

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Flusso traffico](#)

[Configurazioni](#)

[- Configurazione del portale di amministrazione Duo](#)

[- Configurazione Duo Access Gateway \(DAG\)](#)

[- Configurazione ASA](#)

[- Configurazione di ISE](#)

[Verifica](#)

[Esperienza utente](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

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:

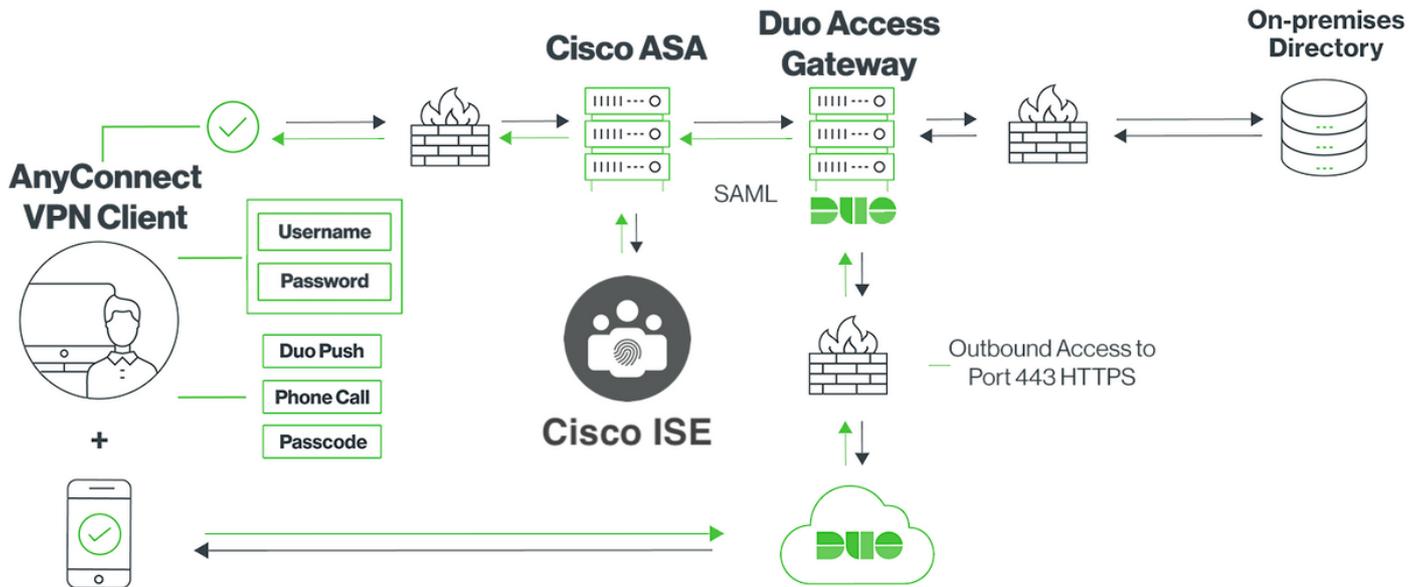
- Software Cisco Adaptive Security Appliance versione 9.12(3)12
- Duo Access Gateway
- Duo Security
- Cisco Identity Services Engine versione 2.6 e successive
- Microsoft Windows 10 con AnyConnect versione 4.8.03052

 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.

admin-77d04ebc.duosecurity.com/applications/protect/types

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 ciscoduobl

Dashboard > Applications > Protect an Application

Protect an Application

ASA

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

2. 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

Device Insight

Policies

Applications

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Administrators

Reports

Settings

Billing

Need Help?

Chat with Tech Support

Email Support

Call us at 1-855-386-2884

Account ID

2010-1403-48

Deployment ID

DU057

Helpful Links

Documentation

Cisco ASA - Duo Access Gateway

Authentication Log | Remove Application

Reset Secret Key

Configure Cisco ASA

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

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

Service Provider

Base URL

Enter the Cisco ASA Base URL.

Tunnel Group

Enter the Tunnel Group you are protecting with SSO.

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

Mail attribute

The attribute containing the email address of the user.

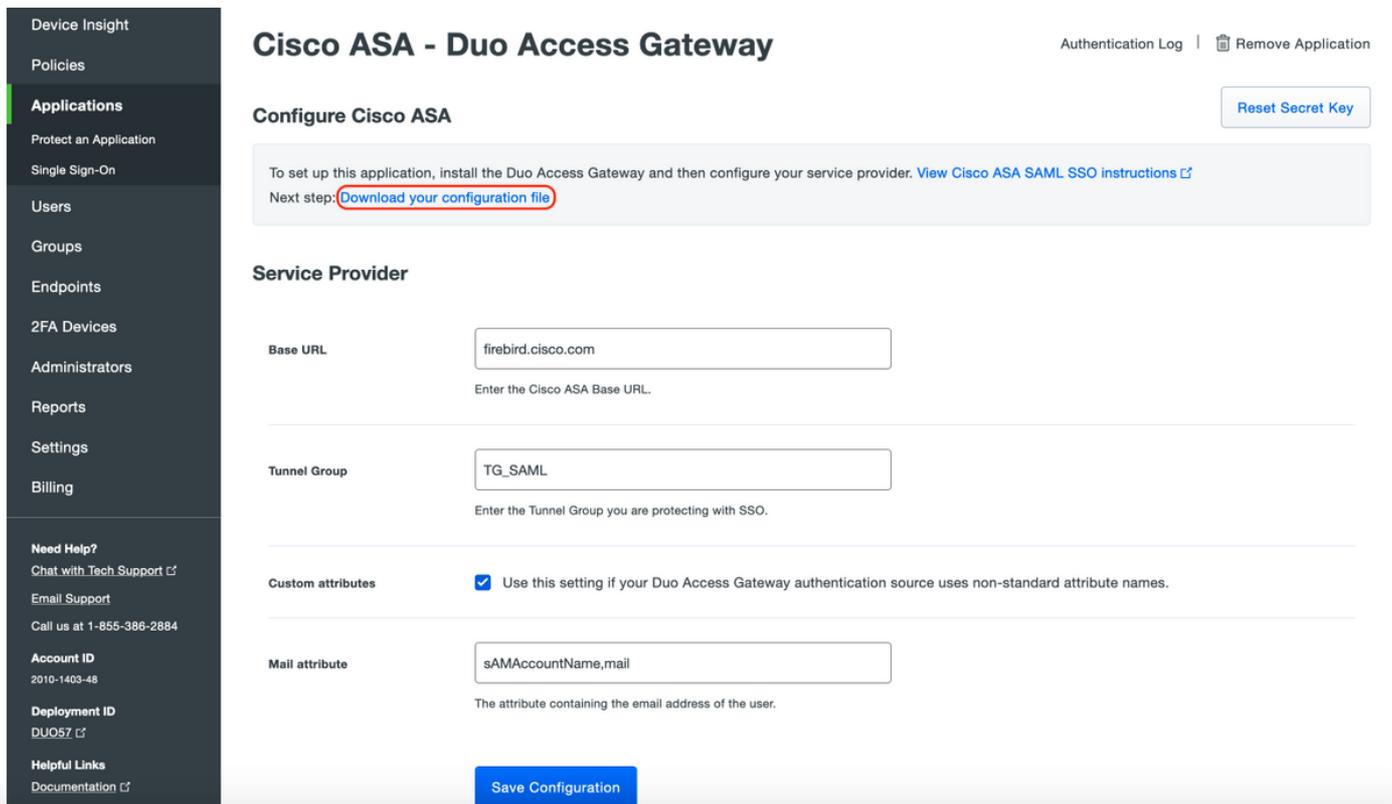
[Save Configuration](#)

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

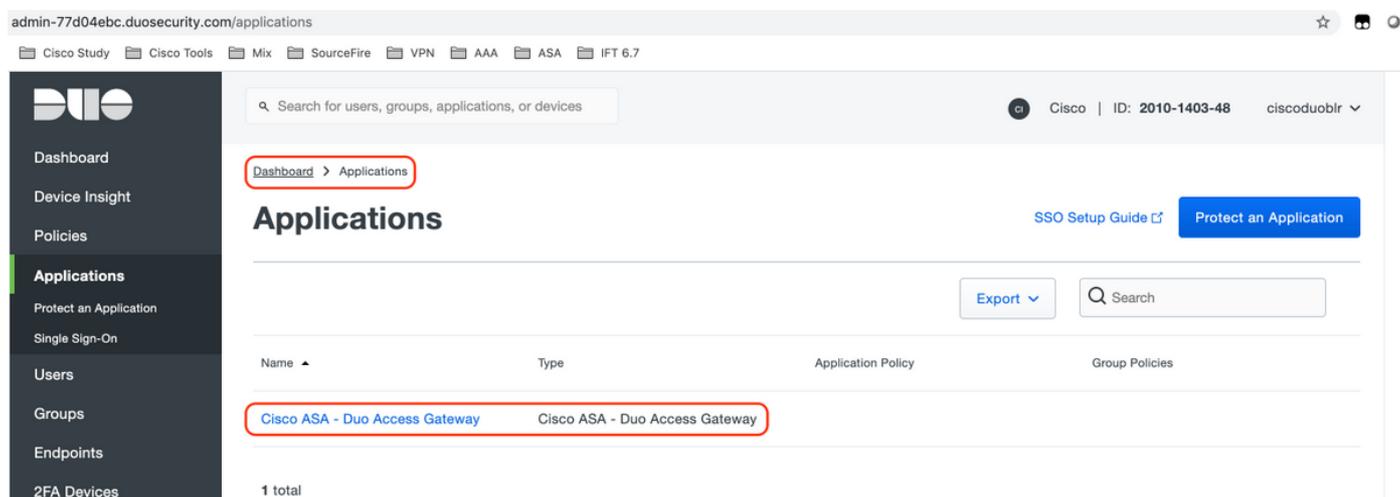
impostarli in base ai requisiti del cliente.

