

Configurazione di ISE BYOD con Single e Dual SSID in ISE 3.3

Sommario

[Introduzione](#)

[Introduzione](#)

[Prerequisiti](#)

[Componente utilizzato](#)

[Che cos'è Single SSID e Dual SSID BYOD su ISE?](#)

[Single SSID BYOD](#)

[Doppio SSID BYOD](#)

[Configurazione WLC](#)

[Creazione di una WLAN per CWA](#)

[Configurazione server RADIUS](#)

[Configurazione dei server AAA](#)

[Configurazione dei criteri di sicurezza per la WLAN](#)

[Configurazione dell'ACL di preautenticazione](#)

[Configura profilo criteri](#)

[Applica tag e distribuisci](#)

[Configurare un SSID aperto/non protetto](#)

[Configurazione di ISE](#)

[Prerequisiti](#)

[Certificati](#)

[Configurazione DNS](#)

[Configura dispositivo di rete ISE](#)

[Creazione di un portale BYOD](#)

[Scarica l'ultima versione di Cisco IOS®](#)

[Creazione di un profilo di endpoint](#)

[Modello di certificato](#)

[Mappare un profilo di endpoint al portale di provisioning client](#)

[Configurazione dei set di criteri ISE per Single SSID BYOD](#)

[Configurazione dei set di criteri ISE per Dual SSID BYOD](#)

[Risoluzione dei problemi](#)

[Frammento di log](#)

[Log Guest](#)

[Registri Ise-Psc](#)

[Download profilo endpoint](#)

Introduzione

Nel documento viene descritto come configurare ISE e risolvere i problemi relativi a BYOD.

Introduzione

BYOD è una funzione che permette agli utenti di integrare i propri dispositivi personali su ISE in modo che possano utilizzare le risorse di rete sull'ambiente. Consente inoltre all'amministratore di rete di impedire all'utente di accedere alla risorsa critica dai dispositivi personali.

A differenza del flusso guest, in cui il dispositivo viene autenticato con la pagina Guest tramite il punto vendita interno o Active Directory su ISE. Il BYOD consente all'amministratore di rete di installare un profilo dell'endpoint sull'endpoint per scegliere il tipo di metodo EAP. In scenari come EAP-TLS, il certificato client viene firmato dall'ISE stessa per creare un trust tra l'endpoint e ISE.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- controller WLC
- Conoscenze base di ISE

Componente utilizzato

I dispositivi utilizzati non sono limitati a una particolare versione per il flusso BYOD:

- Catalyst 9800-CL Wireless Controller (17.12.3)
- ISE Virtual Machine (3.3)

Che cos'è Single SSID e Dual SSID BYOD su ISE?

Single SSID BYOD

In una configurazione BYOD a un solo SSID, gli utenti connettono i propri dispositivi personali direttamente alla rete wireless aziendale. Il processo di caricamento si verifica sullo stesso SSID, dove ISE semplifica la registrazione dei dispositivi, il provisioning e l'applicazione delle policy. Questo approccio semplifica l'esperienza dell'utente, ma richiede l'accesso sicuro e metodi di autenticazione appropriati per garantire la sicurezza della rete.

Doppio SSID BYOD

In una configurazione BYOD con due SSID, vengono utilizzati due SSID distinti: una per l'onboarding (accesso non protetto o limitato) e un'altra per accedere alla rete aziendale. Inizialmente gli utenti si connettono all'SSID caricato, completano la registrazione del dispositivo e il provisioning tramite ISE, quindi passano all'SSID aziendale sicuro per l'accesso alla rete. Questo fornisce un ulteriore livello di sicurezza separando il traffico in entrata dal traffico di produzione.

Configurazione WLC

Creazione di una WLAN per CWA

1. Selezionare Configurazione > Tag e profili > WLAN.
2. Fare clic su Add (Aggiungi) per creare una nuova WLAN.
 - Impostare un nome WLAN e un SSID (ad esempio, BYOD-WiFi).
 - Abilitare la WLAN.

Add WLAN

GeneralSecurityAdvanced

Profile Name*

Enter Name

SSID*

BYOD-SSID

WLAN ID*

9

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status

ENABLED

ⓘ

✖ WPA3 Enabled

✔ Dot11ax Enabled

5 GHz

Status

ENABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

▼

↶ Cancel

📄 Apply to Device

Configurazione server RADIUS

1. Selezionare Configurazione > Sicurezza > AAA > RADIUS > Server.

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

[+ Add](#)

[- Delete](#)

RADIUS

TACACS+

LDAP

Servers

Server Groups

Acct Port "Contains" 1814

Name	Address	Auth Port	Acct Port
0			10

No items to display

For Radius fallback to work, please make sure the [Dead Criteria](#) and [Dead Time](#) configuration exists on the device

2. Fare clic su Add (Aggiungi) per configurare ISE come server RADIUS:

- IP server: Indirizzo IP dell'ISE.
- Segreto condiviso: Trova la corrispondenza con il segreto condiviso configurato su ISE.

Create AAA Radius Server

Name* BYOD

Server Address* 10.x.x.x

PAC Key ☐

Key Type Clear Text

Key*

Confirm Key*

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA [i](#)

ENABLED ☒

CoA Server Key Type

Clear Text

CoA Server Key [i](#)

.....

Confirm CoA Server Key

.....

Automate Tester

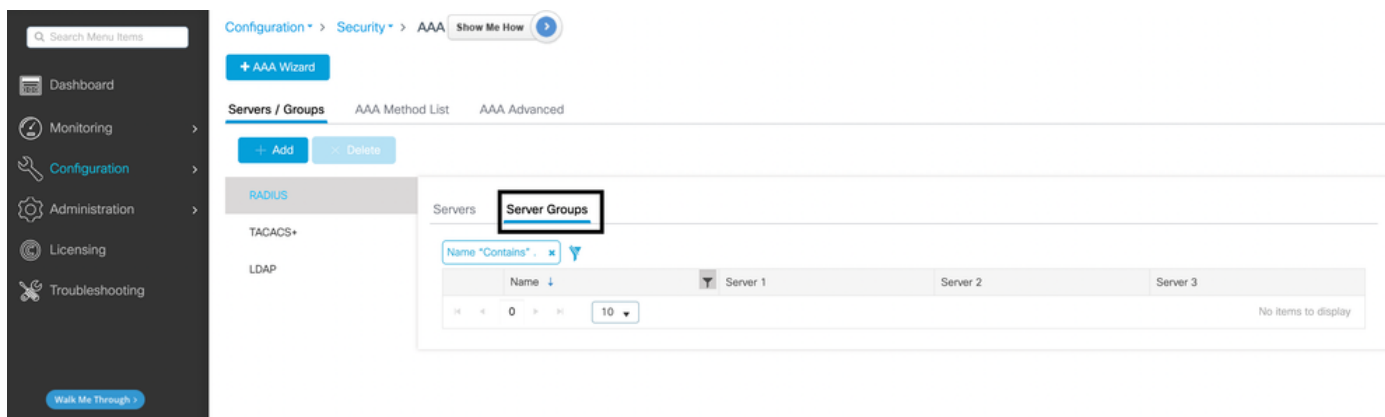
☐

[Cancel](#)

[Apply to Device](#)

Configurazione dei server AAA

1. Passare a Configurazione > Sicurezza > AAA > Server/Gruppi.



2. Assegnare il server RADIUS a un gruppo di server nuovo o esistente.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Load Balance ☐

Source Interface VLAN ID

Available Servers

Assigned Servers

> < >> <<

Cancel Apply to Device

Configurazione dei criteri di sicurezza per la WLAN

1. Selezionare Configurazione > Tag e profili > WLAN. Modificare la WLAN creata in precedenza.
2. Nella scheda Protezione > Livello 2:
 - Abilita WPA+WPA2
 - Impostazione di AES(CCMP128) con la crittografia WPA2
 - Gestione chiavi di autenticazione come 802.1X

Edit WLAN



⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☒ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

WPA2 Policy

☒

GTK Randomize

☐

OSEN Policy

☐

WPA2 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Disabled

Fast Transition

Status

Adaptive Ena... ▼

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

802.1X

☒

PSK

☐

Easy-PSK

☐

CCKM ⚠

☐

FT + 802.1X

☐

FT + PSK

☐

802.1X-SHA256

☐

PSK-SHA256

☐

MPSK Configuration

Cancel



Update & Apply to Device

3. Nella scheda Protezione > Livello 3, selezionare globale dall'elenco a discesa Mappa parametri autenticazione Web.

Edit WLAN ✕

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

Web Policy

☐

Show Advanced Settings >>>

Web Auth Parameter Map

global

▼

🔗

Authentication List

Select a value

▼

🔗

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

↶ Cancel

🔄 Update & Apply to Device

Configurazione dell'ACL di preautenticazione

Creare un ACL per consentire le azioni per il reindirizzamento:

- traffico DNS.
- HTTP/HTTPS sul portale ISE.
- Tutti i servizi back-end necessari.

