

Risoluzione dei problemi di Wired Dot1x in ISE 3.2 e Windows

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

Introduzione

In questo documento viene descritto come configurare un'autenticazione PEAP 802.1X di base per Identity Services Engine (ISE) 3.2 e il supplicant Windows Native.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PEAP (Protected Extensible Authentication Protocol)
- PEAP 802.1x

Componenti usati

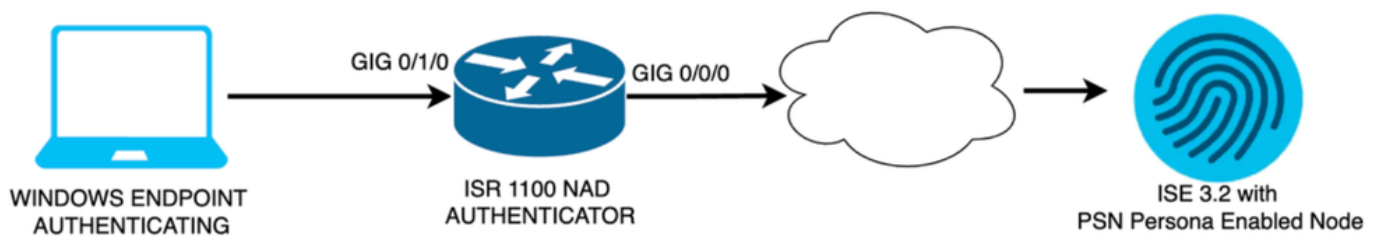
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Services Engine (ISE) versione
- Software Cisco IOS® XE C117, versione 17.12.02
- Notebook con Windows 10

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.

Configurazione

Esempio di rete



Esempio di rete

Configurazioni

Per configurare, effettuare le seguenti operazioni:

Passaggio 1. Configurare ISR 1100 router.

Passaggio 2. Configurare Identity Service Engine 3.2.

Passaggio 3. Configurare Windows Native Supplicant.

Passaggio 1. Configurazione di ISR 1100 Router

In questa sezione viene illustrata la configurazione di base di cui deve disporre almeno il NAD per consentire il funzionamento del dot1x.

Nota: per la distribuzione ISE a più nodi, configurare l'IP del nodo con la persona PSN abilitata. Per abilitare questa funzione, selezionare ISE nella scheda Amministrazione > Sistema > Distribuzione.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
  client A.B.C.D server-key <Your shared secret>
!
!
radius server ISE-PSN-1
  address ipv4 A.B.C.D auth-port 1645 acct-port 1646
  timeout 15
  key <Your shared secret>
```

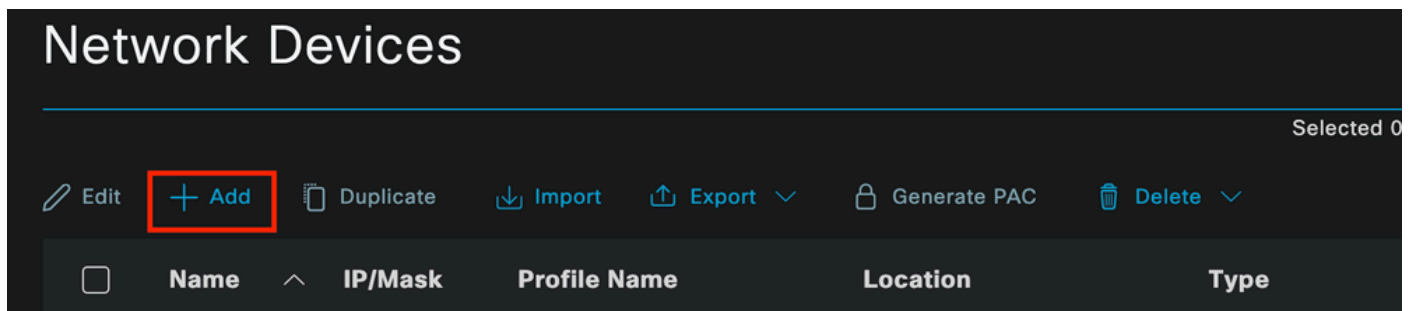
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication priority dot1x mab  
  authentication port-control auto  
  dot1x pae authenticator  
  spanning-tree portfast
```

Passaggio 2. Configurare Identity Service Engine 3.2.

