

# Configurar o ISE BYOD com SSID único e duplo no ISE 3.3

## Contents

---

[Introdução](#)

[Background](#)

[Pré-requisitos](#)

[Componente usado](#)

[O que é SSID único e BYOD SSID duplo no ISE?](#)

[BYOD de SSID único](#)

[BYOD SSID duplo](#)

[Configuração de WLC](#)

[Criar uma WLAN para o CWA](#)

[Configurar servidores RADIUS](#)

[Configurar servidores AAA](#)

[Configurar políticas de segurança para a WLAN](#)

[Configurar ACL de pré-autenticação](#)

[Configurar Perfil de Política](#)

[Aplicar marcas e implantar](#)

[Configurar um SSID aberto/ não seguro](#)

[Configuração do ISE](#)

[Pré-requisitos](#)

[Certificados](#)

[Configuração DNS](#)

[Configurar o dispositivo de rede do ISE](#)

[Crie um portal BYOD](#)

[Faça o download da versão mais recente do Cisco IOS®](#)

[Criar um Perfil de Ponto de Extremidade](#)

[Modelo de certificado](#)

[Mapeie um Perfil de Ponto Final para o Portal de Provisionamento de Cliente](#)

[Configurar conjuntos de políticas do ISE para BYOD de SSID único](#)

[Configurar conjuntos de políticas do ISE para BYOD com SSID duplo](#)

[Troubleshooting](#)

[Trecho de log](#)

[Logs de convidado](#)

[Logs Ise-Psc](#)

[Download de Perfil de Endpoint](#)

---

## Introdução

O documento descreve como configurar e solucionar problemas de BYOD no ISE.

## Background

O BYOD é um recurso que permite ao usuário integrar seus dispositivos pessoais no ISE para que ele possa usar o recurso de rede no ambiente. Ele também ajuda o administrador de rede a restringir o acesso do usuário ao recurso crítico a partir de dispositivos pessoais.

Ao contrário do fluxo de convidado, em que o dispositivo é autenticado com a página Convidado usando o armazenamento interno ou o Ative Directory no ISE. O BYOD permite que o administrador de rede instale um perfil de endpoint no endpoint para escolher o tipo de método EAP. Em cenários como EAP-TLS, o certificado do cliente é assinado pelo próprio ISE para criar uma confiança entre o endpoint e o ISE.

## Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- controlador de WLC
- Conhecimento básico sobre ISE

## Componente usado

Esses dispositivos usados não estão restritos a uma versão específica para o fluxo de BYOD:

- Catalyst 9800-CL Wireless Controller (17.12.3)
- Máquina virtual do ISE (3.3)

## O que é SSID único e BYOD SSID duplo no ISE?

### BYOD de SSID único

Em uma configuração de BYOD de SSID único, os usuários conectam seus dispositivos pessoais diretamente à rede sem fio corporativa. O processo de integração ocorre no mesmo SSID, onde o ISE facilita o registro, o provisionamento e a aplicação de políticas do dispositivo. Essa abordagem simplifica a experiência do usuário, mas exige integração segura e métodos de autenticação adequados para garantir a segurança da rede.

### BYOD SSID duplo

Em uma configuração de BYOD de SSID duplo, dois SSIDs separados são usados: um para integração (acesso não seguro ou restrito) e outro para acessar a rede corporativa. Inicialmente, os usuários se conectam ao SSID integrado, completam o registro e o provisionamento de dispositivos via ISE e, em seguida, mudam para o SSID corporativo seguro para acesso à rede.

Isso fornece uma camada adicional de segurança, segregando o tráfego integrado do tráfego de produção.

## Configuração de WLC

### Criar uma WLAN para o CWA

1. Vá para Configuration > Tags & Profiles > WLANs.
2. Clique em Add para criar uma nova WLAN.
  - Defina um Nome de WLAN e um SSID (por exemplo, BYOD-WiFi).
  - Ativar a WLAN.

**Add WLAN**

**General** Security Advanced

Profile Name\*

SSID\*

WLAN ID\*

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

### Configurar servidores RADIUS

1. Navegue até Configuration > Security > AAA > RADIUS > Servers.

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add X Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Acct Port "Contains" 1814

Name	Address	Auth Port	Acct Port
No items to display			

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

2. Clique em Adicionar para configurar o ISE como um servidor RADIUS:

- IP do servidor: Endereço IP do ISE.
- shared secret: Faça a correspondência do segredo compartilhado configurado no 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  ENABLED

CoA Server Key Type Clear Text

CoA Server Key

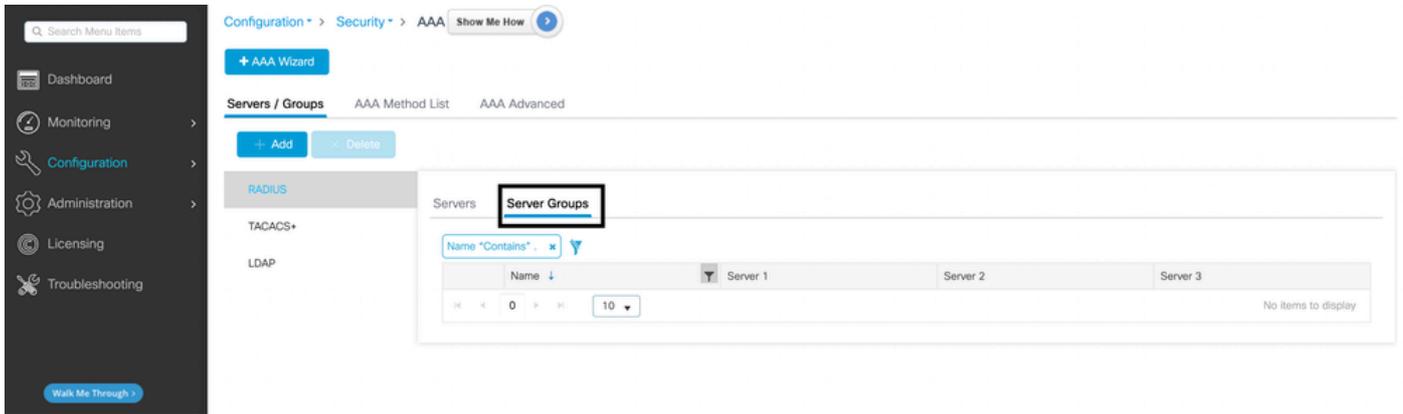
Confirm CoA Server Key

Automate Tester

Cancel Apply to Device

## Configurar servidores AAA

1. Navegue até Configuration > Security > AAA > Servers/Groups.



2. Atribua o servidor RADIUS a um grupo de servidores novo ou existente.

### Create AAA Radius Server Group

Name\*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Load Balance  DISABLED

Source Interface VLAN ID

Available Servers

Assigned Servers

## Configurar políticas de segurança para a WLAN

1. Navegue até Configuration > Tags & Profiles > WLANs. Edite a WLAN criada anteriormente.
2. Na guia Security > Layer 2:
  - Habilitar WPA+WPA2
  - Definir AES(CCMP128) sob criptografia WPA2
  - Auth Key Mgmt as 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

Fast Transition

Status   
 Over the DS   
 Reassociation Timeout \*

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. Na guia Security > Layer 3, seleccione global na lista suspensa para Web Auth Parameter Map.

⚠ 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

## Configurar ACL de pré-autenticação

Crie uma ACL para permitir aUsar ações para redirecionamento:

- Tráfego DNS.
- HTTP/HTTPS para o portal do ISE.
- Quaisquer serviços de backend necessários.

Para fazer isso:

1. Navegue até Configuration > Security > ACLs > Access Control Lists.
2. Crie uma nova ACL com regras para permitir o tráfego necessário.

### Edit ACL

ACL Name\*  ACL Type

**Rules**

Sequence\*  Action

Source Type

Destination Type

Protocol

Log  DSCP

	Sequence ↑	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/>	10	deny	ISE-IP-Address		any		ip	None	None	None	Disabled
<input type="checkbox"/>	20	deny	any		ISE-IP-Address		ip	None	None	None	Disabled
<input type="checkbox"/>	30	deny	any		any		udp	None	eq domain	None	Disabled
<input type="checkbox"/>	40	deny	any		any		udp	eq domain	None	None	Disabled
<input type="checkbox"/>	50	permit	any		any		tcp	None	eq www	None	Disabled

1 - 5 of 5 items

## Configurar Perfil de Política

1. Navegue até Configuration > Tags & Profiles > Policy. Você pode criar ou usar a política padrão

Configuration > Tags & Profiles > Policy

Description "Contains" default

Admin Status	Associated Policy Tags	Policy Profile Name	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>	default-policy-profile	default policy profile

1 - 1 of 1 items

2. Atribua a VLAN apropriada em Access Policies (Políticas de acesso)

### 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  ⓘ

**VLAN**

VLAN/VLAN Group  ⓘ

Multicast VLAN

**WLAN ACL**

IPv4 ACL  ⓘ

IPv6 ACL  ⓘ

**URL Filters** ⓘ

Pre Auth  ⓘ

Post Auth  ⓘ

3. Ative também Allow AAA Override e NAC state em Advanced of the policy.

## 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**

### WLAN Timeout

Session Timeout (sec)  ⓘ

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

### DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

### AAA Policy

Allow AAA Override

NAC State

Policy Name  ⓘ

Accounting List  ⓘ

Fabric Profile   ⓘ

Link-Local Bridging

mDNS Service Policy  ⓘ  
[Clear](#)

Hotspot Server  ⓘ

### User Defined (Private) Network

Status

Drop Unicast

### DNS Layer Security

DNS Layer Security Parameter Map  ⓘ  
[Clear](#)

