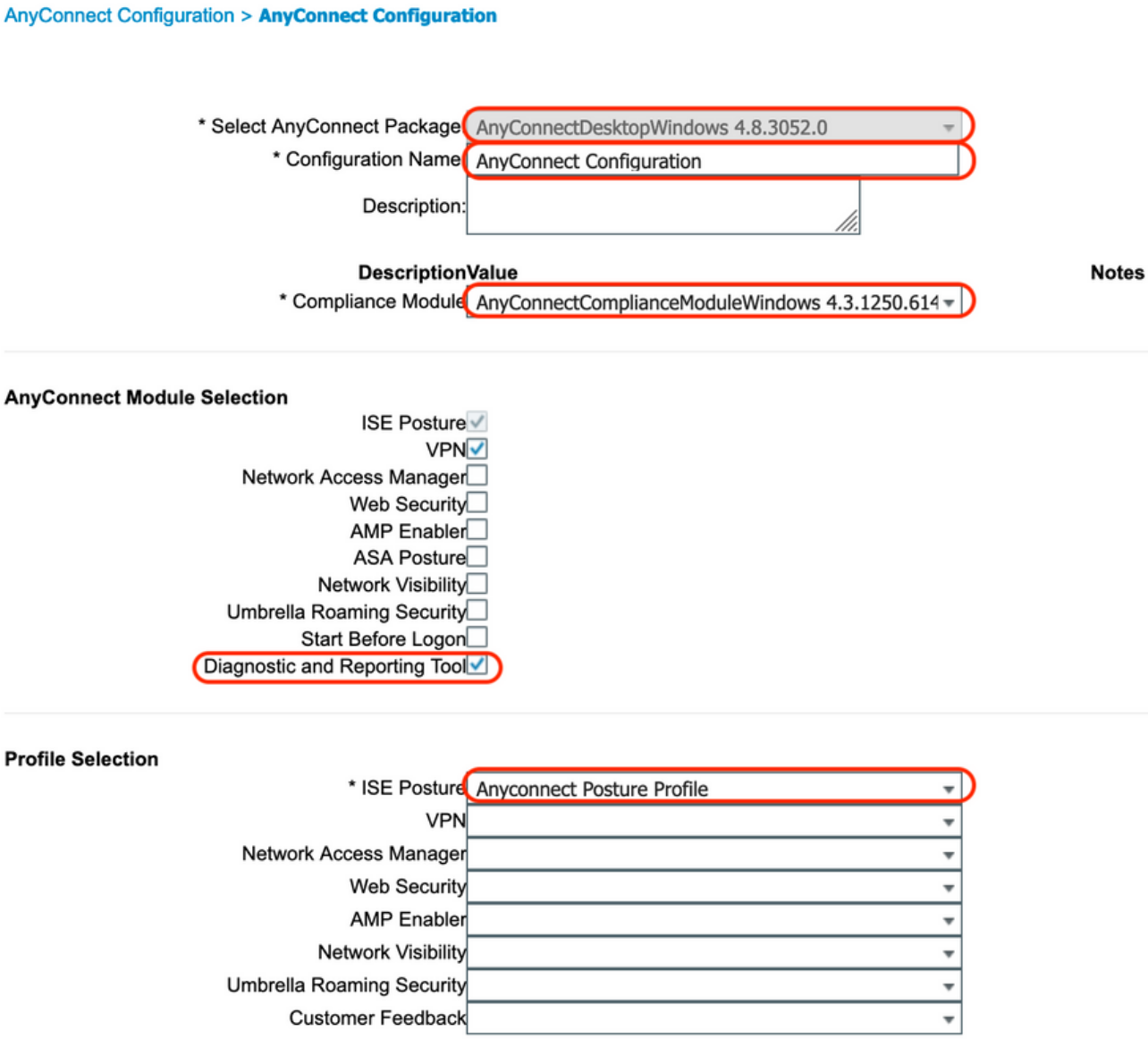
5. Creazione Della Configurazione Di Anyconnect

A. Passare a "Policy > Elementi criteri > Risultati > Client Provisioning > Risorse". Fare clic su "Add" (Aggiungi) e selezionare "AnyConnect Configuration"

B. Selezionare il pacchetto AnyConnect, immettere il nome della configurazione e selezionare il modulo di conformità richiesto

