

Configuración de ISE BYOD con SSID único y dual en ISE 3.3

Contenido

[Introducción](#)

[Background](#)

[Prerequisites](#)

[Componente utilizado](#)

[¿Qué es BYOD con SSID único y SSID dual en ISE?](#)

[BYOD con SSID único](#)

[BYOD SSID dual](#)

[Configuración de WLC](#)

[Creación de una WLAN para CWA](#)

[Configure los servidores RADIUS](#)

[Configuración de servidores AAA](#)

[Configuración de las políticas de seguridad para la WLAN](#)

[Configurar ACL de autenticación previa](#)

[Configurar perfil de directiva](#)

[Aplicación de etiquetas e implementación](#)

[Configuración de un SSID abierto/no seguro](#)

[Configuración de ISE](#)

[Requisitos previos](#)

[Certificados](#)

[Configuración de DNS](#)

[Configuración del dispositivo de red ISE](#)

[Creación de un portal BYOD](#)

[Descargar la última versión de Cisco IOS®](#)

[Crear un perfil de terminal](#)

[Plantilla de certificado](#)

[Asignar un perfil de terminal al portal de aprovisionamiento de clientes](#)

[Configuración de conjuntos de políticas de ISE para BYOD con SSID único](#)

[Configuración de conjuntos de políticas de ISE para BYOD SSID dual](#)

[Resolución de problemas](#)

[Fragmento de registro](#)

[Registros de invitados](#)

[Registros De Ise-Psc](#)

[Descarga de perfiles de terminales](#)

Introducción

El documento describe cómo configurar y solucionar problemas de BYOD en ISE.

Background

BYOD es una función que permite al usuario incorporar sus dispositivos personales en ISE para que el usuario pueda utilizar los recursos de red del entorno. También ayuda al administrador de red a restringir el acceso del usuario al recurso crítico desde los dispositivos personales.

A diferencia del flujo de invitados, en el que el dispositivo se autentica con la página Invitado mediante el almacén interno o Active Directory en ISE. BYOD permite al administrador de red instalar un perfil de terminal en el terminal para elegir el tipo de método EAP. En escenarios como EAP-TLS, el certificado de cliente está firmado por el propio ISE para crear una relación de confianza entre el terminal e ISE.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- controlador WLC
- Conocimientos básicos sobre ISE

Componente utilizado

Estos dispositivos no se limitan a una versión concreta para el flujo de BYOD:

- Controlador inalámbrico Catalyst 9800-CL (17.12.3)
- Máquina virtual ISE (3.3)

¿Qué es BYOD con SSID único y SSID dual en ISE?

BYOD con SSID único

En una configuración BYOD con un solo SSID, los usuarios conectan sus dispositivos personales directamente a la red inalámbrica corporativa. El proceso de incorporación se produce en el mismo SSID, donde ISE facilita el registro de dispositivos, el aprovisionamiento y la aplicación de políticas. Este enfoque simplifica la experiencia del usuario, pero requiere una incorporación segura y métodos de autenticación adecuados para garantizar la seguridad de la red.

BYOD SSID dual

En una configuración BYOD con SSID dual, se utilizan dos SSID independientes: una para la incorporación (acceso no seguro o restringido) y otra para el acceso a la red corporativa. Los usuarios se conectan inicialmente al SSID incorporado, finalizan el registro y el aprovisionamiento de dispositivos mediante ISE y, a continuación, cambian al SSID corporativo seguro para acceder

a la red. Esto proporciona una capa adicional de seguridad al segregar el tráfico de incorporación del tráfico de producción.

Configuración de WLC

Creación de una WLAN para CWA

1. Vaya a Configuration > Tags & Profiles > WLANs.
2. Haga clic en Add para crear una nueva WLAN.
 - Establezca un nombre de WLAN y un SSID (por ejemplo, BYOD-WiFi).
 - Active la WLAN.

Add WLAN

General

Security

Advanced

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

Configure los servidores RADIUS

1. Vaya a Configuration > Security > AAA > RADIUS > Servers.

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

[+ Add](#) [- Delete](#)

RADIUS

TACACS+

LDAP

Servers Server Groups

Acct Port "Contains" 1814 x				
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. Haga clic en Agregar para configurar ISE como servidor RADIUS:

- IP del servidor: Dirección IP de ISE.
- secreto compartido: Coincida con el secreto compartido configurado en ISE.

Create AAA Radius Server

Name* BYOD

Support for CoA ⓘ

ENABLED

Server Address* 10.x.x.x

CoA Server Key Type

Clear Text

PAC Key ☐

CoA Server Key ⓘ

Key Type Clear Text

Confirm CoA Server Key

Key* ⓘ *****

Automate Tester

☐

Confirm Key* *****

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

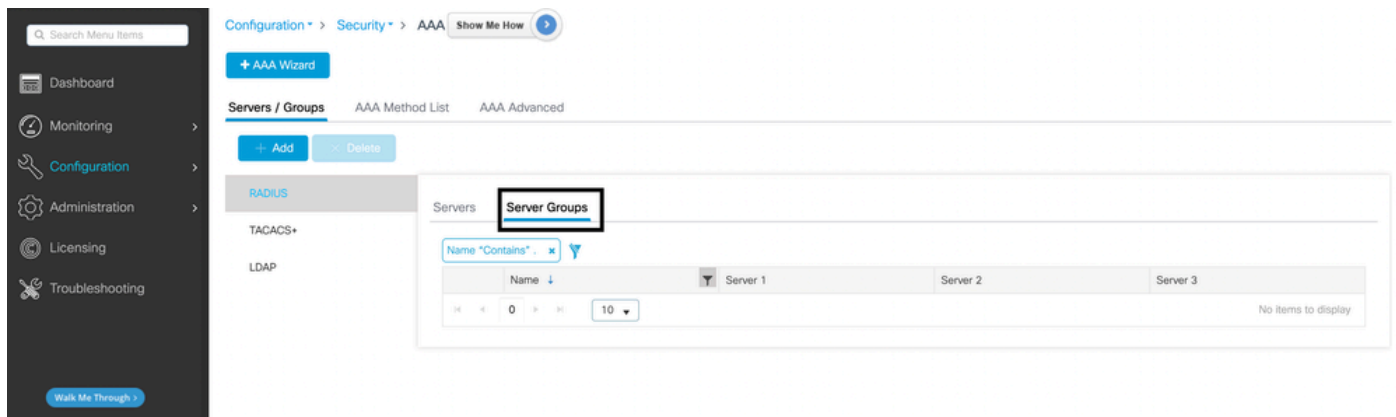
Retry Count 0-100

[Cancel](#)

[Apply to Device](#)

Configuración de servidores AAA

1. Vaya a Configuration > Security > AAA > Servers/Groups.



2. Asigne el servidor RADIUS a un grupo de servidores nuevo o existente.

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

Configuración de las políticas de seguridad para la WLAN

1. Vaya a Configuration > Tags & Profiles > WLANs. Edite la WLAN creada anteriormente.
2. En la pestaña Security > Layer 2:
 - Activar WPA+WPA2
 - Establecer AES (CCMP128) con encriptación WPA2
 - Gestión de claves de autenticación como 802.1X

⚠ 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. En la pestaña Security > Layer 3, seleccione global en el menú desplegable para Web Auth Parameter Map.

Edit WLAN

⌵

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

GeneralSecurityAdvancedAdd To Policy Tags

Layer2Layer3AAA

Web Policy☐

Show Advanced Settings >>>

Web Auth Parameter Mapglobal

Authentication ListSelect 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

Configurar ACL de autenticación previa

Cree una lista de control de acceso para permitirUtilice acciones para la redirección:

- Tráfico DNS.
- HTTP/HTTPS al portal de ISE.
- Cualquier servicio backend necesario.

Para ello:

1. Vaya a Configuration > Security > ACL > Access Control Lists.
2. Cree una nueva ACL con reglas para permitir el tráfico necesario.

Edit ACL

×

ACL Name*

Test1

ACL Type

IPv4 Extended

Rules

Sequence*

Action

permit

Source Type

any

Destination Type

any

Protocol

ahp

Log

☐

DSCP

None

+ Add

× Delete

	Sequence ↑	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
☐	10	deny	ISE-IP-Address		any		ip	None	None	None	Disabled
☐	20	deny	any		ISE-IP-Address		ip	None	None	None	Disabled
☐	30	deny	any		any		udp	None	eq domain	None	Disabled
☐	40	deny	any		any		udp	eq domain	None	None	Disabled
☐	50	permit	any		any		tcp	None	eq www	None	Disabled

⏮

⏪

1

⏩

⏭

10

1 - 5 of 5 items

↶ Cancel

📄 Apply to Device

Configurar perfil de directiva

1. Vaya a Configuration > Tags & Profiles > Policy. Puede crear o utilizar la directiva predeterminada

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The breadcrumb trail is Configuration > Tags & Profiles > Policy. The page displays a table of policy profiles. The first row is 'default-policy-profile' with a description of 'default policy profile'. The table has columns for Admin Status, Associated Policy Tags, Policy Profile Name, and Description. The page also includes a sidebar with navigation options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting.