A tale scopo:

1. Selezionare Configurazione > Sicurezza > ACL > Access Control Lists.
2. Creare un nuovo ACL con le regole per autorizzare il traffico necessario.

Edit Policy Profile

⌵

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling☒

HTTP TLV Caching☒

DHCP TLV Caching☒

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼ ⓘ

VLAN

VLAN/VLAN Group

VLAN0097 ▼ ⓘ

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼ ⓘ

IPv6 ACL

Search or Select ▼ ⓘ

URL Filters ⓘ

Pre Auth

Search or Select ▼ ⓘ

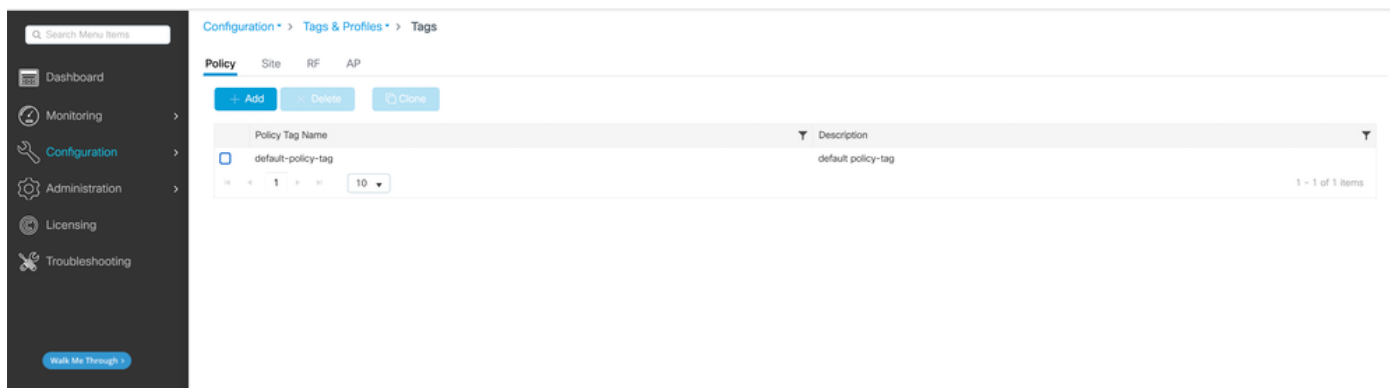
Post Auth

Search or Select ▼ ⓘ

↶ Cancel

📁 Update & Apply to Device

3. Abilitare anche Consenti sostituzione AAA e stato NAC in Avanzate del criterio.



Configurare un SSID aperto/non protetto

Open SSID viene creato solo quando si decide di avere una configurazione BYOD a doppio SSID nel proprio ambiente.

1. Selezionare Configurazione > Tag e profili > WLAN. Fare clic sul pulsante Aggiungi.
2. Specificare un nome SSID nella scheda Generale e abilitare il pulsante WLAN.

Add WLAN

GeneralSecurityAdvanced

Profile Name*BYOD-Open

SSID*BYOD-Open

WLAN ID*10

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status

ENABLED

WPA3 Enabled

Dot11ax Enabled

5 GHz

Status

ENABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

Cancel

Apply to Device

3. Fare clic sulla scheda Protezione nella stessa finestra. Selezionare il pulsante di scelta Nessuno e abilitare il filtro Mac.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. The 'Layer2' sub-tab is active, and the 'None' security option is chosen. The 'MAC Filtering' checkbox is checked. The 'Fast Transition' section is expanded, showing 'Status' as 'Disabled', 'Over the DS' as unchecked, and 'Reassociation Timeout' as 20. The 'Apply to Device' button is visible at the bottom right.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

☐ WPA + WPA2 ☐ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☒ None

MAC Filtering ☒ Authorization List* default ⓘ

OWE Transition Mode ☒ Transition Mode WLAN ID* 0-4096

Lobby Admin Access ☐

Fast Transition

Status Disabled ▼

Over the DS ☐

Reassociation Timeout * 20

Cancel Apply to Device

4. Nel layer 3, in Protezione, selezionare l'impostazione globale per Mappa parametri autenticazione Web. Se sul WLC è configurato un altro profilo di autenticazione Web, è possibile mapparlo anche qui:

Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

Show Advanced Settings >>>

Web Policy

Web Auth Parameter Map

global

Authentication List

Select a value

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Cancel

Apply to Device

Configurazione di ISE

Prerequisiti

- Verificare che Cisco ISE sia installato e concesso in licenza per la funzionalità BYOD.
- Aggiungere il WLC all'ISE come dispositivo di rete con il segreto condiviso RADIUS.

Certificati

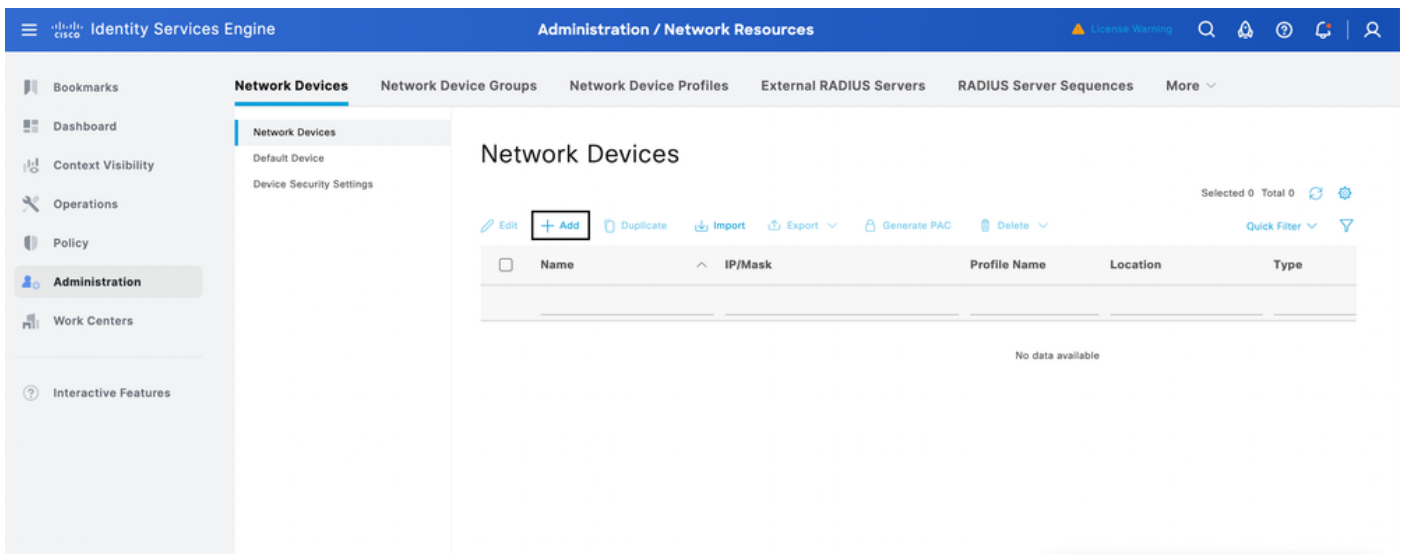
- Installare un certificato server valido su ISE per evitare la visualizzazione di avvisi di protezione del browser.
- Verificare che il certificato sia considerato attendibile dagli endpoint (firmati da una CA nota o da una CA interna con radice attendibile).

Configurazione DNS

- Accertarsi che il DNS risolva il nome host ISE per il portale BYOD.