C. In "AnyConnect Module Selection", selezionare "Diagnostic and Reporting Tool"

D. In "Selezione profilo", selezionare Profilo postura e fare clic su "Salva"

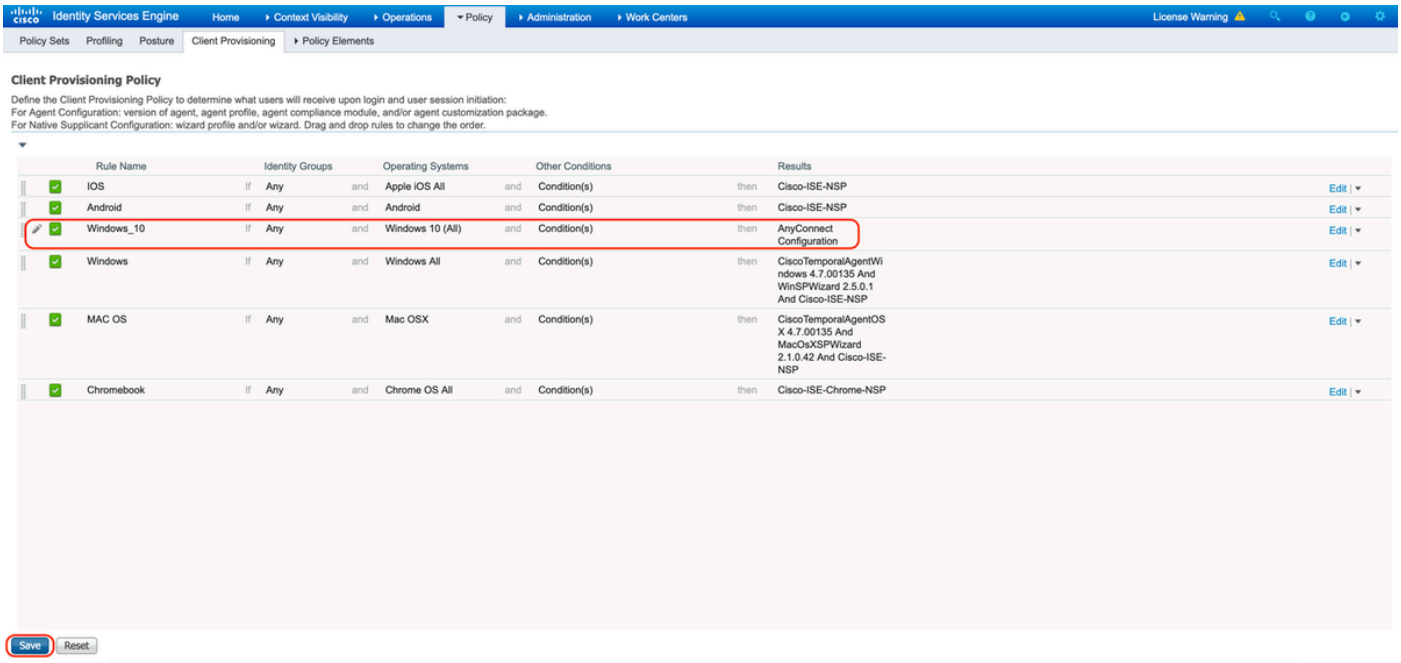


6. Creare criteri di provisioning client

A. Selezionare "Policy > Client Provisioning".

B. Fare clic su "Modifica", quindi selezionare "Inserisci regola"

C. Inserire il nome della regola, selezionare il sistema operativo richiesto, quindi in Risultati (in "Agente" > "Configurazione agente") selezionare "Configurazione AnyConnect" creata nel passaggio 5 e fare clic su "Salva"

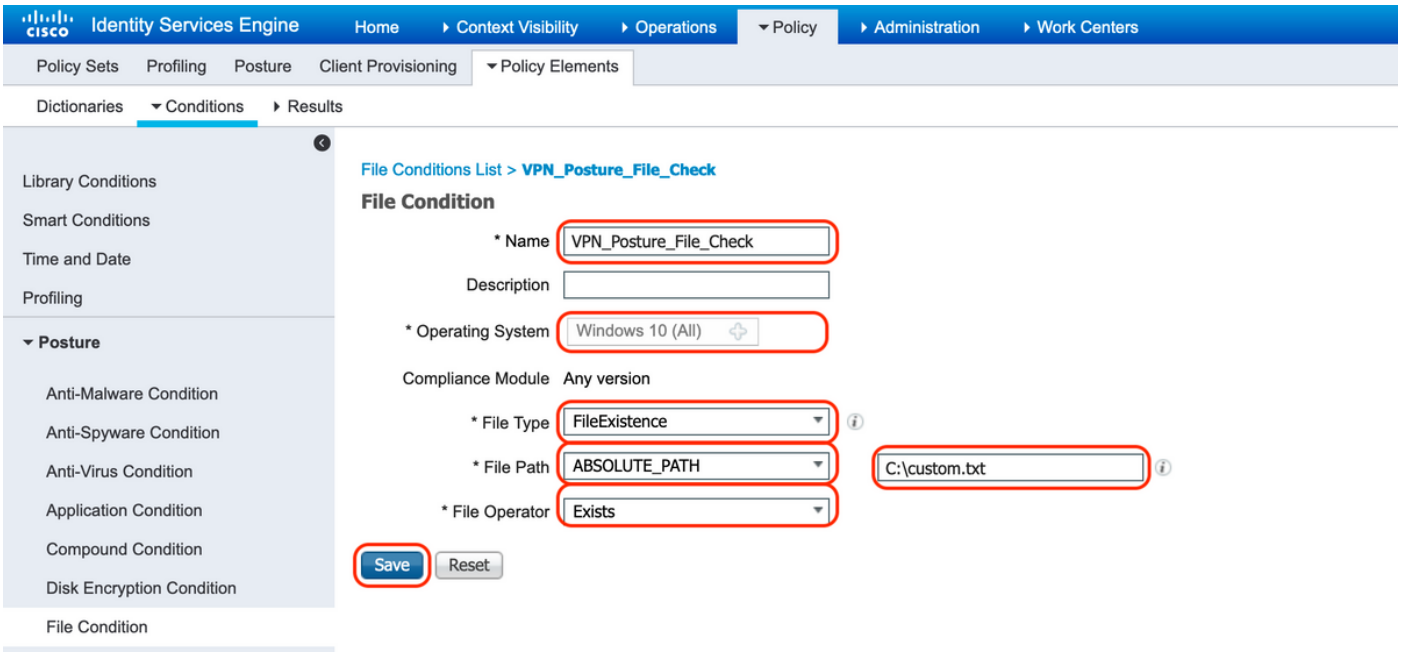


7. Creare una condizione di postura

A. Selezionare "Policy > Elementi criteri > Condizioni > Postura > Condizione file"

B. Fare clic su "Add" (Aggiungi) e configurare il nome della condizione "VPN_Posture_File_Check", il sistema operativo richiesto come "Windows 10(All)", il tipo di file come "FileExistence", il percorso di file come "ABSOLUTE_PATH" e il percorso completo e il nome di file come "C:\custom.txt", quindi selezionare File Operator come "Exists" (Esiste).

C. In questo esempio viene utilizzata la presenza di un file denominato "custom.txt" in unità C: come condizione del file



8. Crea azione di correzione della postura

Passare a "Policy > Elementi criteri > Risultati > Postura > Azioni di risoluzione" per creare l'azione di correzione file corrispondente. In questo documento viene utilizzato "Solo testo messaggio" come azioni di risoluzione configurate nel passaggio successivo.