2. a. Configurare e aggiungere il dispositivo di rete da utilizzare per l'autenticazione.

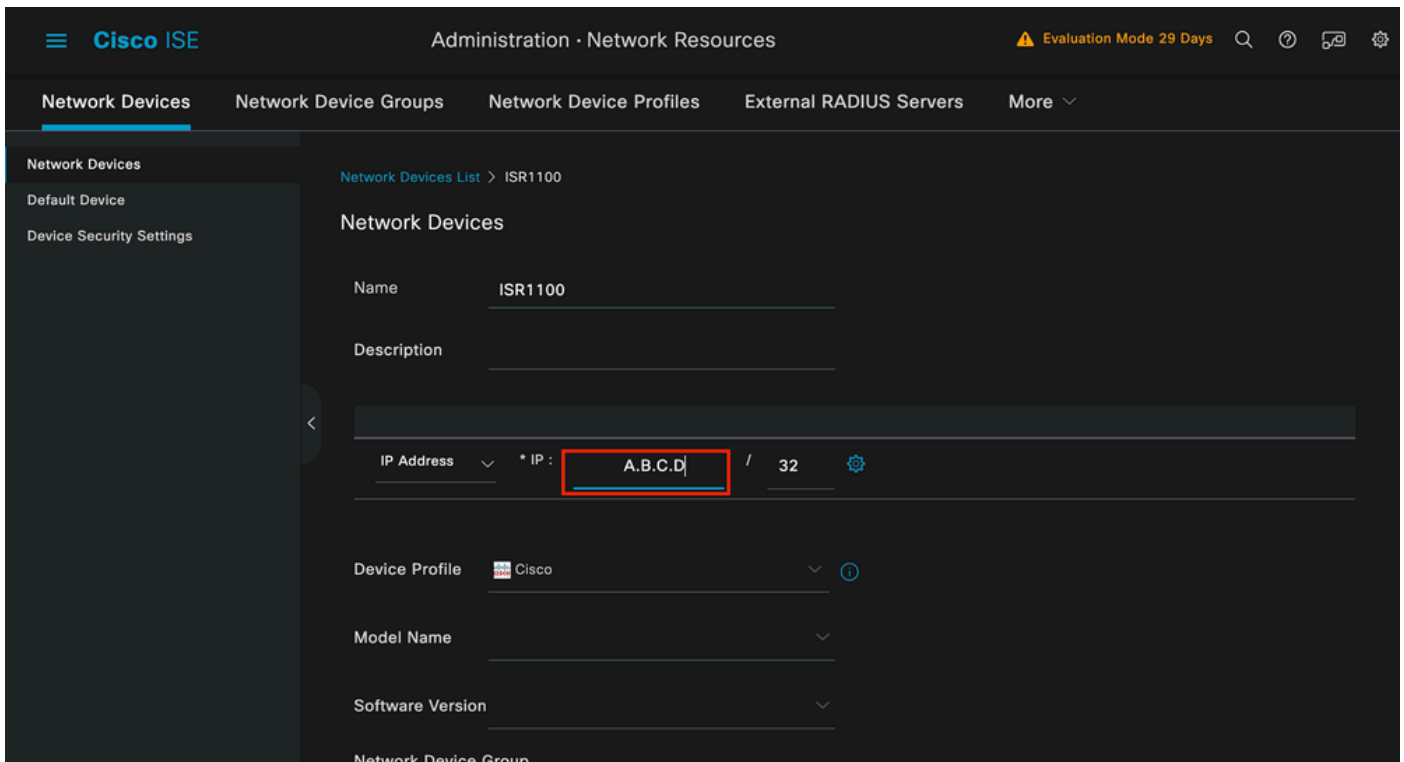
Aggiungere il dispositivo di rete alla sezione ISE Network Devices.

