Configurazione di Single SSID Wireless BYOD su Windows e ISE

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
<u>Teoria</u>
Configurazione
Configurazione di ISE
Configurazione WLC
<u>Verifica</u>
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 sul Cisco Identity Services Engine per i computer Windows utilizzando sia SSID singolo che SSID doppio.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco Identity Services Engine (ISE) versione 3.0
- Configurazione di Cisco WLC
- Metti in funzione il tuo dispositivo (BYOD)

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 l'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 SSID singoli BYOD di Windows

- 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 >	* Name	BYOD_Certificate_template
Certificate Authority $$		
Overview	Description	
Issued Certificates	Subject	
Certificate Authority Certifica	Common Name (CN)	SUserNameS 🕢
Internal CA Settings	Organizational Unit (OU)	tac
Certificate Templates		
External CA Settings	Organization (O)	cisco
	City (L)	bangalore
	State (ST)	Karnataka
	Country (C)	IN
	Subject Alternative Name (SAN)	Image: MAC Address V
	Кеу Туре	RSA V
	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

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.

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

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

E Cisco ISE			Work Centers · BYOD				A Evaluation Me	ode 46 Days
Overview Identities	Identity Groups Network Devic	es Ext Id Sources	Client Provisioning	Portals & Components	Policy Elements	Policy Sets	Reports	More
Client Provisioning Policy	* Name Wirel	essNSP						
Resources	Description							
		Wireless Profile(s)						
	Operating System * ALL	SSID Name *	BYOD-Dot1x					
	Wireless Profile	Proxy Auto-Config File URL		0	sector will be appe	Cod atabally (i.e. to	oli aukasana at	nee (in a)
	Multiple SSIUs can be configured Proxy Auto-Config File URL will b If no Proxy Auto-Config File URL	Proxy Host/IP		0	profile will be app droid 5.0 or above, used for early (pre	e 5.x) versions of A	all subsequent Android.	profiles).
	🖉 Edit 🕂 Add 🚺 Duplicat	Praxy Port						
	SSID Name Pro	Security *	WPA2 Enterprise V		cate Templ			
	BYOD-Dot1x	Allowed Protocol *	TLS 🗸		Certificate_templa			
		Certificate Template	BYOD_Certificate_template	~ <u>0</u>				
		 Optional Setti 	ngs					
		Windows Settings						
		Authentication Mode	0 User	~				

Passaggio 4. Creare 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.

E Cisco ISE		Work	Centers - BYOD		🔺 Evaluation Mode 46 Days 🔍 🛞 🗖
Overview Identities	Identity Groups Network Devices	Ext Id Sources	Client Provisioning Portals &	Components Policy Elements	Policy Sets Reports More \vee
Client Provisioning Policy Resources	Client Provisionin Define the Client Provisioning Policy For Agent Configuration: version of a For Native Supplicant Configuration:	g Policy to determine what users will ri gent, agent profile, agent com wizard profile and/or wizard. D	receive upon login and user session ini mpliance module, and/or agent custom Drag and drop rules to change the ordi	tiation: zation package. M.	
	~				
	Rule Name	Identity Groups	s Operating Systems	Other Conditions	Results
	ios.	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP Edit ~
	Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP Edit ~
	🗄 🗹 Windows	If Any	and Windows All	and Condition(s)	then WinSPWizard 3.0.0.2 Edit ~ And WirelessNSP
	🗄 🗹 MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX Edit ~ 4.8.00176 And MacOsXSPWizard
					Save

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. In questo caso 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.

■ Cisco ISE	Policy · Policy Elements
Dictionaries Conditions	Results
Authentication	* Name BYOD_Wireless_Redirect
Downloadable ACLs	* Access Type ACCESS_ACCEPT Network Device Profile Cisco
Posture	Service Template Track Movement Agentless Posture
Client Provisioning	Passive Identity Tracking
	Common Tasks Web Redirection (CWA, MDM, NSP, CPP)

Passaggio 6. Creare un profilo certificato.

Selezionare ISE > Administration > External Identity Sources > Certificate Profile (ISE > Amministrazione > Origini identità esterne > Profilo certificato). Creare un nuovo profilo certificato o utilizzare il profilo certificato predefinito.

≡ Cisco ISE		Administration - Identity Management
Identities Groups External Iden	tity Sources Identity Sou	rce Sequences Settings
External Identity Sources	Certificate Authentication Profiles Lis	t > cert_profile Profile
✓ Certificate Authentication F	* Name	cert_profile
2 Preloaded_Certificate_Prof	Description	
🔁 ADJoioint		
C LDAP		
C ODBC	Identity Store	[not applicable] V ()
C RADIUS Token		
🗎 RSA SecurID	Use Identity From	O Certificate Attribute Subject - Common № V ()
SAML Id Providers		Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)
🗀 Social Login		0
	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.