Admin Status	Associated Policy Tags	Policy Profile Name	Description
		default-policy-profile	default policy profile

1 - 1 of 1 items

- ## 2. Asigne la VLAN adecuada en Políticas de acceso

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

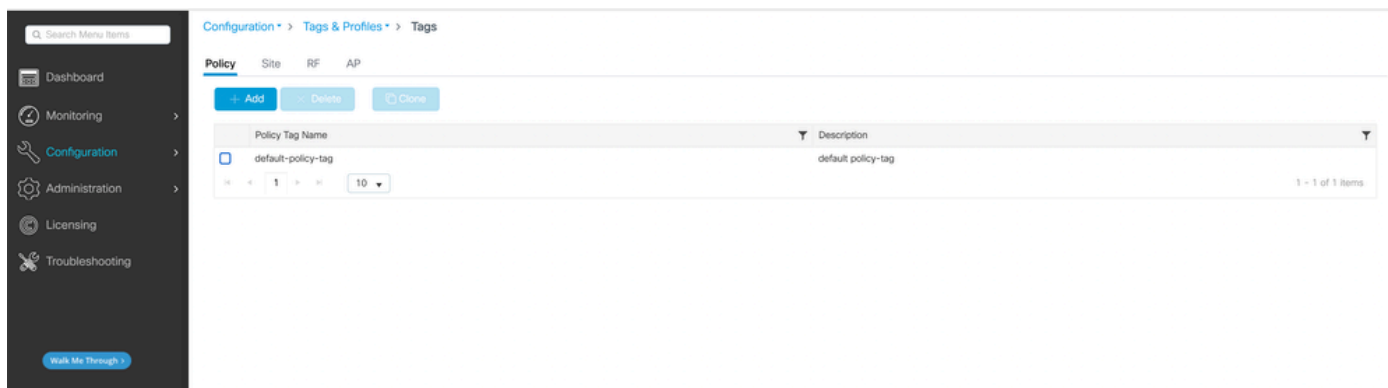
▼

🔗

↶ Cancel

📁 Update & Apply to Device

3. Habilite también Allow AAA Override y NAC state bajo Advanced de la política.



Configuración de un SSID abierto/no seguro

El SSID abierto solo se crea cuando decide tener una configuración BYOD SSID dual en su entorno.

1. Vaya a Configuration > Tags & Profiles > WLANs. 'Haga clic en el botón Add (Agregar).'
2. Proporcione un nombre SSID en la ficha General (General) y active el botón 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 Policy802.11b/g

Cancel

Apply to Device

3. Haga clic en la pestaña Seguridad desde la misma ventana. Seleccione el botón de opción None y active el filtrado de Mac.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. Under the 'Layer2' sub-tab, the 'None' radio button for security is selected. The 'MAC Filtering' checkbox is checked and highlighted with a black box. Other settings include 'Authorization List*' set to 'default', 'OWE Transition Mode' checked, 'Transition Mode WLAN ID*' set to '0-4096', and 'Lobby Admin Access' unchecked. A 'Fast Transition' section is also visible with 'Status' set to 'Disabled', 'Over the DS' unchecked, and 'Reassociation Timeout *' set to '20'. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

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. En Capa 3 bajo Seguridad, seleccione la configuración global para Web Auth Parameter Map. Si tiene cualquier otro perfil de autenticación web configurado en el WLC, también puede asignarlo aquí:

Add WLAN

General

Security

Advanced

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

Apply to Device

Configuración de ISE

Requisitos previos

- Asegúrese de que Cisco ISE está instalado y cuenta con licencia para la funcionalidad BYOD.
- Agregue su WLC a ISE como un dispositivo de red con el secreto compartido RADIUS.

Certificados

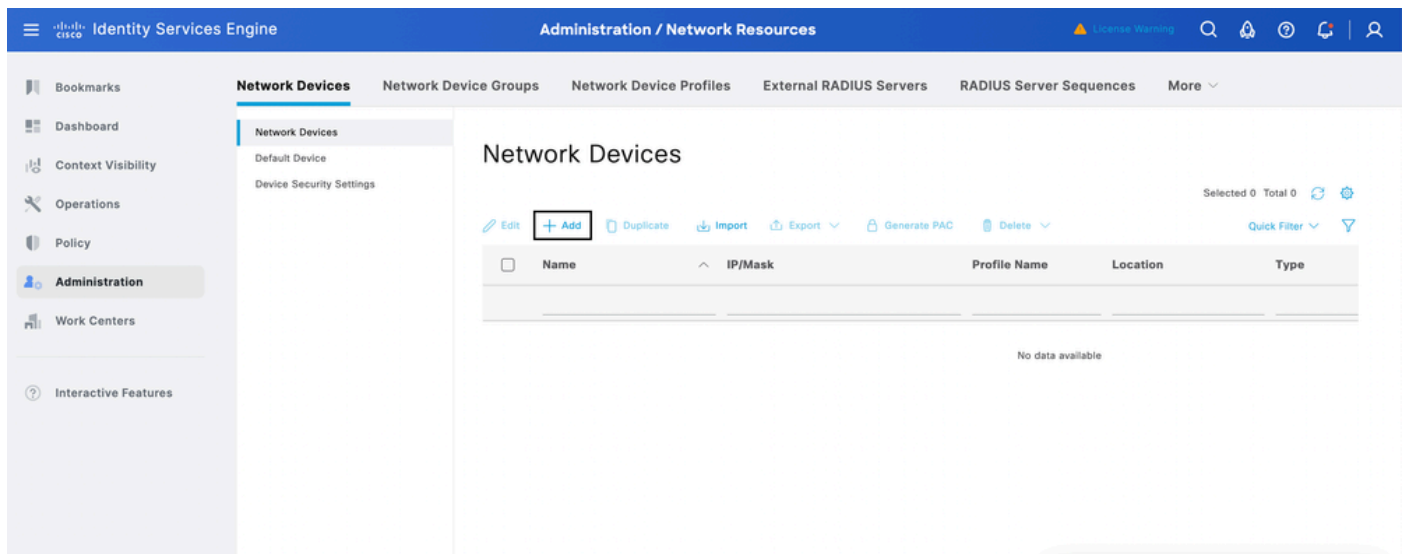
- Instale un certificado de servidor válido en ISE para evitar las advertencias de seguridad del navegador.
- Asegúrese de que los extremos confían en el certificado (firmado por una CA conocida o una CA interna con raíz de confianza).

Configuración de DNS

- Asegúrese de que DNS resuelva el nombre de host de ISE para el portal BYOD.

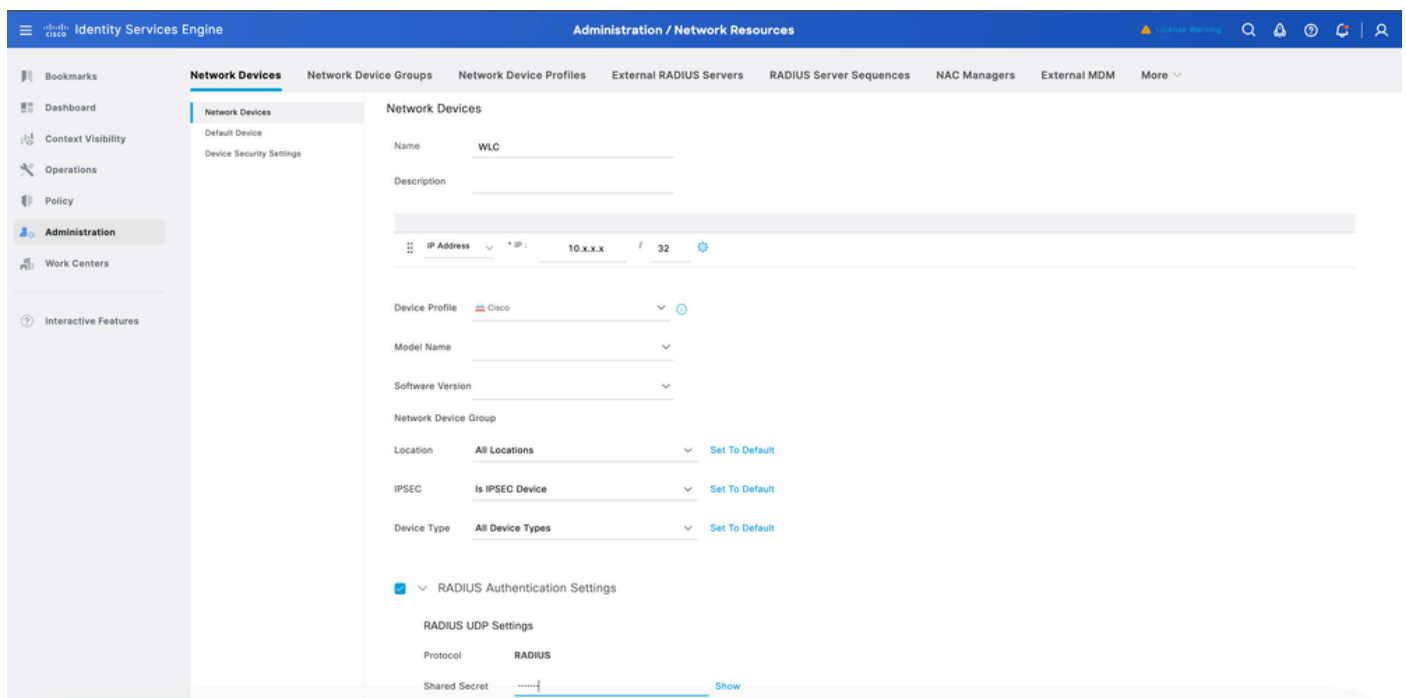
Configuración del dispositivo de red ISE