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

The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with navigation options: Dashboard, Device Insight, Policies, Applications, Users (highlighted), Add User (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, Groups, and Endpoints. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > Add User. The main heading is "Add User". A sub-heading "Adding Users" is followed by the text "Most applications allow users to enroll themselves after they complete primary authentication." and a link "Learn more about adding users". Below this is a form field for "Username" containing the text "duouser". A note below the field says "Should match the primary authentication username." At the bottom of the form is a blue "Add User" button.

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

The screenshot shows the Duo Admin console interface for adding a phone. The sidebar is the same as in the previous image. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > duouser > Add Phone. The main heading is "Add Phone". Below the heading is a link "Learn more about Activating Duo Mobile". Below this is a form for "Type" with two radio buttons: "Phone" (selected) and "Tablet". Below that is a form field for "Phone number" containing the text "+91 9xxx-xxx-xxx". To the right of the field is a link "Show extension field". Below the field is a note "Optional. Example: "+91 91234 56789"". At the bottom of the form is a blue "Add Phone" button.

Attiva "Duo Mobile" per l'utente specifico

Device Info

[Learn more about Activating Duo Mobile](#)



Not using Duo Mobile

[Activate Duo Mobile](#)



Model
Unknown



OS
Generic Smartphone



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:

The screenshot shows the Cisco Duo Mobile activation interface. On the left is a dark sidebar with navigation options: Dashboard, Device Insight, Policies, Applications, Users, Groups, Endpoints, 2FA Devices (highlighted), Phones, Hardware Tokens, WebAuthn & U2F, Administrators, Reports, and Settings. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below the search bar is a breadcrumb trail: "Dashboard > Phone: [redacted] > Activate Duo Mobile". The main heading is "Activate Duo Mobile". Below the heading is a paragraph: "This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push." A note follows: "Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code." Below the note are two fields: "Phone" with a red redaction box, and "Expiration" with a dropdown menu set to "24" and "hours" selected, followed by the text "after generation". At the bottom of the form is a blue button with the text "Generate Duo Mobile Activation Code".

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

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

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

Activate Duo Mobile

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

Phone [REDACTED]

Installation instructions

Send installation instructions via SMS

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

Activation instructions

Send activation instructions via SMS

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

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

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

The screenshot shows the Cisco Duo Admin Center interface. On the left is a dark sidebar with navigation options: Dashboard, Device Insight, Policies, Applications, Users, Groups, Endpoints, 2FA Devices (highlighted), Phones, Hardware Tokens, WebAuthn & U2F, Administrators, Reports, Settings, Billing, and Need Help? (Chat with Tech Support). The main content area has a search bar at the top. Below it is a green notification bar: "Duo Mobile instructions SMS'ed to +91 [redacted]". A breadcrumb trail reads "Dashboard > Phones > Phone: +91 [redacted]". The phone number "+91 [redacted]" is displayed prominently. A "Send SMS Passcodes..." link is visible. A "Shared phone" section states "This phone is attached to multiple users." Below this, two users are listed: "duouser" and "testing 123", both with phone numbers starting with "+91 [redacted]". An "Attach a user" link is present. A note says "Authentication devices can share multiple users". The "Device Info" section includes a link to "Learn more about Activating Duo Mobile". It shows the Duo logo, "Using Duo Mobile" with a "Reactivate Duo Mobile" link, a "Model" of "Unknown" with a phone icon, and an "OS" of "Generic Smartphone" with a question mark icon.

- 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"

Configure Sources

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

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

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

Set Active Source

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

Source type

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

Applications

Add Application

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

Configuration file

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

Applications

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

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

Metadata Recreate Certificate

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

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

Expiration: 2030-04-30 18:57:14

SHA-1 Fingerprint: [REDACTED]

SHA-256 Fingerprint: [REDACTED]

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

- Configurazione ASA

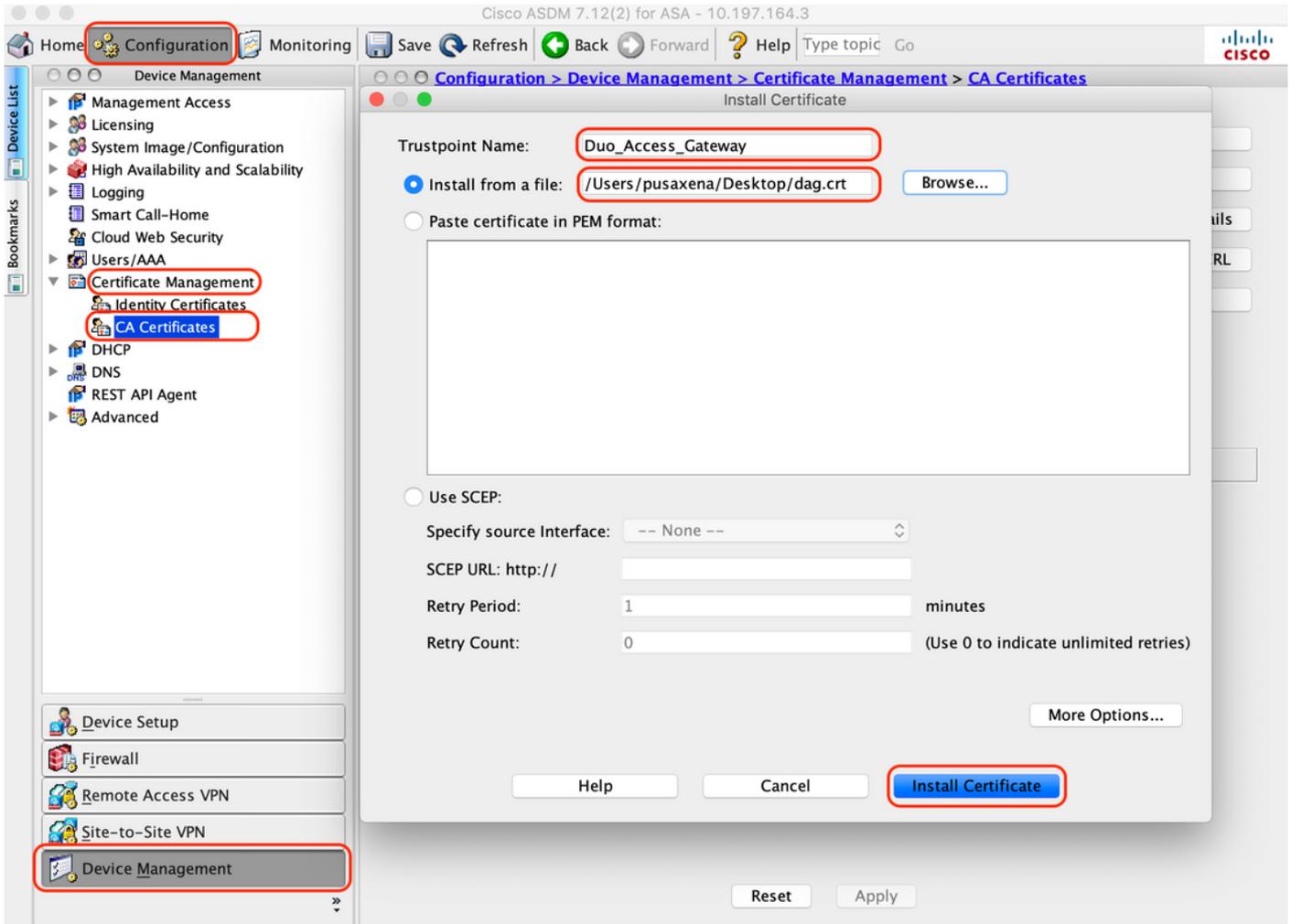
In questa sezione vengono fornite le informazioni per configurare l'ASA per l'autenticazione IDP SAML e la configurazione base di AnyConnect. Nel documento vengono illustrati i passaggi della configurazione ASDM e la configurazione di esecuzione CLI per una panoramica.

