

Configurazione di Single SSID Wireless BYOD su Windows e ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Teoria](#)

[Configurazione](#)

[Configurazione di ISE](#)

[Configurazione WLC](#)

[Verifica](#)

[Verifica flusso di autenticazione](#)

[Controlla il portale I miei dispositivi](#)

[Risoluzione dei problemi](#)

[Informazioni generali](#)

[Analisi log di lavoro](#)

[Log ISE](#)

[Log client \(log spw\)](#)

Introduzione

In questo documento viene descritto come configurare Bring Your Own Device (BYOD) su Cisco Identity Services Engine (ISE) per i computer Windows con Single-SSID e Dual-SSID.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco ISE versioni 3.0
- Configurazione di Cisco WLC
- BYOD funzionante

Componenti usati

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

- Cisco ISE versione 3.0
- Windows 10

- WLC e AP

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

Teoria

In Single SSID BYOD viene utilizzato un solo SSID per entrambe le operazioni di caricamento dei dispositivi e per consentire in seguito l'accesso completo ai dispositivi registrati. L'utente si connette innanzitutto al SSID utilizzando il nome utente e la password (MSCHAPv2). Una volta autenticato correttamente su ISE, l'utente viene reindirizzato al portale BYOD. Al termine della registrazione del dispositivo, il client finale scarica NSA (Native Supplicant Assistant) da ISE. NSA viene installato sul client finale e scarica il profilo e il certificato da ISE. L'NSA configura il supplicant wireless e il client installa il certificato. L'endpoint esegue un'altra autenticazione allo stesso SSID utilizzando il certificato scaricato utilizzando EAP-TLS. ISE controlla la nuova richiesta dal client, verifica il metodo EAP e la registrazione del dispositivo e fornisce l'accesso completo al dispositivo.

Passaggi di Windows BYOD Single SSID-

- Autenticazione iniziale EAP-MSCHAPv2
- Reindirizzamento al portale BYOD
- Registrazione dispositivo
- Download NSA
- Download profilo
- Download certificato
- Autenticazione EAP-TLS

Configurazione

Configurazione di ISE

Passaggio 1. Aggiungere un dispositivo di rete ad ISE e configurare RADIUS e la chiave condivisa.

Selezionare **ISE > Administration > Network Devices > Add Network Device**.

Passaggio 2. Creare un modello di certificato per gli utenti BYOD. L'utilizzo chiavi avanzato per l'autenticazione del client deve essere impostato per il modello. È possibile utilizzare il modello EAP_Certificate_Template predefinito.

Cisco ISE Administration - System

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

Edit Certificate Template

Certificate Management >

Certificate Authority v

Overview

Issued Certificates

Certificate Authority Certifica...

Internal CA Settings

Certificate Templates

External CA Settings

* Name BYOD_Certificate_template

Description

Subject

Common Name (CN) \$UserName\$ ⓘ

Organizational Unit (OU) tac

Organization (O) cisco

City (L) bangalore

State (ST) Karnataka

Country (C) IN

Subject Alternative Name (SAN) ⋮ MAC Address v

Key Type RSA v

Key Size 2048 v

* SCEP RA Profile ISE Internal CA v

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

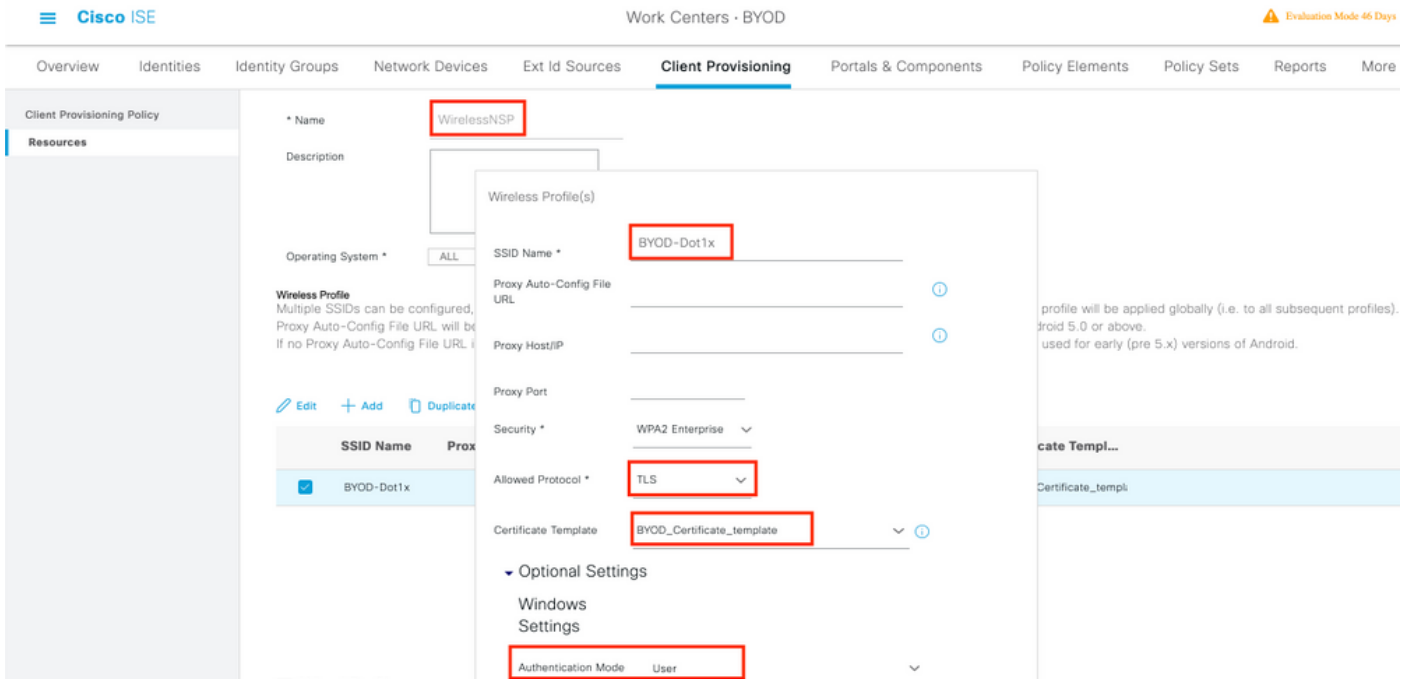
Extended Key Usage Client Authentication Server Authentication

Passaggio 3. Creare un profilo supplicant nativo per un profilo wireless.

Selezionare **ISE > Work Center > BYOD > Client Provisioning**. Fare clic su **Add** (Aggiungi), quindi selezionare **NSP (Native Supplicant Profile)** dall'elenco a discesa.