1. Inicie sesión en la interfaz de usuario web de ISE.
2. Vaya a Administration > Network Resources > Network Devices.



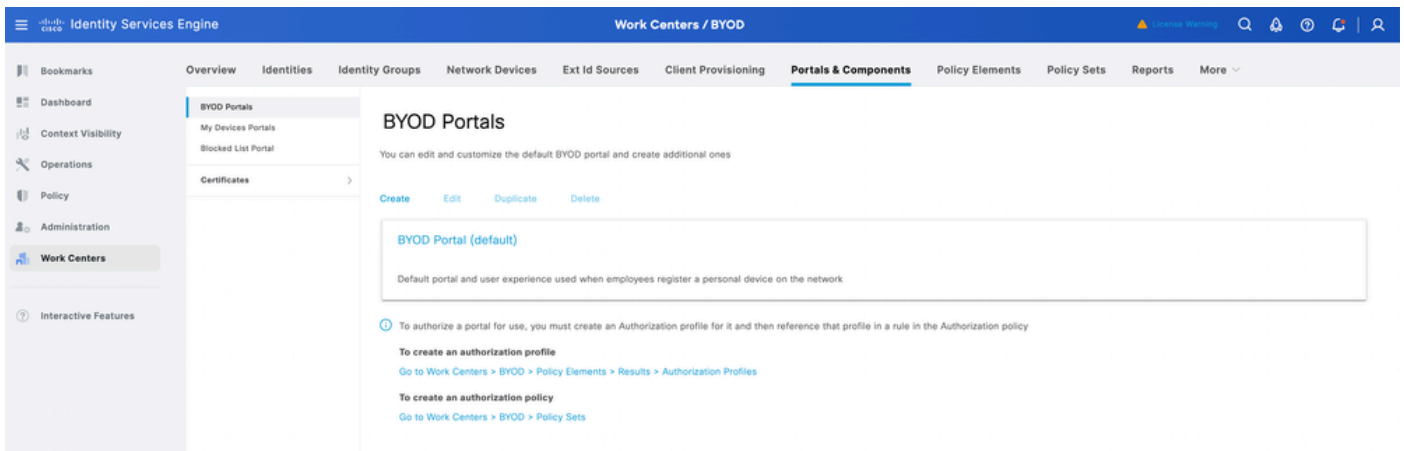
3. Add su WLC como dispositivo de red:

- Nombre: Introduzca un nombre para el WLC.
- IP Address: Introduzca la IP de administración del WLC.
- Secreto compartido RADIUS: Ingrese el mismo secreto compartido que se configuró en el WLC.
- Haga clic en Submit (Enviar).



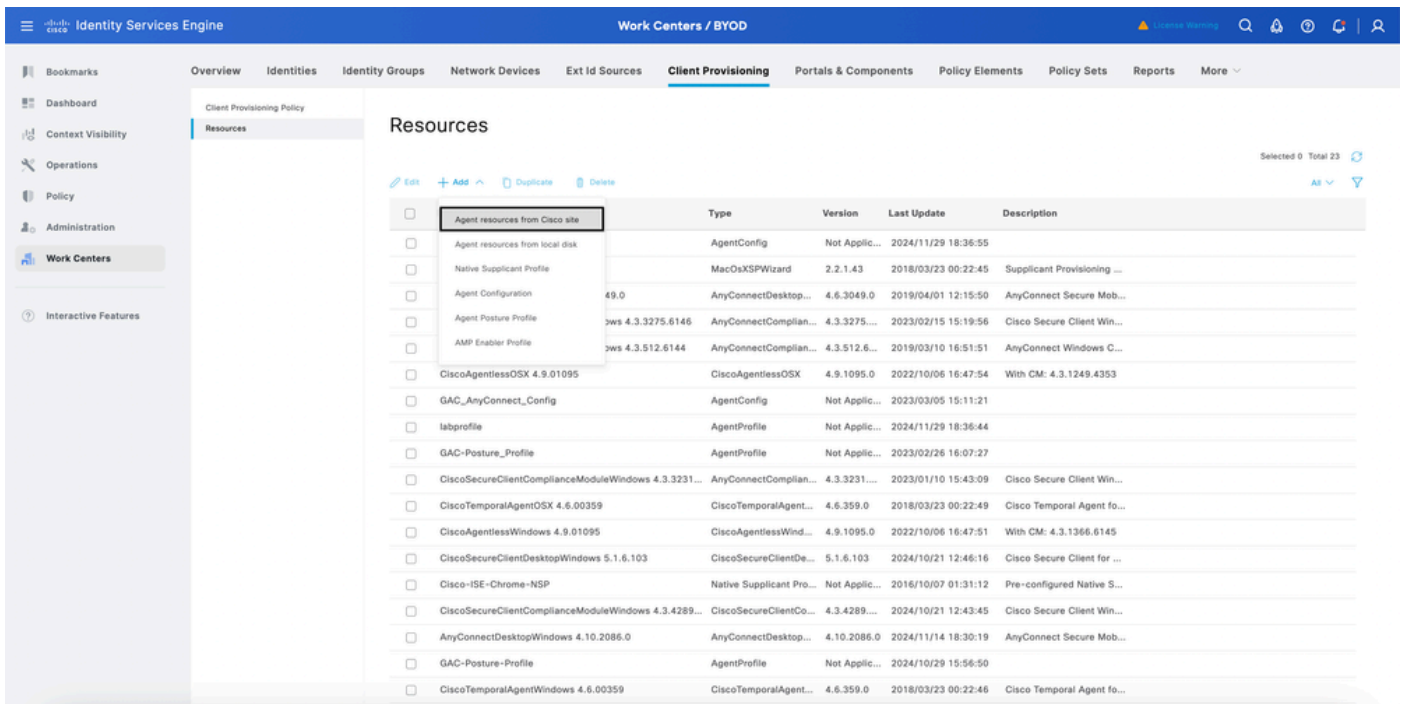
Creación de un portal BYOD

1. Vaya a Centros de trabajo > BYOD > Configuración > Portales y componentes > Portales BYOD.
2. Haga clic en Agregar para crear un portal BYOD o puede utilizar el portal predeterminado existente en ISE.



Descargar la última versión de Cisco IOS®

1. Vaya a Centros de trabajo > BYOD > Aprovisionamiento de clientes > Recursos.
2. Haga clic en el botón Add y seleccione los recursos de agente del sitio de Cisco.