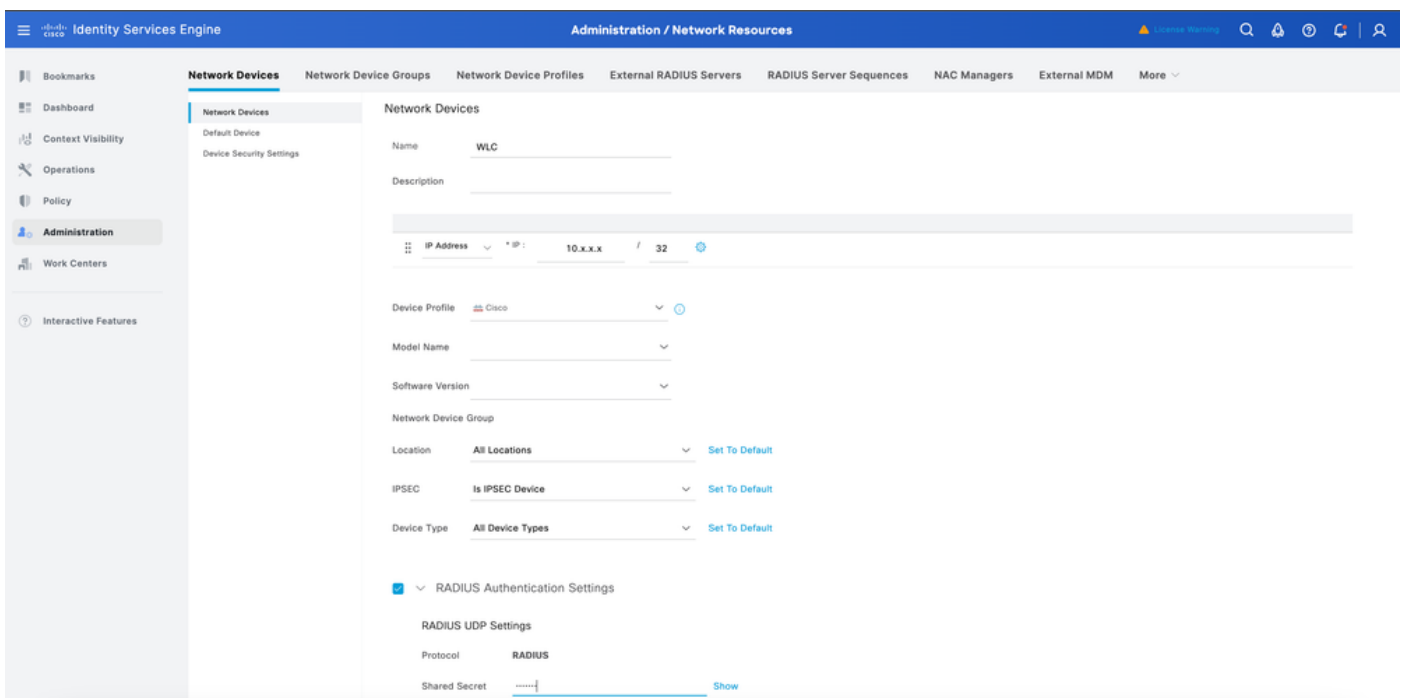
Configura dispositivo di rete ISE

1. Accedere all'interfaccia utente Web di ISE.
2. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete.



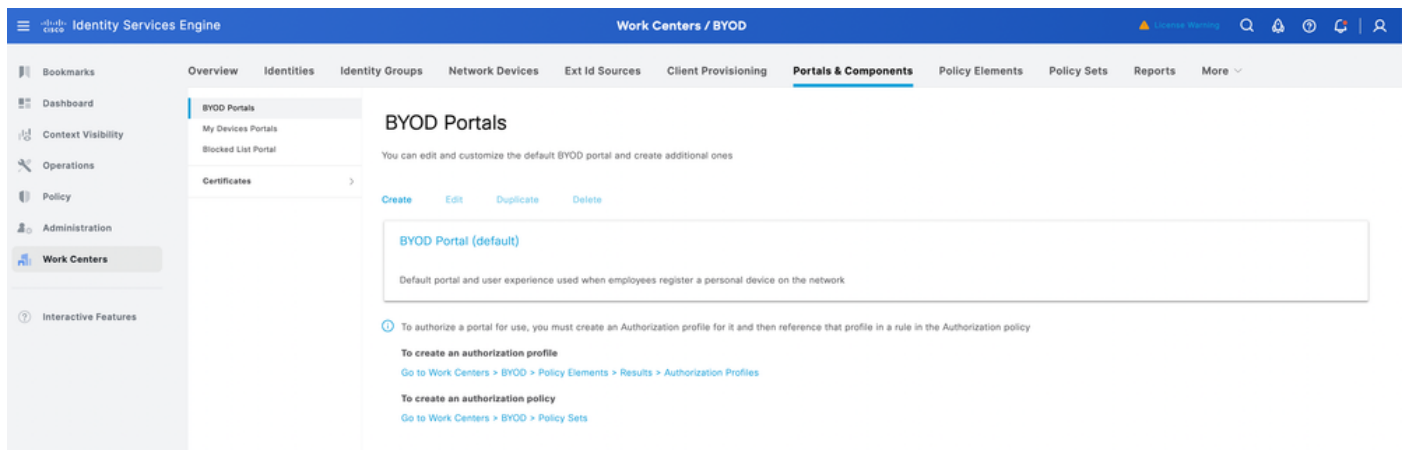
3. Aggiungere il WLC come dispositivo di rete:

- Nome: Immettere un nome per il WLC.
- Indirizzo IP: Immettere l'IP di gestione WLC.
- Segreto condiviso RADIUS: Immettere lo stesso segreto condiviso configurato sul WLC.
- Fare clic su Invia.



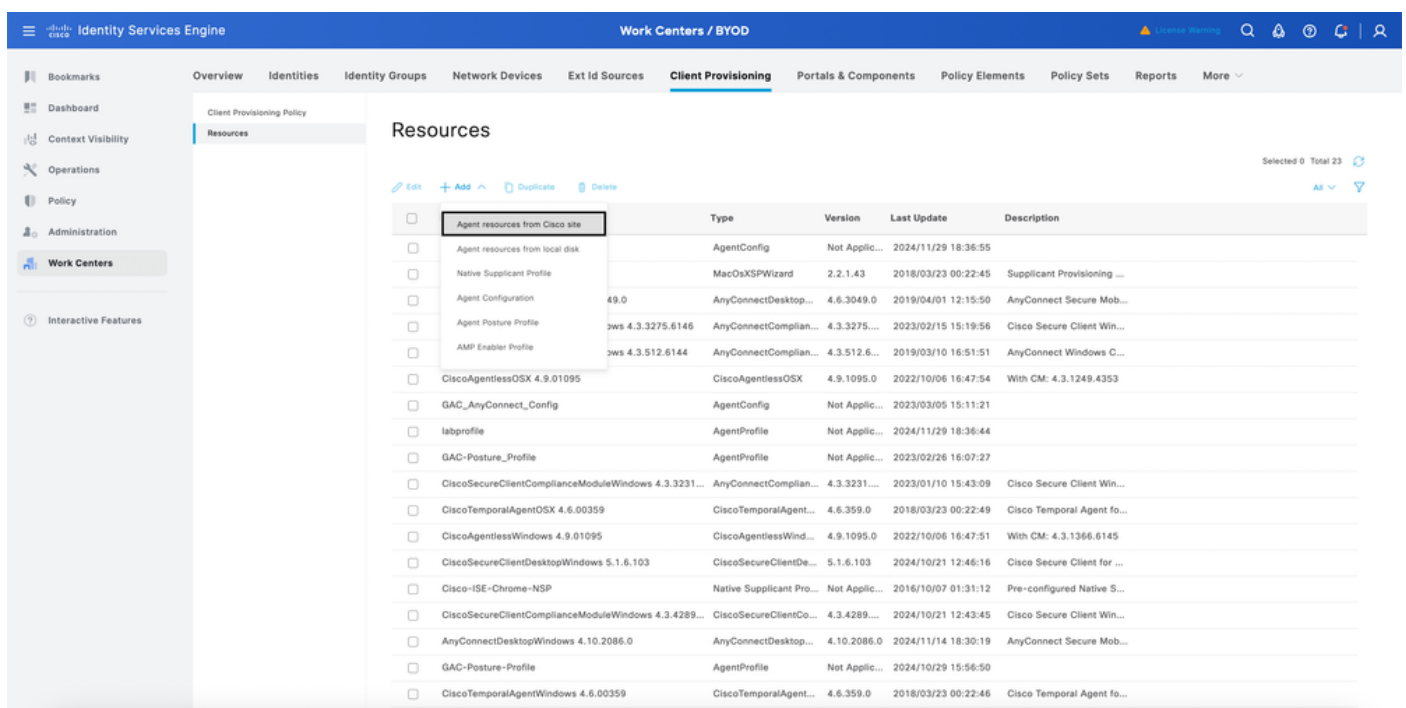
Creazione di un portale BYOD

1. Passare a Centri di lavoro > BYOD > Impostazioni > Portali e componenti > Portali BYOD.
2. Fare clic su Add (Aggiungi) per creare un portale BYOD o è possibile utilizzare il portale predefinito esistente su ISE.