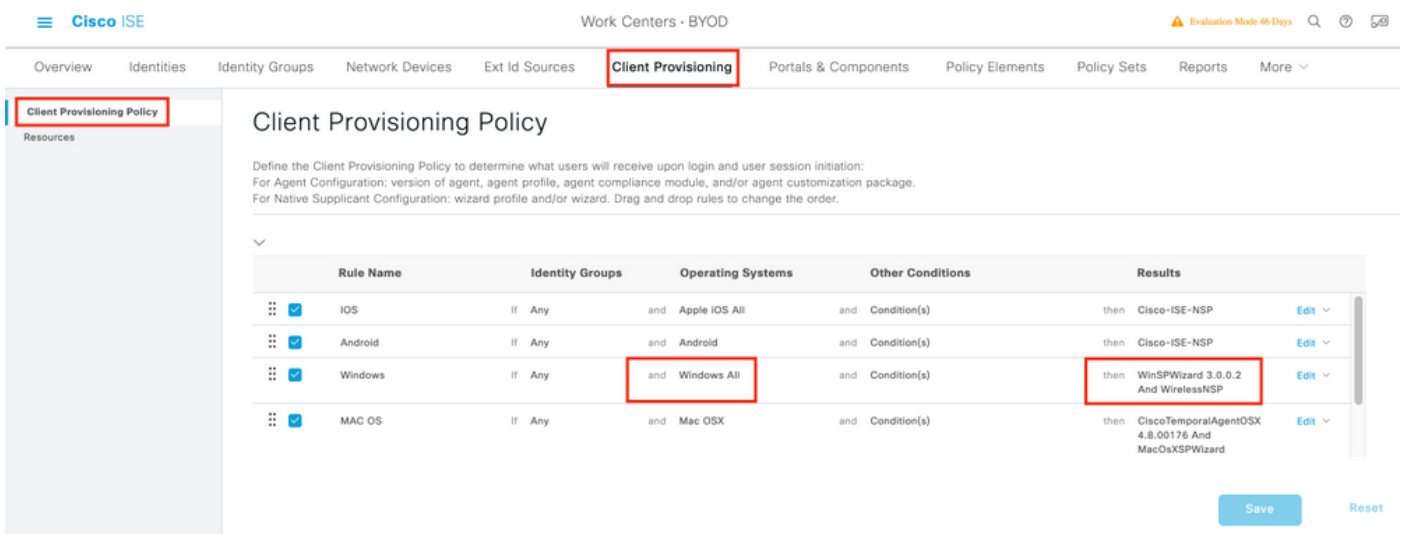
In questo caso, il nome SSID deve essere lo stesso utilizzato per la connessione prima di eseguire un BYOD SSID singolo. Selezionare il protocollo come TLS. Scegliere il modello di certificato creato nel passaggio precedente oppure utilizzare il modello di certificato EAP_Certificate_Template predefinito.

In Impostazioni facoltative selezionare l'autenticazione utente o utente e computer in base alle proprie esigenze. In questo esempio viene configurata come autenticazione utente. Lasciare le altre impostazioni come predefinite.



Passaggio 4. Creare i criteri di provisioning client per il dispositivo Windows.

Selezionare ISE > Work Center > BYOD > Client Provisioning > Client Provisioning Policy. Selezionare il sistema operativo come Windows ALL. Selezionare WinSPWizard 3.0.0.2 e NSP creati nel passaggio precedente.



Passaggio 5. Creare un profilo di autorizzazione per le periferiche non registrate come periferiche BYOD.

Selezionare ISE > Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add.

In Task comune, selezionare Provisioning supplicant nativo. Definire un nome ACL di reindirizzamento creato sul WLC e selezionare il portale BYOD. Viene utilizzato il portale predefinito. È possibile creare un portale BYOD personalizzato. Selezionare ISE > Work Center > BYOD > Portals and components e fare clic su Add.

Dictionarys Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

* Name **BYOD_Wireless_Redirect**

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

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

Native Supplicant Provisioning ACL BYOD-Initial Value BYOD Portal (default)

Passaggio 6. Creare un profilo certificato.

Selezionare ISE > Amministrazione > Origini identità esterne > Profilo certificato. Creare un nuovo profilo certificato o utilizzare quello predefinito.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- Certificate Authentication F
- cert_profile**
- Preloaded_Certificate_Prof
- Active Directory
- ADJoints
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Certificate Authentication Profiles List > cert_profile

Certificate Authentication Profile

* Name **cert_profile**

Description

Identity Store [not applicable]

Use Identity From Certificate Attribute Subject - Common N: ⓘ

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

Passaggio 7. Creare una sequenza di origine identità e selezionare il profilo certificato creato nel passaggio precedente oppure utilizzare il profilo certificato predefinito. Questa operazione è necessaria quando gli utenti eseguono EAP-TLS dopo la registrazione BYOD per ottenere l'accesso completo.

[Identity Source Sequences List](#) > For_Teap

Identity Source Sequence

Identity Source Sequence

* Name

BYOD_id_Store

Description

Certificate Based Authentication



Select Certificate Authentication Profile

cert_profile



Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

Internal Endpoints

Guest Users

Selected

Internal Users

ADJoiint

Passaggio 8. Creare un set di criteri, un criterio di autenticazione e un criterio di autorizzazione.

Selezionare **ISE > Policy > Policy Sets**. Creare un set di criteri e **salvarlo**.

Creare un criterio di autenticazione e selezionare la sequenza di origine dell'identità creata nel passaggio precedente.

Creare un criterio di autorizzazione. È necessario creare due criteri.

1. Per i dispositivi non registrati BYOD. Fornire il profilo di reindirizzamento creato al passaggio 5.
2. Dispositivi registrati BYOD che eseguono EAP-TLS. Concedi accesso completo a questi dispositivi.

Authentication Policy (1)

Status	Rule Name	Conditions	Use
+		Search	
+			
+			
+			
+			
	Default		BYOD_id_Store Options

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results	Profiles	Security Groups
+		Search			
+					
	Full_Access	AND Network Access-EapAuthentication EQUALS EAP-TLS EndPoints-BYODRegistration EQUALS Yes	PermitAccess x	+	Select from list
	BYOD_Redirect	EndPoints-BYODRegistration EQUALS Unknown	BYOD_Wireless_Redire... x	+	Select from list

Configurazione WLC

Passaggio 1. Configurare il server Radius su WLC.

Selezionare **Sicurezza > AAA > Radius > Autenticazione**.

The screenshot shows the 'RADIUS Authentication Servers > Edit' configuration page. The left sidebar contains a navigation tree under 'Security' with 'AAA' expanded to show 'RADIUS' options. The main content area shows configuration fields for server index, address, shared secret, and various authentication settings. Several fields are highlighted with red boxes: 'Server Index' (7), 'Server Address(Ipv4/Ipv6)' (10.106.32.119), 'Apply Cisco ISE Default settings' (checked), 'Port Number' (1812), and 'Support for CoA' (Enabled).

Server Index	7
Server Address(Ipv4/Ipv6)	10.106.32.119
Shared Secret Format	ASCII
Shared Secret
Confirm Shared Secret
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	<input checked="" type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
Realm List	Realm List
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Selezionare Sicurezza > AAA > Raggio > Contabilità.

The screenshot shows the Cisco configuration interface for RADIUS Accounting Servers. The left sidebar is under 'Security' > 'AAA' > 'RADIUS'. The main content area is titled 'RADIUS Accounting Servers > Edit' and shows configuration for server index 7. The following fields are highlighted with red boxes:

- Server Address(Ipv4/Ipv6): 10.106.32.119
- Port Number: 1813

Other visible settings include: Shared Secret Format (ASCII), Shared Secret (masked), Confirm Shared Secret (masked), Apply Cisco ACA Default settings (unchecked), Server Status (Enabled), Server Timeout (5 seconds), Network User (checked), Management (unchecked), Tunnel Proxy (unchecked), PAC Provisioning (unchecked), IPsec (unchecked), and Cisco ACA (unchecked).