Flex DHCP Option for DNS  **ENABLED**

Flex DNS Traffic Redirect  **IGNORE**

### WLAN Flex Policy

VLAN Central Switching

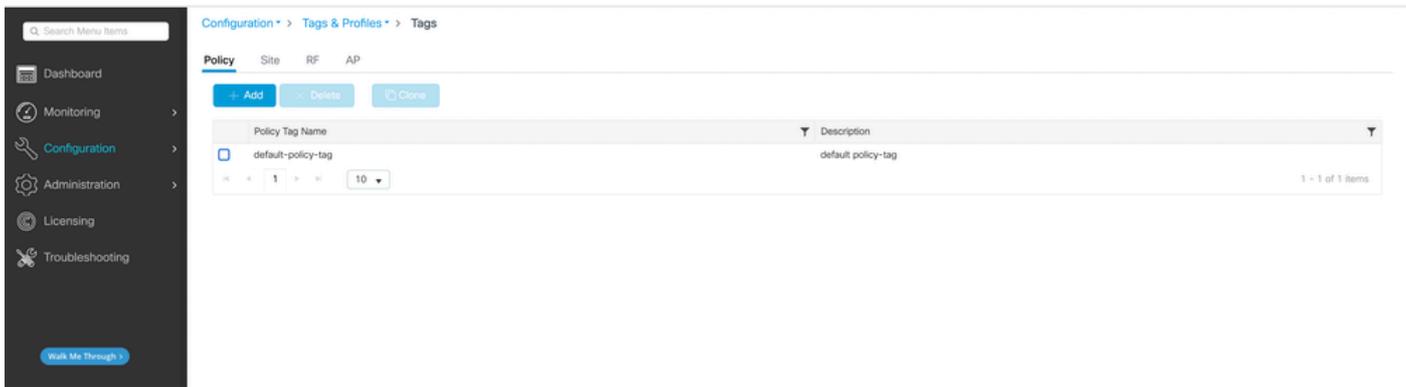
Split MAC ACL  ⓘ

Cancel

Update & Apply to Device

## Aplicar marcas e implantar

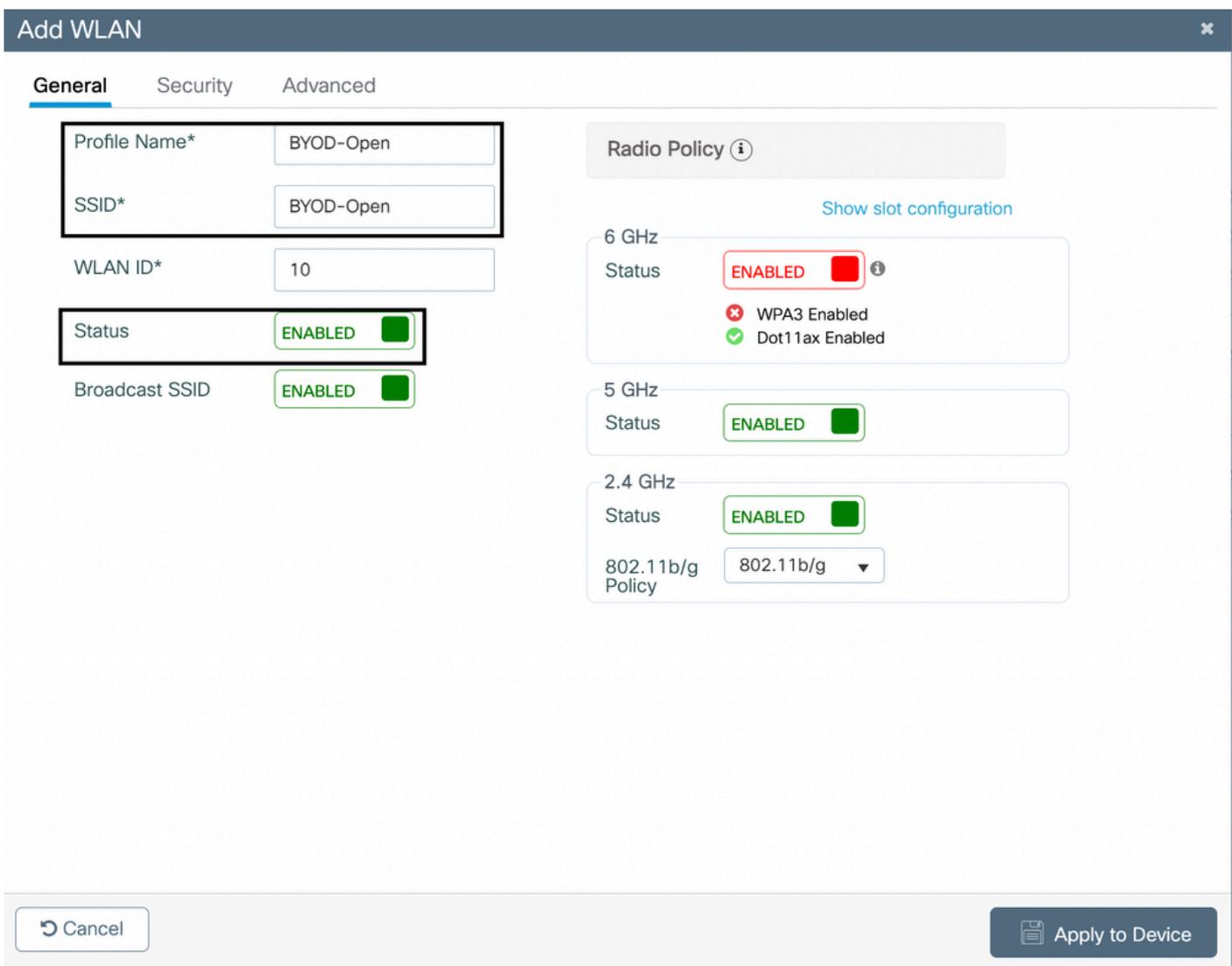
- Navegue até Configuração > Marcas e perfis > Marcas.
- Crie ou edite uma marca para incluir a WLAN e o Policy Profile.
- Atribua a tag aos Pontos de Acesso.



## Configurar um SSID aberto/ não seguro

O SSID aberto é criado apenas quando você decide ter uma configuração BYOD de SSID duplo em seu ambiente.

1. Navegue até Configuration > Tags & Profiles > WLANs. Clique no botão Adicionar.
2. Forneça um nome SSID na guia General (Geral) e habilite o botão WLAN.



3. Clique na guia Segurança na mesma janela. Selecione o botão de opção Nenhum e habilite a Filtragem de Mac.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. Under the 'Layer2' section, the 'None' radio button is selected. The 'MAC Filtering' checkbox is checked and highlighted with a red 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.

4. Na Camada 3 em Segurança, selecione a configuração global para Mapa de Parâmetros de Autenticação da Web. Se você tiver qualquer outro perfil de autenticação da Web configurado na WLC, também poderá mapeá-lo aqui:

## 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

## Configuração do ISE

### Pré-requisitos

- Verifique se o Cisco ISE está instalado e licenciado para a funcionalidade BYOD.
- Adicione sua WLC ao ISE como um dispositivo de rede com o segredo compartilhado RADIUS.

### Certificados

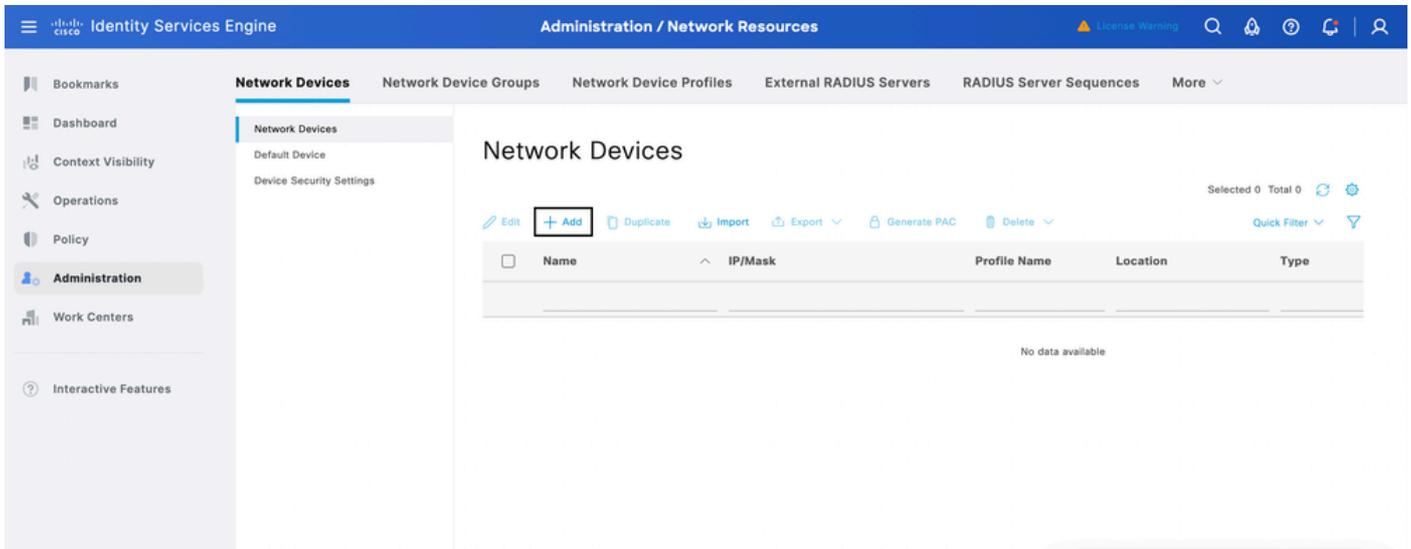
- Instale um certificado de servidor válido no ISE para evitar avisos de segurança do navegador.
- Verifique se o certificado é confiável para pontos de extremidade (assinados por uma CA conhecida ou uma CA interna com raiz confiável).

### Configuração DNS

- Certifique-se de que o DNS resolva o nome de host ISE para o portal BYOD.