Fare clic sul pulsante Add per avviare.



Dispositivi di rete ISE

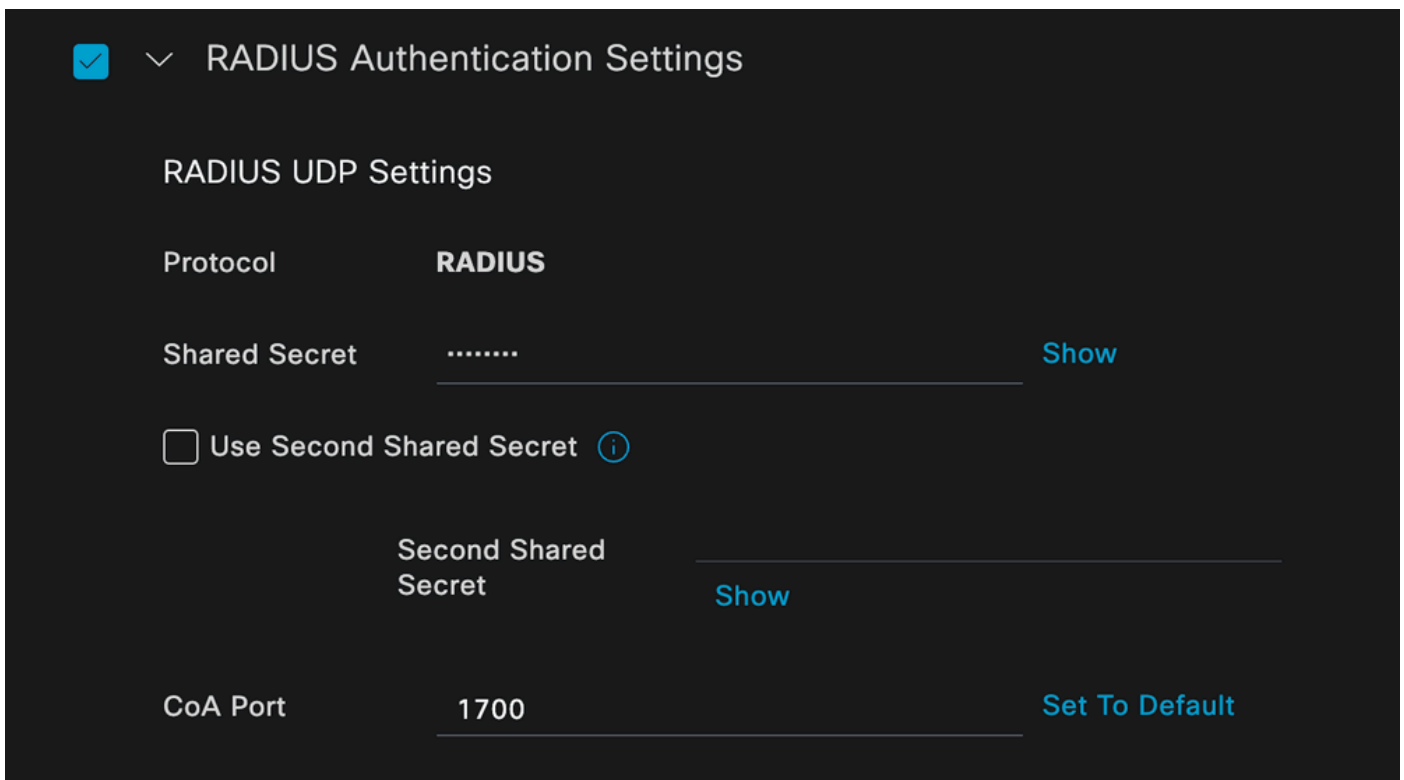
Immettere i valori, assegnare un nome al NAD che si sta creando e aggiungere anche l'indirizzo IP utilizzato dal dispositivo di rete per contattare ISE.