3. En la lista de software, seleccione la última versión de Cisco IOS que se descargará.



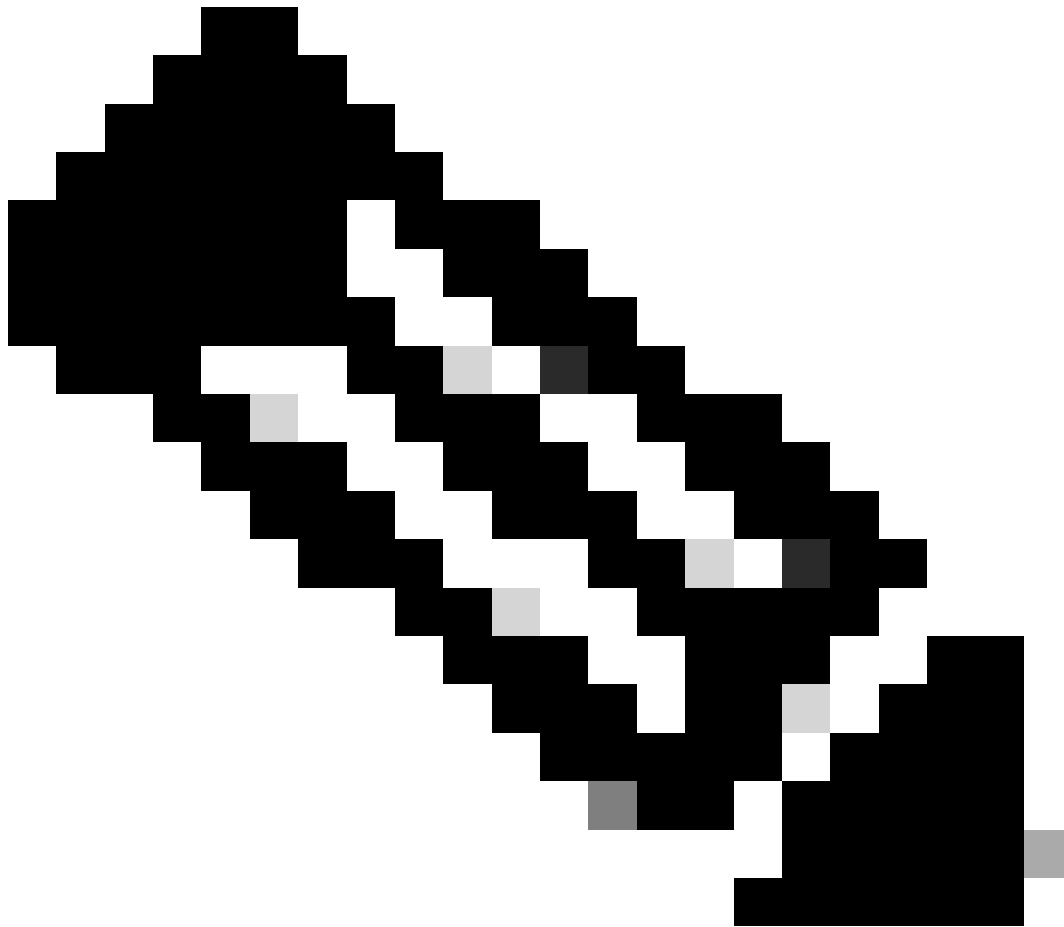
Download Remote Resources

☐	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

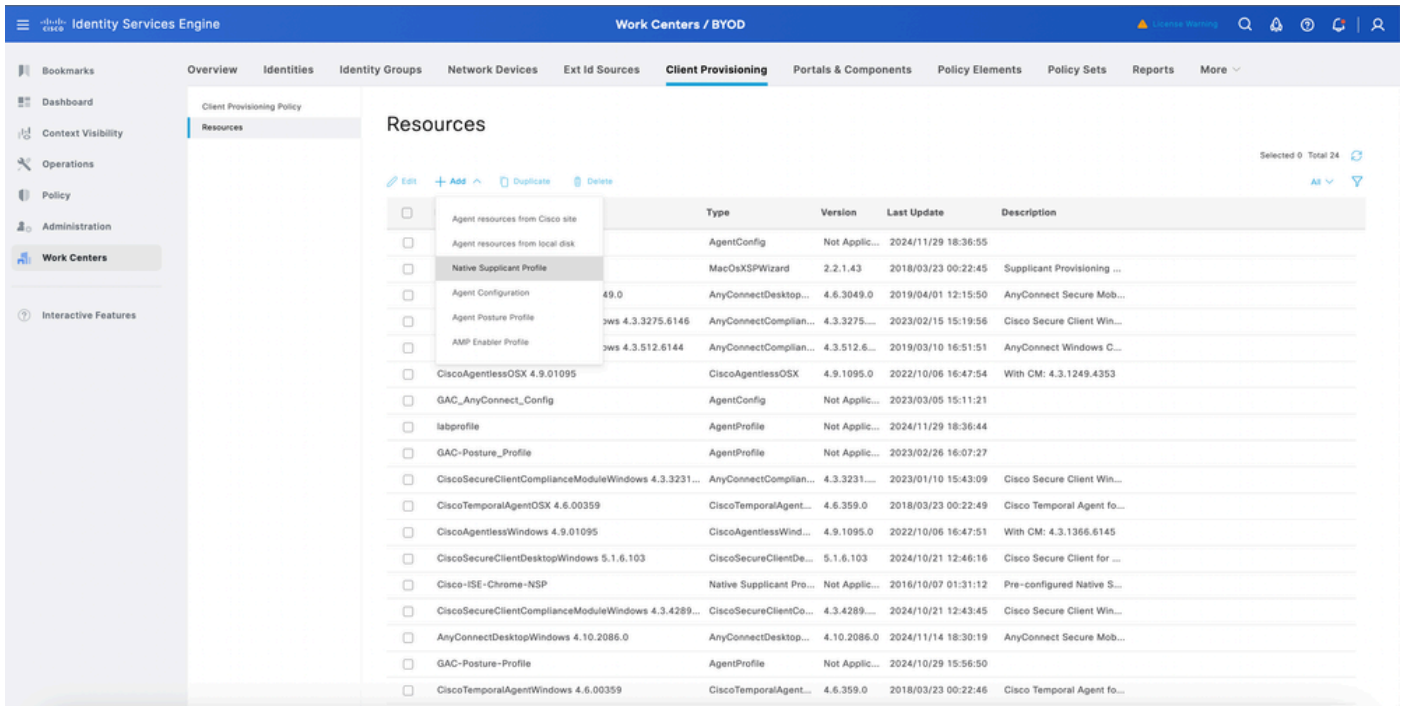
Save



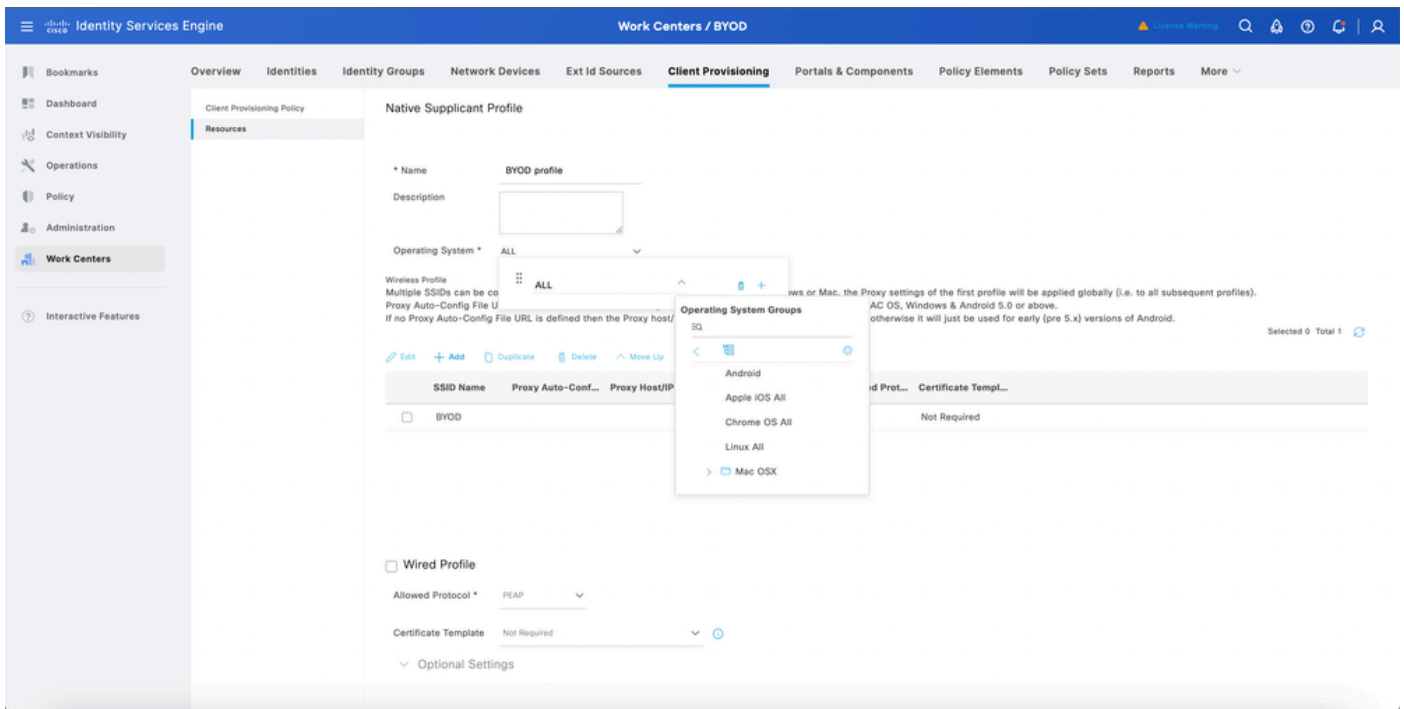
Nota: El software Cisco IOS se descarga en ISE para terminales Windows y MacOS. Para Apple iPhone IOS, utiliza un suplicante nativo para aprovisionar el dispositivo y para el dispositivo Android, tiene un asistente de configuración de red que debe descargarse de Play Store.

Crear un perfil de terminal

1. Vaya a Centros de trabajo > BYOD > Aprovisionamiento de clientes > Recursos.
2. Haga clic en Agregar, seleccione Perfil de solicitante nativo en el menú desplegable.