Passaggio 2. Configurare un SSID Dot1x.

The screenshot shows the Cisco configuration interface for WLANs. The left sidebar is under 'WLANs' > 'Advanced'. The main content area is titled 'WLANs > Edit 'BYOD-Dot1x''. The 'General' tab is selected and highlighted with a red box. The following fields are highlighted with red boxes:

- Profile Name: BYOD-Dot1x
- Type: WLAN
- SSID: BYOD-Dot1x
- Status: Enabled
- Interface/Interface Group(G): management

Other visible settings include: Security Policies ([WPA2][Auth(802.1X)]), Radio Policy (All), Multicast Vlan Feature (unchecked), Broadcast SSID (checked), NAS-ID (none), and Lobby Admin Access (unchecked).

WLANs

- WLANs
- Advanced

WLANs > Edit 'BYOD-Dot1x'

General Security **QoS** Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security

Security Type

MAC Filtering

WPA2+WPA3 Parameters

Policy WPA2 WPA3

Encryption Cipher CCMP128(AES) CCMP256 GCMP128 GCMP256

Fast Transition

Fast Transition

Over the DS

Reassociation Timeout Seconds

Protected Management Frame

PMF

Authentication Key Management

802.1X-SHA1 Enable

WLANs

- WLANs
- Advanced

WLANs > Edit 'BYOD-Dot1x'

General Security **QoS** Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

Apply Cisco ISE Default Settings Enabled

Authentication Servers

Accounting Servers

Server	Enabled	IP:Port	Enabled	IP:Port
Server 1	<input checked="" type="checkbox"/>	IP:10.106.32.119, Port:1812	<input checked="" type="checkbox"/>	IP:10.106.32.119, Port:1813
Server 2	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 3	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 4	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 5	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 6	<input type="checkbox"/>	None	<input type="checkbox"/>	None

EAP Parameters

Enable

Authorization ACA Server

Accounting ACA Server

Enabled Enabled

Passaggio 3. Configurare l'ACL di reindirizzamento per fornire accesso limitato per il provisioning del dispositivo.

- Consente il traffico UDP verso DHCP e DNS (DHCP è consentito per impostazione predefinita).
- Comunicazione ad ISE.
- Negare il traffico di altro tipo.

Nome: BYOD-Initial (O qualsiasi nome assegnato manualmente all'ACL nel profilo di autorizzazione)

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	10.106.32.119 / 255.255.255.255	Any	Any	Any	Any	Any	0
3	Permit	10.106.32.119 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
4	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

Verifica

Verifica flusso di autenticazione

Live Logs Live Sessions

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	1	0	0

Refresh Never Show Latest 20 records Within Last 5 minutes

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Identity Group	Authenti...	Authorization Policy	Authorization Profiles	Ei
Nov 29, 2020 11:13:47.4...	●		0	dot1xuser	50:3E:AA:E4:8...		Wireless >...	Wireless >> Full_Access	PermitAccess	W
Nov 29, 2020 11:13:47.2...	■			dot1xuser	50:3E:AA:E4:8...	RegisteredDevices	Wireless >...	Wireless >> Full_Access	PermitAccess	W
Nov 29, 2020 11:10:57.9...	■			dot1xuser	50:3E:AA:E4:8...	Profiled	Wireless >...	Wireless >> BYOD_Redirect	BYOD_Wireless_Redirect	TF

1. Al primo accesso, l'utente esegue l'autenticazione PEAP utilizzando un nome utente e una password. Ad ISE, l'utente visita la pagina Redirect Rule BYOD-Redirect.

Cisco ISE

Overview


Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Endpoint Profile	TP-LINK-Device
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> BYOD_Redirect
Authorization Result	BYOD_Wireless_Redirect

Authentication Details

Source Timestamp	2020-11-29 11:10:57.955
Received Timestamp	2020-11-29 11:10:57.955
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
User Type	User
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	TP-LINK-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	WLC1

2. Dopo la registrazione BYOD, l'utente viene aggiunto al dispositivo registrato ed ora esegue EAP-TLS e ottiene l'accesso completo.

Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6 
Endpoint Profile	Windows10-Workstation
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> Full_Acceed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2020-11-29 11:13:47.246
Received Timestamp	2020-11-29 11:13:47.246
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	Windows10-Workstation
Identity Group	RegisteredDevices
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	WLC1

Controlla il portale I miei dispositivi

Passare al portale MyDevices e accedere con le credenziali. È possibile visualizzare il nome del dispositivo e lo stato di registrazione.

È possibile creare un URL per il portale MyDevices.

Selezionare **ISE > Work Center > BYOD > Portal and Components > My Devices Portal > Login Settings (ISE > Centri di lavoro > BYOD > Portale e componenti > My Devices Portal > Impostazioni di accesso)**, quindi immettere l'URL completo.

Manage Devices
 Need to add a device? Select **Add**. Was your device lost or stolen? Select your device from the list to manage it.
 Number of registered devices:2/5

Add **Refresh**

MAC Address...

Lost Stolen Edit PIN Lock Full Wipe Unenroll Reinststate Delete

<input type="checkbox"/>	MAC Address	Device Name	Description	Status
<input type="checkbox"/>	50:3E:AA:E4:81:B6	MyWindows_Device		Registered

Risoluzione dei problemi

Informazioni generali

Per il processo BYOD, questi componenti ISE devono essere abilitati nel debug sui nodi PSN -

scep: messaggi di log scep. File di log di destinazione **guest.log** e **ise-psc.log**.

client-webapp: il componente responsabile dei messaggi di infrastruttura. File di log di destinazione **-ise-psc.log**

portal-web-action: componente responsabile dell'elaborazione dei criteri di provisioning client. File di log di destinazione **-guest.log**.

portale: tutti gli eventi correlati al portale. File di log di destinazione **-guest.log**

portal-session-manager -File di log di destinazione - **Messaggi di debug correlati alla sessione del portale - gues.log**

ca-service-ca-service messages -Target log files **-caservice.log** and **caservice-misc.log**

ca-service-cert-ca-service messaggi di certificato - File di log di destinazione - **caservice.log** e **caservice-misc.log**

admin-ca-ca-service messaggi admin -File di log di destinazione **ise-psc.log**, **caservice.log** e **caservice-misc.log**

certprovisioningportal- messaggi del portale per il provisioning dei certificati - **file di registro di destinazione ise-psc.log**

nsf - Messaggi correlati a NSF - File di log di destinazione **ise-psc.log**

nsf-session- Messaggi relativi alla cache della sessione - File di log di destinazione **ise-psc.log**

runtime-AAA: tutti gli eventi di runtime. File di log di destinazione **-prrt-server.log**.

Per i log sul lato client:

Cercare %temp%\spwProfileLog.txt (ad esempio:
C:\Users\\AppData\Local\Temp\spwProfileLog.txt)

Analisi log di lavoro

Log ISE

Access-Accept iniziale con ACL di reindirizzamento e URL di reindirizzamento per il portale BYOD.