Scarica l'ultima versione di Cisco IOS®

1. Passare a Centri di lavoro > BYOD > Provisioning client > Risorse.
2. Fare clic sul pulsante Add (Aggiungi) e selezionare le risorse agente dal sito Cisco.



3. Nell'elenco del software, selezionare la versione più recente di Cisco IOS da scaricare.



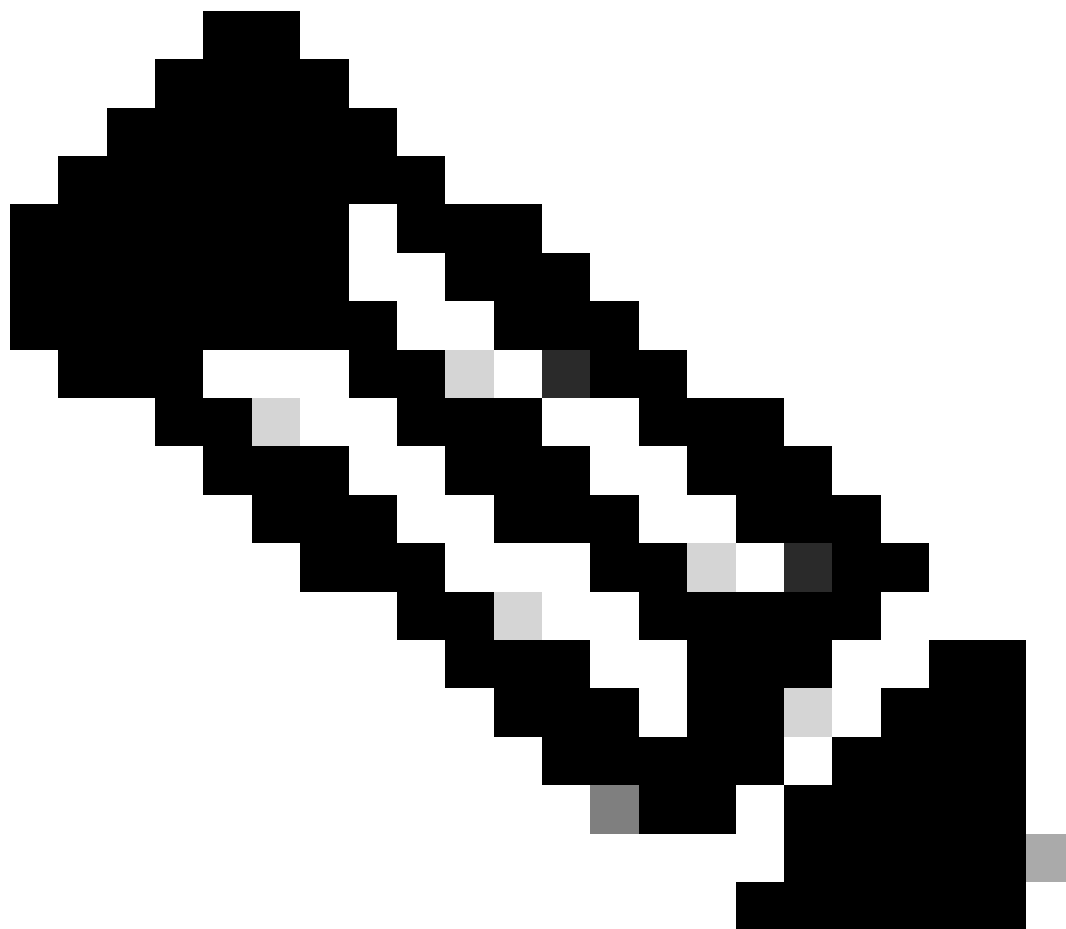
Download Remote Resources

☐	Name	Description
☐	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
☐	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
☒	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save



Nota: Il software Cisco IOS viene scaricato sull'ISE per gli endpoint Windows e MacOS. Per Apple iPhone IOS, utilizza un supplicant nativo per effettuare il provisioning del dispositivo e Per il dispositivo android, si dispone di Network setup assistant che deve essere scaricato da Play Store.

Creazione di un profilo di endpoint

1. Passare a Centri di lavoro > BYOD > Provisioning client > Risorse.
2. Fare clic su Aggiungi, quindi selezionare Profilo supplicant nativo dal menu a discesa.

Identity Services Engine Work Centers / BYOD

Overview Identities Identity Groups Network Devices Ext Id Sources **Client Provisioning** Portals & Components Policy Elements Policy Sets Reports More

Client Provisioning Policy Resources

Selected 0 Total 24

Type	Version	Last Update	Description
Agent resources from Cisco site			
Agent resources from local disk			
Native Supplicant Profile			
Agent Configuration	4.9.0	2019/04/01 12:15:50	AnyConnect Secure Mob...
Agent Posture Profile	4.3.3275.6146	2023/02/15 15:19:56	Cisco Secure Client Win...
AMP Enabler Profile	4.3.512.6144	2019/03/10 16:51:51	AnyConnect Windows C...
CiscoAgentlessOSX 4.9.01095	4.9.1095.0	2022/10/06 16:47:54	With CM: 4.3.1249.4353
GAC_AnyConnect_Config	AgentConfig	Not Applic...	2023/03/05 15:11:21
labprofile	AgentProfile	Not Applic...	2024/11/29 18:36:44
GAC-Posture_Profile	AgentProfile	Not Applic...	2023/02/26 16:07:27
CiscoSecureClientComplianceModuleWindows 4.3.3231...	AnyConnectComplan...	4.3.3231...	2023/01/10 15:43:09 Cisco Secure Client Win...
CiscoTemporalAgentOSX 4.6.00359	CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:49 Cisco Temporal Agent fo...
CiscoAgentlessWindows 4.9.01095	CiscoAgentlessWind...	4.9.1095.0	2022/10/06 16:47:51 With CM: 4.3.1366.6145
CiscoSecureClientDesktopWindows 5.1.6.103	CiscoSecureClientDe...	5.1.6.103	2024/10/21 12:46:16 Cisco Secure Client for ...
Cisco-ISE-Chrome-NSP	Native Supplicant Pro...	Not Applic...	2016/10/07 01:31:12 Pre-configured Native S...
CiscoSecureClientComplianceModuleWindows 4.3.4289...	CiscoSecureClientCo...	4.3.4289...	2024/10/21 12:43:45 Cisco Secure Client Win...
AnyConnectDesktopWindows 4.10.2086.0	AnyConnectDesktop...	4.10.2086.0	2024/11/14 18:30:19 AnyConnect Secure Mob...
GAC-Posture_Profile	AgentProfile	Not Applic...	2024/10/29 15:56:50
CiscoTemporalAgentWindows 4.6.00359	CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:46 Cisco Temporal Agent fo...

3. Sotto l'elenco a discesa Sistema operativo, selezionare il sistema operativo richiesto che si desidera incorporare il dispositivo o impostarlo come ALL per tutti gli endpoint presenti nell'ambiente:

Identity Services Engine Work Centers / BYOD

Overview Identities Identity Groups Network Devices Ext Id Sources **Client Provisioning** Portals & Components Policy Elements Policy Sets Reports More

Client Provisioning Policy Resources

Native Supplicant Profile

* Name BYOD profile

Description

Operating System * ALL

Wireless Profile
Multiple SSIDs can be co
Proxy Auto-Config File U
If no Proxy Auto-Config File URL is defined then the Proxy host

Operating System Groups

- ALL
- Android
- Apple iOS All
- Chrome OS All
- Linux All
- Mac OSX

SSID Name Proxy Auto-Conf... Proxy Host/IP

BYOD

Wired Profile

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

4. Fare clic su Add dalla pagina per creare il profilo dell'endpoint e configurare 802.1X per l'endpoint:

Wireless Profile(s)

SSID Name *	BYOD	
Proxy Auto-Config File URL		i
Proxy Host/IP		i
Proxy Port		
Security *	WPA2 Enterprise	▼
Allowed Protocol *	PEAP	▼
Certificate Template	Not Required	▼ i

▼ Optional Settings

Windows Settings

Authentication Mode	User or Computer	▼
☐ Automatically use logon name and password (and domain if any)		
☒ Enable fast reconnect		
☐ Enable quarantine checks		
☐ Disconnect if server does not present cryptobinding TLV		
☐ Do not prompt user to authorize new servers or trusted certification authorities		
☒ Connect even if the network is not broadcasting its name (SSID)		

iOS Settings

☐ Enable if target network is hidden

Android Settings

Certificate Enrollment Protocol: [i](#)

A seconda delle esigenze, configurare il profilo dell'endpoint per l'endpoint nell'ambiente. Il profilo degli endpoint consente di configurare EAP-PEAP, EAP-TLS.