1. Carica certificato Duo Access Gateway

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

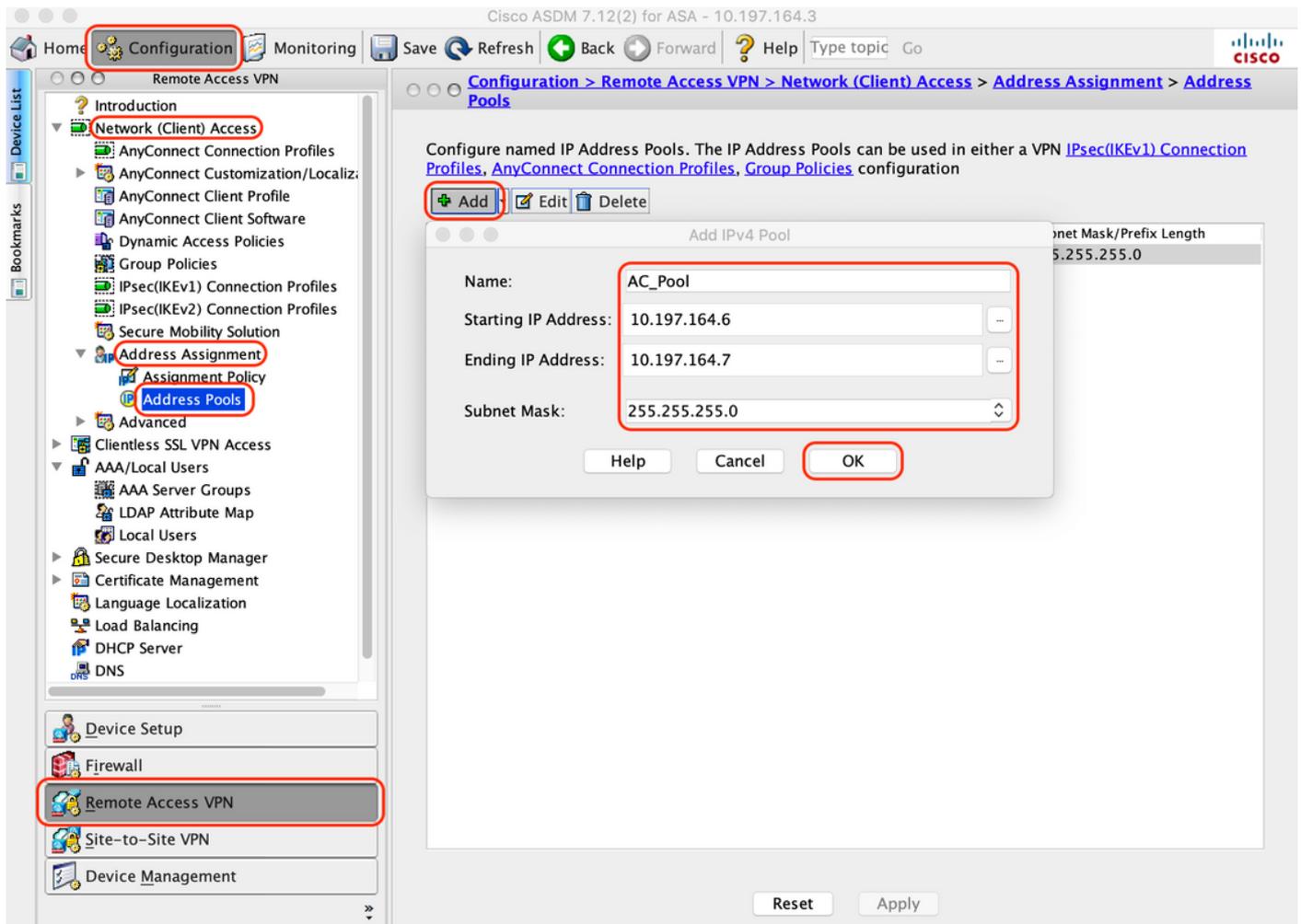
B. Nella pagina "Installa certificato", configurare il nome del punto di accesso:
Duo_Access_Gateway

C. Fare clic su "Sfogliare" 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).

Home Configuration Monitoring Save Refresh Back Forward Help Type topic Go

Remote Access VPN

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

AAA Server Groups

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

Add AAA Server Group

AAA Server Group: ISE

Protocol: RADIUS

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

Enable interim accounting update

Update Interval: 24 Hours

Enable Active Directory Agent mode

ISE Policy Enforcement

Enable dynamic authorization

Dynamic Authorization Port: 1700

Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

Help Cancel OK

Find: Match Case

LDAP Attribute Map

Reset Apply

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

Cisco ASDM 7.12(2) for ASA - 10.197.164.3

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

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

Add AAA Server

Server Group: ISE

Interface Name: outside

Server Name or IP Address: 10.106.44.77

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: [REDACTED]

Common Password: [REDACTED]