Port-server.log-

```
Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30-  
primary/392215758/699,CPMSessionID=0a6a21b20000009f5fc770c7,user=dotluser,CallingStationID=50-  
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=254 Length=459 [1] User-Name -  
value: [dotluser] [25] Class - value: [****] [79] EAP-Message - value: [ñ [80] Message-  
Authenticator - value: [.2{wëbÛ"Åp05<Z] [26] cisco-av-pair - value: [url-redirect-acl=BYOD-  
Initial] [26] cisco-av-pair - value: [url-  
redirect=https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009f5fc770c7&portal=7f8  
ac563-3304-4f25-845d-be9faac3c44f&action=nsp&token=53a2119de6893df6c6fca25c8d6bd061] [26] MS-  
MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-Key - value: [****] ,RADIUSHandler.cpp:2216
```

Quando un utente finale tenta di accedere a un sito Web e viene reindirizzato da WLC all'URL di reindirizzamento di ISE.

Guest.log -

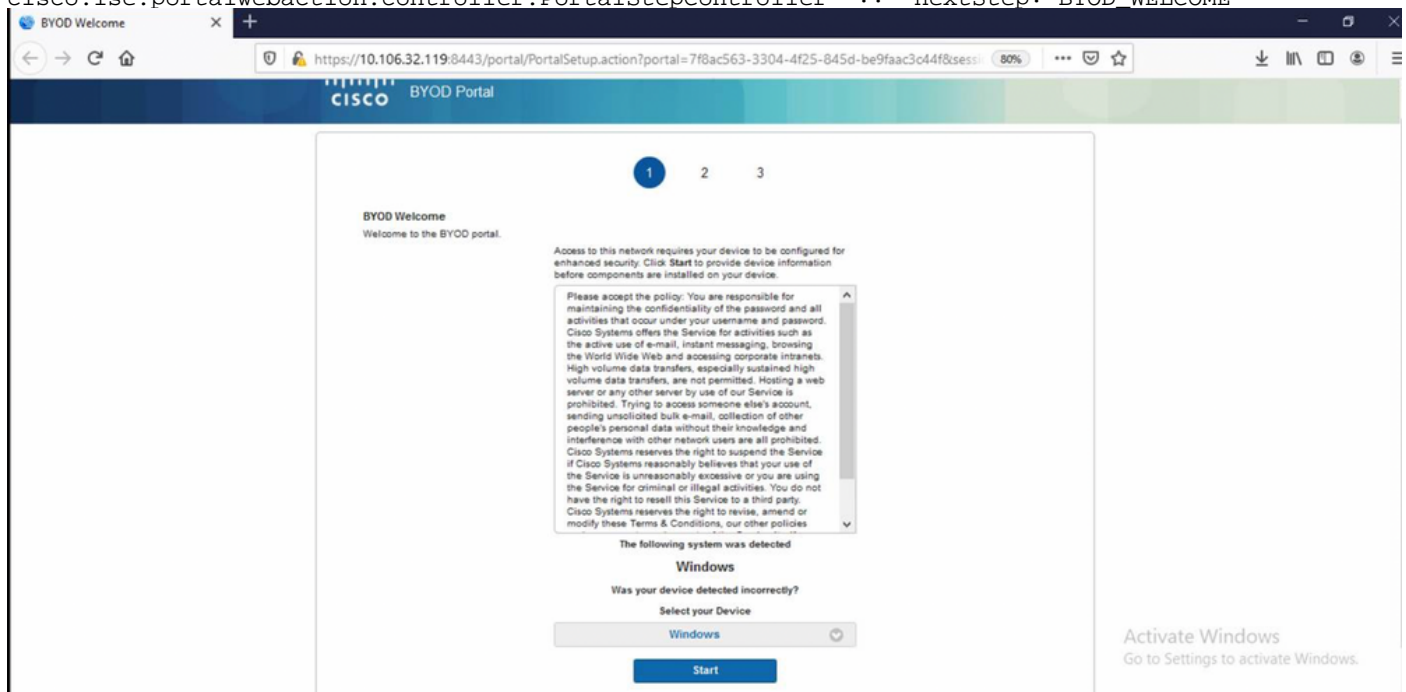
```
2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][  
com.cisco.ise.portal.Gateway -::- Gateway Params (after update):  
redirect=www.msftconnecttest.com/redirect client_mac=null daysToExpiry=null ap_mac=null  
switch_url=null wlan=null action=nsp sessionId=0a6a21b20000009f5fc770c7 portal=7f8ac563-3304-  
4f25-845d-be9faac3c44f isExpired=null token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02  
05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][  
cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- sessionId=0a6a21b20000009f5fc770c7 :  
token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-5][ cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- Session  
token successfully validated. 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-  
exec-5][ cisco.ise.portal.util.PortalUtils -::- UserAgent : Mozilla/5.0 (Windows NT 10.0;  
Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-5][ cisco.ise.portal.util.PortalUtils -::- isMozilla: true 2020-12-02  
05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][ com.cisco.ise.portal.Gateway -  
::- url: /portal/PortalSetup.action?portal=7f8ac563-3304-4f25-845d-  
be9faac3c44f&sessionId=0a6a21b20000009f5fc770c7&action=nsp&redirect=www.msftconnecttest.com%2Fre  
direct 2020-12-02 05:43:58,355 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][  
cisco.ise.portalwebaction.controller.PortalFlowInterceptor -::- start guest flow interceptor...  
2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][  
cisco.ise.portalwebaction.actions.BasePortalAction -::- Executing action PortalSetup via request  
/portal/PortalSetup.action 2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-  
exec-7][ cisco.ise.portalwebaction.actions.PortalSetupAction -::- executeAction... 2020-12-02  
05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][  
cisco.ise.portalwebaction.actions.BasePortalAction -::- Result from action, PortalSetup: success  
2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][  
cisco.ise.portalwebaction.actions.BasePortalAction -::- Action PortalSetup Complete for request  
/portal/PortalSetup.action 2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-  
exec-7][ cpm.guestaccess.flowmanager.processor.PortalFlowProcessor -::- Current flow step:  
INIT, otherInfo=id: 226ea25b-5e45-43f5-b79d-fb59cab96def 2020-12-02 05:43:58,361 DEBUG [https-  
jsse-nio-10.106.32.119-8443-exec-7][ cpm.guestaccess.flowmanager.step.StepExecutor -::- Getting  
next flow step for INIT with TranEnum=PROCEED 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
```



```

10.106.32.119-8443-exec-7][[] cpm.guestaccess.flowmanager.step.StepExecutor -:- StepTran for
Step=INIT=> tranEnum=PROCEED, toStep=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-7][[] cpm.guestaccess.flowmanager.step.StepExecutor -:- Find Next
Step=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][[]
cpm.guestaccess.flowmanager.step.StepExecutor -:- Step : BYOD_WELCOME will be visible! 2020-12-
02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][[]
cpm.guestaccess.flowmanager.step.StepExecutor -:- Returning next step =BYOD_WELCOME 2020-12-02
05:43:58,362 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][[]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -:- Looking up Guest user with
uniqueSubjectId=5f5592a4f67552b855ecc56160112db42cf7074e 2020-12-02 05:43:58,365 DEBUG [https-
jsse-nio-10.106.32.119-8443-exec-7][[]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -:- Found Guest user 'dotlxuserin
DB using uniqueSubjectID '5f5592a4f67552b855ecc56160112db42cf7074e'. authStoreName in
DB=Internal Users, authStoreGUID in DB=9273fe30-8c01-11e6-996c-525400b48521. DB ID=bab8f27d-
c44a-48f5-9fe4-5187047bffc0 2020-12-02 05:43:58,366 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][[] cisco.ise.portalwebaction.controller.PortalStepController -:- ++++ updatePortalState:
PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is INITIATED and current step
is BYOD_WELCOME 2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][[]
com.cisco.ise.portalSessionManager.PortalSession -:- Setting the portal session state to ACTIVE
2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][[]
cisco.ise.portalwebaction.controller.PortalStepController -:- nextStep: BYOD_WELCOME