5. Fare clic su Save, quindi su Submit (Invia) nel profilo dell'endpoint.

Modello di certificato

Il profilo dell'endpoint è preconfigurato per eseguire EAP-TLS. È necessario aggiungere un modello di certificato al profilo. Per impostazione predefinita, ISE ha due modelli predefiniti che possono essere scelti dal menu a discesa.

Wireless Profile(s)

SSID Name *

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

Allowed Protocol * TLS

Certificate Template EAP_Authentication_Certificate_Template

Optional Settings

EAP_Authentication_Certificate_Template

pxGrid_Certificate_Template

Save

Per creare un nuovo modello di certificato, eseguire la procedura seguente:

1. Passare a Amministrazione > Sistema > Certificati > Autorità di certificazione > Modelli di certificato.

2. Fare clic sul pulsante Aggiungi nella pagina.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The main content area is titled 'Certificate Templates' and includes a table with columns: Template Name, Description, Key Type, Key Size, and Curve Type. The table lists three templates: CA_SERVICE_Certificate_Template, EAP_Authentication_Certificate_Tem..., and pxGrid_Certificate_Template. The 'Add' button is highlighted with a red box.

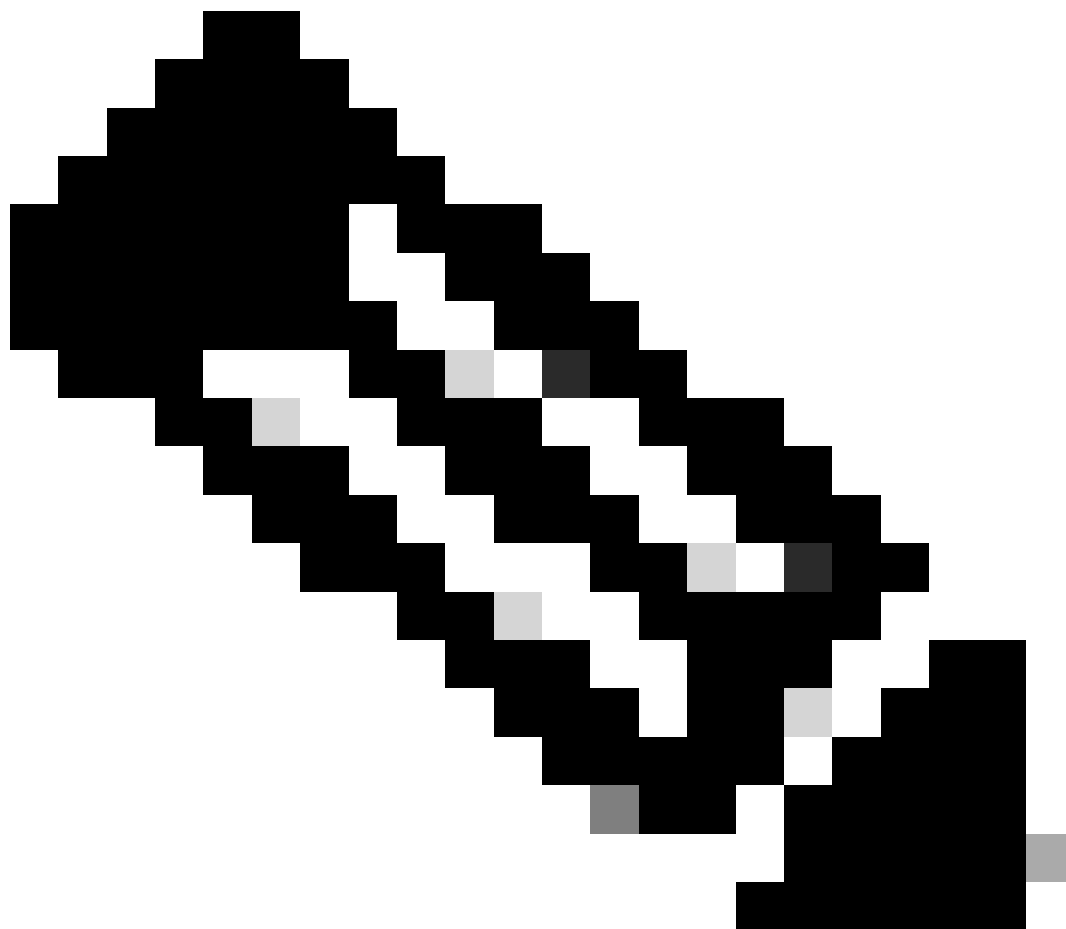
Template Name	Description	Key Type	Key Size	Curve Type
CA_SERVICE_Certificate_Template	This template will be used when ...	RSA	2048	N/A
EAP_Authentication_Certificate_Tem...	This template will be used to issue...	RSA	2048	N/A
pxGrid_Certificate_Template	This template will be used when ...	RSA	2048	N/A

3. Inserire i dettagli adatti alle esigenze specifiche dell'organizzazione.

The screenshot shows the 'Add Certificate Template' form in the Cisco Identity Services Engine (ISE) Administration / System page. The form fields are visible, including Name, Description, Subject, Common Name (CN), Organizational Unit (OU), Organization (O), City (L), State (ST), Country (C), Subject Alternative Name (SAN), Key Type, Key Size, SCEP RA Profile, Valid Period, and Extended Key Usage. The 'Add' button is highlighted with a red box.

* Name
Description
Subject
Common Name (CN) \$UserName\$
Organizational Unit (OU)
Organization (O)
City (L)
State (ST)
Country (C)
Subject Alternative Name (SAN) MAC Address
Key Type RSA
Key Size 2048
* SCEP RA Profile ISE Internal CA
Valid Period 3652 Day(s) (Valid Range 1 - 3652)
Extended Key Usage Client Authentication Server Authentication

4. Fare clic su Sottometti per salvare le modifiche.



Nota: Il modello di certificato può essere utile in scenari in cui sono presenti domini diversi e l'utente viene segmentato aggiungendo un valore diverso nell'unità organizzativa del certificato.

Mappare un profilo di endpoint al portale di provisioning client

1. Passare a Centri di lavoro > BYOD > Provisioning client > Criteri di provisioning client.
2. Fare clic su v in una delle regole per creare una nuova regola di provisioning client.

Identity Services Engine Work Centers / BYOD Evaluation Mode 63 Days

Overview Identities Identity Groups Network Devices Ext Id Sources **Client Provisioning** Portals & Components Policy Elements Policy Sets Reports More

Client Provisioning Policy Resources

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.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM64 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session as follows:
1 Session.OS-Architecture EQUALS arm64 , or
2 Cisco-av-pair EQUALS mdm-tlv=device-platform=win-arm64.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AnyConnect	If Any	and Windows All	and CiscoISE:ExternalGroups EQUALS ITSLMY:ITSLDomain.com/Users/Domain Users	then AnyConnect5.1
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
DownloadAnyConnect	If Any	and Windows All	and Condition(s)	then AnyConnect5.1

Actions: Duplicate above, Duplicate below, Insert new policy above, Insert new policy below, Delete

3. Contabilizzazione della creazione della nuova regola nella pagina

4. Aggiungere il gruppo di identità se si desidera limitare l'utilizzo del portale BYOD a determinati utenti

5. Aggiungere il sistema operativo che si desidera avere accesso al portale BYOD

6. Mappare la versione di Cisco IOS dall'elenco a discesa e selezionare anche il profilo dell'endpoint creato dal risultato

Identity Services Engine Work Centers / BYOD Evaluation Mode 63 Days

Overview Identities Identity Groups Network Devices Ext Id Sources **Client Provisioning** Portals & Components Policy Elements Policy Sets Reports More