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

Message Table

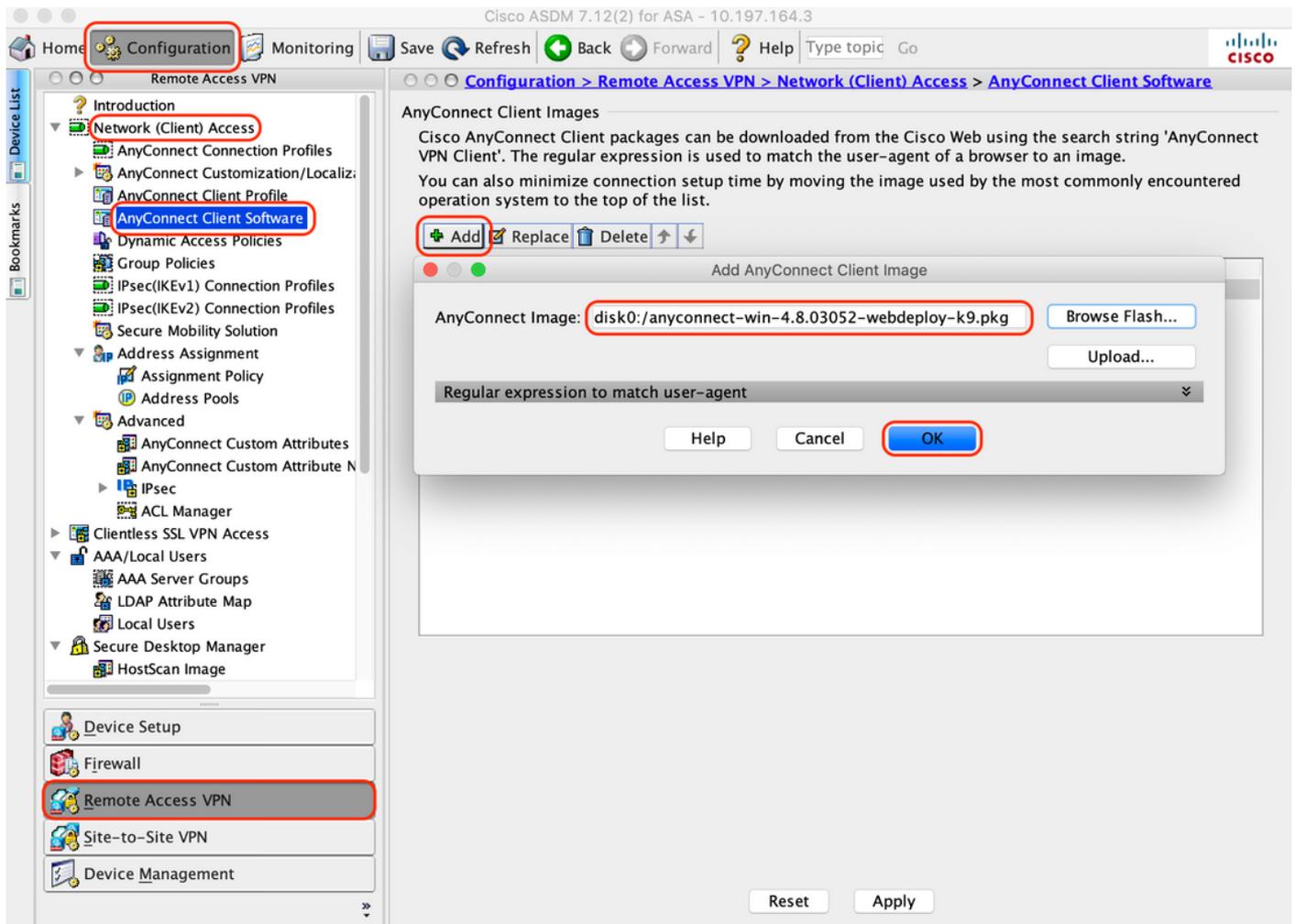
Help Cancel OK

Reset Apply

4. Mappa il software client AnyConnect

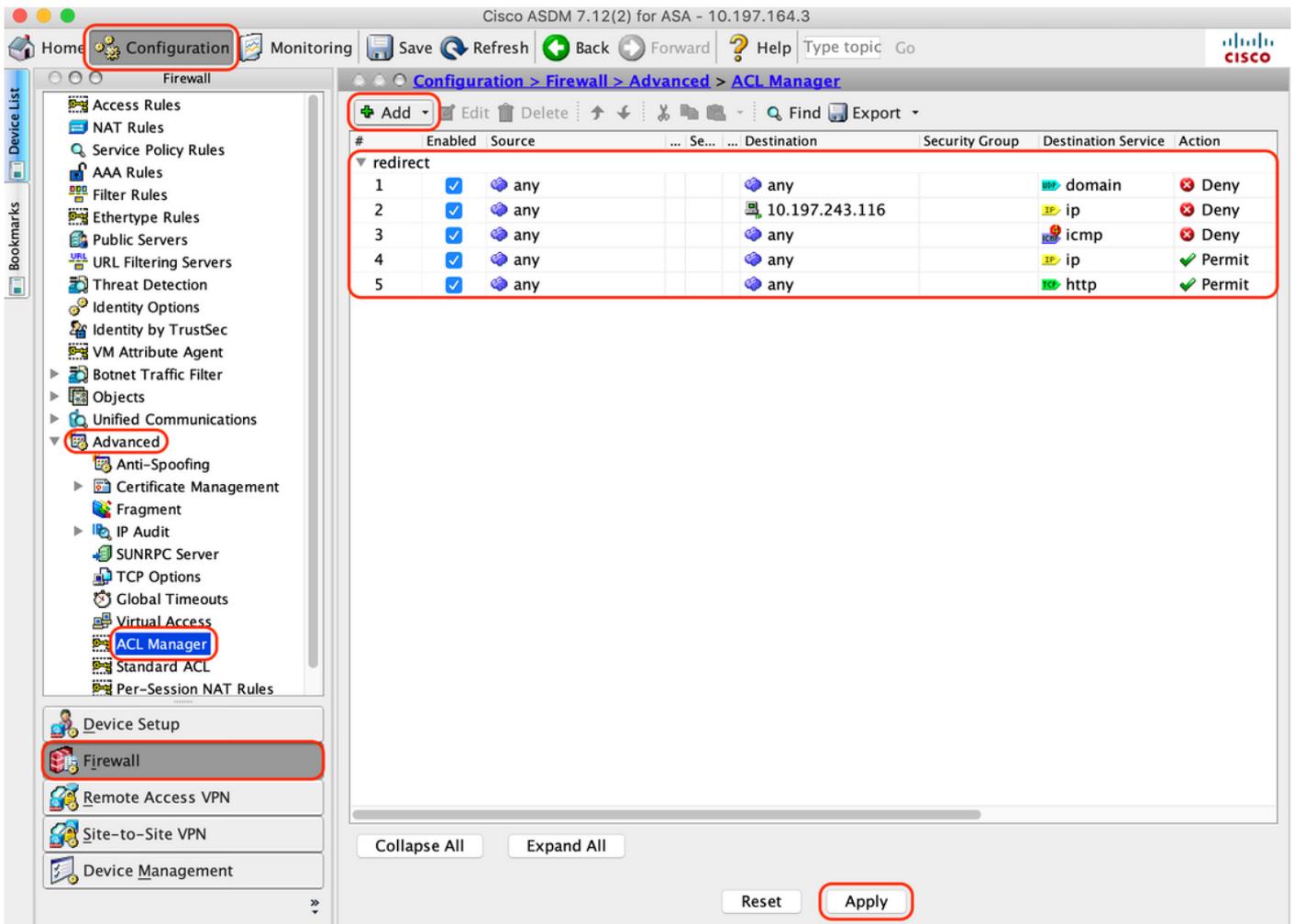
A. Mappare l'immagine WebDeployment del software client AnyConnect 4.8.03052 per usare Windows per WebVPN

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



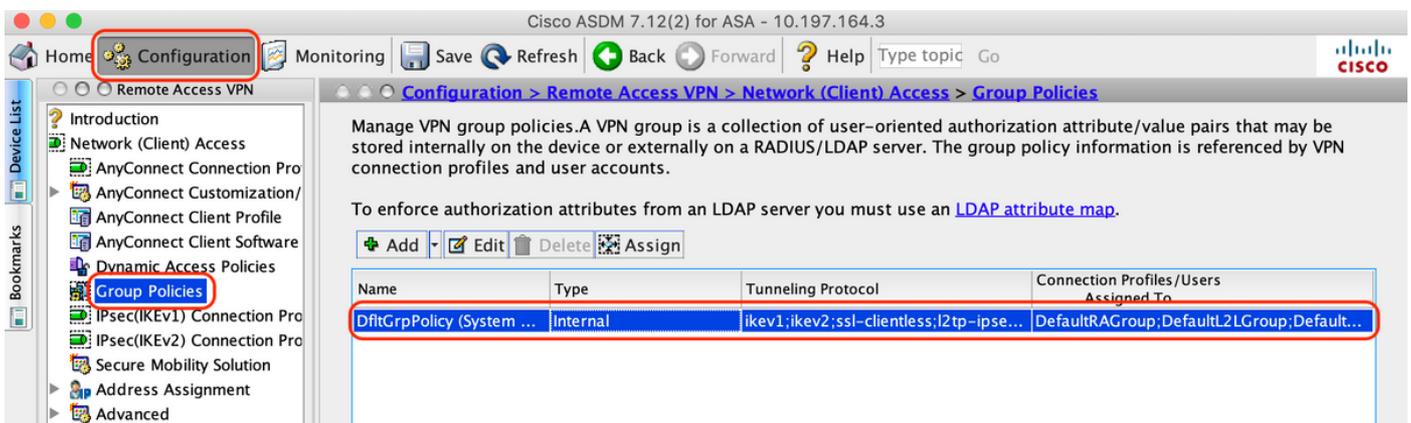
5. Configurare l'ACL di reindirizzamento su cui viene eseguito il push come risultato di ISE

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

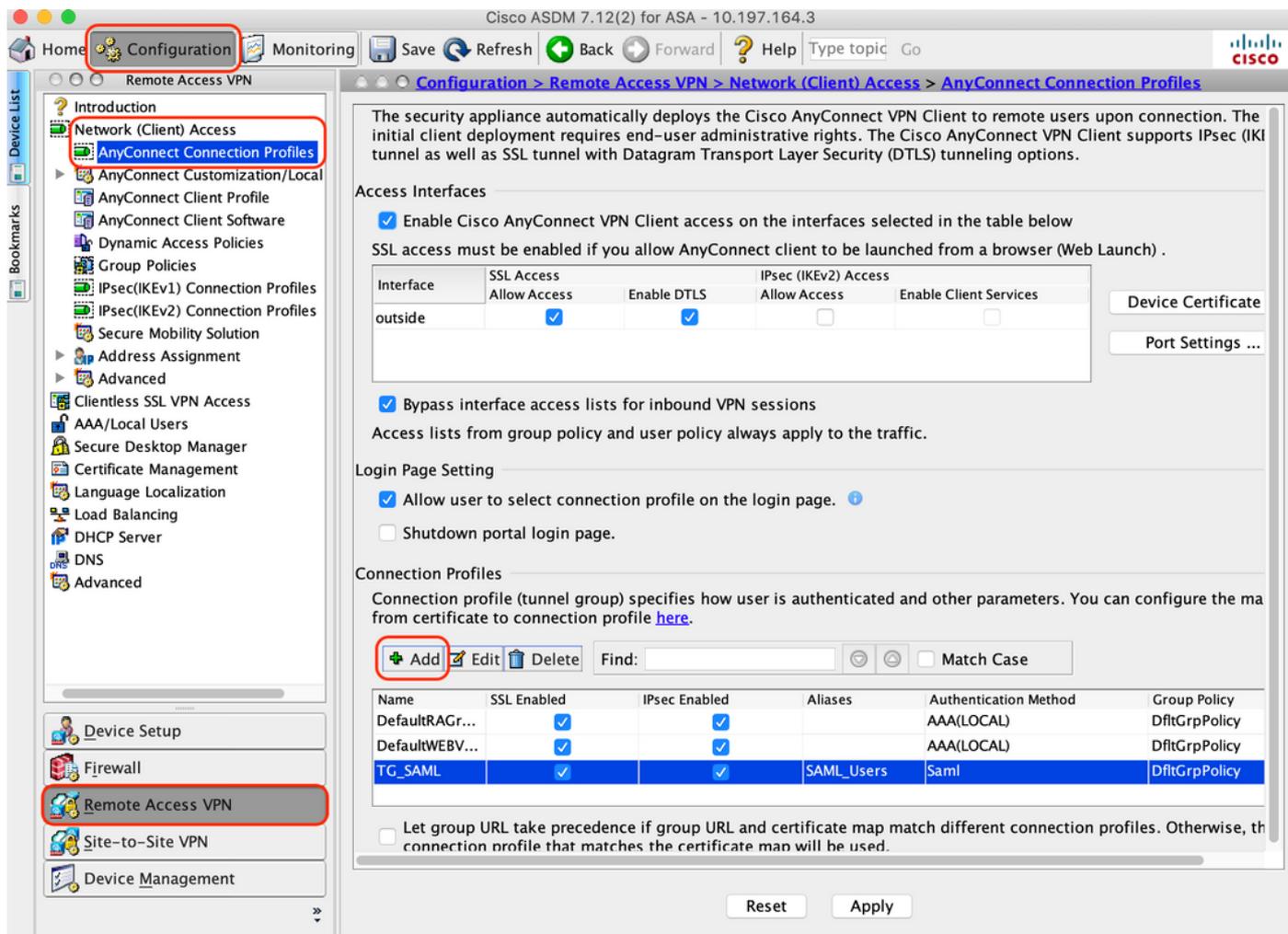
R. Questa impostazione utilizza i criteri di gruppo predefiniti e può essere visualizzata in: "Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo"