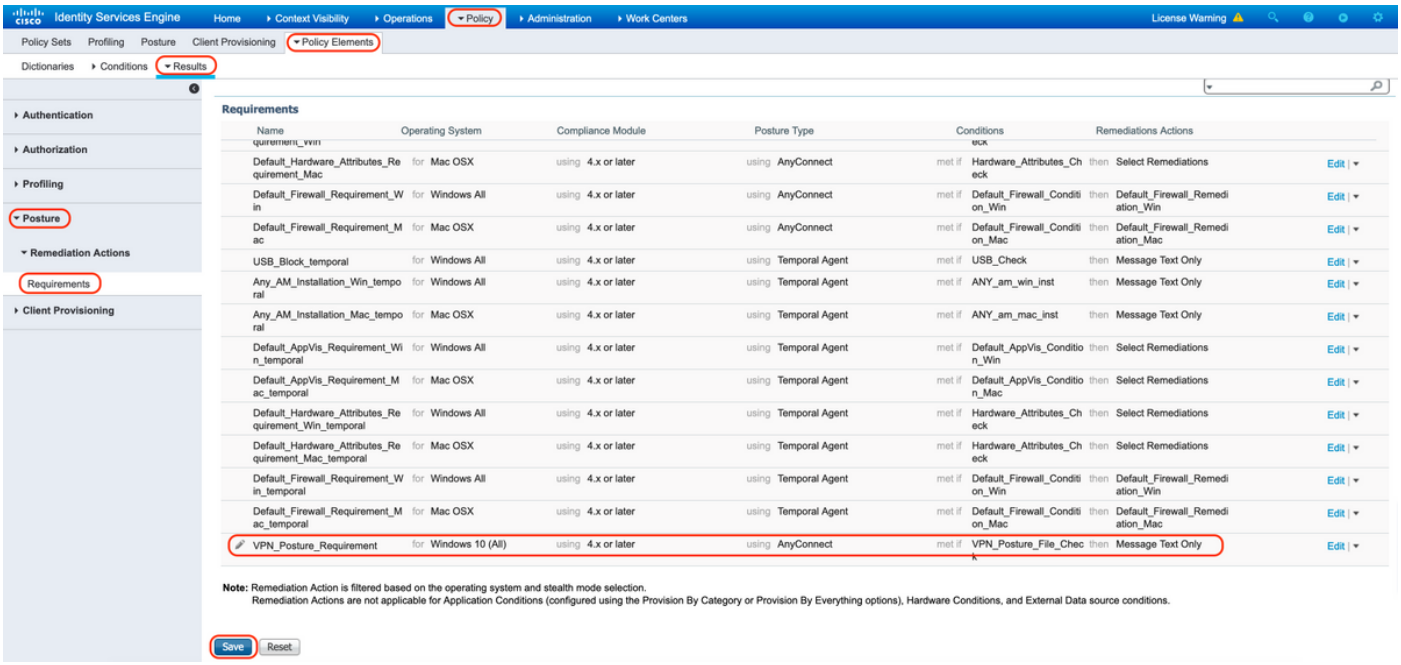
9. Crea regola fabbisogno postura

A. Passare a "Policy > Elementi criteri > Risultati > Postura > Requisiti"

B. Fare clic su "Modifica", quindi selezionare "Inserisci nuovo requisito"

C. Configurare il nome della condizione "VPN_Posture_Requirement", il sistema operativo richiesto "Windows 10(All)", il modulo di conformità "4.x o versioni successive", il tipo di postura "Anyconnect"

D. Condizioni come "VPN_Posture_File_Check" (create al passo 7) e in Azioni di risoluzione, selezionare Azione come "Solo testo messaggio" e immettere il messaggio personalizzato per l'utente agente

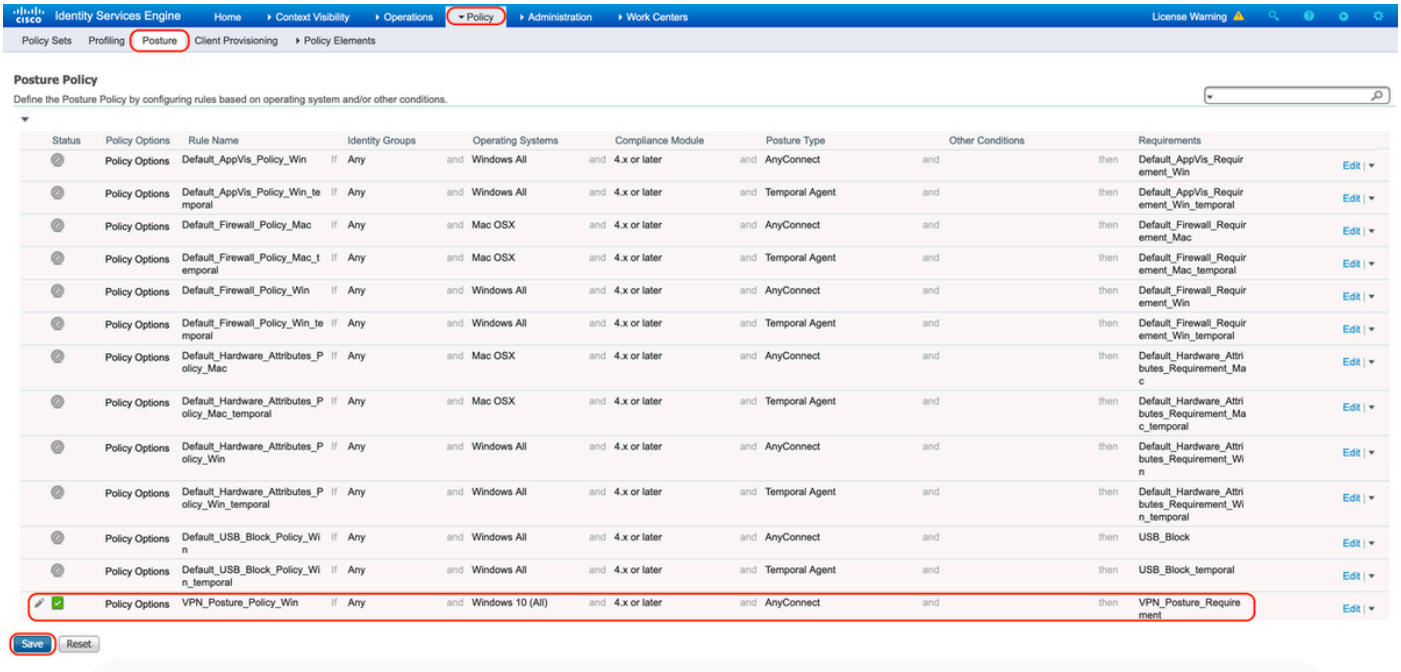


10. Creazione di un criterio di postura

A. Selezionare "Policies > Posture" (Criteri > Postura).

B. Configurare il nome della regola come "VPN_Posture_Policy_Win", il sistema operativo

richiesto come "Windows 10(All)", il modulo di conformità come "4.x o versioni successive", il tipo di postura come "Anyconnect" e i requisiti come "VPN_Posture_Requirement" come configurato nel passo 9