3. En el menú desplegable Sistema operativo, seleccione el sistema operativo requerido que desea incorporar al dispositivo o puede configurarlo como ALL (TODOS) para incorporar todos los terminales de su entorno:



4. Haga clic en Agregar en la página para crear el perfil de terminal para configurar 802.1X para el terminal:

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](#)

En función de sus necesidades, configure el perfil de terminal para el terminal de su entorno. El perfil de terminales nos permite configurar EAP-PEAP, EAP-TLS.

5. Haga clic en Guardar y, a continuación, en Enviar en el perfil de terminal.

Plantilla de certificado

El perfil de terminal está preconfigurado para realizar EAP-TLS. Se debe agregar una plantilla de certificado al perfil. De forma predeterminada, ISE tiene dos plantillas predefinidas que se pueden seleccionar en el menú desplegable.

The screenshot shows the 'Wireless Profile(s)' configuration page. The 'Certificate Template' dropdown is open, displaying two options: 'EAP_Authentication_Certificate_Template' (highlighted) and 'pxGrid_Certificate_Template'. The 'Save' button is located at the bottom right of the form.

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	

Para crear una nueva plantilla de certificado, siga estos pasos:

1. Vaya a Administration > System > Certificates > Certificate Authority > Certificate Templates.
2. Haga clic en el botón Agregar de la página.

Identity Services Engine Administration / System Evaluation Mode 62 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Bookmarks Dashboard Context Visibility Operations Policy **Administration** Work Centers Interactive Help

Certificate Management Certificate Authority Overview Issued Certificates Certificate Authority Certificates Internal CA Settings **Certificate Templates** External CA Settings

Certificate Templates

Edit **+ Add** Duplicate Delete

☐	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 issu...	RSA	2048	N/A
☐	pxGrid_Certificate_Template	This template will be used when ...	RSA	2048	N/A

3. Rellene los datos personalizados para satisfacer los requisitos específicos de su organización.

Identity Services Engine Administration / System Evaluation Mode 62 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Bookmarks Dashboard Context Visibility Operations Policy **Administration** Work Centers Interactive Help

Certificate Management Certificate Authority Overview Issued Certificates Certificate Authority Certificates Internal CA Settings **Certificate Templates** External CA Settings

Add Certificate Template

* 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 ▾

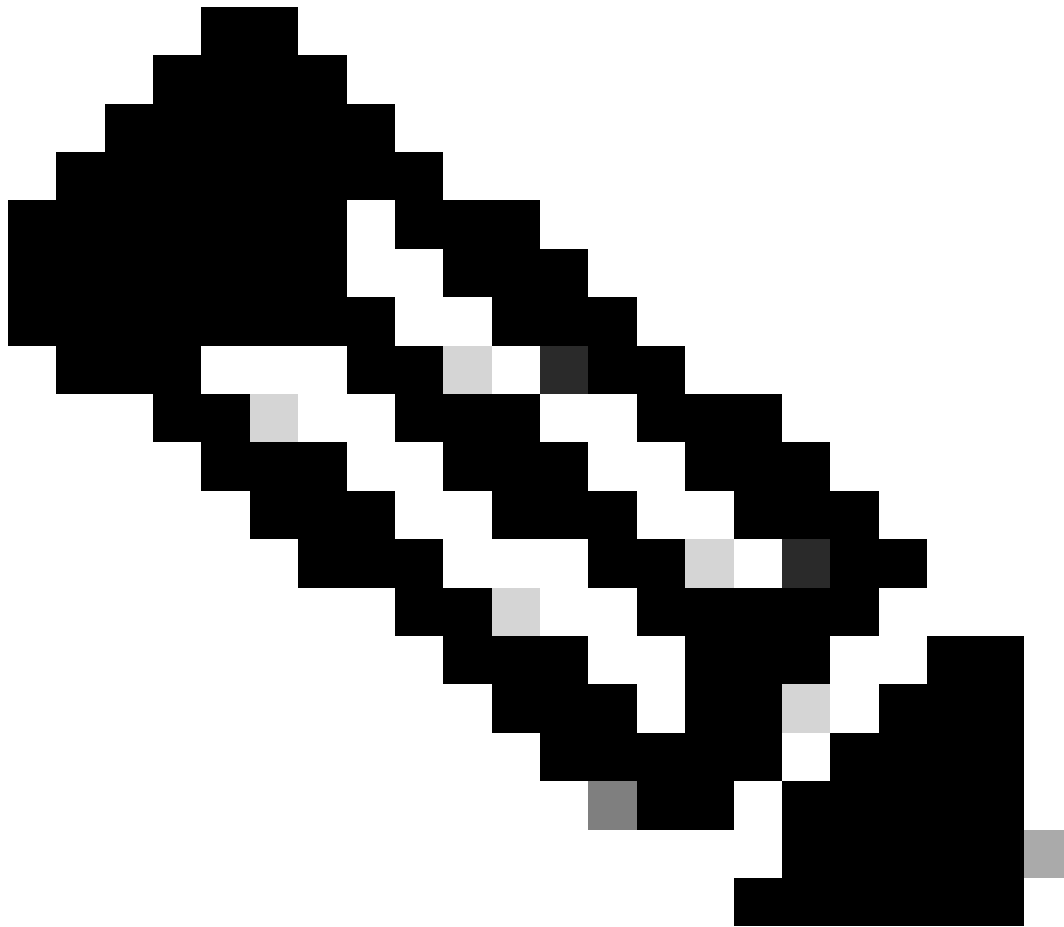
* SCEP RA Profile ISE Internal CA ▾

Valid Period 3652 Day(s) (Valid Range 1 - 3652)

Extended Key Usage ☒ Client Authentication ☐ Server Authentication

Submit Cancel

4. Haga clic en Enviar para guardar los cambios.



Nota: La plantilla de certificado podría ser útil en situaciones en las que tiene diferentes dominios y segmenta al usuario agregando un valor diferente en la unidad organizativa del certificado.

Asignar un perfil de terminal al portal de aprovisionamiento de clientes

1. Vaya a Centros de trabajo > BYOD > Aprovisionamiento de clientes > Política de aprovisionamiento de clientes.
2. Haga clic en **v** en de las reglas para crear una nueva regla de aprovisionamiento de cliente.

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.

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

3. Contabilizar la creación de la nueva regla en la página

4. Agregue el grupo de identidad si desea restringir el uso del portal BYOD por parte de determinados usuarios

5. Agregue el sistema operativo al que desea tener acceso en el portal BYOD

6. Asigne la versión de Cisco IOS de la lista desplegable y también seleccione el perfil de terminal que ha creado a partir del resultado

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.

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

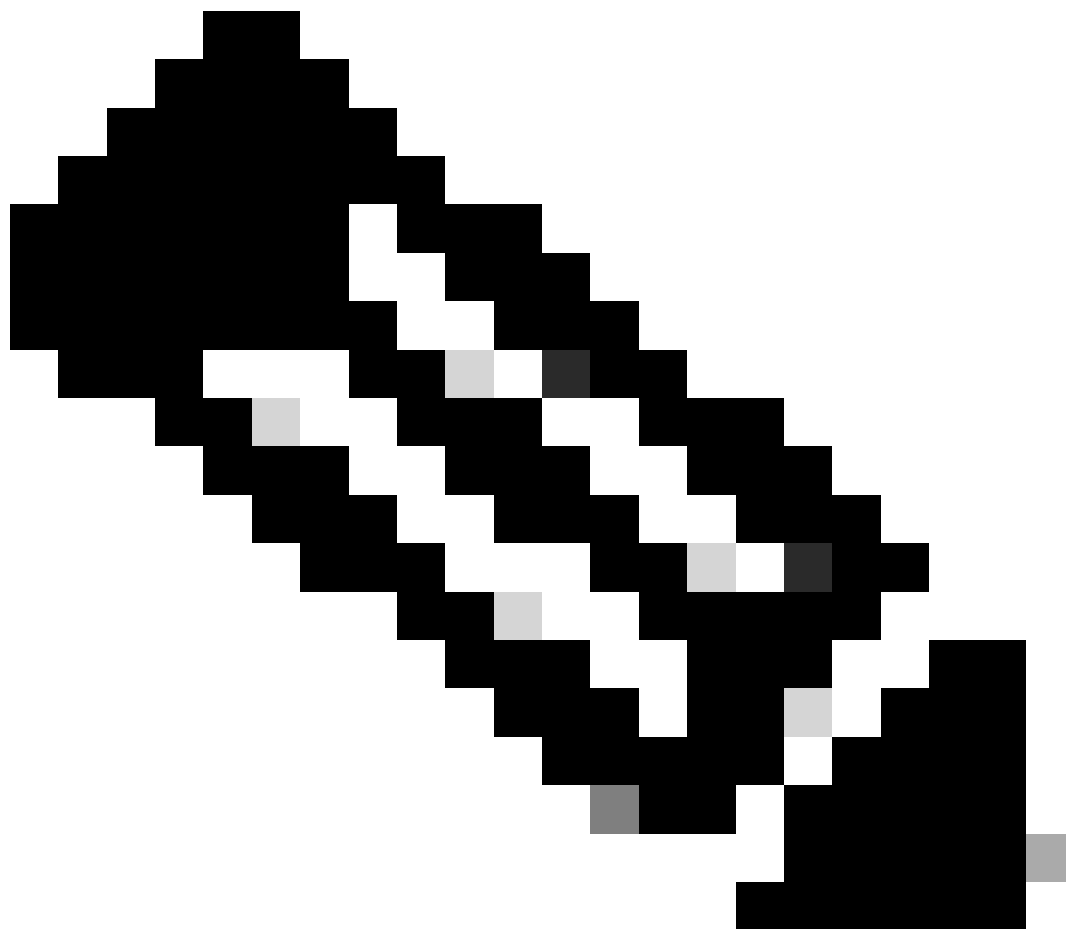
Choose an Agent Is Upgrade Mandatory ☐

Native Supplicant Configuration

WinSPWizard 3.2.0.1

Cisco-ISE-NSP

7. Haga clic en Finalizado, a continuación, en el botón Guardar.



Nota: Esta política afecta tanto al aprovisionamiento de clientes de estado como al aprovisionamiento de BYOD, donde la sección Configuración del agente determina el agente de estado y el módulo de cumplimiento de normativas aplicados para las comprobaciones de estado, mientras que la sección Configuración del suplicante nativo gestiona la configuración de los flujos de aprovisionamiento de BYOD