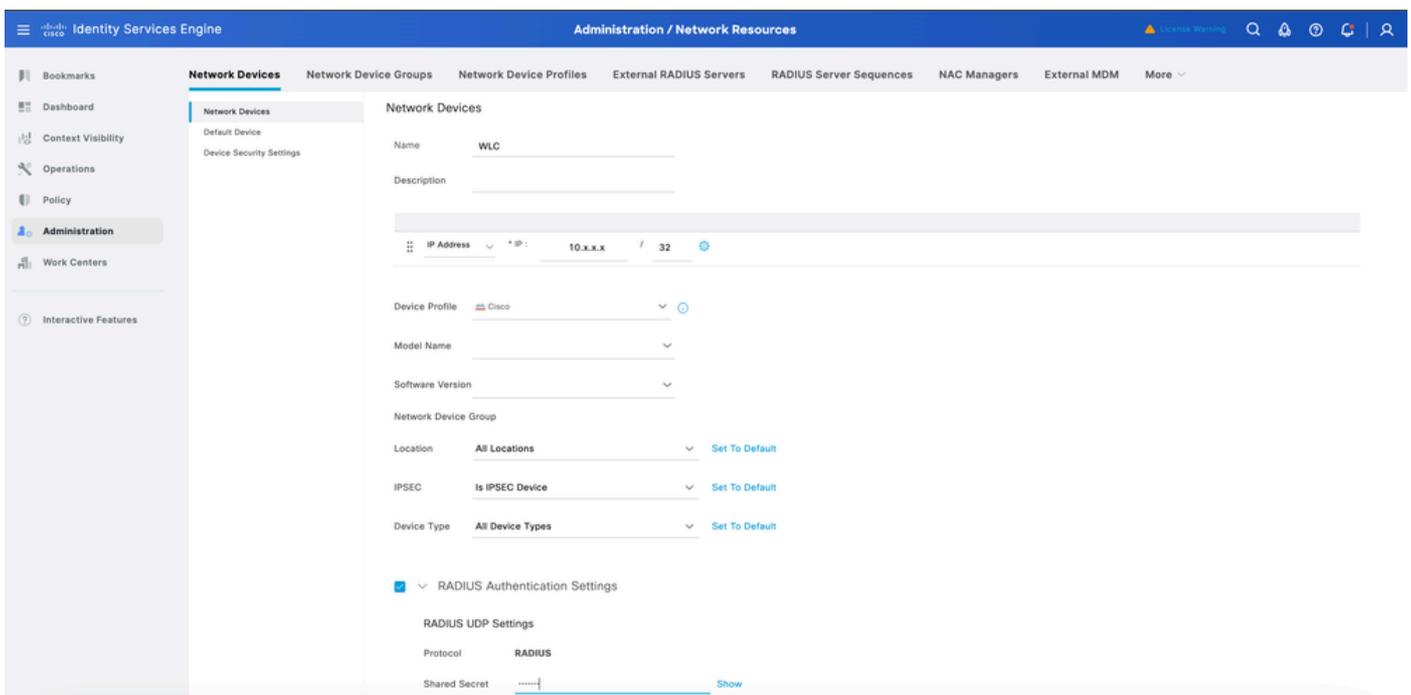
# Configurar o dispositivo de rede do ISE

1. Faça login na interface do usuário da Web do ISE.
2. Navegue até Administração > Recursos de rede > Dispositivos de rede.



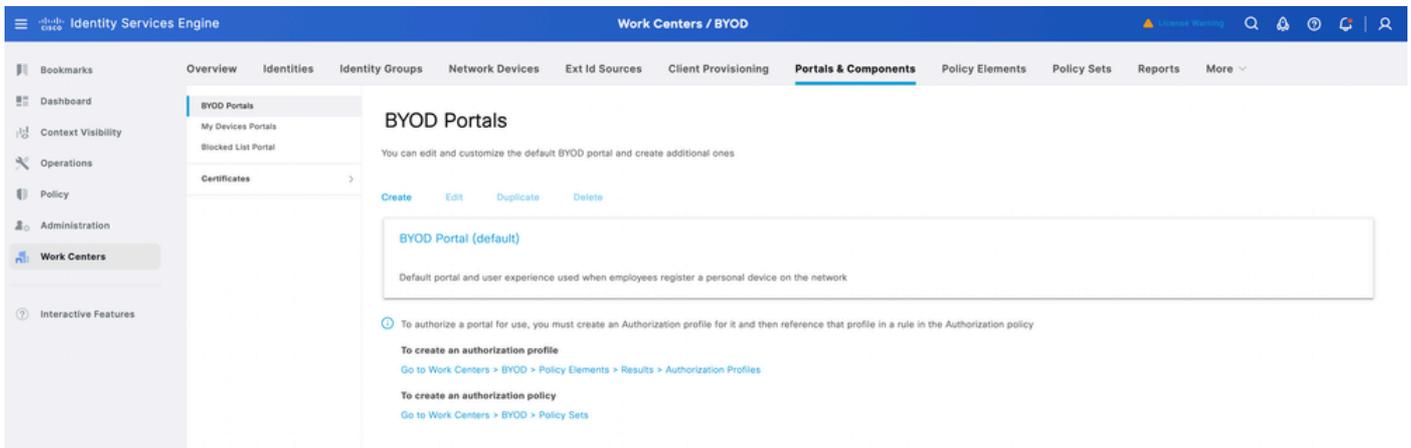
3. Adicione sua WLC como um dispositivo de rede:

- Nome: Digite um nome para a WLC.
- Endereço IP: Insira o IP de gerenciamento da WLC.
- Segredo compartilhado RADIUS: Insira o mesmo segredo compartilhado configurado no WLC.
- Clique em Submit.



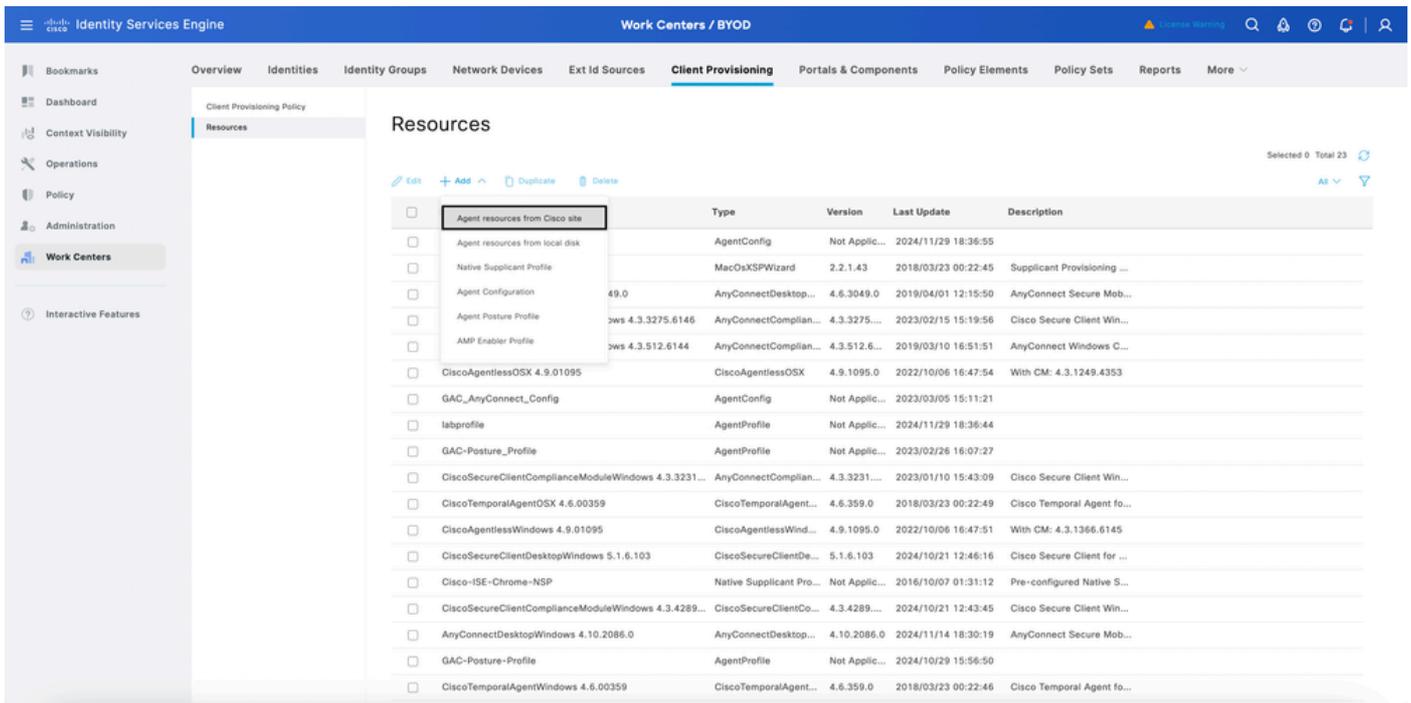
Crie um portal BYOD

1. Navegue até Centros de trabalho > BYOD > Configurações > Portais e componentes > Portais de BYOD.
2. Clique em Adicionar para criar um portal BYOD ou você pode usar o portal padrão existente no ISE.



## Faça o download da versão mais recente do Cisco IOS®

1. Navegue até Centros de trabalho > BYOD > Provisionamento de cliente > Recursos.
2. Clique no botão Add e selecione os recursos do agente no site da Cisco.



3. Na lista de softwares, selecione a versão mais recente do Cisco IOS para download.



# Download Remote Resources

<input type="checkbox"/>	Name	^	Description
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1		Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
<input type="checkbox"/>	MacOsXSPWizard 3.1.0.1		Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
<input type="checkbox"/>	MacOsXSPWizard 3.1.0.2		Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
<input type="checkbox"/>	MacOsXSPWizard 3.2.0.1		Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
<input type="checkbox"/>	MacOsXSPWizard 3.4.0.0		Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
<input type="checkbox"/>	WinSPWizard 3.0.0.2		Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
<input checked="" type="checkbox"/>	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

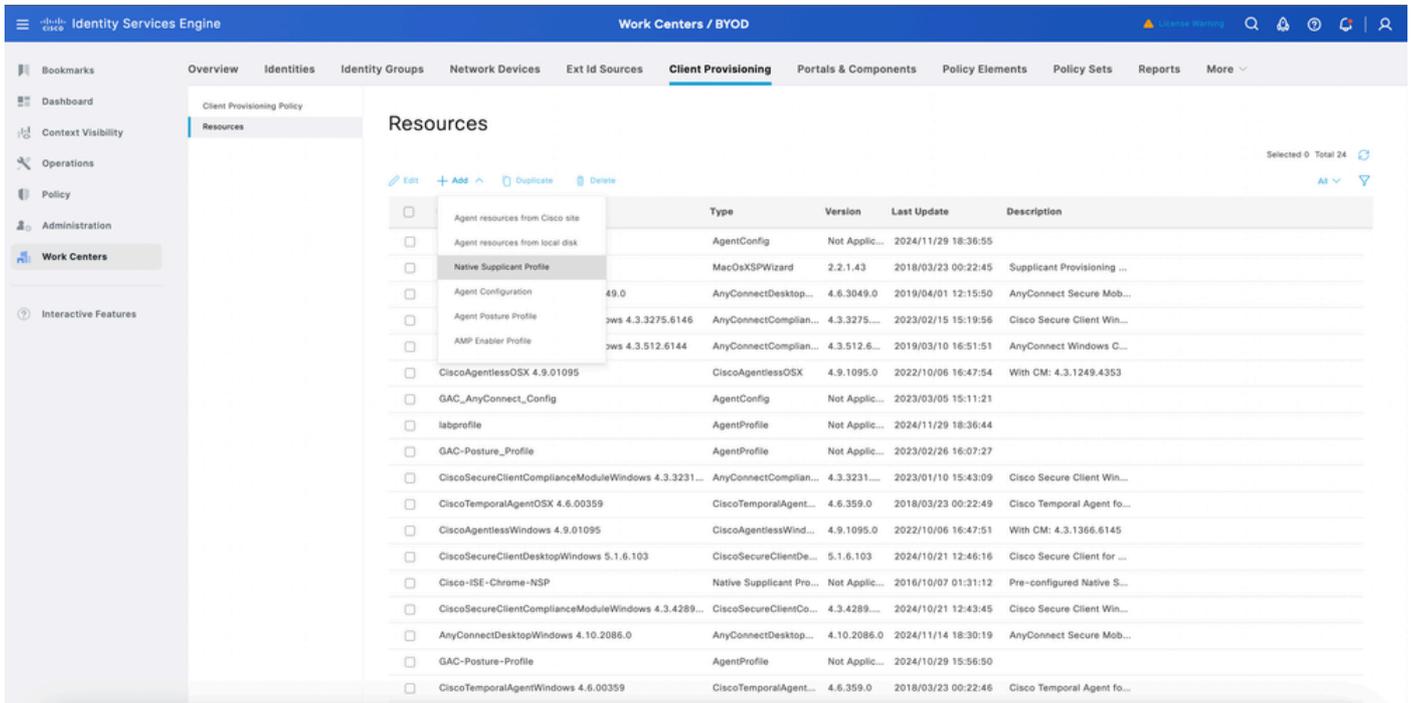


Note: O software Cisco IOS é baixado no ISE para endpoints Windows e MacOS. Para o Apple iPhone IOS, ele usa um suplicante nativo para provisionar o dispositivo e Para o dispositivo Android, você tem o assistente de configuração de rede que precisa ser baixado da Play Store.