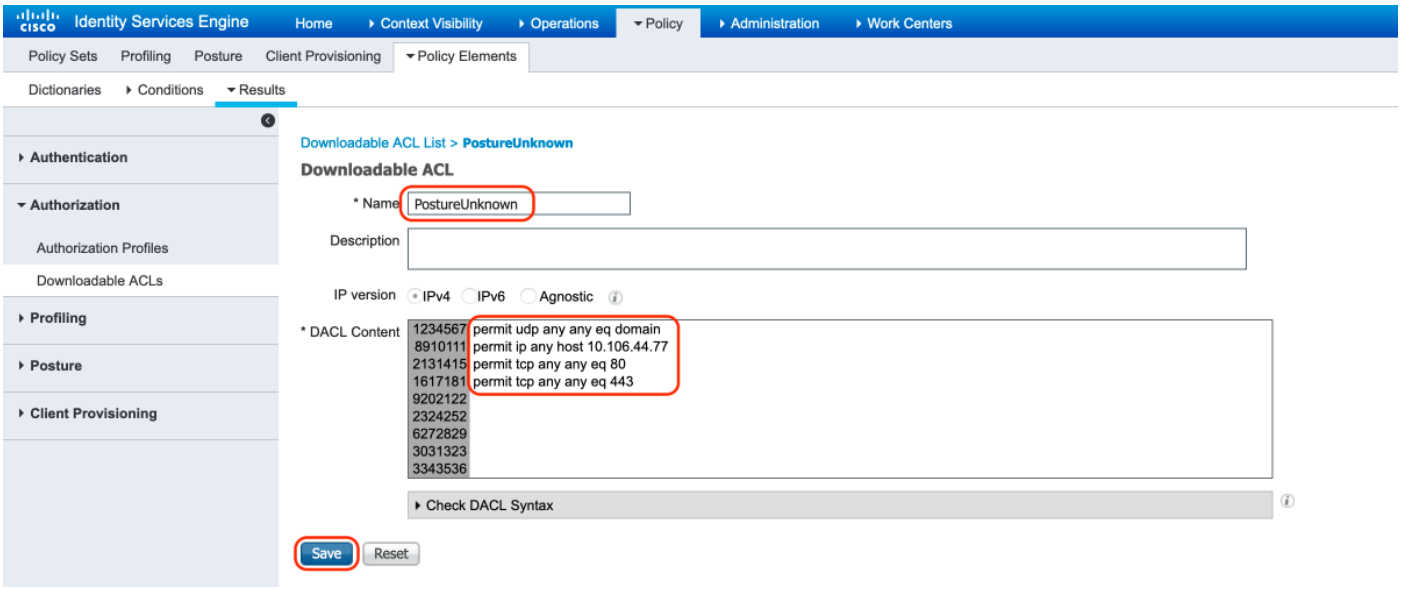


11. Creazione di ACL dinamici

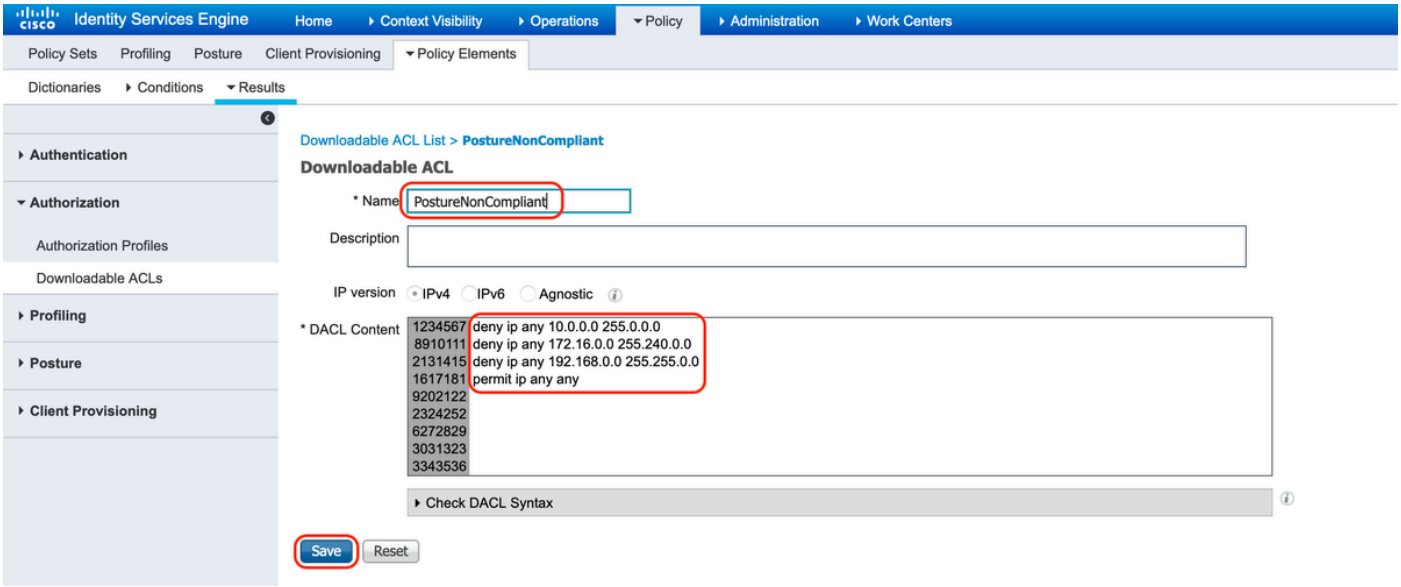
Selezionare "Policy > Policy Elements > Results > Authorization > Downlodable ACLS" (Policy > Elementi criteri > Risultati > Autorizzazione > ACL scaricabili) e creare gli ACL per diversi stati di postura.