```



Fare clic su **Start** nella pagina di benvenuto di BYOD.

```

2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][[]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- Executing action ByodStart via
request /portal/ByodStart.action 2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3][[] cisco.ise.portalwebaction.controller.PortalPreResultListener -:dotlxuser:-
currentStep: BYOD_WELCOME

```

A questo punto, ISE valuta se i file/le risorse necessari per BYOD sono presenti o meno e si imposta sullo stato BYOD INIT.

```

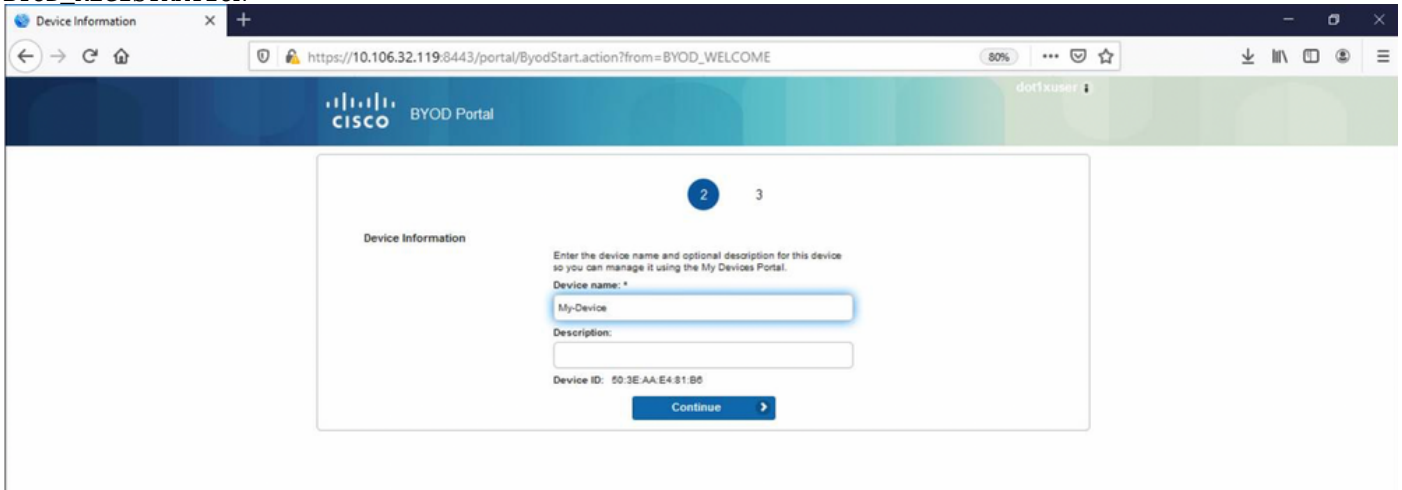
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][[]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dotlxuser:- userAgent=Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All),
nspStatus=SUCCESS 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][[]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dotlxuser:- NSP Downloadable
Resource data=>, resource=DownloadableResourceInfo :WINDOWS_10_ALL

```

```

https://10.106.32.119:8443/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b2000009f5fc770c7&os=WINDOWS_10_ALL null null
https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/ null
null https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-
81141ec42d2d/NetworkSetupAssistant.exe, coaType=NoCoa 2020-12-02 05:44:01,936 DEBUG [https-jsse-
nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager.utils.NSPProvAccess -:dotlxuser:-
It is a WIN/MAC! 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cpm.guestaccess.flowmanager.step.StepExecutor -:dotlxuser:- Returning next step
=BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.controller.PortalStepController -:dotlxuser:- +++ updatePortalState:
PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE and current step is
BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.controller.PortalStepController -:dotlxuser:- nextStep:
BYOD_REGISTRATION