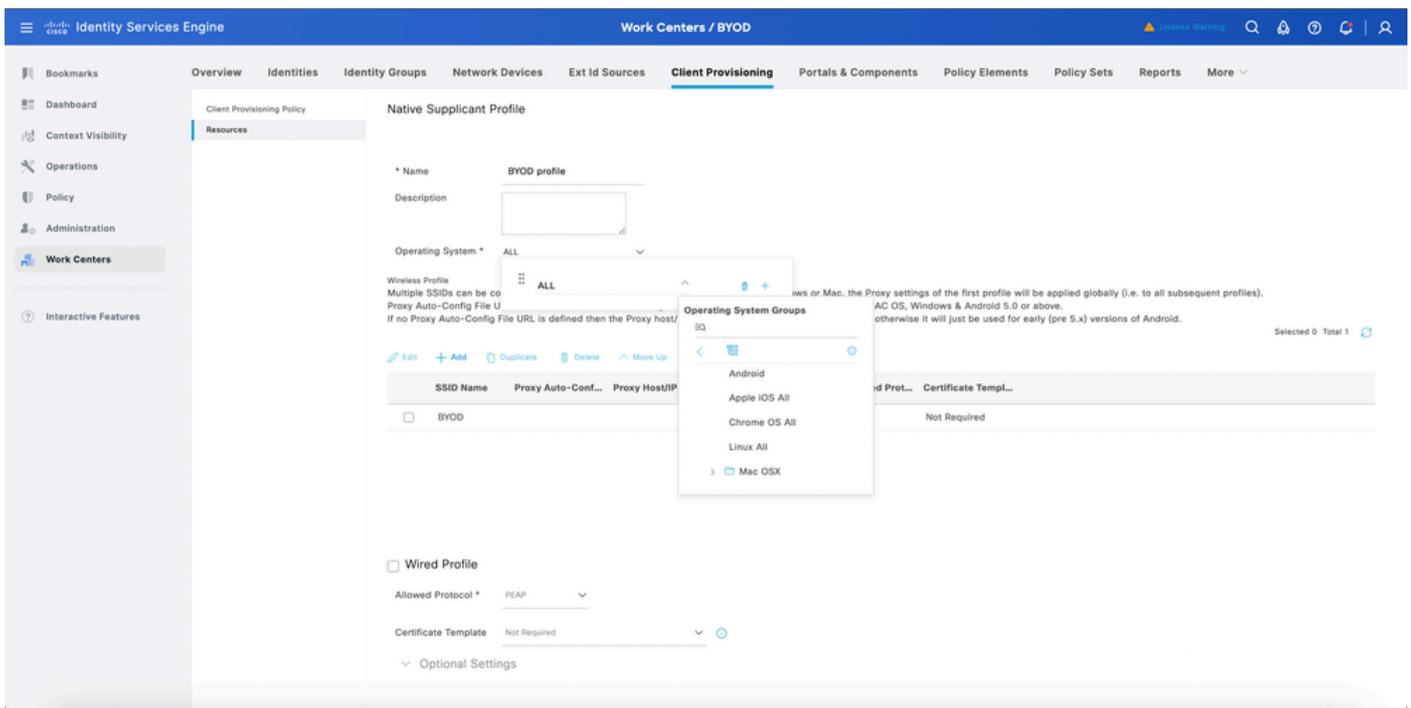
---

## Criar um Perfil de Ponto de Extremidade

1. Navegue até Centros de trabalho > BYOD > Provisionamento de cliente > Recursos.
2. Clique em Adicionar, selecione Perfil do suplicante nativo no menu suspenso.



3. No menu suspenso Sistema operacional, selecione o sistema operacional necessário que você gostaria de integrar o dispositivo ou você pode defini-lo como TODOS para integrar todos os endpoints em seu ambiente:



4. Clique em Adicionar na página para criar o perfil de ponto final para configurar o 802.1X para o ponto final:



: Dependendo de sua necessidade, configure o perfil do endpoint para o endpoint em seu ambiente. O perfil de endpoints nos permite configurar EAP-PEAP, EAP-TLS.

5. Clique em Salvar e, em seguida, em Enviar no perfil do ponto final.

## Modelo de certificado

O perfil de endpoint é pré-configurado para executar EAP-TLS. Um Modelo de certificado deve ser adicionado ao perfil. Por padrão, o ISE tem dois modelos predefinidos que podem ser escolhidos no menu suspenso.

**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

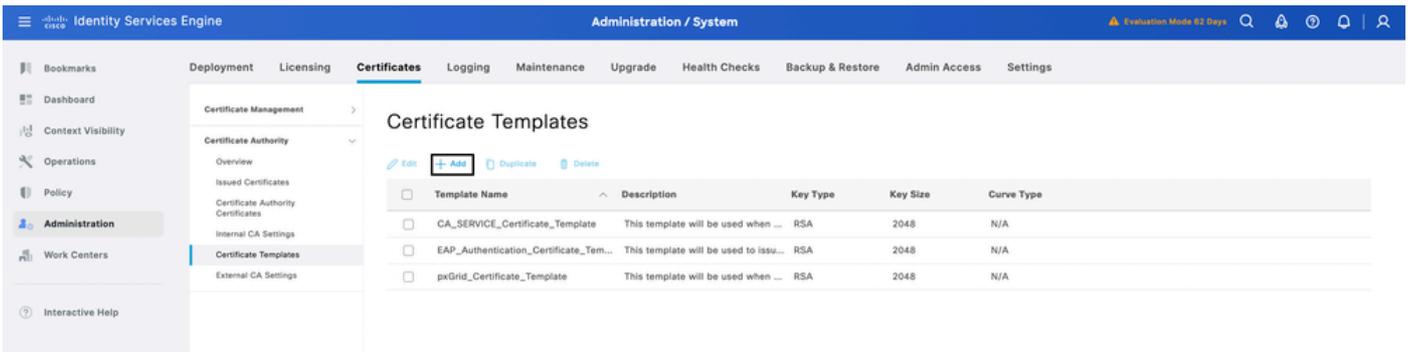
- EAP\_Authentication\_Certificate\_Template
- pxGrid\_Certificate\_Template

Save

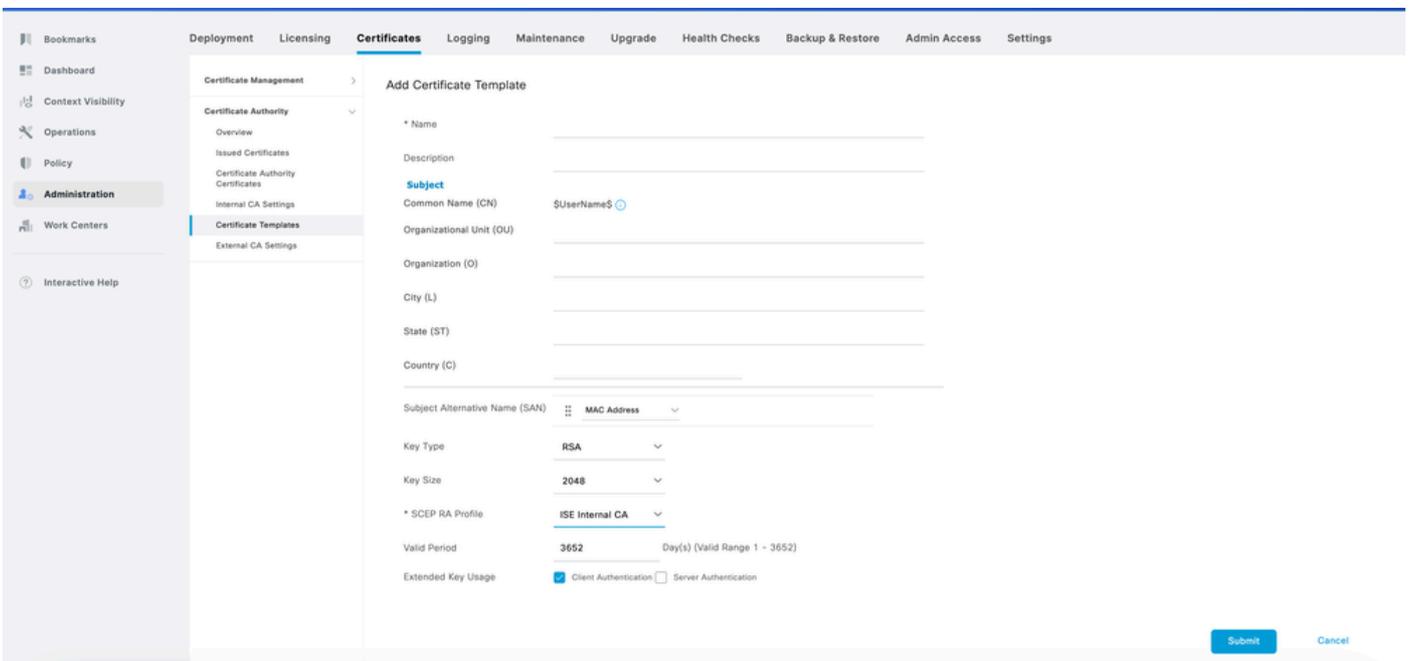
Para criar um novo modelo de certificado, siga estas etapas:

1. Navegue até Administração > Sistema > Certificados > Autoridade de certificação > Modelos de certificado.

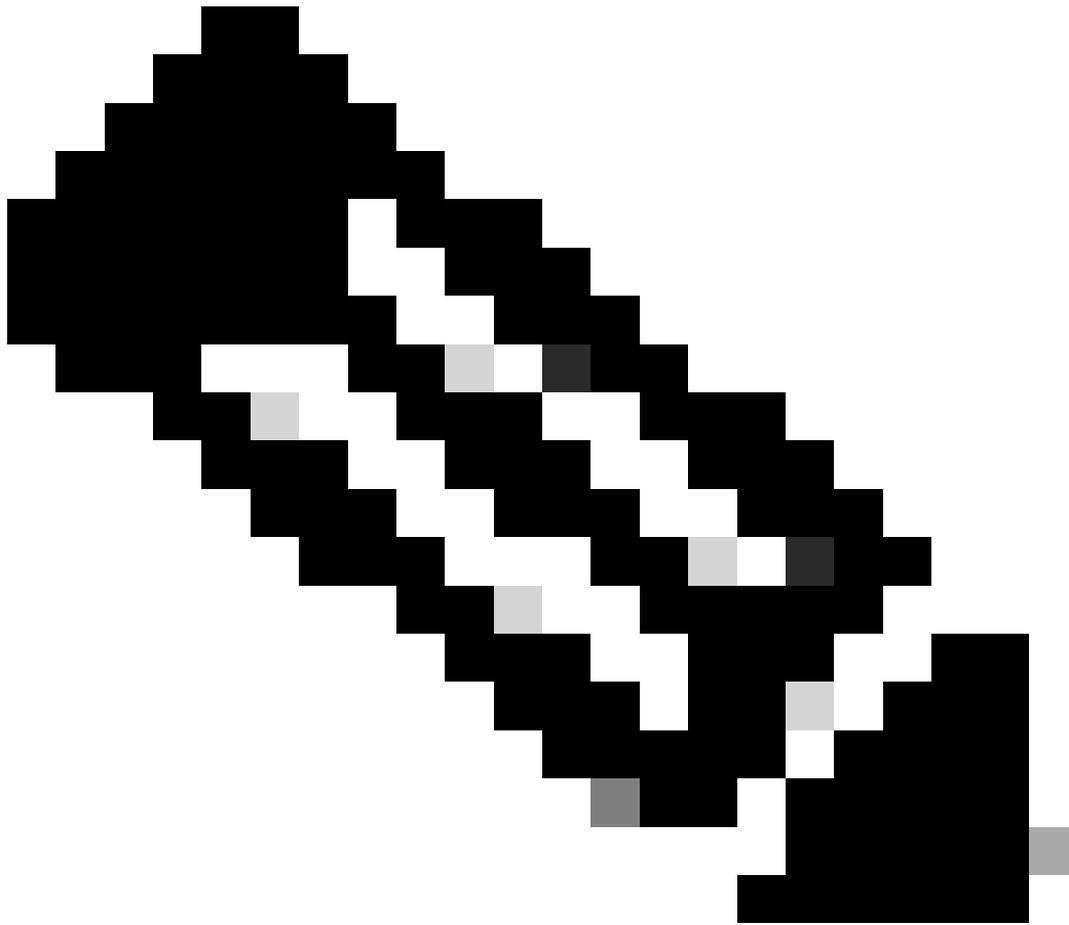
2. Clique no botão Adicionar na página.



3. Preencha os detalhes personalizados para atender aos requisitos específicos da sua organização.



4. Clique em Submeter para salvar as alterações.

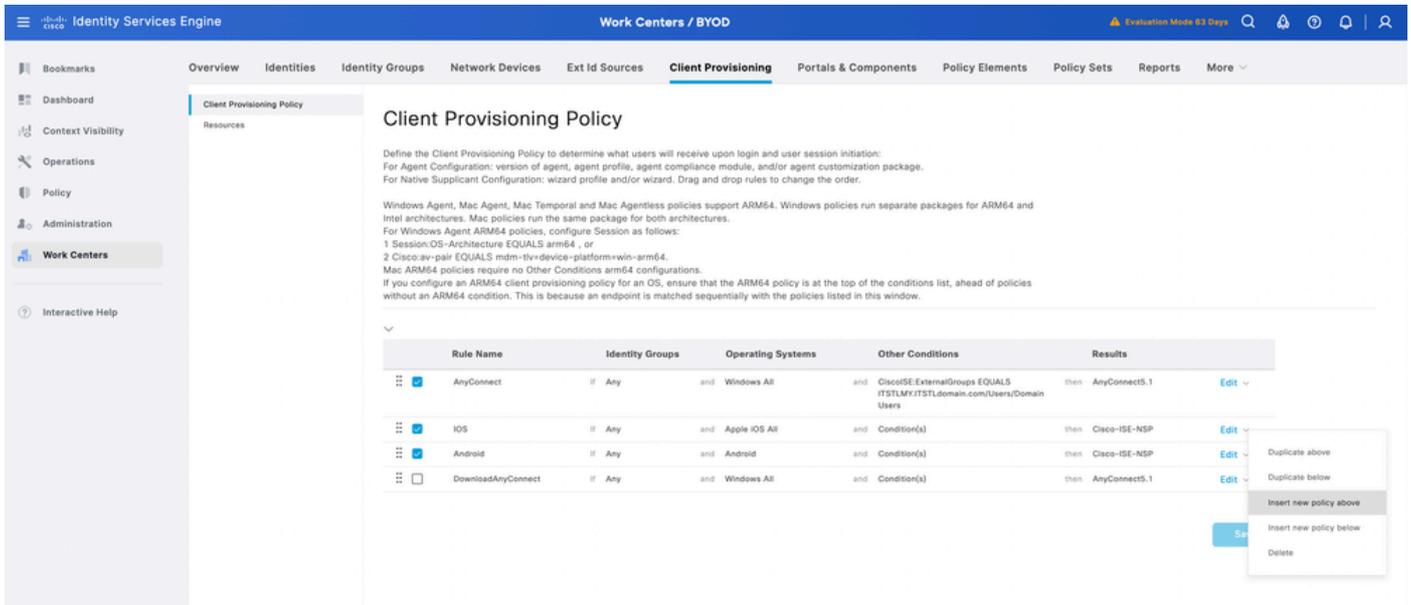


Note: O modelo de certificado pode ser útil no cenário quando você tem domínios diferentes e segmenta o usuário adicionando um valor diferente na OU do certificado.

---

## Mapeie um Perfil de Ponto Final para o Portal de Provisionamento de Cliente

1. Navegue até Centros de trabalho > BYOD > Provisionamento de cliente > Política de provisionamento de cliente.
2. Clique em v em uma das regras para criar uma nova regra de provisionamento de cliente.