Client Provisioning Policy Resources

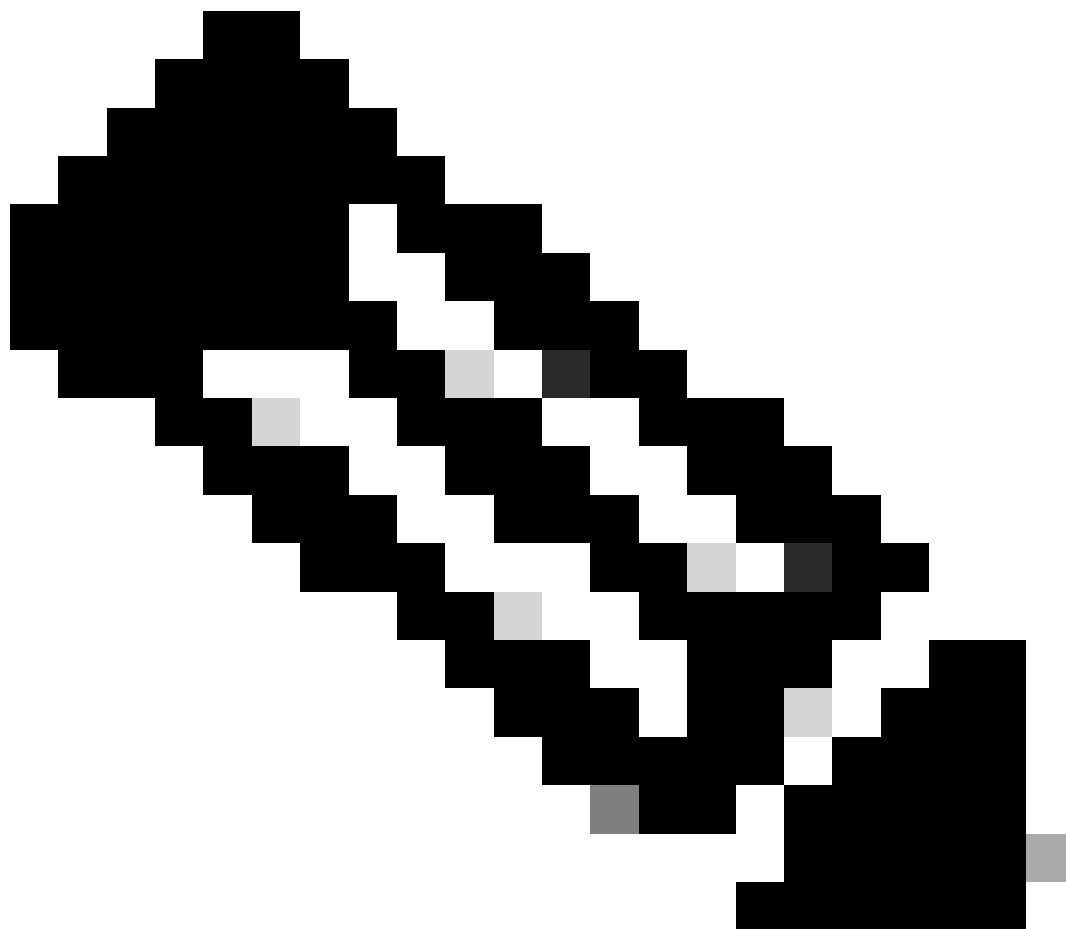
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.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

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM64 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session as follows:
1 Session.OS-Architecture EQUALS arm64 , or
2 Cisco-av-pair EQUALS mdm-tlv=device-platform=win-arm64.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AnyConnect	If Any	and Windows All	and CiscoISE:ExternalGroups EQUALS ITSLMY:ITSLDomain.com/Users/Domain Users	then AnyConnect5.1
BYOD	If Any +	and Windows All +	and Condition(s) +	then Result X Done
iOS	If Any	and Apple iOS All	and Condition(s)	then
Android	If Any	and Android	and Condition(s)	then

Agent Configuration: Choose an Agent, Is Upgrade Mandatory, Native Supplicant Configuration: WinSPWizard 3.2.0.1, Cisco-ISE-NSP

7. Fare clic su Fine, quindi sul pulsante Salva.



Nota: Questo criterio influisce sia sul provisioning del client di postura che sul provisioning BYOD, dove la sezione Configurazione agente determina l'agente di postura e il modulo di conformità applicati per i controlli di postura, mentre la sezione Configurazione richiedente nativo gestisce le impostazioni per i flussi di provisioning BYOD

Configurazione dei set di criteri ISE per Single SSID BYOD

1. Selezionare Policy > Policy Set (Policy > Set) e creare una policy per il flusso BYOD sull'ISE:

Policy Sets

Reset

Reset Policy Set Hit Counts

Save

 Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
 Search							
	BYOD		 Wireless_802.1X	Default Network Access	 	0	 
	Default	Default policy set		Default Network Access	 	0	 

Reset

Save

2. Passare quindi a Amministrazione > Gestione delle identità > Origini identità esterne > Profilo di autenticazione certificato. Fare clic sul pulsante Aggiungi per creare il profilo del certificato:

Identity Services Engine

Administration / Identity Management

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Identities

Groups

External Identity Sources

Identity Source Sequences

Settings

External Identity Sources

Certificate Authentic...

Active Directory

CiscoISE

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

REST

Certificate Authentication Profile

Edit

Add

Duplicate

Delete

Name	Description
Preloaded_Certificate_Profile	Precreated Certificate Authorization Profile.

Identity Services Engine

Administration / Identity Management

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Identities

Groups

External Identity Sources

Identity Source Sequences

Settings

External Identity Sources

Certificate Authentic...

Active Directory

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

REST

Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

* Name

BYOD

Description

Identity Store

[not applicable]

Use Identity From

Certificate Attribute

Subject - Common Nar

Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate in Identity Store

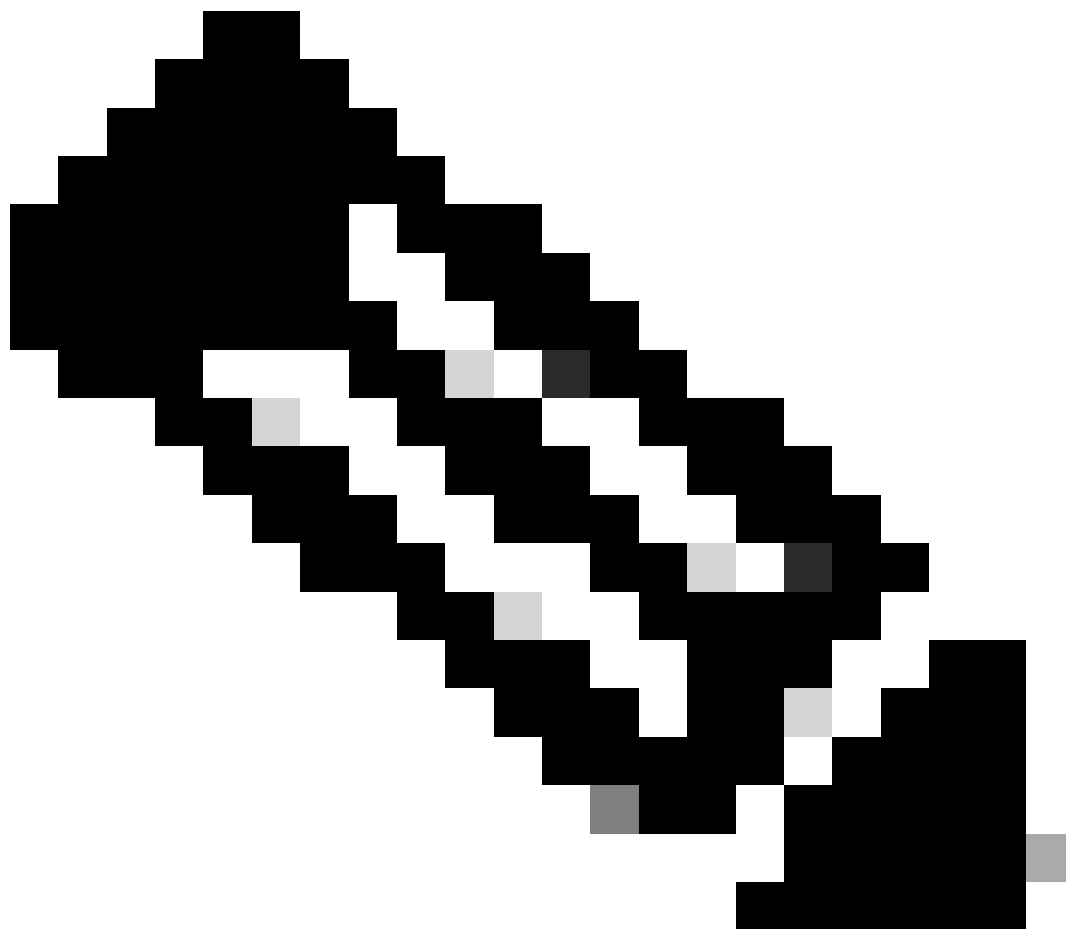
Never

Only to resolve identity ambiguity

Always perform binary comparison

Submit

Cancel



Nota: Nell'Identity Store è sempre possibile selezionare Active Directory integrato in ISE per eseguire una ricerca utente dal certificato per una maggiore sicurezza.