In questo documento vengono utilizzati i seguenti DACL.

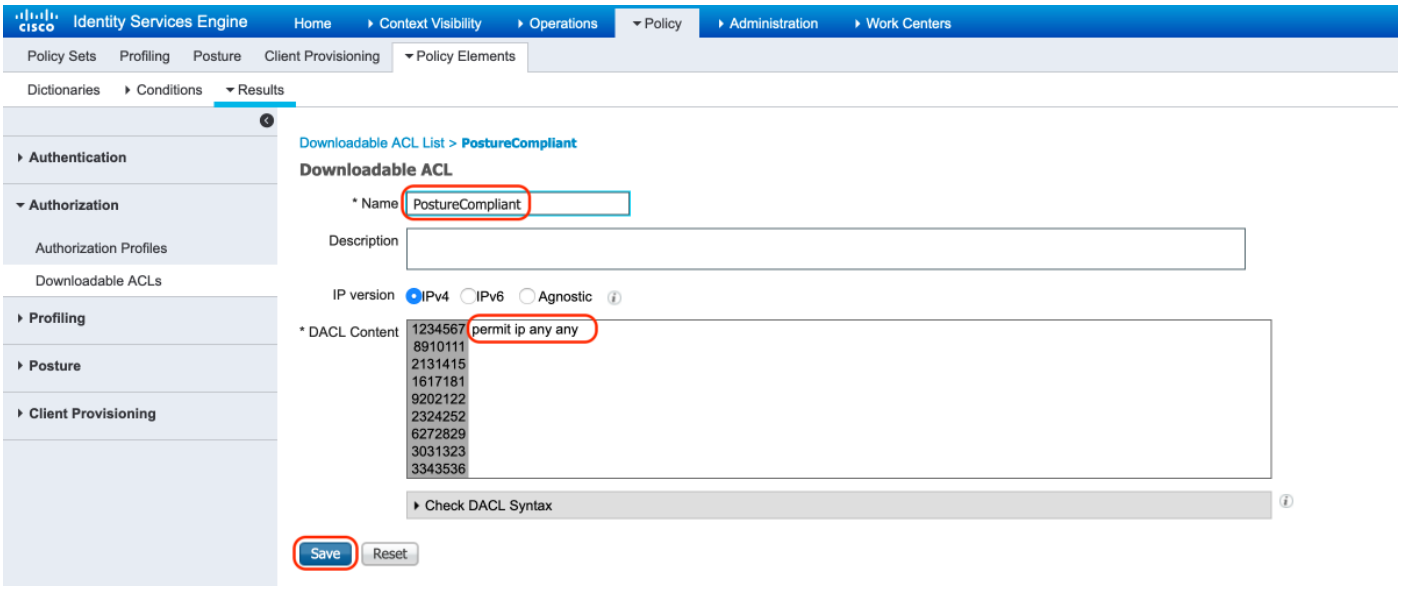
A. Postura sconosciuta: consente il traffico verso DNS, PSN, HTTP e HTTPS