Pagina Creazione dispositivo di rete

Nella stessa pagina scorrere verso il basso per individuare le impostazioni di autenticazione Radius. Come mostrato nell'immagine seguente.

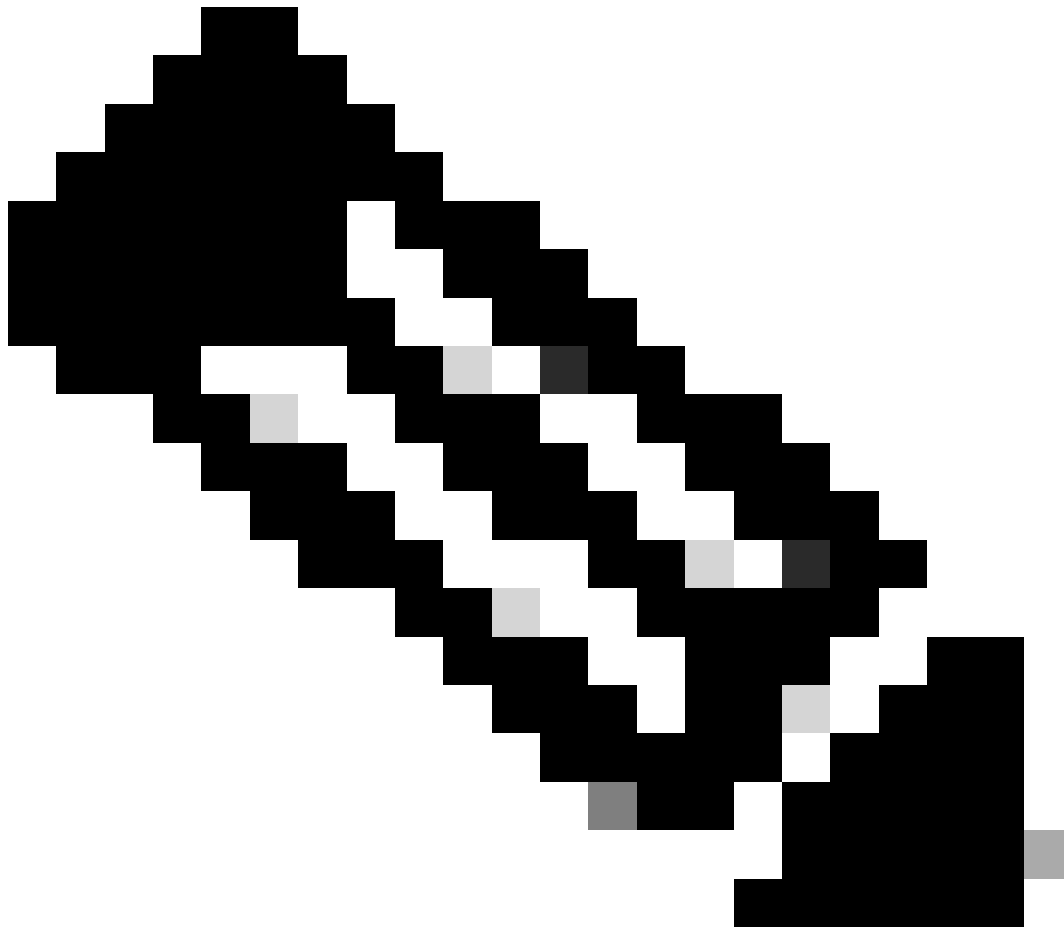
Aggiungere il segreto condiviso utilizzato nella configurazione NAD.