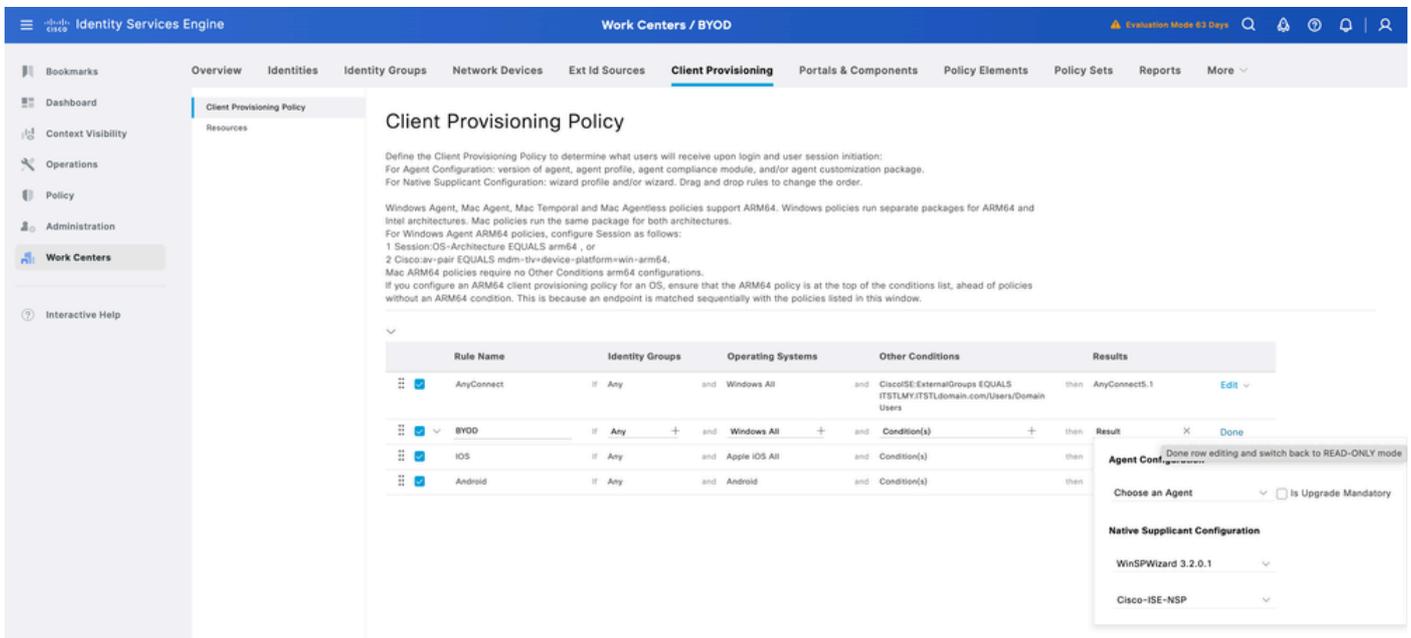


3. Contabilize a criação da nova regra na página

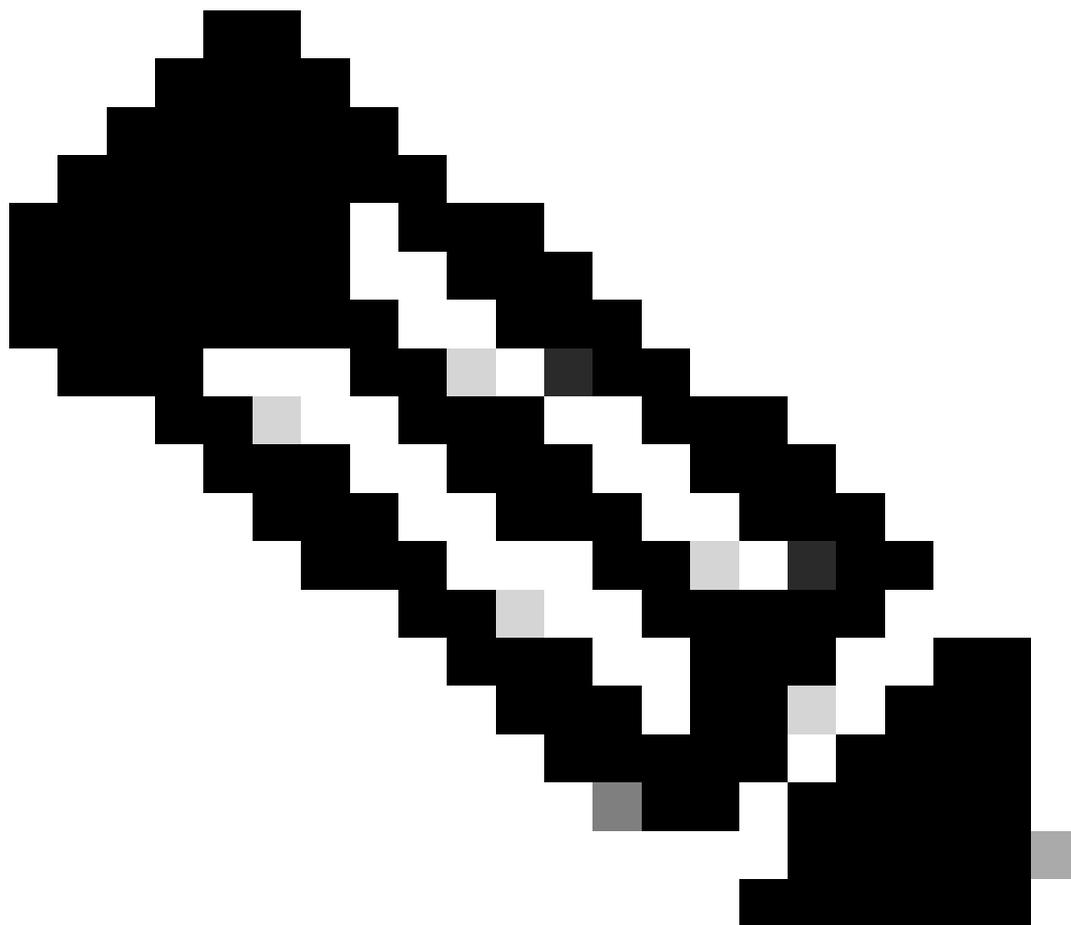
4. Adicione o grupo de identidade se desejar restringir determinados usuários a usar o portal BYOD

5. Adicione o sistema operacional que você gostaria de ter acesso ao portal BYOD

6. Mapeie a versão do Cisco IOS no menu suspenso e selecione também o perfil de endpoint que você criou no resultado



7. Clique em Concluído e, em seguida, no botão Salvar.



Note: Essa política afeta o provisionamento de clientes de postura e o provisionamento de BYOD, em que a seção Configuração do agente determina o agente de postura e o módulo de conformidade aplicados para verificações de postura, enquanto a seção Configuração do solicitante nativo gerencia as configurações para fluxos de provisionamento de BYOD

---

## Configurar conjuntos de políticas do ISE para BYOD de SSID único

1. Navegue até Policy > Policy Set e crie uma política para o fluxo de BYOD no ISE:

Policy Sets Reset [Reset Policy Set Hit Counts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	BYOD		Wireless_802.1X	Default Network Access	0		
<span style="color: green;">●</span>	Default	Default policy set		Default Network Access	0		

Reset [Save](#)

2. Em seguida, navegue até Administração > Gerenciamento de identidades > Fontes de identidade externas > Perfil de autenticação do certificado. Clique no botão Add para criar o perfil de certificado:

Identity Services Engine Administration / Identity Management

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

External Identity Sources

- Certificate Authentic...
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST

### Certificate Authentication Profile

\* Name: BYOD

Description:

Identity Store: [not applicable]

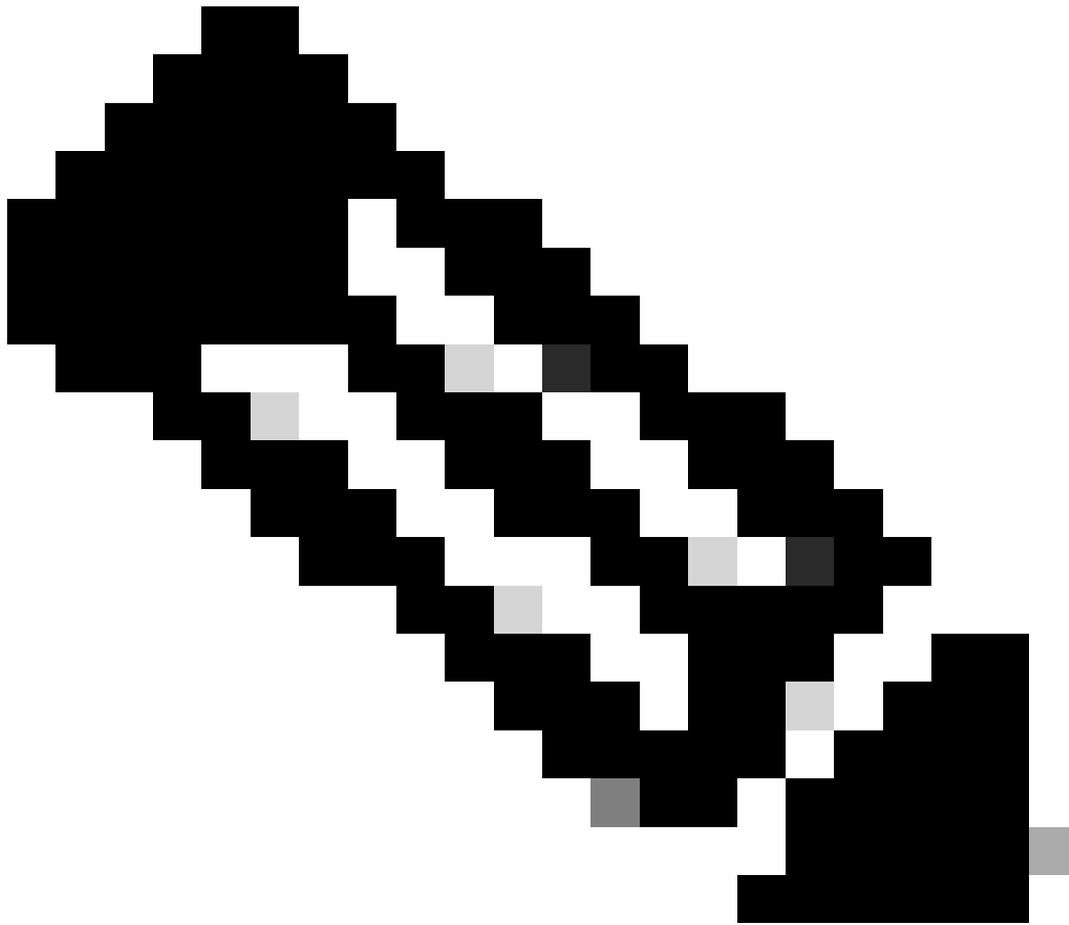
Use Identity From:
 

- 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

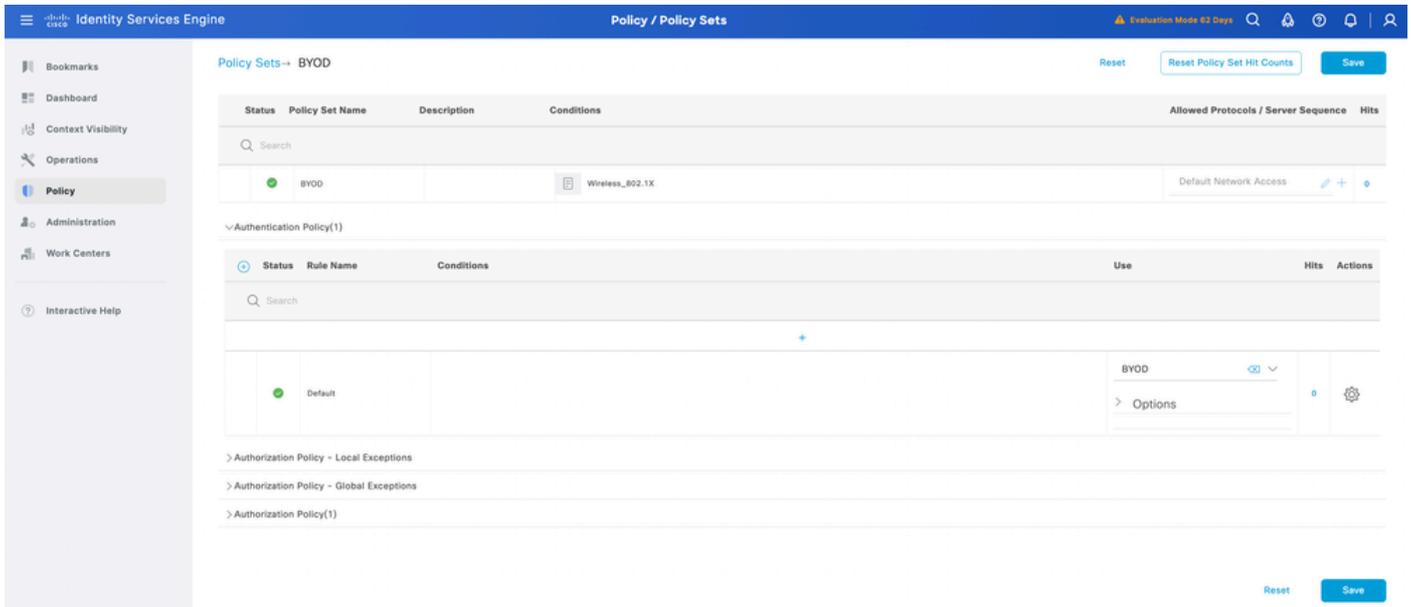
[Submit](#) [Cancel](#)



Note: No Repositório de identidades, você sempre pode selecionar seu Ative Directory que foi integrado ao ISE para executar uma pesquisa de usuário a partir do certificado para segurança adicional.