B. Postura non conforme: nega l'accesso alle subnet private e consente solo il traffico Internet



C. Conforme alla postura: consente tutto il traffico per gli utenti finali conformi alla postura

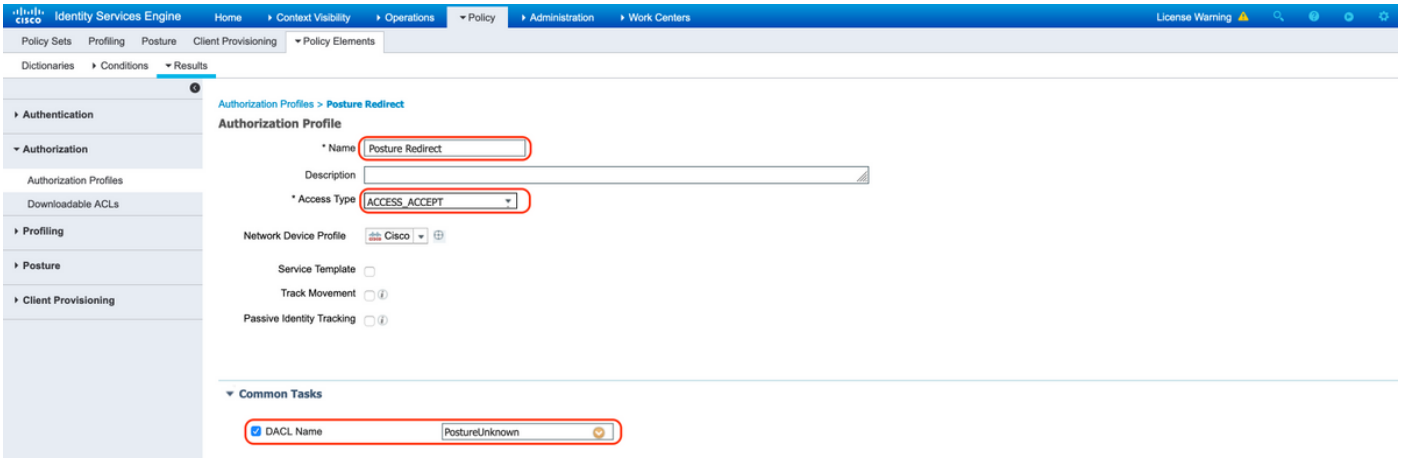


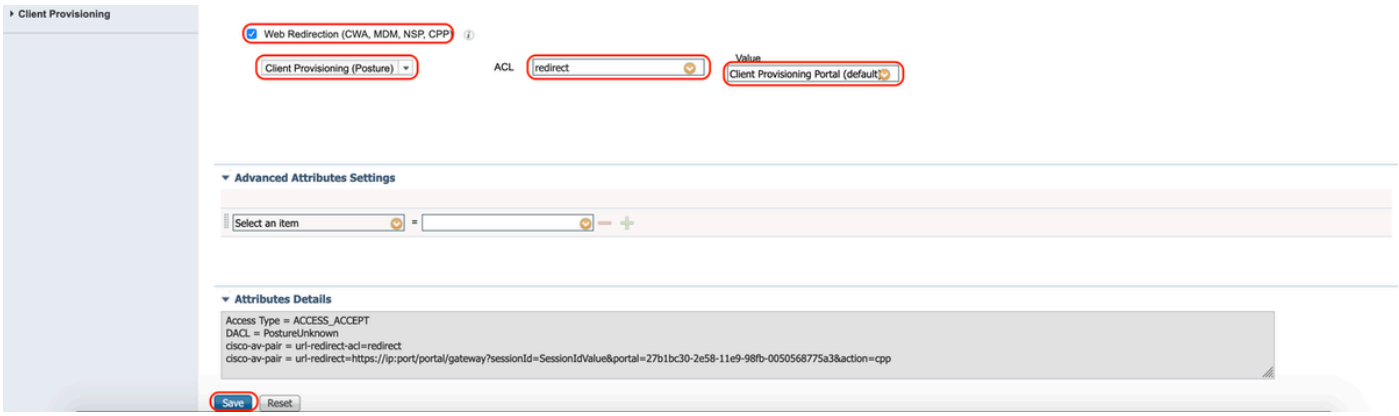
12. Creazione di profili di autorizzazione

Selezionare "Policy > Policy Elements > Results > Authorization > Authorization Profiles" (Criteri > Elementi criteri > Risultati > Autorizzazione > Profili autorizzazione).

A. Profilo di autorizzazione per la postura sconosciuta

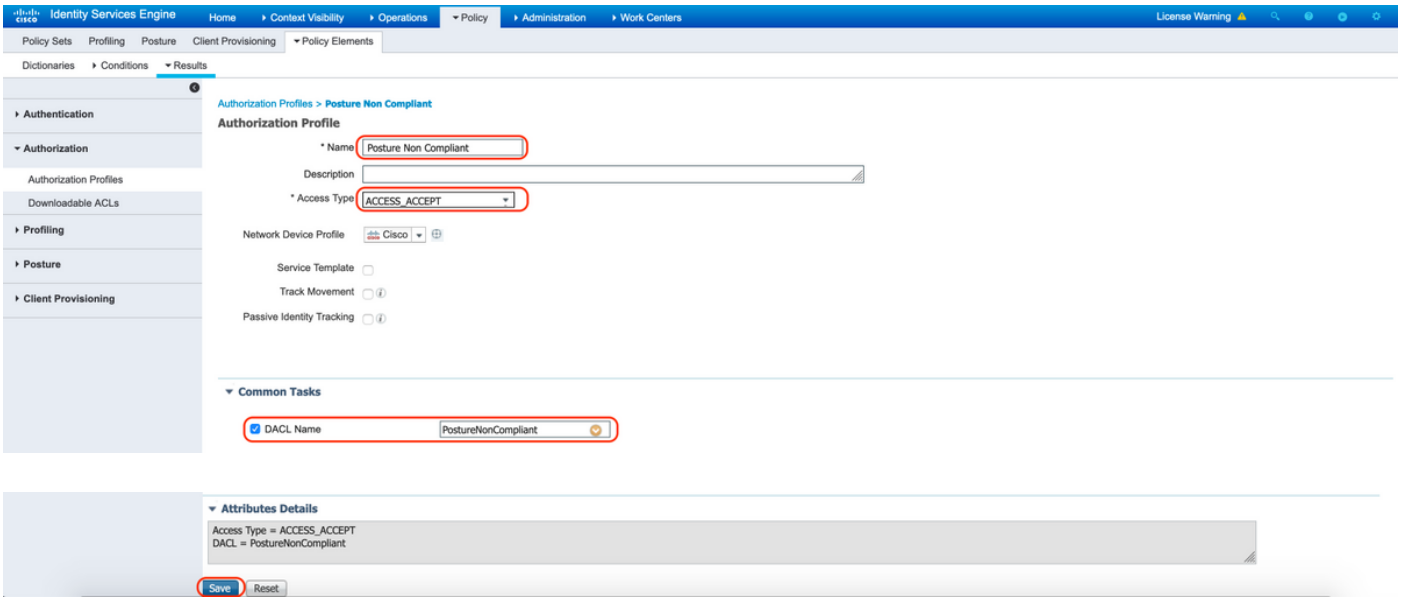
Selezionare DACL "PostureUnknown" (Postura sconosciuta), selezionare Web Redirection (Reindirizzamento Web), selezionare Client Provisioning (Postura) (Postura), configurare il nome ACL di reindirizzamento "redirect" (da configurare sull'appliance ASA) e selezionare il portale di provisioning client (predefinito)





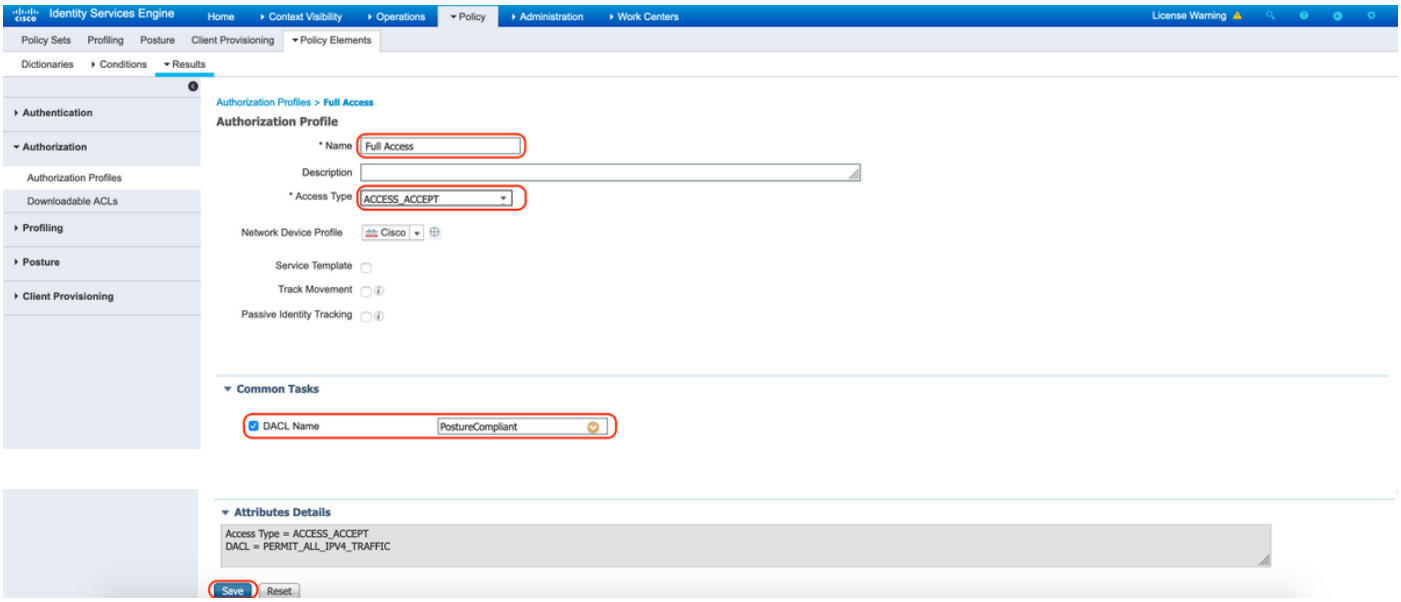
B. Profilo di autorizzazione per la postura non conforme