E Cisco ISE	Administration - Identity Management
Identities Groups External Identity Source	Identity Source Sequences Settings
Identity Source Sequences List > For_Teep	
✓ Identity Source Sequence * Name BYOD_id_Store Description	
 ✓ Certificate Based Authentication ✓ Select Certificate Authentication Profile 	rt_profile ~
 Authentication Search List A set of identity sources that will be accessed 	n sequence until first authentication succeeds
Available	Selected
Internal Endpoints	Internal Users
Guest Users	ADJoioint

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 identità di origine 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 nel passaggio 5.

2. Per i dispositivi registrati BYOD che eseguono EAP-TLS, fornire accesso completo a tali dispositivi.

=	Cisco IS	E			Policy · Policy Sets			A Evaluation
∨ Aι	thenticatio	n Policy (1)						
Œ	Status	Rule Name	Con	nditions				Use
(Q Search							
					+			
								BYOD_id_Store
	0	Default						> Options
> Au	thorization	Policy - Local Exceptions						
> Ai	thorization	Policy - Global Exceptions						
$\vee A_{i}$	thorization	Policy (3)						
						Results		
Œ	Status	Rule Name	Con	nditions		Profiles		Security Groups
(Q Search							
	0	Full_Acceess	AND	Ø	Network Access-EapAuthentication EQUALS EAP-TLS	PermitAccess ×	×+	Select from list
	-			F	EndPoints-BYODRegistration EQUALS Yes		-	
	Ø	BYOD_Redirect	Ŀ	EndPoi	nts-BYODRegistration EQUALS Unknown	BYOD_Wireless_Redire ×	×+	Select from list

Configurazione WLC

Passaggio 1. Configurare il server Radius su WLC.

Selezionare Sicurezza > AAA > Radius > Autenticazione.

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Security	RADIUSA	uthenti	cation Server	s > Edit					
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies 	Server Ind Server Add Shared Sea Shared Sea Confirm Sh Key Wrap Apply Cisco Apply Cisco Port Numb Server Sta	ex iress(Ipv4; cret Forma cret nared Secri- o ISE Defa o ACA Defa er tus	/Ipv6) t et ult settings sult settings	7 10.106.32.1 ASCII V (Designed for 1812 Enabled V	19 or FIPS custome	ers and requires a k	ey wrap compliar	nt RADIUS) (j) 5 server)
Local EAP	Support fo	r CoA		Enabled 🗸					
Advanced EAP	Server Tim	eout		5 seco	nds				
Priority Order	Network U	ser		Enable					
Certificate	Manageme	nt		Enable					
Access Control Lists	Manageme	nt Retrans	mit Timeout	5 secon	ds				
Wireless Protection Policies	Tunnel Pro	ху		Enable					
Web Auth	PAC Provis	ioning		Enable					
TrustSec	IPSec			Enable					
Local Policies	Cisco ACA			Enable					
Umbrella									
Advanced									

Passare a Sicurezza > AAA > Raggio > Contabilità.

	<u>M</u> onitor <u>W</u> lans <u>C</u> ontr	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Security	RADIUS Accounting Ser	vers > Edit					
▼ AAA General ▼ RADIUS	Server Index Server Address(Ipv4/Ipv6)	7					
Authentication Accounting Auth Cached Users Fallback DNS	Shared Secret Format Shared Secret Confirm Shared Secret	ASCII ~				@ @	
Downloaded AVP TACACS+ LDAP Local Net Users	Apply Cisco ACA Default settin Port Number	ngs					
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Server Status Server Timeout Network User	5 seconds					
 Local EAP Advanced EAP Briggity Order 	Management Tunnel Proxy <u>Realm List</u>	Enable Enable					
Certificate	PAC Provisioning IPSec	Enable Enable					
Access Control Lists Wireless Protection Policies Web Auth	Cisco ACA	Enable					
TrustSec							

TrustSec

،، ،،، ،، cısco	MONITOR WLANS CONTROLL	ler W <u>i</u> reless <u>s</u> ecurit	y m <u>a</u> nagement	COMMANDS HELP	FEEDBACK
WLANs	WLANs > Edit 'BYOD-Dot	1x'			
▼ WLANs WLANs	General Security Qo	S Policy-Mapping A	dvanced		
Advanced	Profile Name	BYOD-Dot1x	±.		
	Туре	WLAN BYOD-Dot1x			
	Status	Enabled			
	Radio Policy	All	ity tab will appear afte	r applying the changes.)	
	Interface/Interface Group(G)	management 🗸			
	Multicast Vlan Feature	Enabled			
	Broadcast SSID	Z Enabled			
	NAS-ID	none			
	Lobby Admin Access				