```

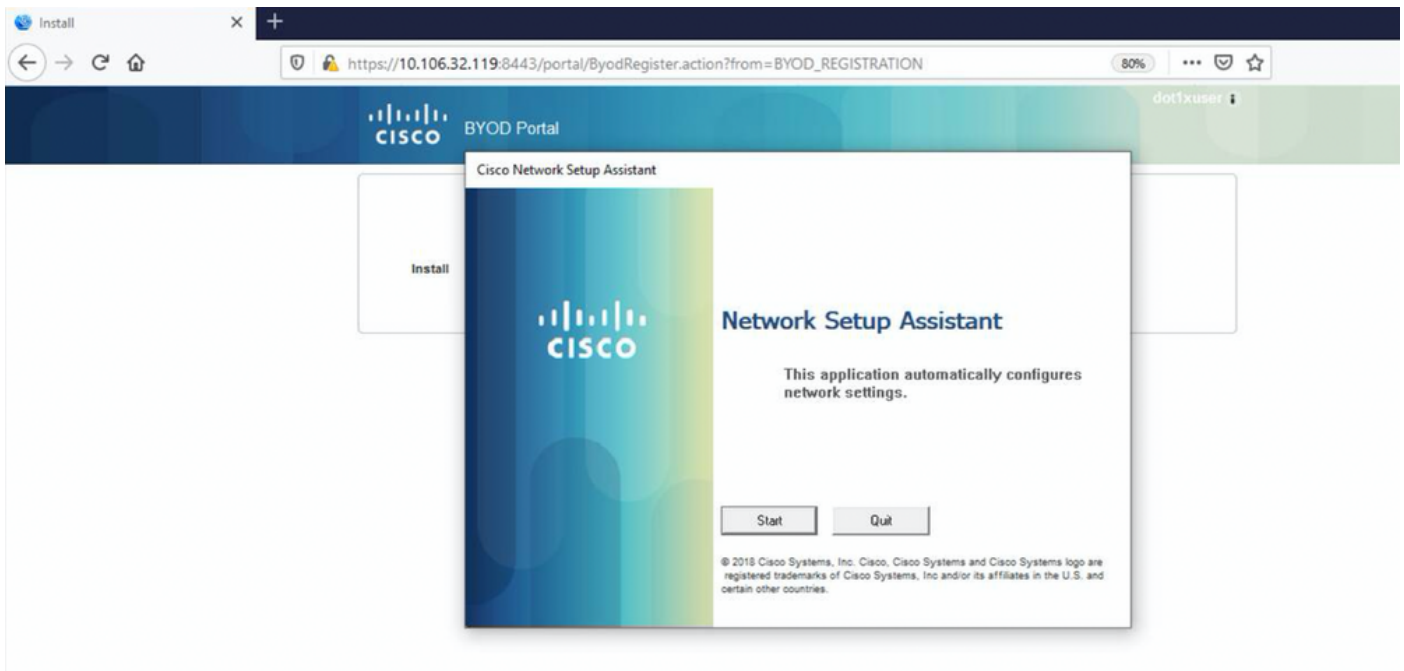


Immettere il nome del dispositivo e fare clic su Register.

```

2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- Executing action ByodRegister
via request /portal/ByodRegister.action Request Parameters: from=BYOD_REGISTRATION
token=PZBMFBHX3FBPXT8QF98U717ILNOTD68D device.name=My-Device device.description= 2020-12-02
05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portal.actions.ByodRegisterAction -:dotlxuser:- executeAction... 2020-12-02
05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- Result from action,
ByodRegister: success 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- Action ByodRegister Complete
for request /portal/ByodRegister.action 2020-12-02 05:44:14,683 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices.mydevices.MyDevicesServiceImpl -
:dotlxuser:- Register Device : 50:3E:AA:E4:81:B6 username= dotlxuser idGroupID= aal3bb40-8bff-
11e6-996c-525400b48521 authStoreGUID= 9273fe30-8c01-11e6-996c-525400b48521 nadAddress=
10.106.33.178 isSameDeviceRegistered = false 2020-12-02 05:44:14,900 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cpm.guestaccess.flowmanager.step.StepExecutor -:dotlxuser:-
Returning next step =BYOD_INSTALL 2020-12-02 05:44:14,902 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-1][] cisco.ise.portalwebaction.controller.PortalStepController -:dotlxuser:- +++
updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE
and current step is BYOD_INSTALL 2020-12-02 05:44:01,954 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3][] cisco.ise.portalwebaction.controller.PortalFlowInterceptor -:dotlxuser:- result:
success 2020-12-02 05:44:14,969 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
URI:/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/NetworkSetupAssistant.exe

```



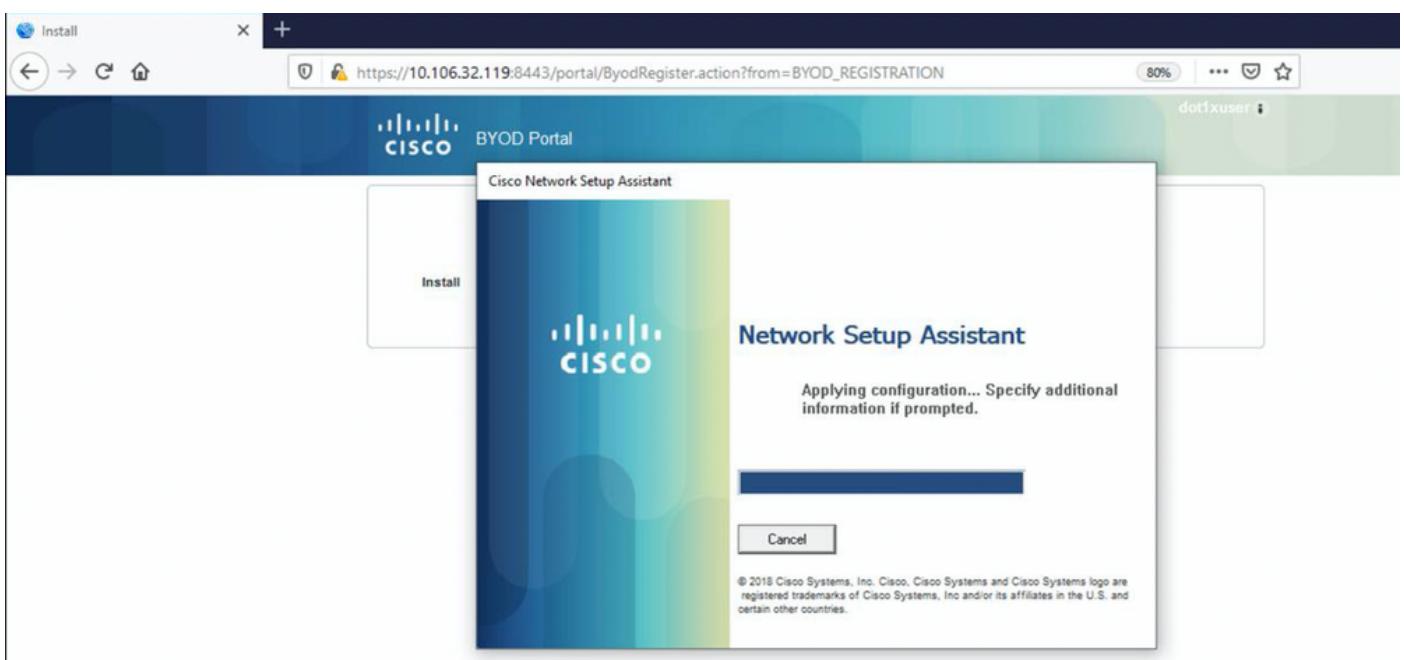
Ora, quando l'utente fa clic su Start sull'NSA, un file denominato **spwProfile.xml** viene creato temporaneamente sul client copiando il contenuto da Cisco-ISE-NSP.xml scaricato sulla porta TCP 8905.

Guest.log -

```
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][[]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
URI:/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-e4ec38ee188c/WirelessNSP.xml 2020-12-02
05:45:03,275 DEBUG [portal-http-service15][[] cisco.cpm.client.provisioning.StreamingServlet -::-
Streaming to ip:10.106.33.167 file type: NativeSPProfile file name:WirelessNSP.xml 2020-12-02
05:45:03,308 DEBUG [portal-http-service15][[] cisco.cpm.client.provisioning.StreamingServlet -::-
SPW profile :: 2020-12-02 05:45:03,308 DEBUG [portal-http-service15][[]
cisco.cpm.client.provisioning.StreamingServlet -::-
```

Dopo aver letto il contenuto di **spwProfile.xml**, l'NSA configura il profilo di rete e genera un CSR e lo invia all'ISE per ottenere un certificato utilizzando l'URL

<https://10.106.32.119:8443/auth/pkclient.exe>



ise-psc.log-

```
2020-12-02 05:45:11,298 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Found incoming certificate request for  
internal CA. Increasing Cert Request counter. 2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-1][ cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Key type  
is RSA, retrieving ScepCertRequestProcessor for caProfileName=ISE Internal CA 2020-12-02  
05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
cisco.cpm.provisioning.cert.CertRequestValidator -::::- Session user has been set to = dotlxuser  
2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
cisco.cpm.scep.util.ScepUtil -::::- Algorithm OID in CSR: 1.2.840.113549.1.1.1 2020-12-02  
05:45:11,331 INFO [https-jsse-nio-10.106.32.119-8443-exec-1][  
com.cisco.cpm.scep.ScepCertRequestProcessor -::::- About to forward certificate request  
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dotlxuser with transaction id n@P~N6E to server  
http://127.0.0.1:9444/caservice/scep 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-1][ org.jscep.message.PkiMessageEncoder -::::- Encoding message:  
org.jscep.message.PkcsReq@5c1649c2[transId=4d22d2e256a247a302e900ffa71c35d75610de67,messageType=  
PKCS_REQ,senderNonce=Nonce  
[7d9092a9fab204bd7600357e38309ee8],messageData=org.bouncycastle.pkcs.PKCS10CertificationRequest@  
4662a5b0] 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
org.jscep.message.PkcsPkiEnvelopeEncoder -::::- Encrypting session key using key belonging to  
[issuer=CN=Certificate Services Endpoint Sub CA - isee30-primary;  
serial=162233386180991315074159441535479499152] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-1][ org.jscep.message.PkiMessageEncoder -::::- Signing message using  
key belonging to [issuer=CN=isee30-primary.anshsinh.local;  
serial=126990069826611188711089996345828696375] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-1][ org.jscep.message.PkiMessageEncoder -::::- SignatureAlgorithm  
SHA1withRSA 2020-12-02 05:45:11,334 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
org.jscep.message.PkiMessageEncoder -::::- Signing  
org.bouncycastle.cms.CMSProcessableByteArray@5aa9dfcc content
```