Selezionare DACL "PostureNonCompliant" per limitare l'accesso alla rete



C. Profilo di autorizzazione per la conformità alla postura

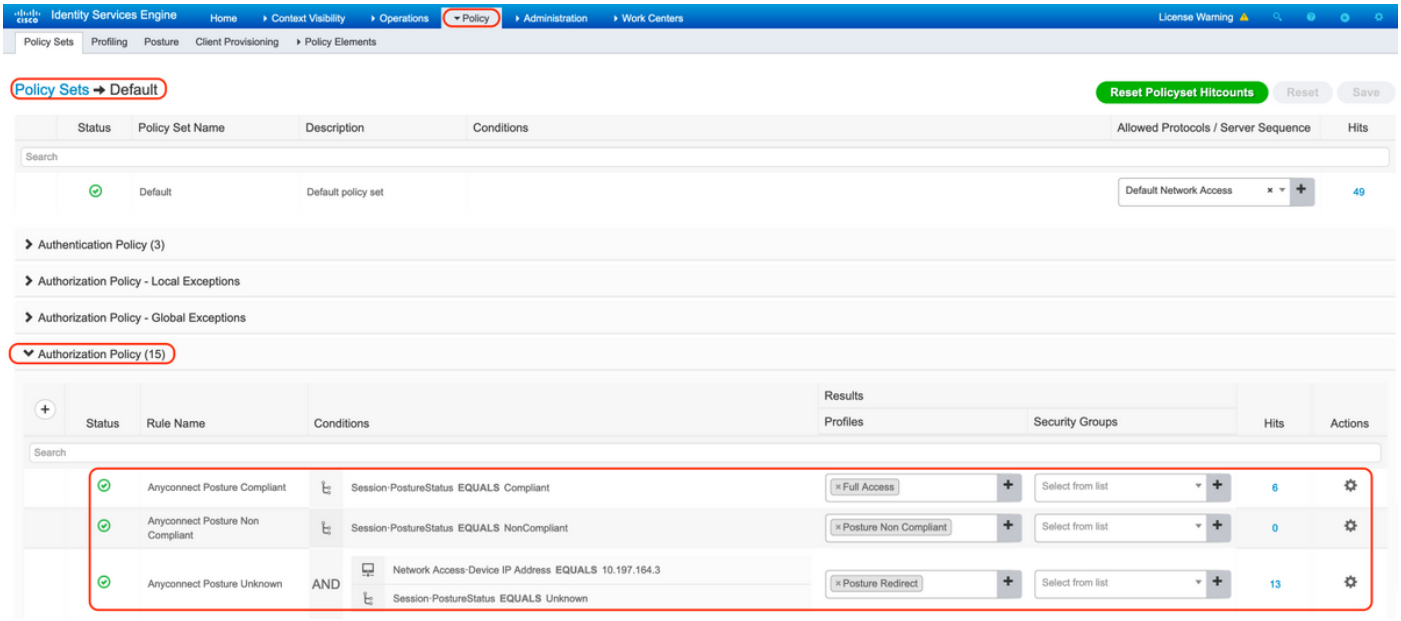
Selezionare DACL "PostureCompliant" per consentire accesso completo alla rete



12. Configurare i criteri di autorizzazione

Utilizzare i profili di autorizzazione configurati nel passaggio precedente per configurare 3 criteri di autorizzazione per Postura conforme, Postura non conforme e Postura sconosciuta.

La condizione comune "Sessione: Stato postura" viene utilizzata per determinare i risultati per ogni criterio



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per verificare se l'autenticazione dell'utente è riuscita, eseguire il comando seguente sull'appliance 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
```

Una volta completata la valutazione della postura, l'accesso utente viene modificato in accesso completo, come osservato nell'elenco DACL premuto nel campo "Nome 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 :
```