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)

cisco	MONI	for <u>w</u> l	ans <u>c</u> ontrolle	R WIRELESS	SECURITY MAN	NAGEMENT COMMAND	s help	FEEDBACK					
curity	Acce	ss Cont	rol Lists > Edit	-									
AA ocal EAP	Gene	ral											
dvanced EAP	Access	List Name	BYOD-Init	al									
Priority Order	Deny (ounters	0										
Certificate	Seq	Action	Source IP/Mask		Destination II	P/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
cess Control Lists	1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	Any	Any	Any	0	
PU Access Control Lists	2	Permit	0.0.0.0	/ 0.0.0.0	10.106.32.119	/ 255.255.255.255	Any	Any	Any	Any	Any	0	
exConnect ACLs	3	Permit	10.106.32.119	/ 255.255.255.25	5 0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	0	
RL ACLS	4	Deny	0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	0	
ireless Protection plicies													
eb Auth													
ustSec													
cal Policies													
nbrella													
hanced													

Passaggio 2. Configurare un SSID Dot1x.

Verifica

Verifica flusso di autenticazione

≡ Cisco ISE	Operations - RADIUS				🛕 Evaluatio	m Mode 46 Days	Q (0)	P	0		
Live Logs Live Sessions											
Misconfigured Supplicants 🕕	Mis	configured I	Network Devices 🕕 🛛 R	ADIUS Drops 🕕		Client Stopp	ed Responding 🕕		Repeat 0	Counter	
0			0	1			0			0	
🖉 Refresh 🛛 🕤 Reset Repest Count:	s ሰ Export To 🗸					Refre	sh Show ar <u>V</u> Latest 20	records 🗸	Within Last 5 m V Fi	inutes Iter 🗸 🕴	<u>~</u>
Time	Status Details	Repea	Identity	Endpoint ID	Identity Group	Authenti	Authorization Policy	Authorizatio	n Profile	s	E
×	~		Identity	Endpoint ID	Identity Group	Authenticat	Authorization Policy	Authorization F	Profiles		E
Nov 29, 2020 11:13:47.4	•	0	dot1xuser	50:3E:AA:E4:8		Wireless >	Wireless >> Full_Acceess	PermitAccess			w
Nov 29, 2020 11:13:47.2	2		dot1xuser	50:3E:AA:E4:8	RegisteredDevices	Wireless >	Wireless >> Full_Acceess	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	

Cisco ISE

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	0a6a21b2000009a5fc3d3ad
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.

Cisco ISE

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_Acceess
Authorization Result	PermitAccess

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 Centers > BYOD > Portal and Components > My Devices Portal > Login Settings (Risorse per i dispositivi > Centri di lavoro > BYOD > Portale e componenti > Portale dei dispositivi > Impostazioni di accesso), quindi immettere l'URL completo.

CISCO My Devices	Portal				
Manage Devices					
leed to add a device? Select Add. W	Vas 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 Ed	lit PIN Lock Fu	ll Wipe Unenroll	Reinstate Delete		
		•			
MAC Address	Dev	rice Name	Description	Status	

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 - 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 del 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 e caservice-misc.log

ca-service-cert - messaggi certificati ca-service - 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 casrvice-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\<nomeutente>\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,C
[1] User-Name - value: [dot1xuser]
[25] Class - value: [****]
[79] EAP-Message - value: [ñ
[80] Message-Authenticator - value: [.2{wëbÙ<sup>~</sup>Ap05<Z]
[26] cisco-av-pair - value: [url-redirect-acl=BY0D-Initial]
[26] cisco-av-pair - value: [url-redirect=https://10.106.32.119:8443/portal/gateway?sessionId=0a6a
[26] MS-MPPE-Send-Key - value: [****],RADIUSHandler.cpp:2216</pre>
```

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
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.u
```

```
2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portalwebaction.u
```

2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portal.util.Porta 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portal.util.Porta 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][] com.cisco.ise.portal.Gatewa

2020-12-02 05:43:58,355 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.c

2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a

2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a

2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a 2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a

2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,362 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager 2020-12-02 05:43:58,365 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,366 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.co 2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][] com.cisco.ise.portalSession 2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][] cisco.ise.portalwebaction.co



Fare clic su Start nella pagina iniziale BYOD.