ca-service.log -

```
2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67  
0x67ee11d5 request] com.cisco.cpm.caservice.CrValidator -::::- performing certificate request  
validation: version [0] subject [C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dotlxuser] ---  
output omitted--- 2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job  
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request validation]  
com.cisco.cpm.caservice.CrValidator -::::- RDN value = dotlxuser 2020-12-02 05:45:11,379 DEBUG  
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request]  
com.cisco.cpm.caservice.CrValidator -::::- request validation result CA_OK
```

caservice-misc.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67  
0x67ee11d5 request issuance] cisco.cpm.scep.util.ScepUtil -::::- Algorithm OID in CSR:  
1.2.840.113549.1.1.1 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job  
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]  
com.cisco.cpm.scep.CertRequestInfo -::::- Found challenge password with cert template ID.
```

caservice.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67  
0x67ee11d5 request issuance] cisco.cpm.caservice.util.CaServiceUtil -::::- Checking cache for  
certificate template with ID: e2c32ce0-313d-11eb-b19e-e60300a810d5 2020-12-02 05:45:11,380 DEBUG  
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]  
com.cisco.cpm.caservice.CertificateAuthority -::::- CA SAN Extensions = GeneralNames: 1: 50-3E-  
AA-E4-81-B6 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job  
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]  
com.cisco.cpm.caservice.CertificateAuthority -::::- CA : add SAN extension... 2020-12-02
```

```
05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5
request issuance] com.cisco.cpm.caservice.CertificateAuthority -:::::- CA Cert Template name =
BYOD_Certificate_template 2020-12-02 05:45:11,395 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
cisco.cpm.caservice.util.CaServiceUtil -:::::- Storing certificate via REST for serial number:
518fa73a4c654df282ffdb026080de8d 2020-12-02 05:45:11,395 INFO [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -:::::- issuing Certificate Services Endpoint
Certificate: class [com.cisco.cpm.caservice.CaResultHolder] [1472377777]: result: [CA_OK]
subject [CN=dot1xuser, OU=tac, O=cisco, L=bangalore, ST=Karnataka, C=IN] version [3] serial
[0x518fa73a-4c654df2-82ffdb02-6080de8d] validity [after [2020-12-01T05:45:11+0000] before [2030-
11-27T07:35:10+0000]] keyUsages [ digitalSignature nonRepudiation keyEncipherment ]
```

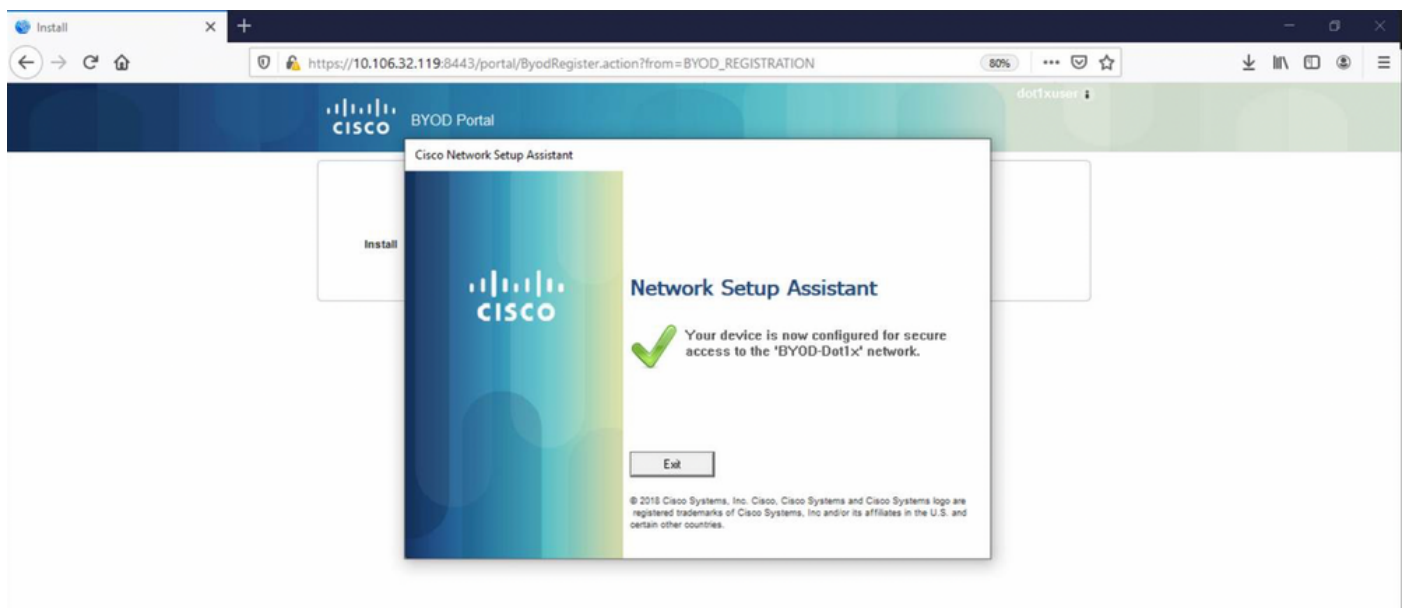
ise-psc.log

```
2020-12-02 05:45:11,407 DEBUG [AsyncHttpClient-15-9][] org.jscep.message.PkiMessageDecoder -
::::- Verifying message using key belonging to 'CN=Certificate Services Endpoint RA - isee30-
primary'
```

caservice.log -

```
2020-12-02 05:45:11,570 DEBUG [Infra-CAServiceUtil-Thread][]
cisco.cpm.caservice.util.CaServiceUtil -:::::- Successfully stored endpoint certificate.
```

ise-psc.log



```
2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -:::::- Performing doGetCertInitial found
Scep certificate processor for txn id n@P~N6E 2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCertRequestProcessor -:::::- Polling
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser for certificate request n@P~N6E with
id {} 2020-12-02 05:45:13,385 INFO [https-jsse-nio-10.106.32.119-8443-exec-10][]
com.cisco.cpm.scep.ScepCertRequestProcessor -:::::- Certificate request Complete for
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser Trx Idn@P~N6E 2020-12-02 05:45:13,596
DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -:::::- BYODStatus:COMPLETE_OTA_NSP
```

Dopo l'installazione del certificato, i client avviano un'altra autenticazione utilizzando EAP-TLS e ottengono l'accesso completo.