Configurazione Radius

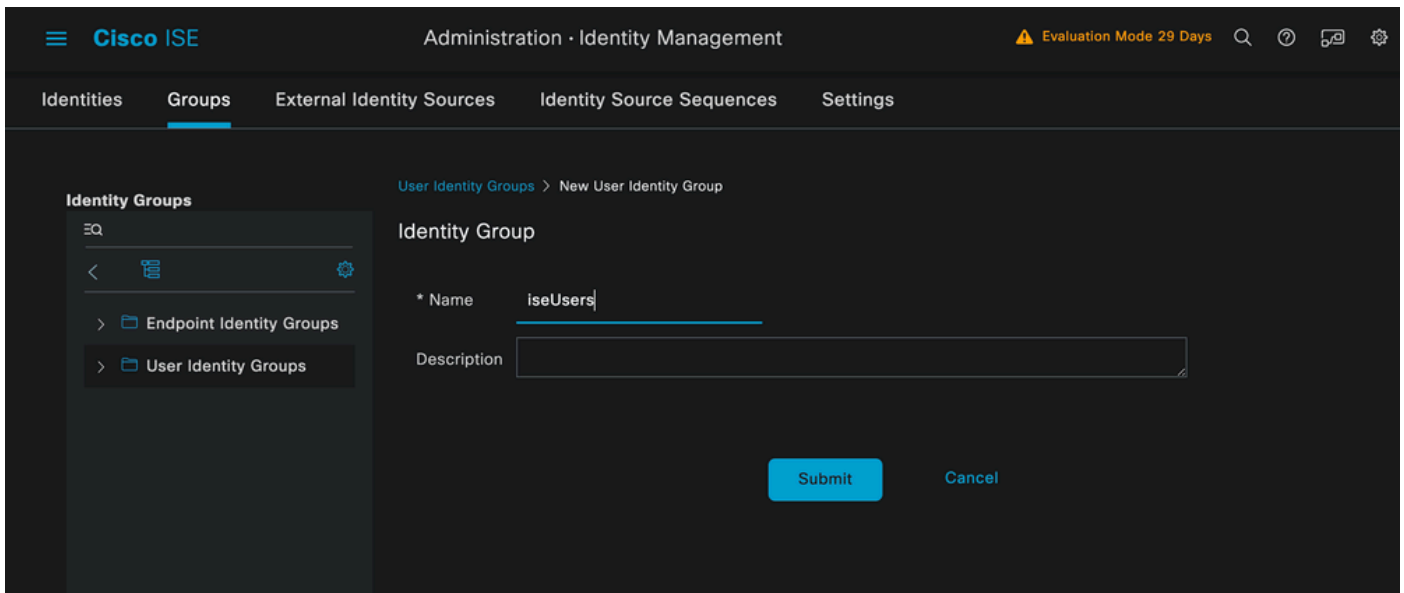
Salvare le modifiche.

2. b. Configurare l'identità utilizzata per autenticare l'endpoint.



Nota: per mantenere questa guida alla configurazione, viene usata la semplice autenticazione ISE locale.

Passare alla scheda Amministrazione > Gestione delle identità > Gruppi. Per creare il gruppo e l'identità, il gruppo creato per questa dimostrazione è iseUsers.