020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.ac

2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c

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.ste

2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] guestaccess.flowmanager.ste 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager

2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.co 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.co

Sevice Information	+ 여상 방법 방법 방법 문화방법 위험 위험 위험 위험 위험 위험 방법 방법 방법 방법 방법 위험 위험 위험 위험 위험 위험 -	0	×
← → ♂ ŵ	🔘 🔒 https://10.106.32.119:8443/portal/ByodStart.action?from=BYOD_WELCOME	•	Ξ
	dottxuser a CISCO BYOD Portal		
	2 3		
	Device Information Enter the device name and optional description for this device to you can manage it using the MV Devices Portal.		
	Device name: *		
	Description:		
	Device ID: 50:3E AA E4:31 B0		
	Continue >		

Immettere il nome del dispositivo e fare clic su registra.

2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a

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.By
```

```
2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a
2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a
```

```
2020-12-02 05:44:14,683 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices
username= dot1xuser
idGroupID= aa13bb40-8bff-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

2020-12-02 05:44:14,902 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.c

2020-12-02 05:44:01,954 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c

2020-12-02 05:44:14,969 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.client.provision



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 2020-12-02 05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
```

```
2020-12-02 05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet 2020-12-02 05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
```

WirelessNSP

2.0

ALL

wireless

BYOD-Dot1x

WPA2

TLS

false

e2c32ce0-313d-11eb-b19e-e60300a810d5

---output omitted---

```
2020-12-02 05:45:03,310 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 <u>PKI Client</u>



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

2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert

2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert

```
2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.scep.util.ScepUti
2020-12-02 05:45:11,331 INFO [https-jsse-nio-10.106.32.119-8443-exec-1][] com.cisco.cpm.scep.ScepCert
2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkcsPkiEn
2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
```

ca-service.log

2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

version [0]

subject [C=IN,ST=Karnataka,L=bangalore,0=cisco,0U=tac,CN=dot1xuser]

---output omitted---

2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e 2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

caservice-misc.log

2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

caservice.log

2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e 1: 50-3E-AA-E4-81-B6

2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

```
2020-12-02 05:45:11,395 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67er
2020-12-02 05:45:11,395 INFO [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67er
class [com.cisco.cpm.caservice.CaResultHolder] [1472377777]: result: [CA_0K]
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 -::::- Veri

caservice.log

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

ise-psc.log

🇐 Install	× +				- 0	×
€ → ୯ û	🖲 🔒 https://10.106.	32.119:8443/portal/ByodRegister.a	action?from=BYOD_REGISTRATION	80% … 🛛 ☆	± m ⊡ ⊛	Ξ
	uluulu cisco	BYOD Portal		dottxuser 1		
	Instal	Cisco Network Setup Assistant	Network Setup Assistant Image: Setup Assist			

2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.provisioning.cer 2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCer 2020-12-02 05:45:13,385 INFO [https-jsse-nio-10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCer 2020-12-02 05:45:13,596 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.provisioning.cer

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,CPMS ,EapParser.cpp:150

Radius, 2020-12-02 05:46:57, 435, DEBUG, 0x7f433e3b5700, cntx=0008591362, sesn=isee30-primary/392215758/701, C

[1] User-Name - value: [dot1xuser]

[25] Class - value: [****]

[79] EAP-Message - value: [E

[80] Message-Authenticator - value: [Ù(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: [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 [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 0K

Location: https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009c5fc4fb5e&portal=7f8ac563-

[Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path = /auth/provisioning/d

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=b [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: [{65E78DD [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 avvia l'applicazione del profilo.

[Mon Nov 30 03:34:37 2020] ApplyProfile - Start... [Mon Nov 30 03:34:37 2020] User Id: dot1xuser, sessionid: 0a6a21b20000009c5fc4fb5e, Mac: 50-3E-AA-E4-81 [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 : [BY0D-Dot1x] [Mon Nov 30 03:34:37 2020] applying certificate for ssid [BY0D-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 = dot1xuser and subjectSuffix = OU=tac;0=c [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 le 17 cb 73 5f ba
] 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
[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-e60300a81

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-Dot1x] [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

Profilo

BYOD-Dot1x

true

ESS

auto

false

WPA2

AES

true

true

user

false

5b a2 08 1e 17 cb 73 5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b

false

Wireless interface succesfully initiated, continuing to configure SSID [Mon Nov 30 03:34:51 2020] Currently connected to SSID: [BYOD-Dot1x]

[Mon Nov 30 03:34:51 2020] Wireless profile: [BYOD-Dot1x] configured successfully
[Mon Nov 30 03:34:51 2020] Connect to SSID
[Mon Nov 30 03:34:51 2020] Successfully connected profile: [BYOD-Dot1x]
[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-Dot1x], profile ssid: [BYOD-Dot1x], Single
[Mon Nov 30 03:35:21 2020] WirelessProfile::IsSingleSSID - End

[Mon Nov 30 03:36:07 2020] Device configured successfully.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).