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

Basic
▶ Advanced

Name: TG_SAML

Aliases: SAML_Users

Authentication

Method: SAML

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

SAML Identity Provider

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

Client Address Assignment

DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: AC_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: DfltGrpPolicy Manage...

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

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

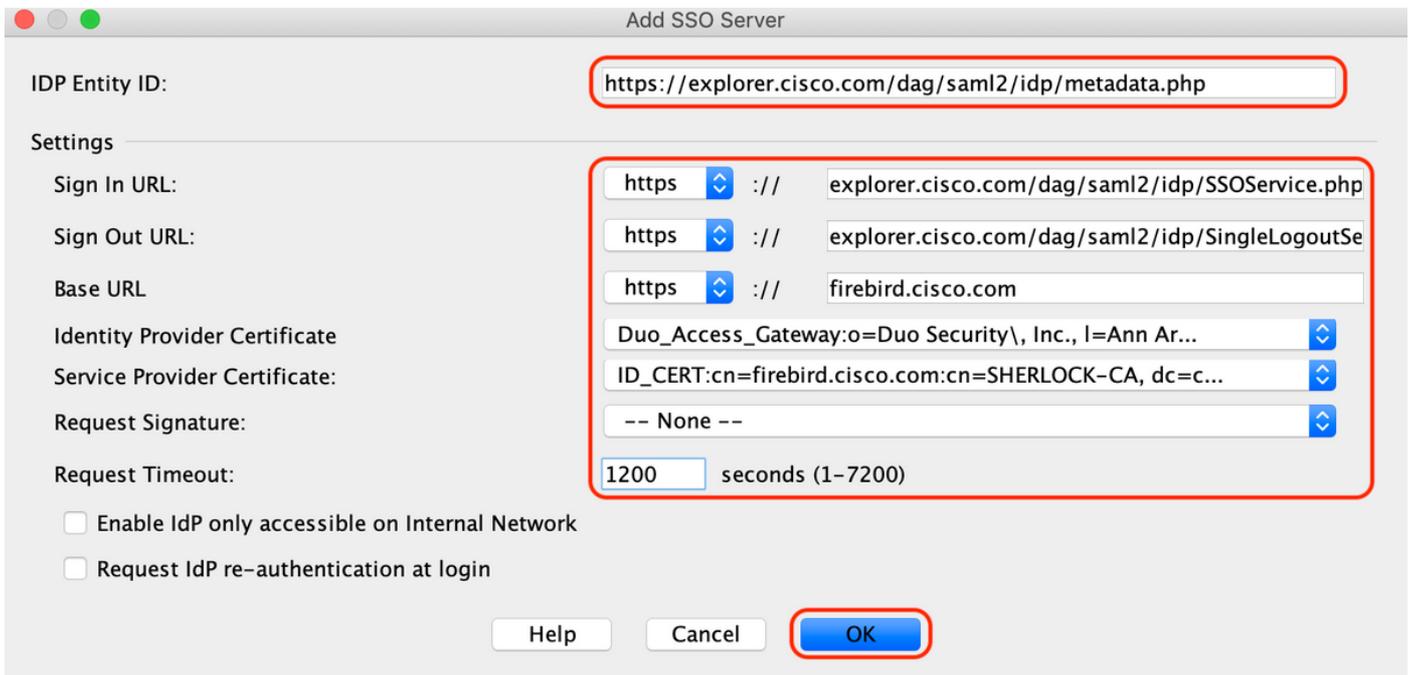
Find: Next Previous

Help Cancel OK

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

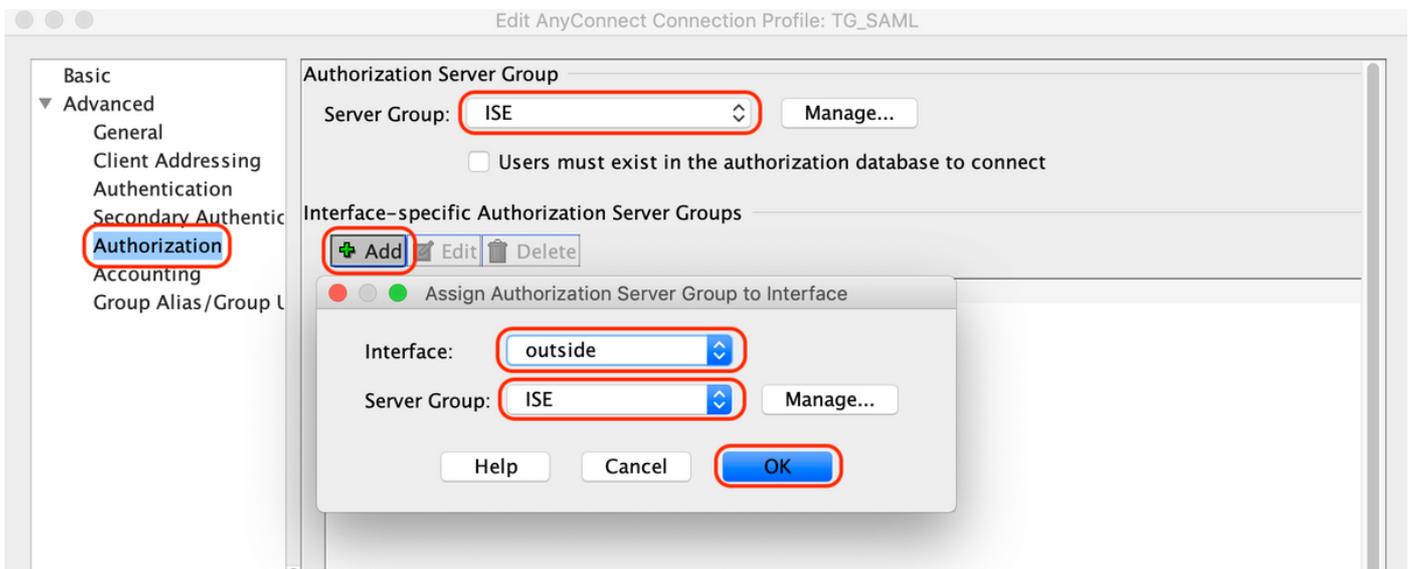
ID entità IDP	https://explorer.cisco.com/dag/saml2/idp/metadata.php
URL di accesso	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
URL di disconnessione	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://exp
URL di base	https://firebird.cisco.com