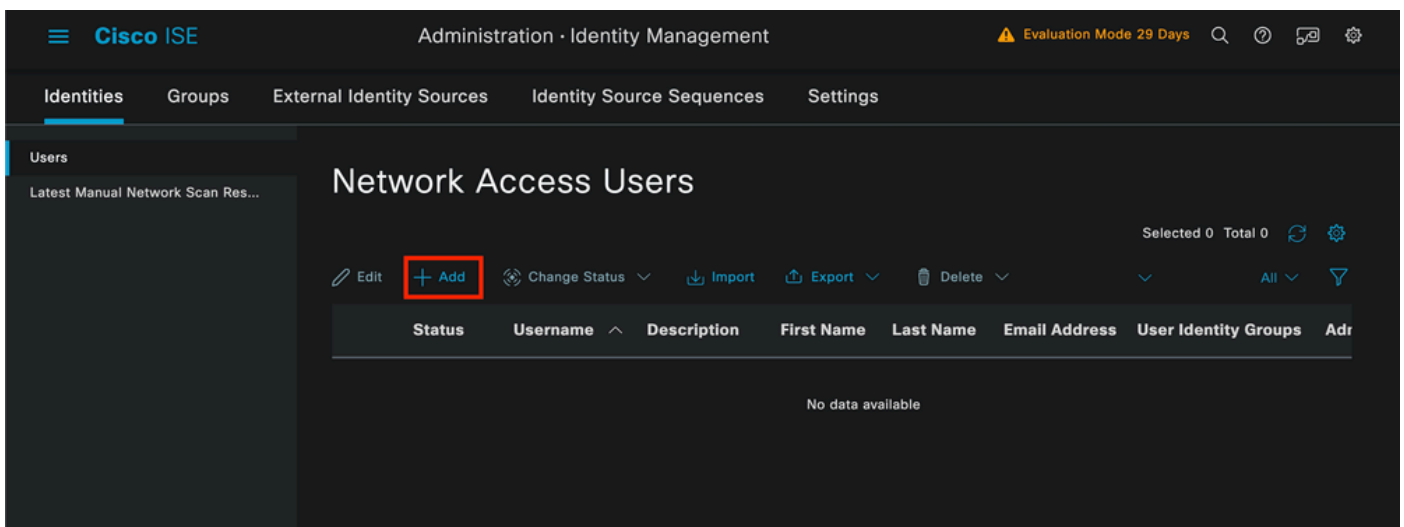


Pagina Creazione gruppo di identità

Fare clic sul pulsante Invia.

Passare quindi a Amministrazione > Gestione delle identità > scheda Identità.

Fare clic su Add.



Pagina Creazione utente

I campi obbligatori iniziano con il nome dell'utente. Nell'esempio riportato viene utilizzato il nome utente iseischool.

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Nome assegnato al nome utente

Il passaggio successivo consiste nell'assegnare una password al nome utente creato. Vainilla ISE97 è utilizzata nella dimostrazione.

Passwords

Password Type: ▼

Password Lifetime:

- With Expiration ⓘ
Password will expire in 60 days
- Never Expires ⓘ

Password

Re-Enter Password

* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

Creazione password

Assegnare l'utente al gruppo iseUsers.

User Groups



iseUsers



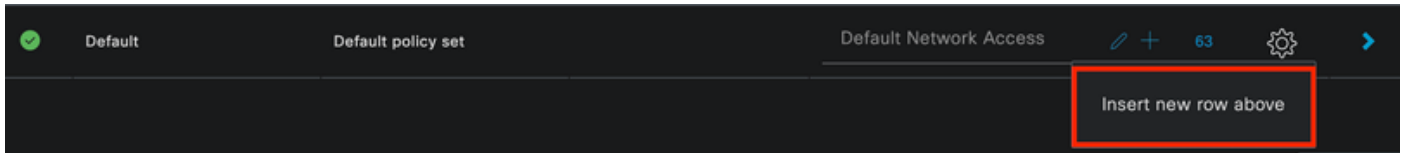
Assegnazione gruppo utenti

2. c. Configurare il set di criteri

Selezionare Menu ISE > Policy > Policy Sets.