Configuración de conjuntos de políticas de ISE para BYOD con SSID único

1. Vaya a Policy > Policy Set y cree una política para el flujo de BYOD en 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. Luego, navegue hasta Administración > Administración de identidad > Orígenes de identidad externos > Perfil de autenticación de certificado. Haga clic en el botón Add para crear el perfil de certificado:

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 Evaluation Mode 62 Days

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 Profile

Certificate Authentication Profiles List > New Certificate Authentication Profile

* Name BYOD

Description

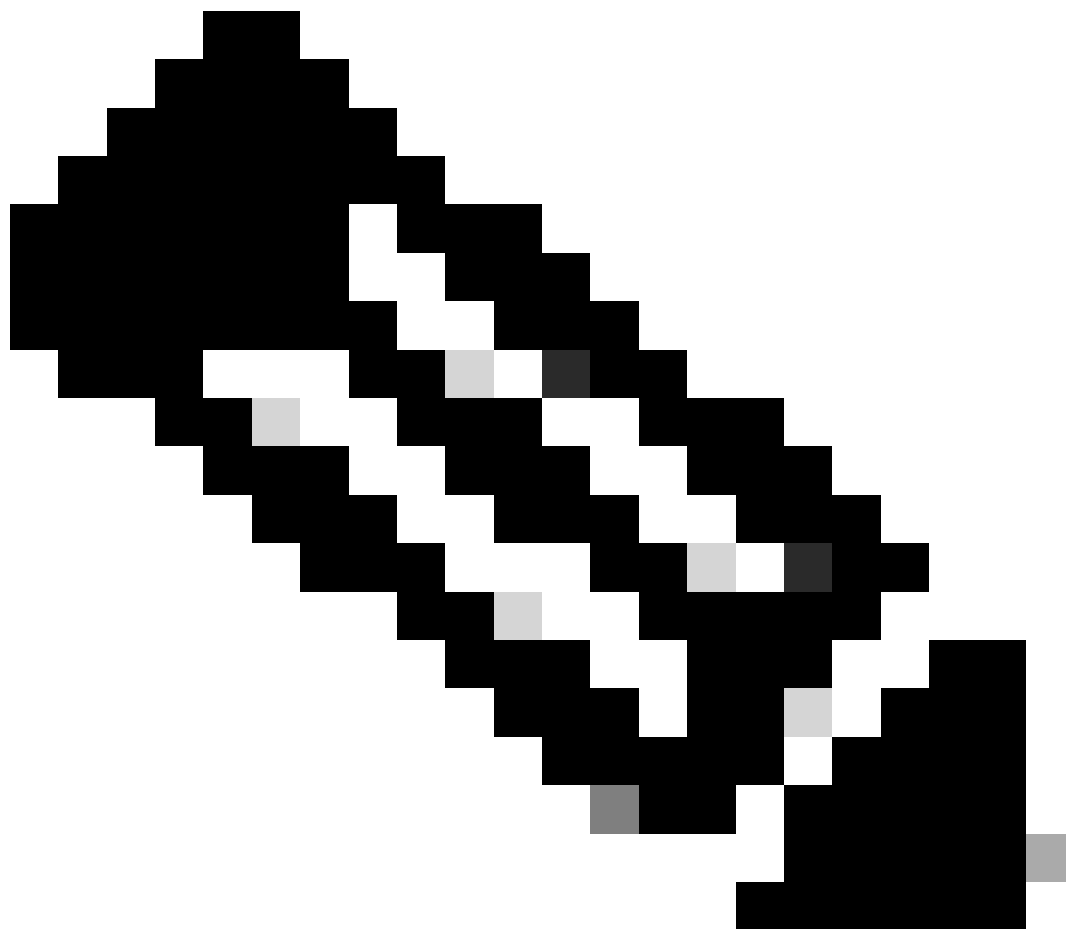
Identity Store [not applicable]

Use Identity From Certificate Attribute Subject - Common Name

Match Client Certificate Against Certificate in Identity Store

Never Only to resolve identity ambiguity Always perform binary comparison

Submit Cancel



Nota: En el almacén de identidades, siempre puede seleccionar su Active Directory que se ha integrado en ISE para realizar una búsqueda de usuario desde el certificado para obtener seguridad adicional.

3. Haga clic en Enviar para guardar la configuración. A continuación, asigne el perfil del certificado al conjunto de políticas para BYOD:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Policy / Policy Sets'. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Help. The main content area displays 'Policy Sets -> BYOD'. It features a table of Policy Sets and a table of Authentication Policies. The 'Default' authentication policy is selected, and its 'Options' are visible, showing 'BYOD' and 'Options'.

4. Configure el perfil de autorización para la redirección de BYOD y el acceso completo después del flujo de BYOD. Vaya a Política > Elementos de política > Resultados > Autorización > Perfiles de autorización.

5. Haga clic en Agregar y cree un perfil de autorización. Consulte Web Redirection (CWA, MDM, NSP, CPP) y asigne la página del portal BYOD. Además, agregue el nombre de la ACL de redirección del WLC al perfil. Para el perfil de acceso completo, configure un permiso de acceso con la VLAN corporativa respectiva en el perfil.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Policy / Policy Elements'. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Help. The main content area displays 'External Identity Sources' and 'Authorization Profiles'. The 'Authorization Profile' configuration is shown, with fields for Name, Description, Access Type, Network Device Profile, Service Template, Track Movement, Agentless Posture, and Passive Identity Tracking. The 'Common Tasks' section includes checkboxes for various tasks, with 'Web Redirection (CWA, MDM, NSP, CPP)' checked and 'Value' set to 'BYOD_CWA'.

6. Asigne el perfil de autorización a la regla de autorización. El acceso completo a BYOD debe tener la regla EndPoints·BYODRegistration igual que yes para que el usuario tenga acceso completo a la red después del flujo de BYOD.

Identity Services Engine Policy / Policy Sets Evaluation Mode 82 Days

Policy Sets → BYOD

Reset Reset Policy Set Hit Counts Save

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	

Configuración de conjuntos de políticas de ISE para BYOD SSID dual

En la configuración de BYOD con SSID dual, el conjunto de dos políticas se configura en ISE. El primer conjunto de políticas es para el SSID abierto/no seguro, donde la configuración del conjunto de políticas redirige al usuario a la página BYOD al conectarse al SSID abierto/no seguro

1. Vaya a Policy > Policy Set y cree una política para el flujo de BYOD en ISE.
2. Cree un conjunto de políticas para el SSID abierto/no seguro y el SSID corporativo que autentique al usuario BYOD registrado en ISE.