port-server.log -

```
Eap,2020-12-02 05:46:57,175,INFO ,0x7f433e6b8700,cntx=0008591342,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,CallingStationID=50-3e-aa-e4-81-
b6,EAP: Recv EAP packet, code=Response, identifier=64, type=EAP-TLS, length=166
,EapParser.cpp:150 Radius,2020-12-02
05:46:57,435,DEBUG,0x7f433e3b5700,cntx=0008591362,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,user=dotluser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=5 Length=231 [1] User-Name -
value: [dotluser] [25] Class - value: [****] [79] EAP-Message - value: [E [80] Message-
Authenticator - value: [Û(ØyËöžö|kÔ,}] [26] MS-MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-
Key - value: [****] ,RADIUSHandler.cpp:2216
```

Log client (log spw)

Il client avvia il download del profilo.

```
[Mon Nov 30 03:34:27 2020] Downloading profile configuration... [Mon Nov 30 03:34:27 2020]
Discovering ISE using default gateway [Mon Nov 30 03:34:27 2020] Identifying wired and wireless
network interfaces, total active interfaces: 1 [Mon Nov 30 03:34:27 2020] Network interface -
mac:50-3E-AA-E4-81-B6, name: Wi-Fi 2, type: unknown [Mon Nov 30 03:34:27 2020] Identified
default gateway: 10.106.33.1 [Mon Nov 30 03:34:27 2020] Identified default gateway: 10.106.33.1,
mac address: 50-3E-AA-E4-81-B6 [Mon Nov 30 03:34:27 2020] DiscoverISE - start [Mon Nov 30
03:34:27 2020] DiscoverISE input parameter : strUrl [http://10.106.33.1/auth/discovery] [Mon Nov
30 03:34:27 2020] [HTTPConnection] CrackUrl: host = 10.106.33.1, path = /auth/discovery, user =
, port = 80, scheme = 3, flags = 0 [Mon Nov 30 03:34:27 2020] [HTTPConnection] HttpSendRequest:
header = Accept: /* headerLength = 12 data = dataLength = 0 [Mon Nov 30 03:34:27 2020] HTTP
Response header: [HTTP/1.1 200 OK Location:
https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009c5fc4fb5e&portal=7f8ac563-
3304-4f25-845d-
be9faac3c44f&action=nsp&token=29354d43962243bcb72193cbf9dc3260&redirect=10.106.33.1/auth/discove
ry [Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path =
/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009c5fc4fb5e&os=WINDOWS_10_ALL, user = , port
= 8443, scheme = 4, flags = 8388608 Mon Nov 30 03:34:36 2020] parsing wireless connection
setting [Mon Nov 30 03:34:36 2020] Certificate template: [keytype:RSA, keysize:2048,
subject:OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN, SAN:MAC] [Mon Nov 30 03:34:36 2020] set
ChallengePwd
```

Il client verifica se il servizio WLAN è in esecuzione.

```
[Mon Nov 30 03:34:36 2020] WirelessProfile::StartWlanSvc - Start [Mon Nov 30 03:34:36 2020]
Wlansvc service is in Auto mode ... [Mon Nov 30 03:34:36 2020] Wlansvc is running in auto
mode... [Mon Nov 30 03:34:36 2020] WirelessProfile::StartWlanSvc - End [Mon Nov 30 03:34:36
2020] Wireless interface 1 - Desc: [TP-Link Wireless USB Adapter], Guid: [{65E78DDE-E3F1-4640-
906B-15215F986CAA}]... [Mon Nov 30 03:34:36 2020] Wireless interface - Mac address: 50-3E-AA-E4-
81-B6 [Mon Nov 30 03:34:36 2020] Identifying wired and wireless interfaces... [Mon Nov 30
03:34:36 2020] Found wireless interface - [ name:Wi-Fi 2, mac address:50-3E-AA-E4-81-B6] [Mon
Nov 30 03:34:36 2020] Wireless interface [Wi-Fi 2] will be configured... [Mon Nov 30 03:34:37
2020] Host - [ name:DESKTOP-965F94U, mac addresses:50-3E-AA-E4-81-B6]
```

Il client inizia ad applicare il profilo -

```
[Mon Nov 30 03:34:37 2020] ApplyProfile - Start... [Mon Nov 30 03:34:37 2020] User Id:
dotluser, sessionid: 0a6a21b20000009c5fc4fb5e, Mac: 50-3E-AA-E4-81-B6, profile: WirelessNSP
[Mon Nov 30 03:34:37 2020] number of wireless connections to configure: 1 [Mon Nov 30 03:34:37
2020] starting configuration for SSID : [BYOD-Dot1x] [Mon Nov 30 03:34:37 2020] applying
certificate for ssid [BYOD-Dot1x]
```

Certificato di installazione client.

```
[Mon Nov 30 03:34:37 2020] ApplyCert - Start... [Mon Nov 30 03:34:37 2020] using ChallengePwd
[Mon Nov 30 03:34:37 2020] creating certificate with subject = dotlxuser and subjectSuffix =
OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN [Mon Nov 30 03:34:38 2020] Self signed certificate
[Mon Nov 30 03:34:44 2020] Installed [isee30-primary.anshsinh.local, hash: 5b a2 08 1e 17 cb 73
5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b ] as rootCA [Mon Nov 30 03:34:44 2020] Installed CA cert
for authMode machineOrUser - Success Certificate is downloaded . Omitted for brevity - [Mon Nov
30 03:34:50 2020] creating response file name C:\Users\admin\AppData\Local\Temp\response.cer
[Mon Nov 30 03:34:50 2020] Certificate issued - successfully [Mon Nov 30 03:34:50 2020]
ScepWrapper::InstallCert start [Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert: Reading scep
response file [C:\Users\admin\AppData\Local\Temp\response.cer]. [Mon Nov 30 03:34:51 2020]
ScepWrapper::InstallCert GetCertHash -- return val 1 [Mon Nov 30 03:34:51 2020]
ScepWrapper::InstallCert end [Mon Nov 30 03:34:51 2020] ApplyCert - End... [Mon Nov 30 03:34:51
2020] applied user certificate using template id e2c32ce0-313d-11eb-b19e-e60300a810d5
```

ISE configura il profilo wireless

```
[Mon Nov 30 03:34:51 2020] Configuring wireless profiles... [Mon Nov 30 03:34:51 2020]
Configuring ssid [BYOD-Dotlx] [Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile -
Start [Mon Nov 30 03:34:51 2020] TLS - TrustedRootCA Hash: [ 5b a2 08 1e 17 cb 73 5f ba 5b 9f a2
2d 3b fc d2 86 0d a5 9b]
```

profilo

```
Wireless interface succesfully initiated, continuing to configure SSID [Mon Nov 30 03:34:51
2020] Currently connected to SSID: [BYOD-Dotlx] [Mon Nov 30 03:34:51 2020] Wireless profile:
[BYOD-Dotlx] configured successfully [Mon Nov 30 03:34:51 2020] Connect to SSID [Mon Nov 30
03:34:51 2020] Successfully connected profile: [BYOD-Dotlx] [Mon Nov 30 03:34:51 2020]
WirelessProfile::SetWirelessProfile. - End [Mon Nov 30 03:35:21 2020]
WirelessProfile::IsSingleSSID - Start [Mon Nov 30 03:35:21 2020] Currently connected to SSID:
[BYOD-Dotlx], profile ssid: [BYOD-Dotlx], Single SSID [Mon Nov 30 03:35:21 2020]
WirelessProfile::IsSingleSSID - End [Mon Nov 30 03:36:07 2020] Device configured successfully.
```