3. Fare clic su Sottometti per salvare la configurazione. Mappare quindi il profilo del certificato al criterio impostato per BYOD:

Policy Sets -> BYOD

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	BYOD		Wireless_B02.1X	Default Network Access	

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		BYOD	0	Options

> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
> Authorization Policy(1)

4. Configurare il profilo di autorizzazione per il reindirizzamento BYOD e l'accesso completo dopo il flusso BYOD. Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione.

5. Fare clic su Add (Aggiungi) e creare un profilo di autorizzazione. Controllare il reindirizzamento Web (CWA,MDM,NSP,CPP) ed eseguire il mapping della pagina del portale BYOD. Inoltre, aggiungere il nome ACL di reindirizzamento dal WLC al profilo. Per il profilo di accesso completo, configurare un'autorizzazione di accesso con la rispettiva VLAN aziendale nel profilo.

Policy / Policy Elements

External Identity Sources

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: BYOD-redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: ☐

Track Movement: ☐

Agentless Posture: ☐

Passive Identity Tracking: ☐

Common Tasks

☐ DACL Name

☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

☐ Security Group

☐ VLAN

☐ Voice Domain Permission

☒ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth: ACL Test1 Value: BYOD_CWA

☒ Display Certificates Renewal Message

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

6. Mappare il profilo di autorizzazione alla regola di autorizzazione. L'accesso completo BYOD deve avere la regola EndPoints·BYODRegistration uguale a yes in modo che l'utente ottenga l'accesso completo alla rete dopo il flusso BYOD.

Identity Services Engine Policy / Policy Sets Evaluation Mode 62 Days

Policy Sets → BYOD

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	BYOD		Wireless_802.1X	Default Network Access	0

> Authentication Policy(1)
 > Authorization Policy - Local Exceptions
 > Authorization Policy - Global Exceptions
 > Authorization Policy(3)

Status	Rule Name	Conditions	Results			
			Profiles	Security Groups	Hits	Actions
●	BYOD-Full access	AND EndPoints-BYODRegistration EQUALS Yes Network Access EapAuthentication EQUALS EAP-TLS Normalised Radius RadiusFlowType EQUALS Wireless802_1x	PermitAccess	Select from list	0	
●	BYOD-Redirection	AND Network Access EapAuthentication EQUALS EAP-MSCHAPv2 Normalised Radius RadiusFlowType EQUALS Wireless802_1x	BYOD-redirect	Select from list	0	
●	Default		DenyAccess	Select from list	0	

Configurazione dei set di criteri ISE per Dual SSID BYOD

Nella configurazione Dual SSID BYOD, il set di due regole è configurato su ISE. Il primo set di criteri è per il SSID aperto/non protetto, in cui la configurazione del set di criteri reindirizza l'utente alla pagina BYOD al momento della connessione al SSID aperto/non protetto

1. Selezionare Policy > Policy Set e creare una policy per il flusso BYOD sull'ISE.
2. Creare un set di criteri per SSID aperto/non protetto e SSID aziendale che autentichi l'utente BYOD registrato su ISE.

Policy Sets

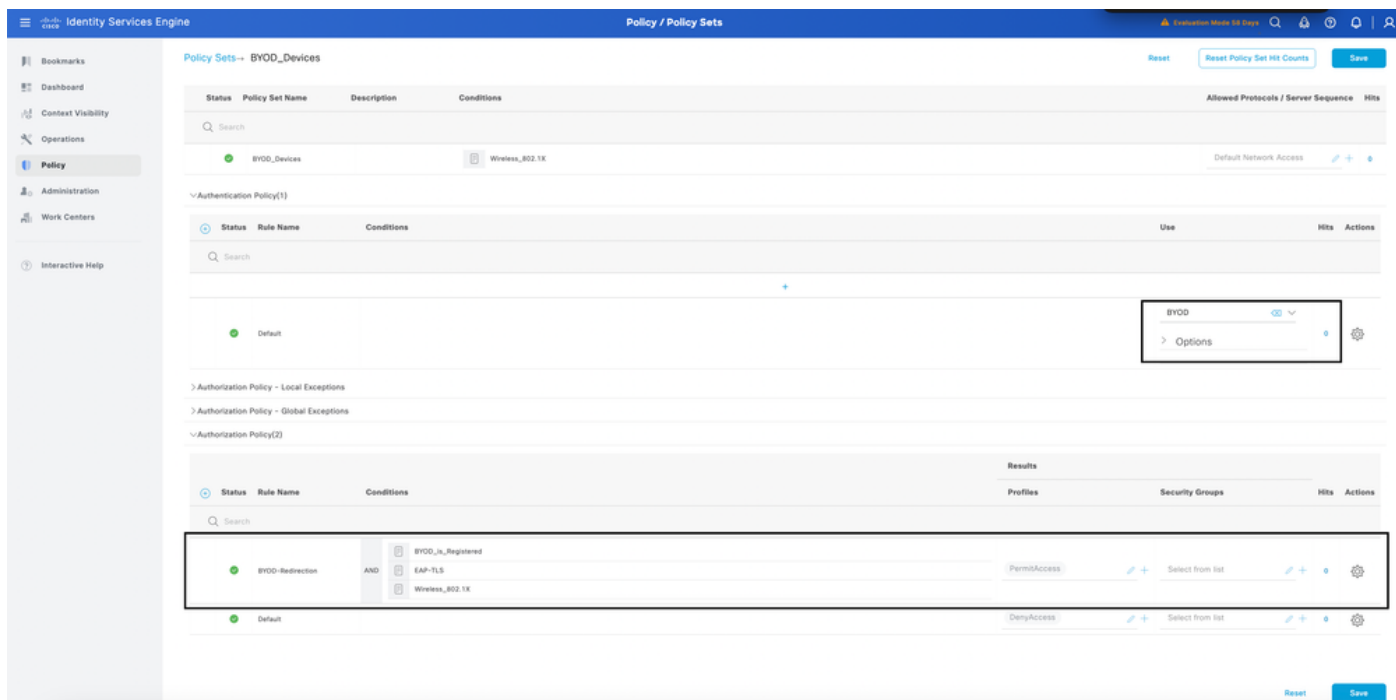
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	BYOD_Devices		Wireless_802.1X	Default Network Access	0		
●	Onboard_Personal_Devices		Wireless_MAB	Default Network Access	0		
●	Default	Default policy set		Default Network Access	0		

3. Nell'insieme di criteri di caricamento, trova Continua selezionato nelle opzioni. Per il criterio di autorizzazione, creare una condizione e mappare il profilo di autorizzazione di reindirizzamento. Gli stessi passaggi sono previsti per la creazione del profilo di autorizzazione, come indicato al punto 4.



4. Nel set di criteri registrati BYOD, configurare il criterio di autenticazione con il profilo del certificato trovato.

in Configure ISE Policy Sets for Single SSID BYOD al punto 2. Creare inoltre una condizione per il criterio di autorizzazione e mappare il profilo di accesso completo al criterio.



Registrazione

Dal live log di ISE, l'autenticazione utente avrà esito positivo e verrà reindirizzata alla pagina del portale BYOD. Dopo aver completato il flusso BYOD, all'utente viene concesso l'accesso alla rete

The screenshot shows the Cisco BYOD Portal interface. At the top, there is a header with the Cisco logo on the left, 'BYOD Portal' in the center, and 'test' with a user icon on the right. Below the header, a progress indicator shows two steps: step 2 is active and highlighted with a blue circle, and step 3 is shown as a plain circle. The main content area is titled 'Device Information' and contains the instruction: 'Enter the device name and optional description for this device so you can manage it using the My Devices Portal.' There are three input fields: 'Device name: *' (required), 'Description:', and 'Device ID:'. The 'Device ID' field contains a masked value represented by black dots. At the bottom of the form is a blue 'Continue' button with a right-pointing arrow.