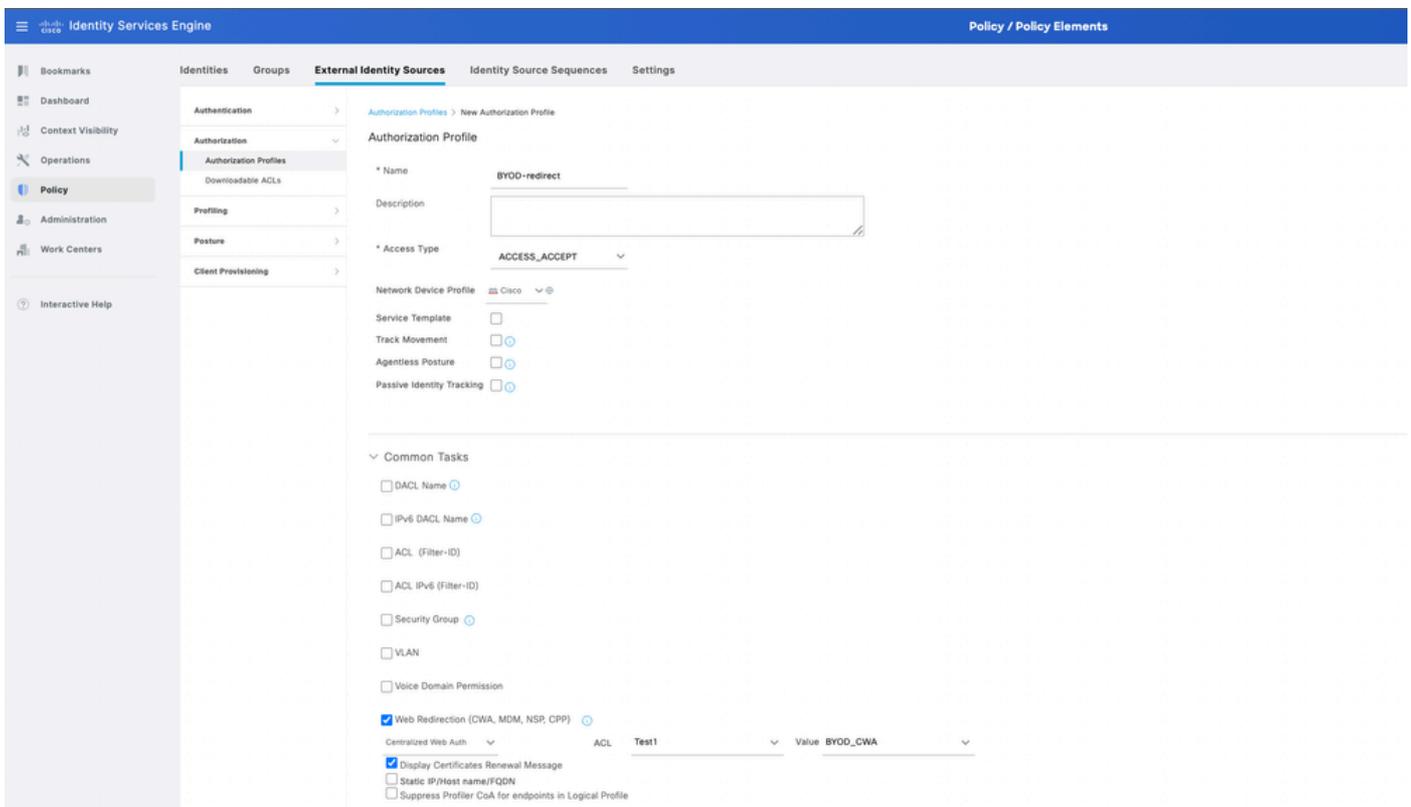
---

3. Clique em Submeter para salvar a configuração. Em seguida, mapeie o perfil do certificado para a política definida para BYOD:

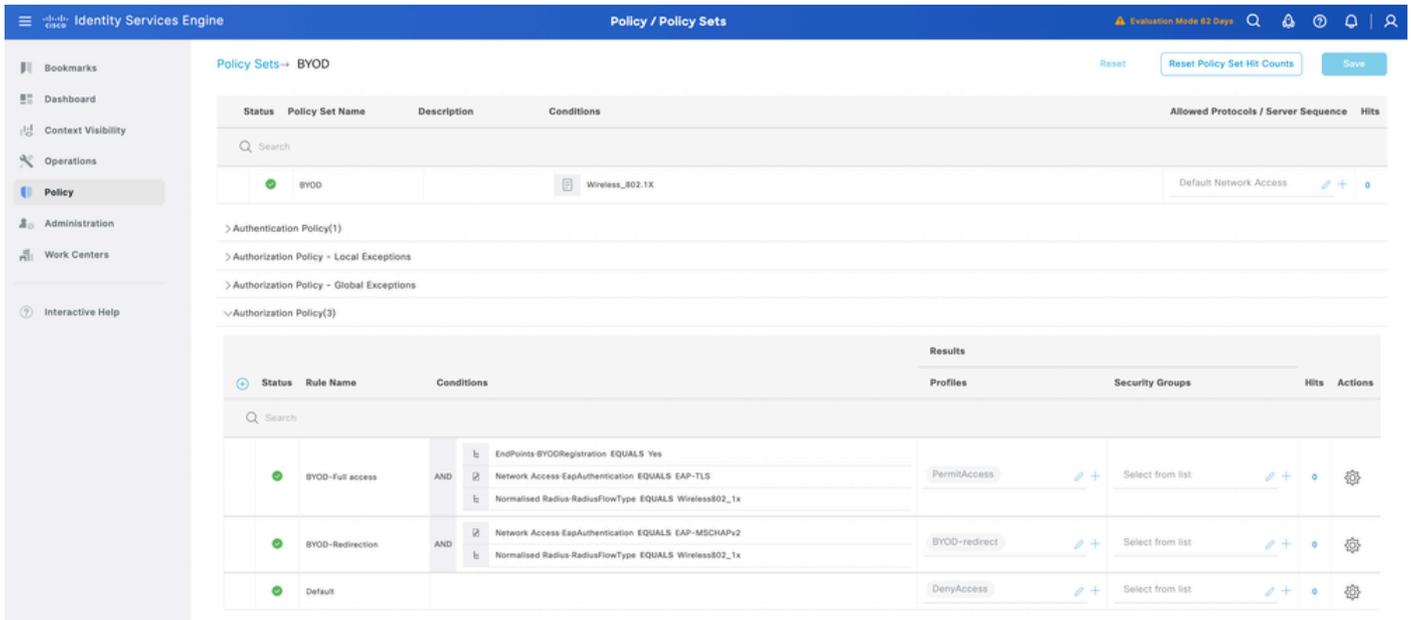


4. Configure o perfil de Autorização para redirecionamento de BYOD e acesso completo após o fluxo de BYOD. Navegue até Política > Elementos de política > Resultados > Autorização > Perfis de autorização.

5. Clique em Adicionar e crie um perfil de autorização. Verifique o Web Redirection (CWA,MDM,NSP,CPP) e mapeie a página do portal BYOD. Além disso, adicione o nome da ACL de redirecionamento da WLC ao perfil. Para o perfil de acesso completo, configure um acesso de permissão com a respectiva VLAN corporativa no perfil.



6. Mapeie o perfil de autorização para a regra de Autorização. O acesso completo BYOD deve ter a regra EndPoints·BYODRegistration igual a sim, para que o usuário obtenha acesso total à rede após o fluxo de BYOD.



## Configurar conjuntos de políticas do ISE para BYOD com SSID duplo

Na configuração BYOD de SSID duplo, o conjunto de duas políticas é configurado no ISE. O primeiro conjunto de políticas é para o SSID aberto/não seguro, em que a configuração do conjunto de políticas redireciona o usuário para a página BYOD ao se conectar ao SSID aberto/não seguro

1. Navegue até Policy > Policy Set e crie uma Policy for BYOD flow no ISE.
2. Crie um conjunto de Políticas para o SSID Aberto/Não Protegido e o SSID Corporativo que autentica o usuário BYOD registrado no ISE.

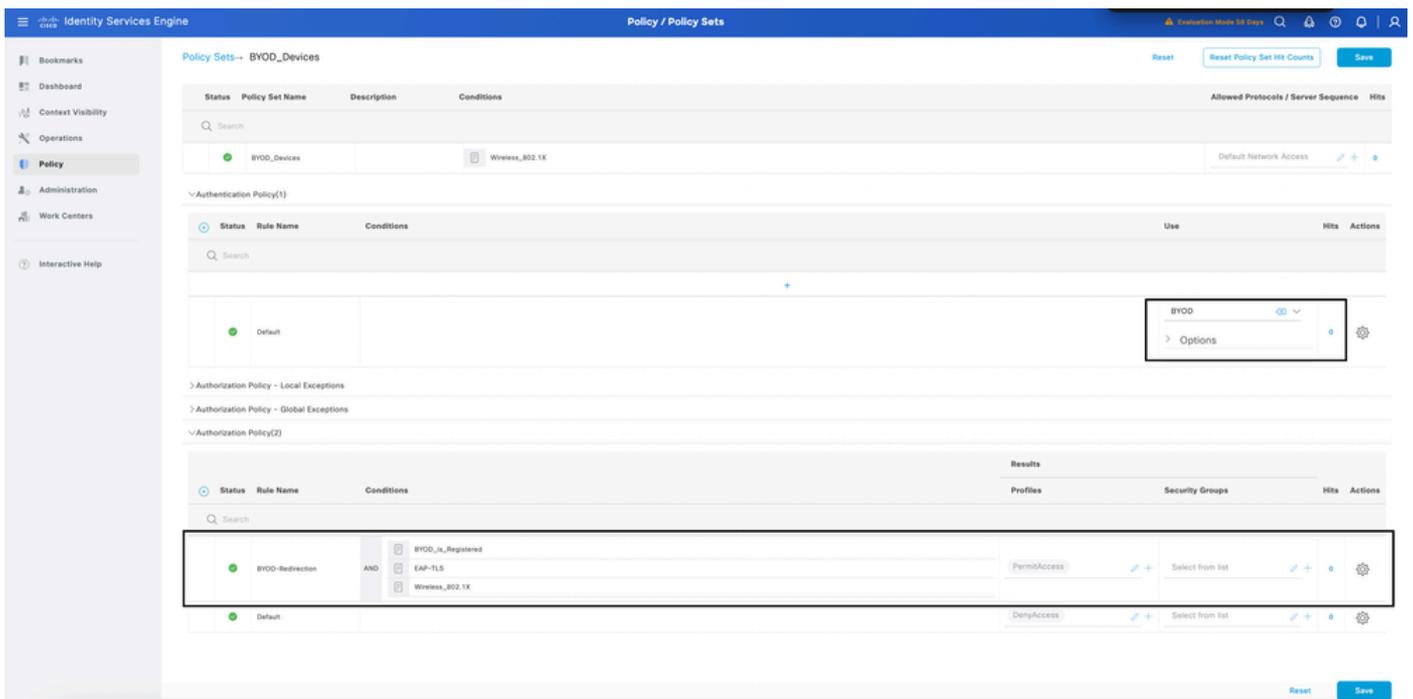


3. No conjunto Política de integração, localize Continuar selecionado nas opções. Para a política de autorização, crie uma condição e mapeie o perfil de autorização de redirecionamento. As mesmas etapas estão envolvidas na criação do perfil de autorização, que pode ser encontrado no ponto 4.