Policy Sets

Reset Reset Policy Set Hit Counts Save

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		

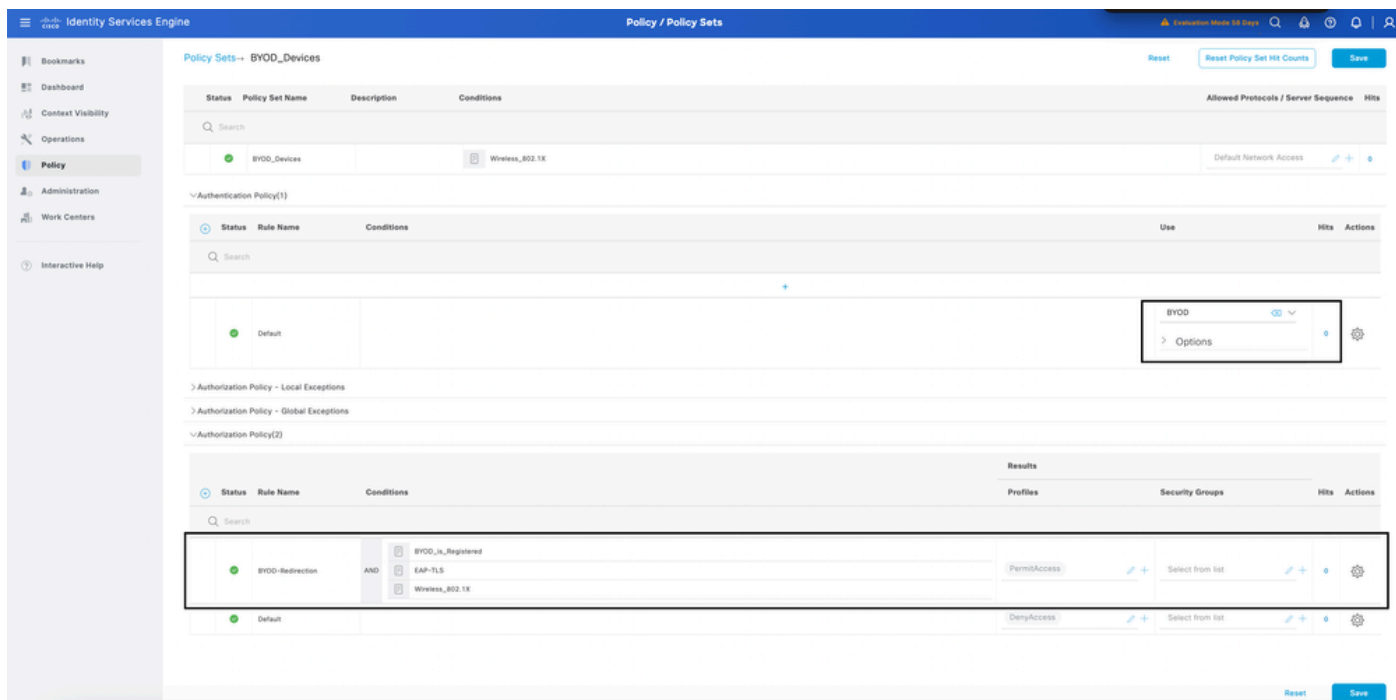
Reset Save

3. En el conjunto de políticas de Onboarding, busque Continue selected en las opciones. Para la directiva de autorización, cree una condición y asigne el perfil de autorización de redirección. Los mismos pasos se aplican en la creación del perfil de autorización, que se puede encontrar en el punto 4.



4. En el conjunto de políticas registradas de BYOD, configure la política de autenticación con el mismo perfil de certificado que encontró.

en Configure ISE Policy Sets for Single SSID BYOD en el punto 2. Cree también una condición para la política de autorización y asigne el perfil de acceso completo a la política.



Registro

A partir del registro en directo de ISE, la autenticación de usuario se realizará correctamente y se redirigirá a la página del portal BYOD. Una vez finalizado el flujo de BYOD, el usuario tendría acceso a la red

↺ Reset Repeat Counts ↗ Export To										Filter			⚙
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authorization Policy	Authoriz...	IP Address	Network De...	Device	
×		▼		Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorization Policy	Authorizatic	IP Address	▼	Network Device	Device
Feb 24, 2025 12:30:18.1...	ⓘ	🔍	0	test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD	PermitAcc...	10.127.196.2...			TenGig...
Feb 24, 2025 12:06:43.0...	✅	🔍		test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...		BYOD-Switch	TenGig...
Feb 24, 2025 12:06:37.9...	✅	🔍		test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...		BYOD-Switch	TenGig...

Desde la perspectiva del usuario, en primer lugar se redirigirían a la página de BYOD y el dispositivo adecuado tendría que seleccionarse en la página web. Para la prueba se utilizó un dispositivo Windows 10

BYOD Portal

test

1

2

3

BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

The following system was detected

Windows

Was your device detected incorrectly?

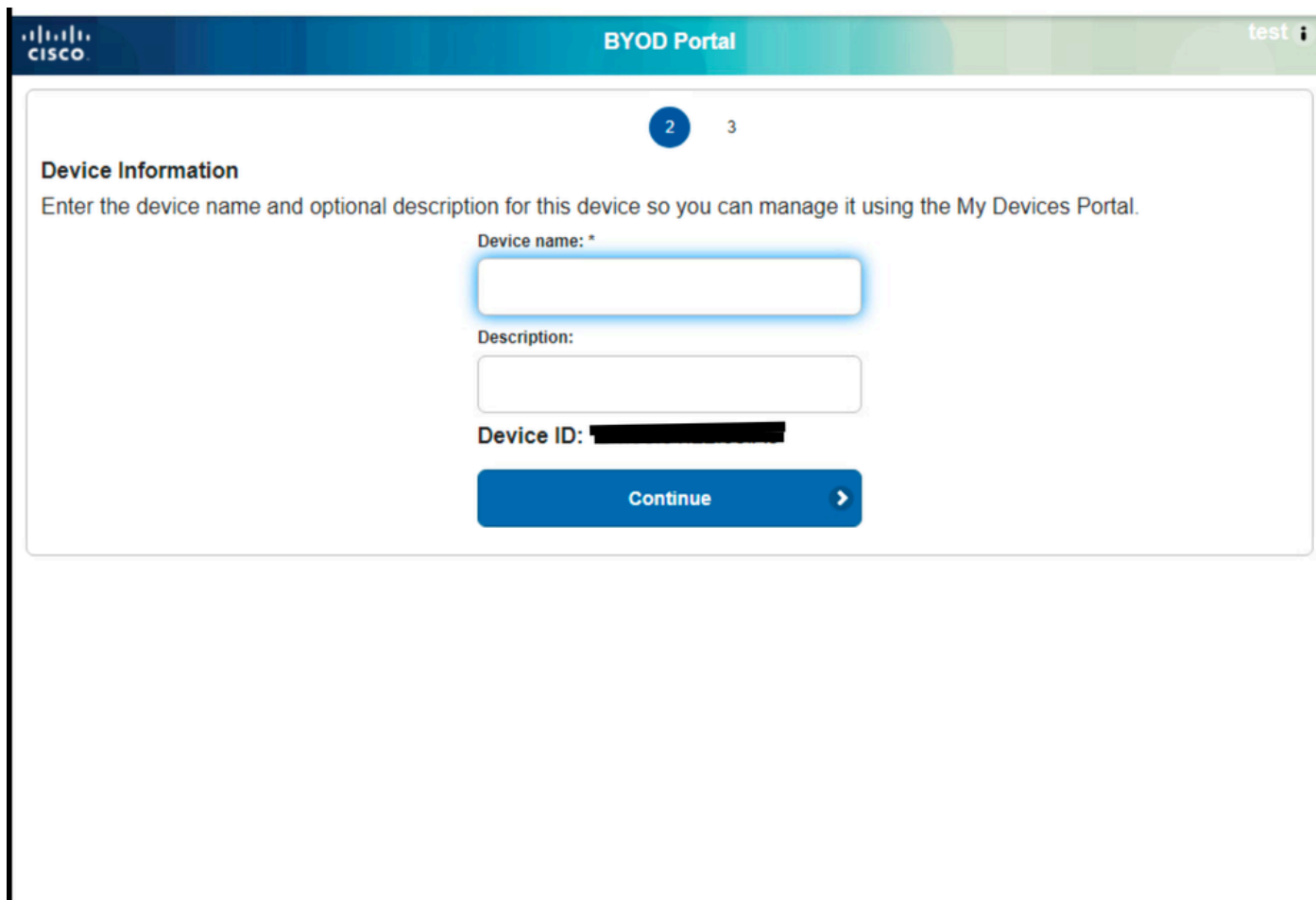
Select your Device

Windows

▼

Start

Después de hacer clic en el botón Next (Siguiente), se le dirigirá a una página en la que se le solicitará al usuario que introduzca el nombre del dispositivo y la descripción



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 number. The main content area is titled "Device Information" and includes 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 redacted value. At the bottom of the form is a blue "Continue" button with a right-pointing arrow.

CISCO BYOD Portal test

2 3

Device Information

Enter the device name and optional description for this device so you can manage it using the My Devices Portal.