E. Fare clic su "Gestisci > Aggiungi"



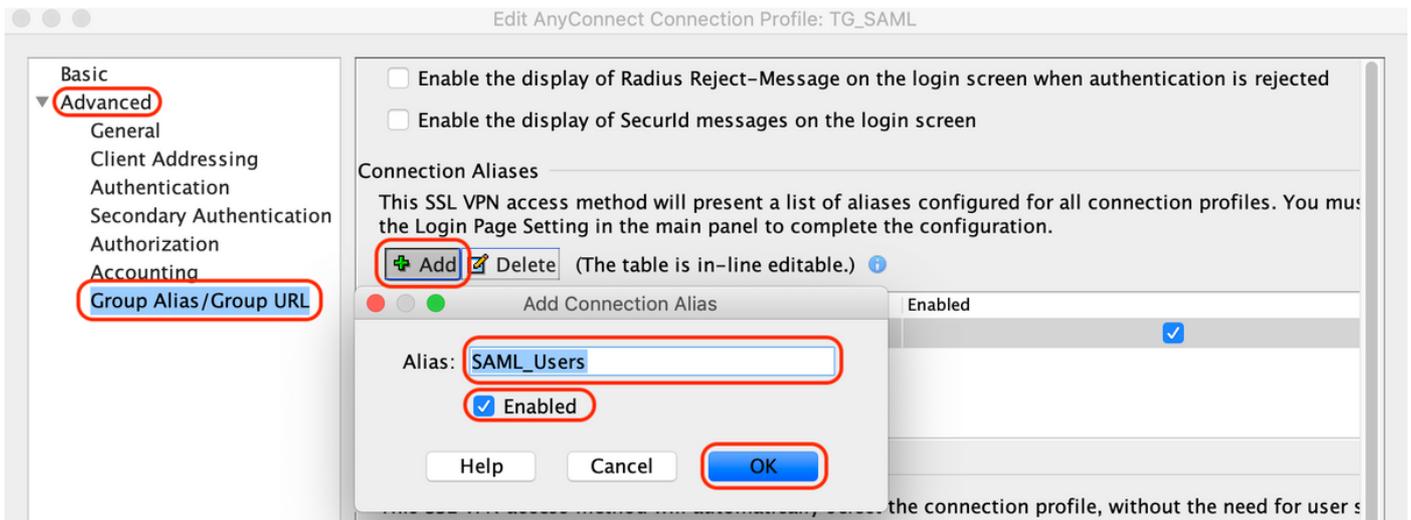
F. Nella sezione Avanzate del profilo di connessione, definire il server AAA per l'autorizzazione.

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

```

-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

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type



▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

DNS Name

General Settings

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL



▶ TACACS Authentication Settings



▶ SNMP Settings



▶ Advanced TrustSec Settings

2. Installare gli ultimi aggiornamenti della postura

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

Posture Updates

Web Offline

* Update Feed URL

Proxy Address ⓘ

Proxy Port HH MM SS

Automatically check for updates starting from initial delay every hours ⓘ

Update Information

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

3. 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" (Sfogliare), 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.

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

Agent Resources From Local Disk

Category ⓘ

Browse...

AnyConnect Uploaded Resources

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

4. 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"

ISE Posture Agent Profile Settings > Anyconnect Posture Profile

* Name:

Description:

Posture Protocol

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

5. 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"

* Select AnyConnect Package **AnyConnectDesktopWindows 4.8.3052.0** ▼

* Configuration Name **AnyConnect Configuration**

Description:

DescriptionValue

* Compliance Module **AnyConnectComplianceModuleWindows 4.3.1250.614** ▼

Notes

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture **Anyconnect Posture Profile** ▼

VPN ▼

Network Access Manager ▼

Web Security ▼

AMP Enabler ▼

Network Visibility ▼

Umbrella Roaming Security ▼

Customer Feedback ▼

6. 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"

Client Provisioning Policy

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

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

Save Reset

7. 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

File Conditions List > VPN_Posture_File_Check

File Condition

* Name: VPN_Posture_File_Check

Description:

* Operating System: Windows 10 (All)

Compliance Module: Any version

* File Type: FileExistence

* File Path: ABSOLUTE_PATH

* File Operator: Exists

C:\custom.txt

Save Reset

8. 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

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

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

Save Reset

10. 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

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

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

Save **Reset**

11. Creazione di ACL dinamici

Selezionare "Policy > Policy Elements > Results > Authorization > Downloadable 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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Downloadable ACL List > PostureUnknown

Downloadable ACL

* Name: PostureUnknown

Description:

IP version: IPv4 IPv6 Agnostic

* DACL Content:

```

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

```

Check DACL Syntax

Save Reset

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Downloadable ACL List > PostureNonCompliant

Downloadable ACL

* Name: PostureNonCompliant

Description:

IP version: IPv4 IPv6 Agnostic

* DACL Content:

```

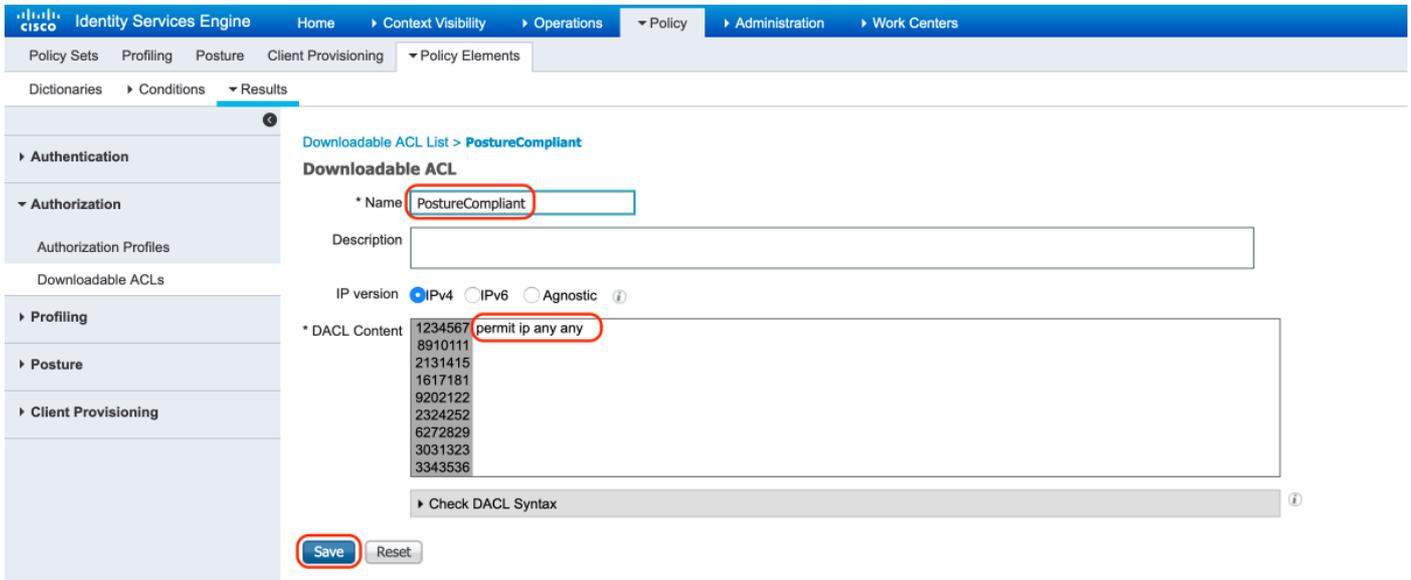
1234567 deny ip any 10.0.0.0 255.0.0.0
8910111 deny ip any 172.16.0.0 255.240.0.0
2131415 deny ip any 192.168.0.0 255.255.0.0
1617181 permit ip any any
9202122
2324252
6272829
3031323
3343536

```

Check DACL Syntax

Save Reset

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

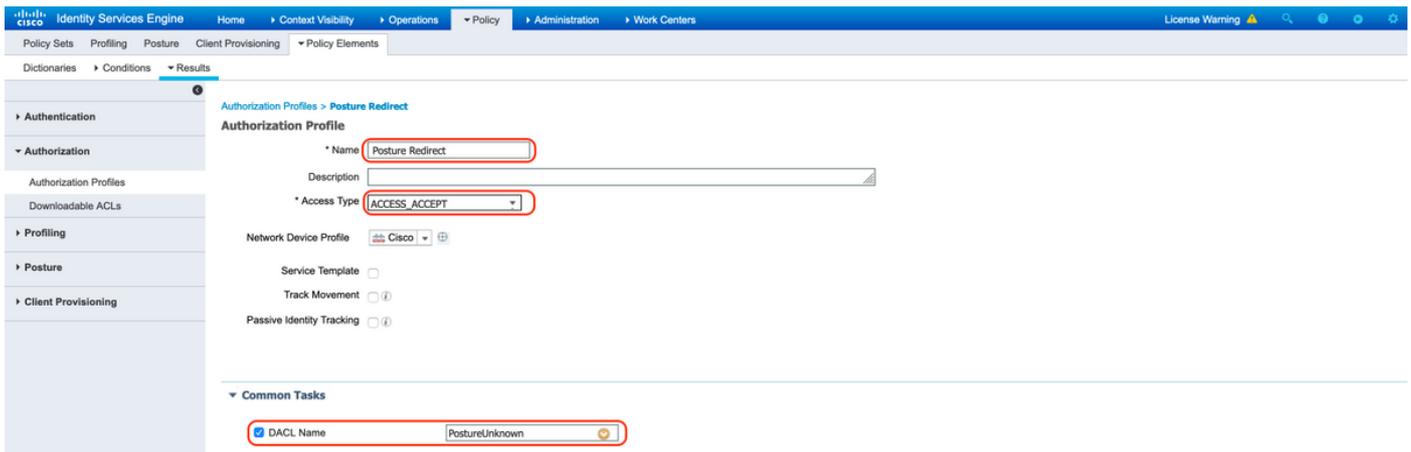


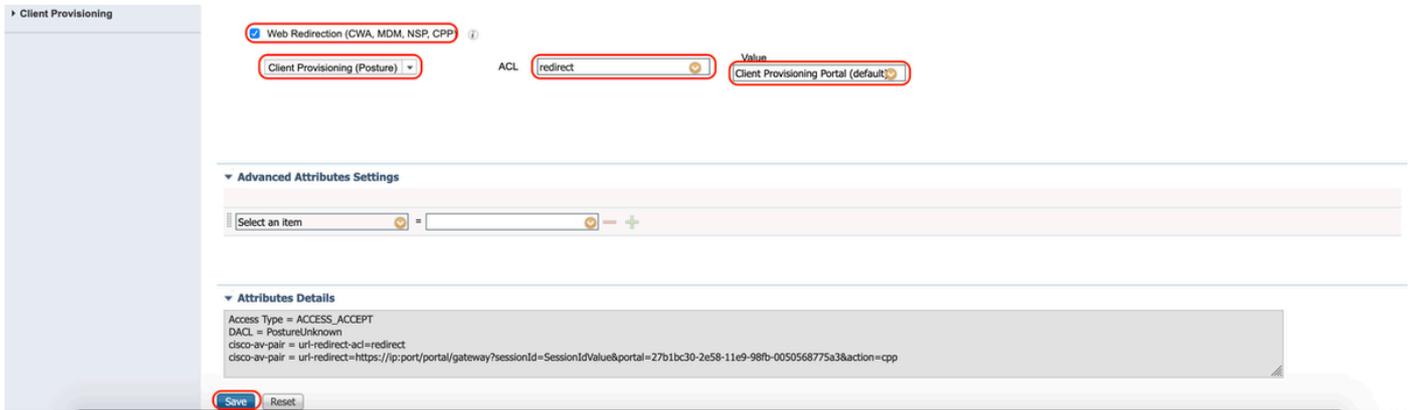
12. Creazione di profili di autorizzazione

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

A. Profilo di autorizzazione per la postura sconosciuta

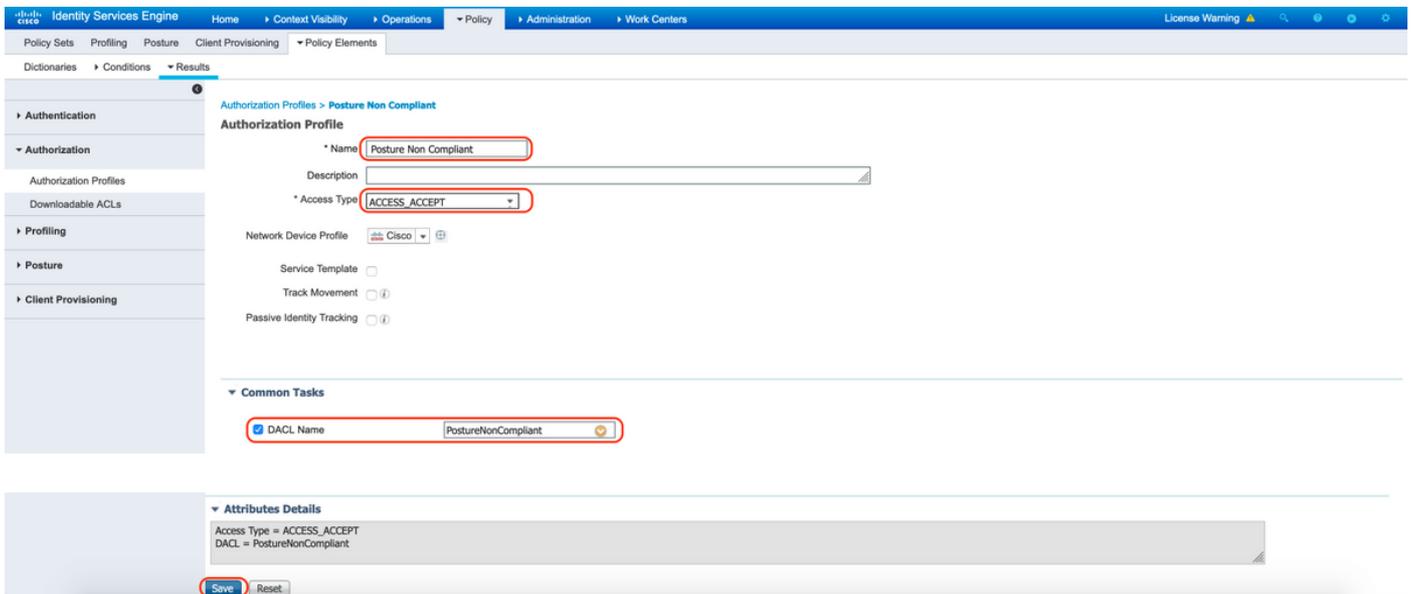
Selezionare DACL "PostureUnknown" (Postura sconosciuta), selezionare Web Redirection (Reindirizzamento Web), selezionare Client Provisioning (Postura) (Postura), configurare il nome ACL di reindirizzamento "redirect" (da configurare sull'appliance ASA) e selezionare il portale di provisioning client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





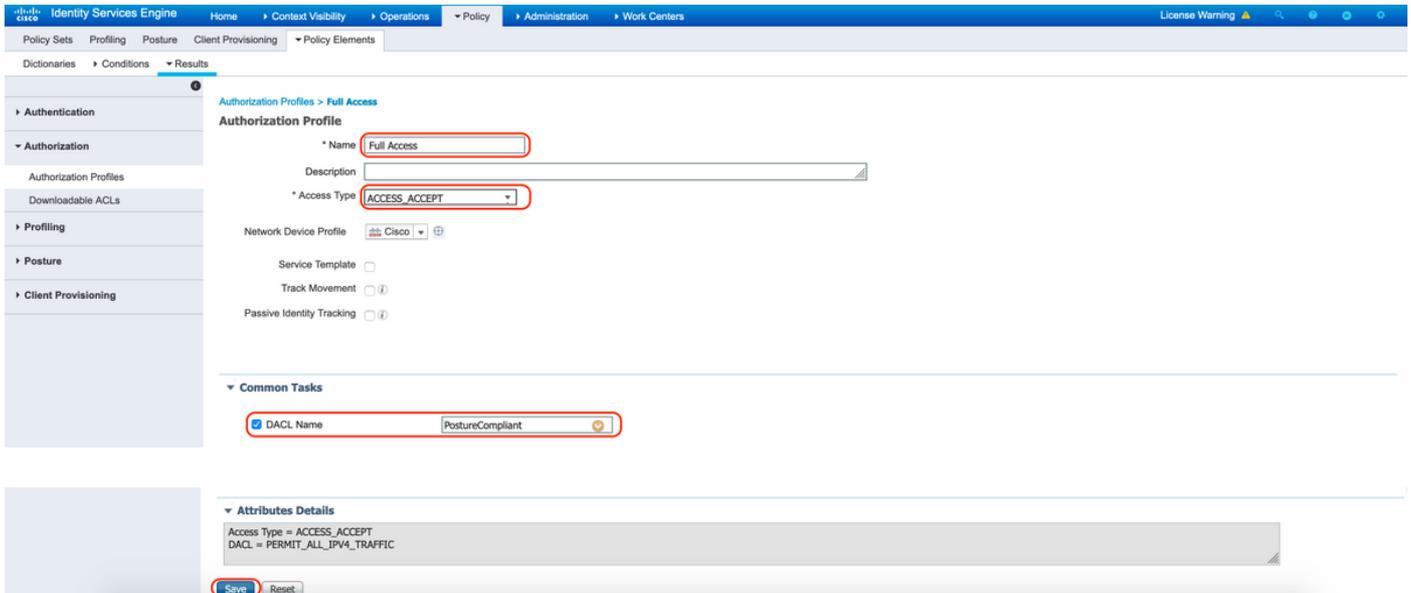
B. Profilo di autorizzazione per la postura non conforme

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



C. Profilo di autorizzazione per la conformità alla postura

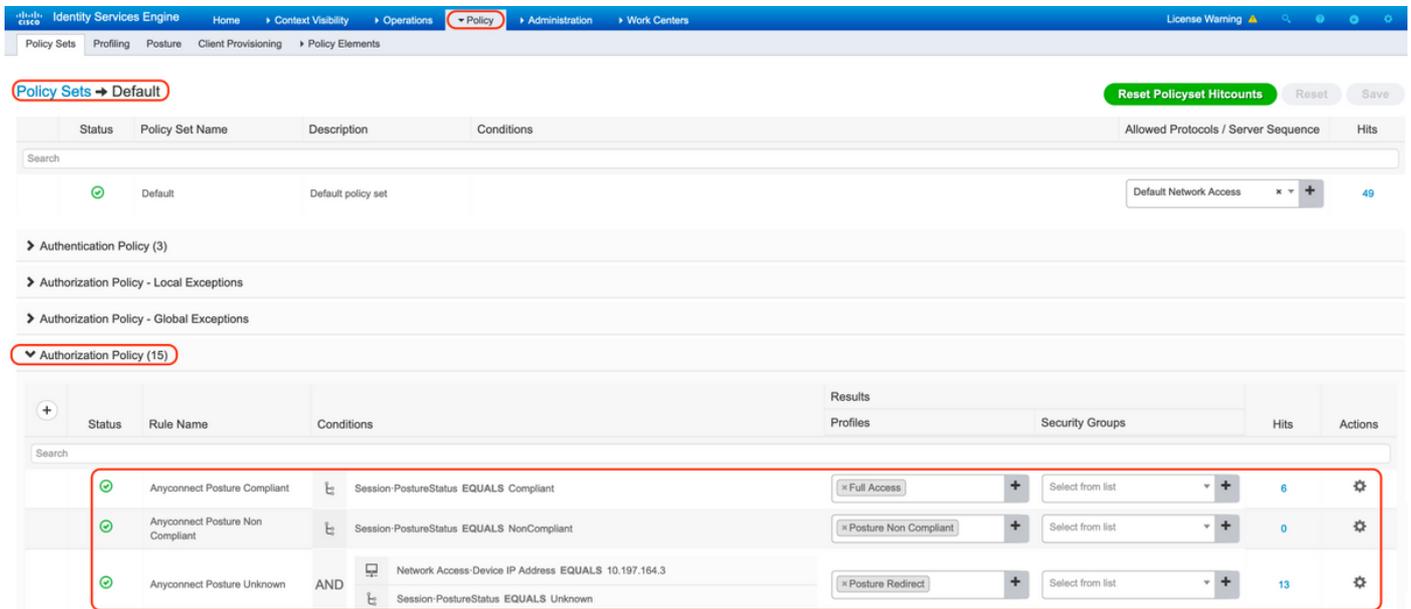