4. No Conjunto de políticas registradas de BYOD, configure a política de autenticação com o mesmo perfil de certificado encontrado.

em Configure ISE Policy Sets for Single SSID BYOD no ponto 2. Além disso, crie uma condição para a política de autorização e mapeie o perfil de acesso completo para a política.



## Registro

No registro ao vivo do ISE, a autenticação do usuário seria bem-sucedida e será redirecionada para a página do portal BYOD. Após concluir o fluxo de BYOD, o usuário receberá acesso à rede

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authorization Policy	Authoriz...	IP Address	Network De...	Device
Feb 24, 2025 12:30:18.1...	<span style="color: blue;">●</span>		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...	<span style="color: green;">■</span>			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...	<span style="color: green;">■</span>			test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...	BYOD-Switch	TenGig...

Da perspectiva do usuário, eles seriam redirecionados primeiro para a página BYOD e o dispositivo apropriado precisaria ser selecionado na página da Web. Para testar se um dispositivo com Windows 10 foi usado

CISCO
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

Depois de clicar no botão Avançar, você será direcionado para uma página onde o usuário será solicitado a inserir o nome do dispositivo e a descrição

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 contains the following text: 'Enter the device name and optional description for this device so you can manage it using the My Devices Portal.' Below this text are three input fields: 'Device name: \*' with a text box, 'Description:' with a text box, and 'Device ID:' with a blacked-out field. At the bottom of the form is a blue button labeled 'Continue' with a right-pointing arrow.

Post que o usuário seria solicitado a fazer o download da ferramenta Network Assistant para fazer o download do perfil de ponto final e do certificado EAP TLS para autenticação, se o perfil estiver configurado para executar a autenticação 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 text: '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.'

Execute o Network Assistant Application em privilégios de administrador e clique no botão Iniciar para iniciar o fluxo de integração:



## Network Setup Assistant

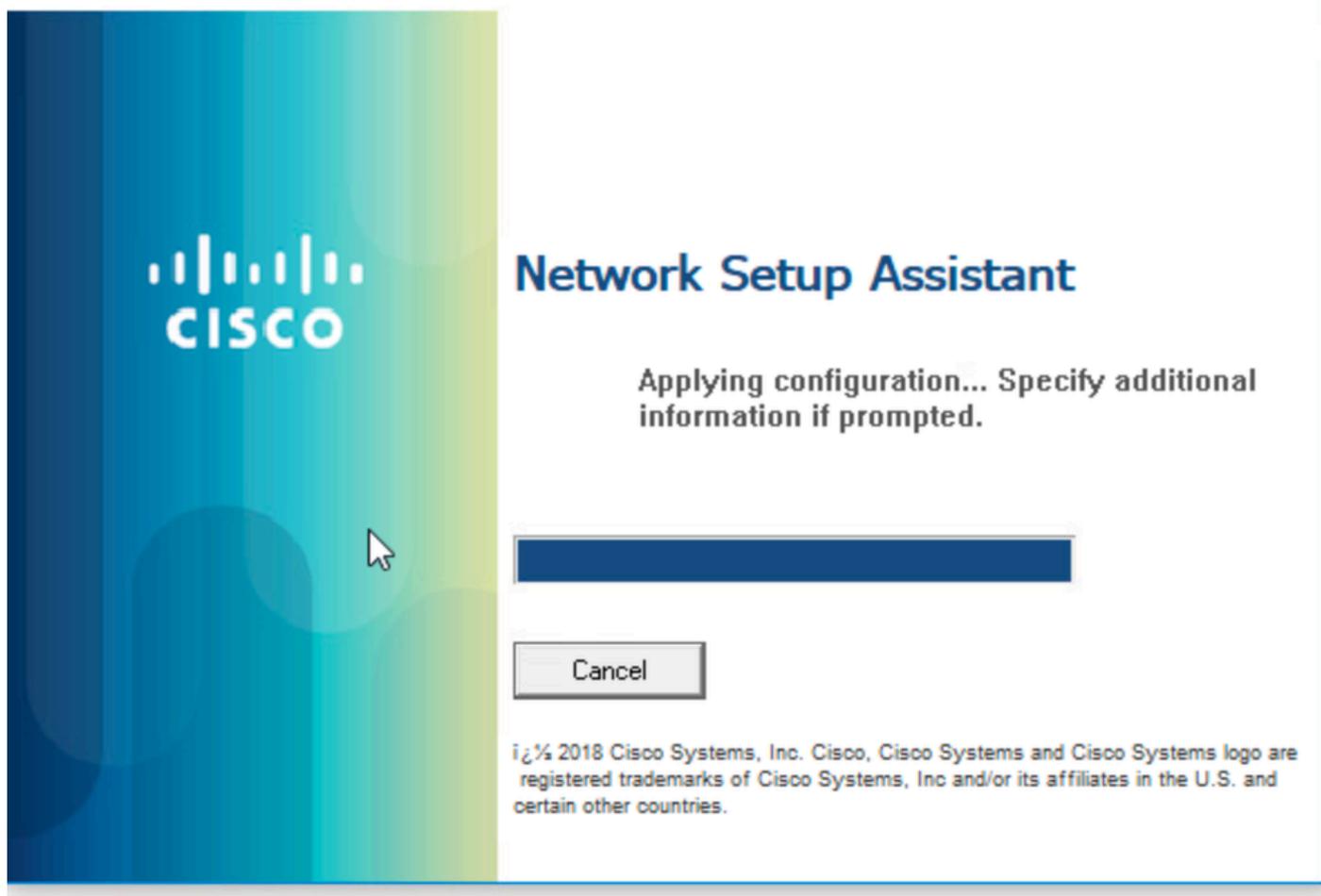


This application automatically configures network settings.

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.



O usuário foi integrado com êxito na rede com seu dispositivo pessoal para acessar os recursos.

## Troubleshooting

Para solucionar o problema com BYOD, habilite essa depuração no ISE

Atributos a serem definidos para o nível de depuração:

- 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)

# Trecho de log

## Logs de convidado

Esses registros indicam que o usuário redirecionou com êxito para a página e fez o download do Network Assistant Application:

```
2025-02-24 12:06:08,053 INFORMAÇÕES [https-jsse-nio-10.127.196.172-8443-exec-4][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5::-
caminho de mapeamento encontrado em forwardaction-forwards, fazendo a:
pages/byodWelcome.jsp // A página de boas-vindas do BYOD
2025-02-24 12:06:09,968 INFORMAÇÕES [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:-
Tamanho do pTranSteps:1
2025-02-24 12:06:09,968 INFORMAÇÕES [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:-
getNextFlowStep, pTranSteps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFORMAÇÕES [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:-
getNextFlowStep, stepTran:d25 13b7b-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::-
caminho de mapeamento encontrado em action-forwards, encaminhando para:
pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFORMAÇÕES [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:-
Tamanho do pTranSteps:1
2025-02-24 12:06:14,643 INFORMAÇÕES [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:-
getNextFlowStep, pTranSteps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFORMAÇÕES [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5:::test:-
getNextFlowStep, stepTran:f20 3b757-9e8a-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::-
caminho de mapeamento encontrado em action-forwards, encaminhando para:
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::- Sessão = 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 = nulo
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 / O aplicativo de Assistência de rede foi enviado ao
```

ponto de extremidade

## Logs Ise-Psc

À medida que o aplicativo é baixado para o endpoint, o aplicativo inicia um fluxo SCEP para obter o certificado do cliente do ISE.

```
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- CertStore contém 4 certificados:
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. '[issur=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 -::::- Selecionando o certificado de criptografia
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selecionando o certificado com keyEncippherment
keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1 certificado(s) encontrado(s) com keyEncippherment
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 criptografia de
mensagens
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selecionando certificado de verificador
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selecionando certificado com digitalSignature keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1 certificado(s) encontrado(s) com 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 verificação de
mensagem
```

2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler\_Worker-5][[]]  
org.jscep.client.CertStoreInspector -::::- Selecionando certificado do emissor  
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler\_Worker-5][[]]  
org.jscep.client.CertStoreInspector -::::- Selecionando certificado com basicConstraints  
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler\_Worker-5][[]]  
org.jscep.client.CertStoreInspector -::::- Foram encontrados 3 certificados com 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 emissor  
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler\_Worker-5][[]]  
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- Métricas de desempenho de servidores SCEP :  
name[live/dead, total de solicitações, total de falhas, solicitações de entrada, RTT médio]  
[http://127.0.0.1:9444/caservice/scep\[ao vivo,96444,1,0,120\]](http://127.0.0.1:9444/caservice/scep[ao vivo,96444,1,0,120])

## Download de Perfil de Endpoint

Após a conclusão do processo SCEP e a instalação do certificado pelo endpoint, o aplicativo faz o download do perfil do endpoint para autenticação futura, que seria executada pelo dispositivo:

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]  
cisco.cpm.client.provisioning.EvaluationServlet -::::- Referência = Windows // O dispositivo  
Windows foi detectado com base na página da Web  
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]  
cisco.cpm.client.provisioning.EvaluationServlet -::::- Sessão = 0000000000000000B30D59CC5  
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]  
cisco.cpm.client.provisioning.EvaluationServlet -::::- Sessão = 0000000000000000B30D59CC5  
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]  
cisco.cpm.client.provisioning.EvaluationServlet -::::- provisionar perfil nsp  
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- Sessão = 0000000000000000B30D59CC5  
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionId = nulo  
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//O perfil NSP é baixado para o endpoint  
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- Streaming para ip: tipo de arquivo: Nome do  
arquivo NativeSPProfile: Cisco-ISE-NSP.xml //O aplicativo Network Assistant  
24-02-2025 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 foi definido para teste  
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]  
cisco.cpm.client.provisioning.StreamingServlet -::::- o tipo de redirecionamento é:

SUCCESS\_PAGE, a URL de redirecionamento é: para mac:

## Sobre esta tradução

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

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

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