Indica che all'utente verrà richiesto di scaricare lo strumento Network Assistant per il download del profilo dell'endpoint e del certificato EAP TLS per l'autenticazione se il profilo è configurato per eseguire l'autenticazione EAP-TLS

The screenshot shows the Cisco BYOD Portal interface at the 'Install' step. The header is identical to the previous screenshot. The progress indicator now shows step 3 as the active step, highlighted with a blue circle. The main content area is titled 'Install' and contains the instruction: 'Please wait while we download the Cisco Network Setup Assistant. You will then need to manually run the Setup Assistant and follow the instructions to finish registering this device.'

Eseguire l'applicazione Network Assistant con privilegi di amministratore e fare clic sul pulsante Start per avviare il flusso di caricamento:



Network Setup Assistant

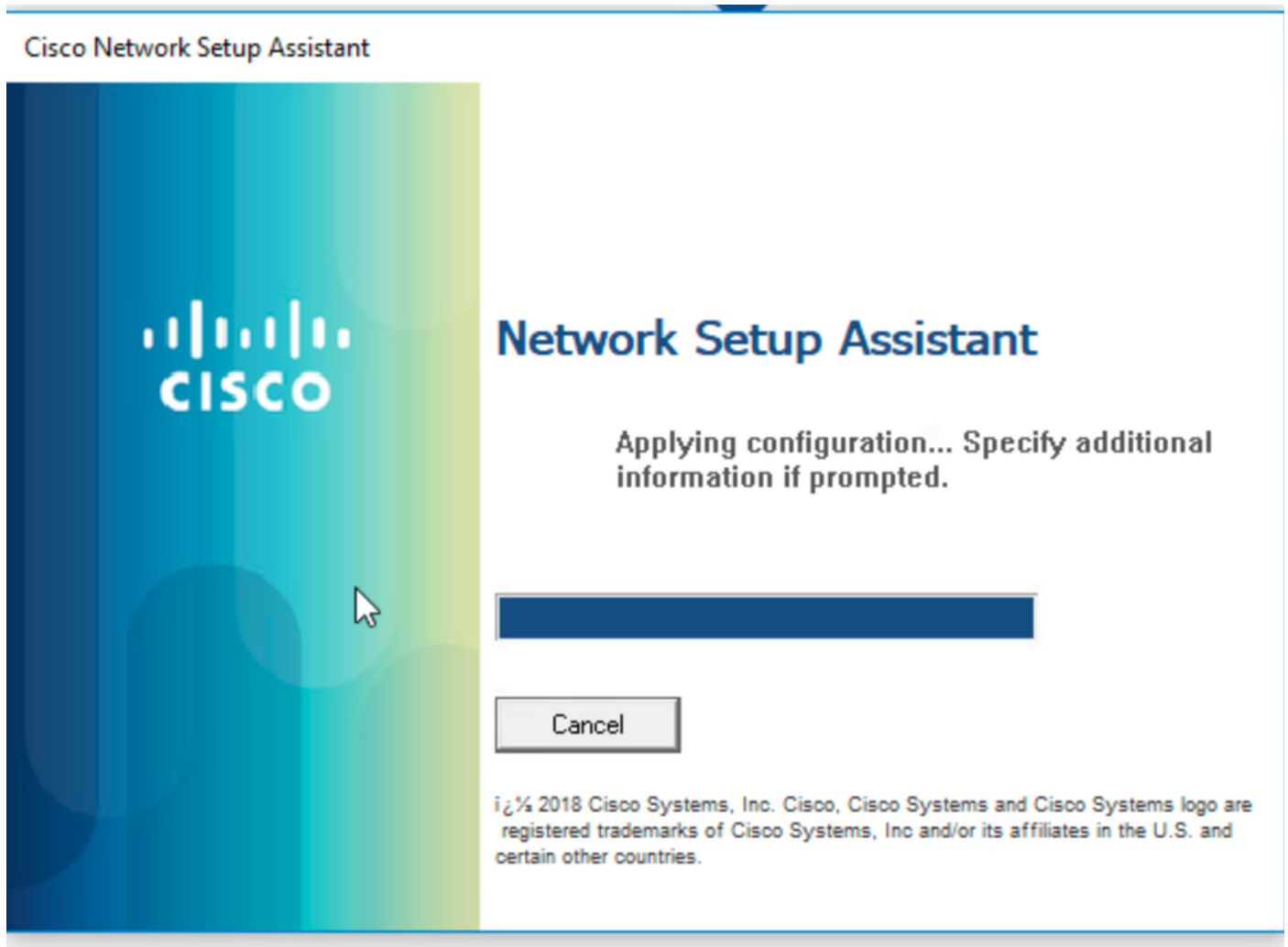


This application automatically configures network settings.

Start

Quit

© 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



L'utente è stato correttamente connesso alla rete con il proprio dispositivo personale per accedere alle risorse.

Risoluzione dei problemi

Per risolvere il problema con BYOD, abilitare il debug su ISE

Attributi da impostare sul livello di debug:

- client (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (prt-server.log)
- nsf (ise-psc.log)
- sessione nsf (ise-psc.log)
- profiler (profiler.log)

Frammento di log

Log Guest

Questi log indicano che l'utente ha eseguito correttamente il reindirizzamento alla pagina e ha scaricato l'applicazione Network Assistant:

```
2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D555:::-
percorso di mapping trovato in azione-inoltro, inoltro a: pages/byodWelcome.jsp // Pagina iniziale
BYOD
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test: di
pTransSteps:1
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:
NextFlowStep, pTransSteps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:
NextFlowStep, stepTran:d2513b7b-7249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:::-
percorso di mapping trovato in inoltri azione, inoltro a: pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test: di
pTransSteps:1
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:
NextFlowStep, pTransSteps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:
NextFlowStep, stepTran:f203b757-9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:::-
percorso di mapping trovato in inoltri azione, inoltro a: pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5::: Session = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5::: portalSessionId
= null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5:::-
StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-
bbb91e8828da/NetworkSetupAssistant.exe // L'applicazione Assistenza di rete è stata inviata
all'endpoint
```

Registri Ise-Psc

Quando l'applicazione viene scaricata sull'endpoint, l'applicazione avvia un flusso SCEP per ottenere il certificato client da ISE.

```
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- CertStore contiene 4 certificati:
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1. '[issuer=CN=Certificate Services Root CA - iseguest;
serial=32281512738768960628252532784663302089]'
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 2. '[issuer=CN=Certificate Services Endpoint Sub CA -
iseguest; serial=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 3. '[issuer=CN=Certificate Services Root CA - iseguest;
serial=68627620160586308685849818775100698224]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 4. '[issuer=CN=Certificate Services Node CA - iseguest;
serial=72934767698603097153932482227548874953]'
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selezione del certificato di crittografia
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selezione del certificato con chiaveEncipherment
keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Trovato 1 certificato/i con chiaveEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Utilizzando [issuer=CN=Certificate Services Endpoint Sub
CA - iseguest; serial=131900858749761727853768227590303808637] per la crittografia dei
messaggi
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selezione del certificato del verificatore
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selezione del certificato con la chiave
digitalSignatureUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Trovato 1 certificato/i con chiave digitalSignatureUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Utilizzando [issuer=CN=Certificate Services Endpoint Sub
CA - iseguest; serial=131900858749761727853768227590303808637] per la verifica dei messaggi
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selezione del certificato emittente
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selezione di un certificato con BasicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
```

org.jscep.client.CertStoreInspector -::::- Trovati 3 certificati con BasicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Utilizzando [issuer=CN=Certificate Services Endpoint Sub
CA - iseguest; serial=131900858749761727853768227590303808637] per l'emittente
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- Metriche delle prestazioni dei server SCEP :
name[attivo/inattivo, richieste totali, errori totali, richieste in esecuzione, RTT medio]
<http://127.0.0.1:9444/caservice/scep/live,96444,1,0,120>

Download profilo endpoint

Dopo il completamento del processo SCEP e l'installazione del certificato da parte dell'endpoint, l'applicazione scarica il profilo dell'endpoint per l'autenticazione futura che verrà eseguita dal dispositivo:

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Riferimento = Windows // È stato rilevato il
dispositivo Windows in base alla pagina Web
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Sessione = 0000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Sessione = 0000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- provisioning profilo nsp
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Sessione = 0000000000000000B30D59CC5
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionId = null
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- StreamingServlet
URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-
NSP.xml//Il profilo NSP viene scaricato sull'endpoint
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Streaming su ip: tipo di file: Nome file
NativeSPProfile:Cisco-ISE-NSP.xml //Applicazione Network Assistant
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- userId è stato impostato su test
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- tipo di reindirizzamento: SUCCESS_PAGE,
URL di reindirizzamento: per mac:

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).