Selezionare DACL "PostureCompliant" per consentire accesso completo alla rete



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&p>
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

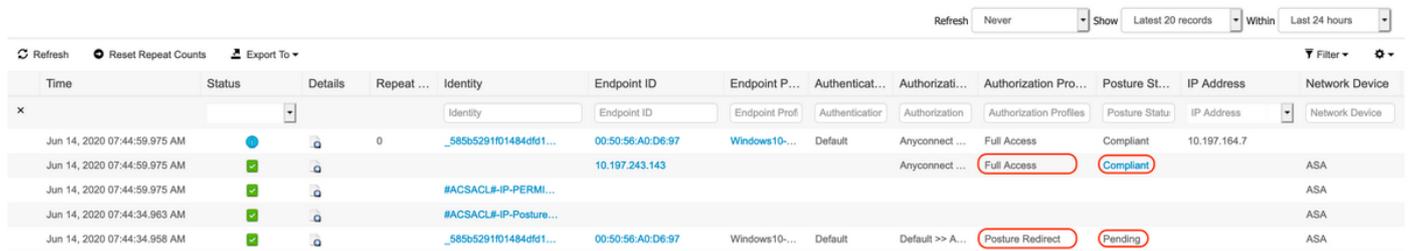
DTLS-Tunnel:

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.



Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentica...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM			0	_585b5291f01484dfd1...	00:50:56:A0:D6:97	Windows10-...	Default	Anyconnect ...	Full Access	Compliant	10.197.164.7	
Jun 14, 2020 07:44:59.975 AM				#ACSACL#-IP-PERMI...	10.197.243.143			Anyconnect ...	Full Access	Compliant		ASA
Jun 14, 2020 07:44:59.975 AM				#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.963 AM												ASA
Jun 14, 2020 07:44:34.958 AM				_585b5291f01484dfd1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA



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>

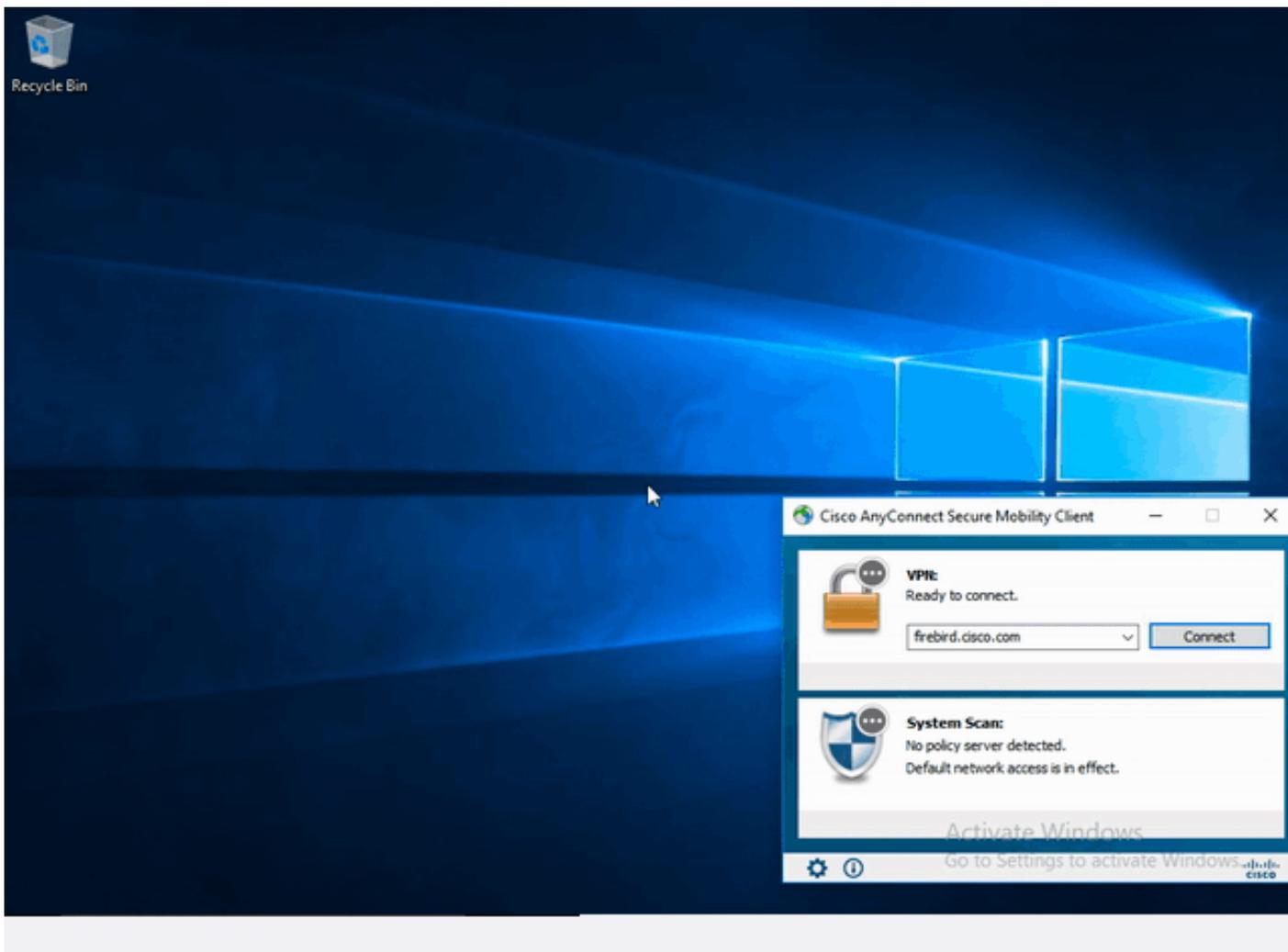
Per verificare lo stato di autenticazione sul portale di amministrazione Duo, fare clic su "Report" sul lato sinistro del pannello di amministrazione che mostra il log di autenticazione.

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-access.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).