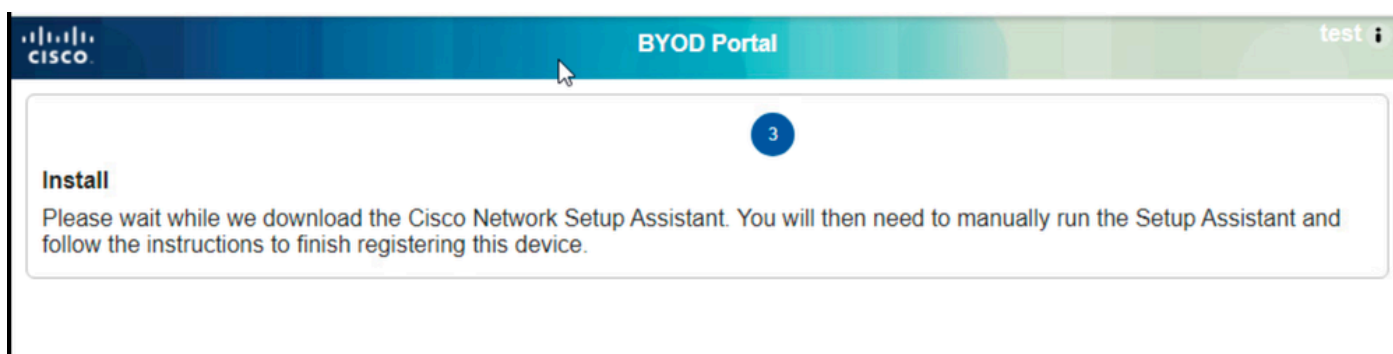
Device name: *

Description:

Device ID: [REDACTED]

Continue

Indicación de que se solicitaría al usuario que descargara la herramienta Network Assistant para descargar el perfil de terminal y el certificado EAP-TLS para la autenticación si el perfil está configurado para realizar la autenticación EAP-TLS



The screenshot shows the Cisco BYOD Portal interface at step 3. The header is identical to the previous screenshot. The progress indicator now shows step 3 as active and highlighted with a blue circle, while step 2 is a plain number. The main content area is titled "Install" and includes 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." There is no input field or button visible in this step.

CISCO BYOD Portal test

2 3

Install

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.

Ejecute la aplicación Network Assistant con privilegios de administrador y haga clic en el botón Start (Iniciar) para iniciar el flujo de incorporación:



Network Setup Assistant

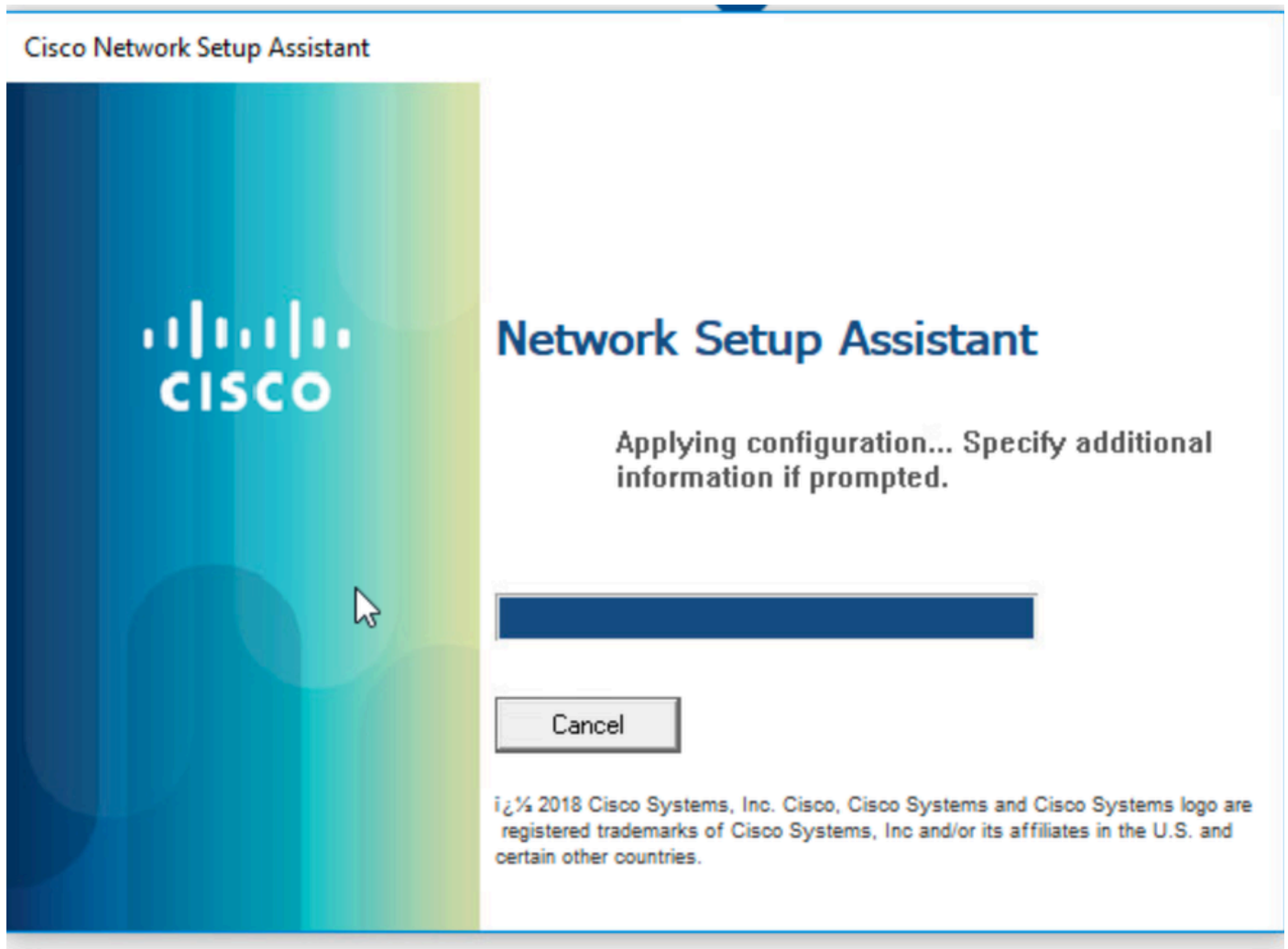


This application automatically configures network settings.

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.



El usuario se ha incorporado correctamente a la red con su dispositivo personal para acceder a los recursos.

Resolución de problemas

Para solucionar el problema de BYOD, habilite esta depuración en ISE

Atributos que se deben establecer en el nivel de depuración:

- cliente (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)
- profiler (profiler.log)

Fragmento de registro

Registros de invitados

Estos registros indican que el usuario se ha redirigido correctamente a la página y ha descargado la aplicación 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 -:0000000000000000B30D59CC5::-
ruta de mapeo encontrada en action-for pupils, reenviar a: pages/byodWelcome.jsp // Página de
bienvenida de 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:-
Tamaño de pTranPasos: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:-
getNextFlowStep, pTransPasos: [id: d2513b7b-7249-4bc3-a423-0e7d9a0b250]
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:-
getNextFlowStep, stepTrans:d2 5513b7b-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::-
ruta de asignación encontrada en acción-hacia adelante, reenvío : 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:-
Tamaño de pTranPasos: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:-
getNextFlowStep, pTransPasos: [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:-
getNextFlowStep, stepTrans:f2 03b757-9e8a-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::-
ruta de mapeo encontrada en action-forward, reenviar 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 // La red La aplicación de asistencia se ha enviado al
terminal
```

Registros De Ise-Psc

A medida que la aplicación se descarga en el terminal, la aplicación inicia un flujo SCEP para obtener el certificado de cliente de ISE.

```
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- CertStore contiene 4 certificado(s):
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1. '[issuer=CN=CA raíz de Servicios de Certificate Server -
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=CA raíz de Servicios de Certificate Server -
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 -::::- Selección del certificado de cifrado
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selección de certificado con keyEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Se han encontrado 1 certificado(s) con keyEncipherment
keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Usando [issuer=CN=Certificate Services Endpoint Sub CA
- iseguest; serial=131900858749761727853768227590303808637] para el cifrado de mensajes
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Seleccionar certificado de verificador
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selección de certificado con digitalSignature keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Encontrado 1 certificado(s) con digitalSignature keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Usando [issuer=CN=Certificate Services Endpoint Sub CA
- iseguest; serial=131900858749761727853768227590303808637] para verificación de mensajes
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selección de certificado de emisor
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selección de certificado con restricciones básicas
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Se han encontrado 3 certificado(s) con restricciones
basicConstraints
```

2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Usando [issuer=CN=Certificate Services Endpoint Sub CA
- iseguest; serial=131900858749761727853768227590303808637] para emisor
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- Mediciones de rendimiento de los servidores
SCEP : name[activo/muerto, total de solicitudes, total de errores, solicitudes en curso, promedio
de RTT]
[http://127.0.0.1:9444/caservice/scep\[activo,96444,1,0,120\]](http://127.0.0.1:9444/caservice/scep[activo,96444,1,0,120])

Descarga de perfiles de terminales

Una vez finalizado el proceso SCEP y cuando el terminal instala el certificado, la aplicación descarga el perfil del terminal para la futura autenticación que realizará el dispositivo:

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Referer = Windows // El dispositivo Windows
se ha detectado en función de la página web
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- perfil de aprovisionamiento de nsp
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Session = 000000000000000B30D59CC5
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//El perfil NSP se descarga en el terminal
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Streaming a ip: tipo de archivo:
NativeSPProfile:Cisco-ISE-NSP.xml //The Network Assistant Application
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 se ha configurado para probar
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- el tipo de redirección es: SUCCESS_PAGE, la
URL de redirección es: para mac:

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).