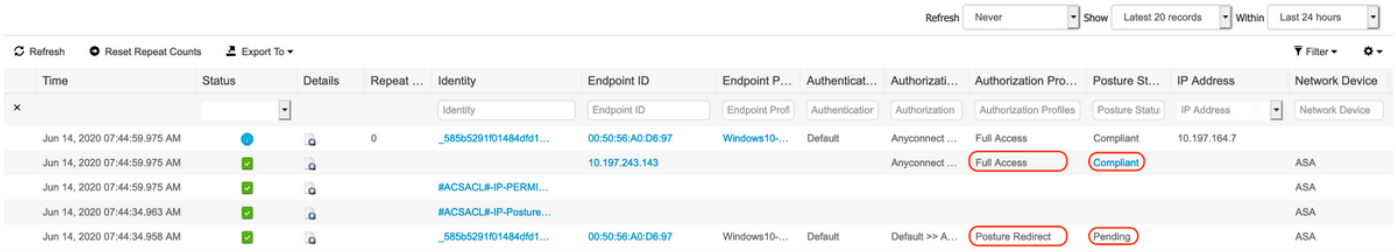
TG_SAML

```
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

Per verificare se l'autorizzazione è stata eseguita correttamente su ISE, selezionare "Operations > RADIUS > Live Logs" (Operazioni > RADIUS > Live Log).

In questa sezione sono riportate le informazioni pertinenti associate all'utente autorizzato, ad esempio identità, profilo di autorizzazione, criteri di autorizzazione e stato della postura.

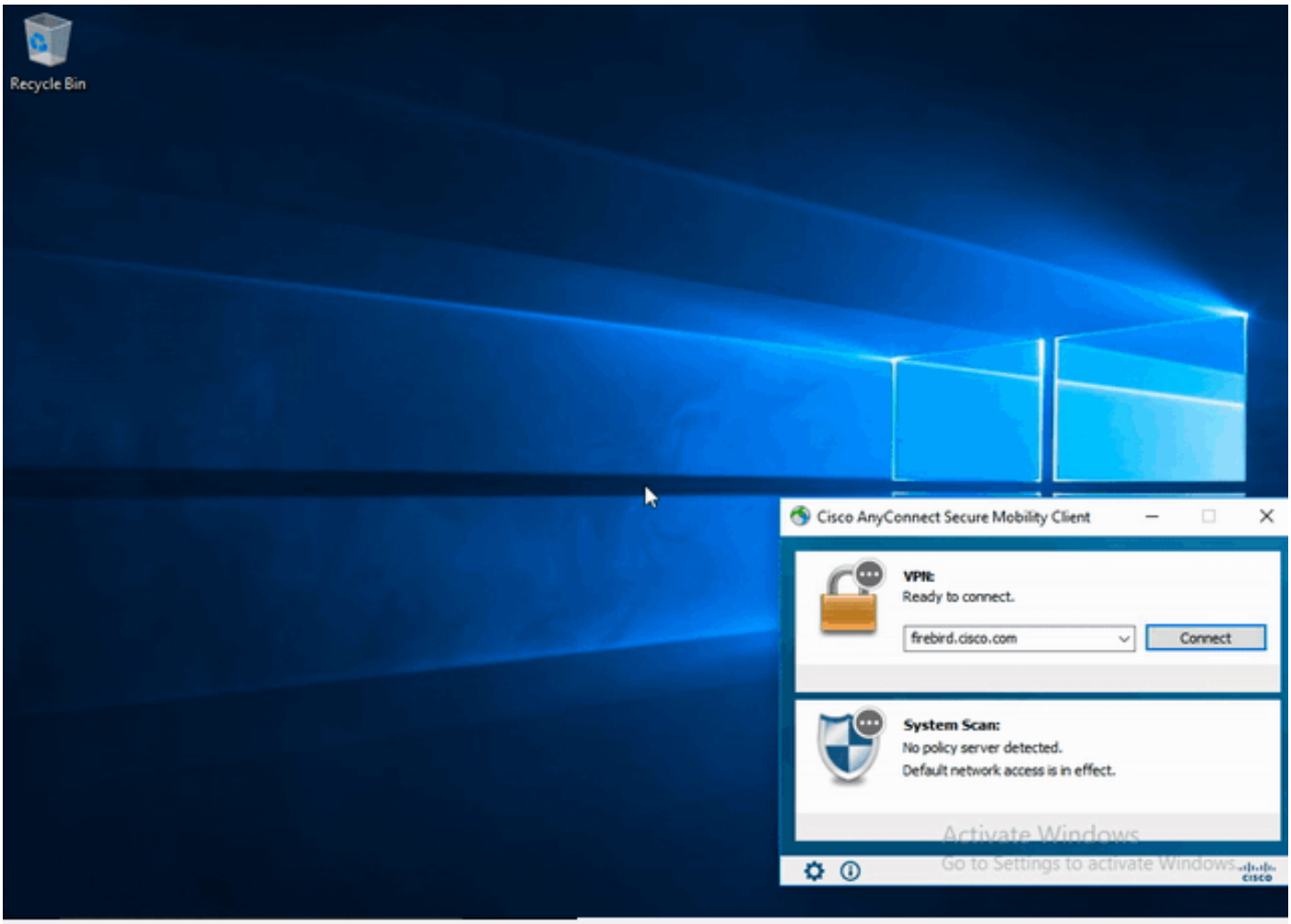


Nota: per la convalida della postura aggiuntiva su ISE, fare riferimento alla seguente documentazione: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc7

Per verificare lo stato di autenticazione sul portale di amministrazione Duo, fare clic su "Report" sul lato sinistro del pannello di amministrazione che mostra il log di autenticazione. Ulteriori informazioni: https://duo.com/docs/administration#reports

Per visualizzare la registrazione di debug per Duo Access Gateway, utilizzare il collegamento seguente: https://help.duo.com/s/article/1623?language=en_US

Esperienza utente



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

Attenzione: sull'appliance ASA, è possibile impostare vari livelli di debug; per impostazione predefinita, viene usato il livello 1. Se si modifica il livello di debug, il livello di dettaglio dei debug potrebbe aumentare. Procedere con cautela, soprattutto negli ambienti di produzione.

La maggior parte delle procedure di risoluzione dei problemi SAML implica una configurazione

errata che può essere rilevata verificando la configurazione SAML o eseguendo i debug.

è possibile usare il comando "debug webvpn saml 255" per risolvere la maggior parte dei problemi, ma negli scenari in cui il debug non fornisce informazioni utili, è possibile eseguire altri debug:

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

Per risolvere i problemi di autenticazione e autorizzazione sull'appliance ASA, usare i seguenti comandi di debug:

```
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)
```

Nota: per un flusso di postura dettagliato e la risoluzione dei problemi con AnyConnect e ISE, fare riferimento al seguente collegamento:
Confronto tra gli stili di postura ISE per le applicazioni pre e post 2.2

Per interpretare e risolvere i problemi relativi ai registri di debug di Duo Access Gateway https://help.duo.com/s/article/5016?language=en_US

Informazioni correlate

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).