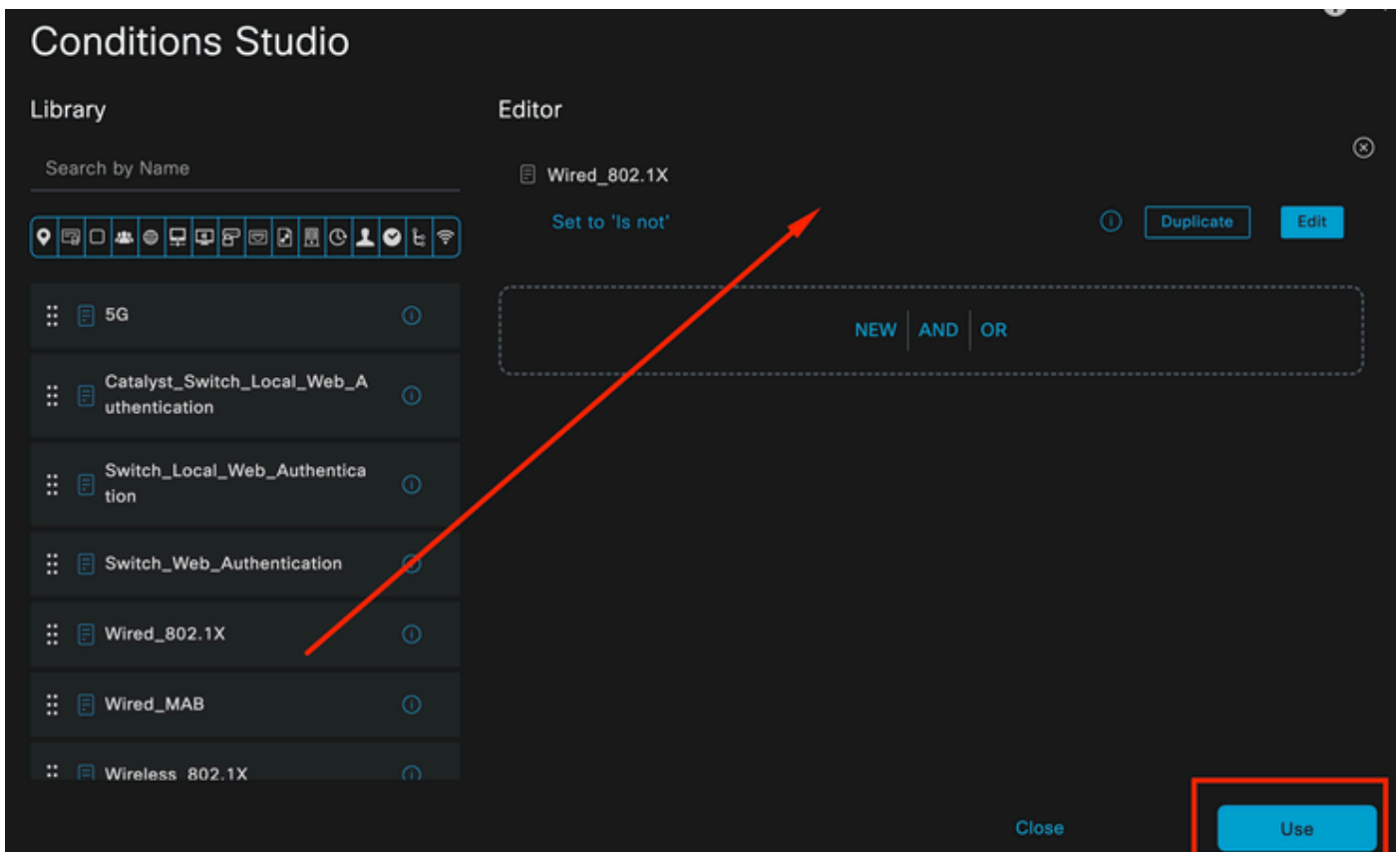
È possibile utilizzare il set di criteri predefinito. Tuttavia, in questo esempio viene creato un set di criteri denominato Wired. La classificazione e la differenziazione dei set di criteri facilita la risoluzione dei problemi,

Se l'icona di aggiunta o di aggiunta non è visibile, è possibile fare clic sull'icona di ingranaggio di qualsiasi set di criteri. Selezionate l'icona dell'ingranaggio, quindi selezionate Inserisci nuova riga (Insert new row).



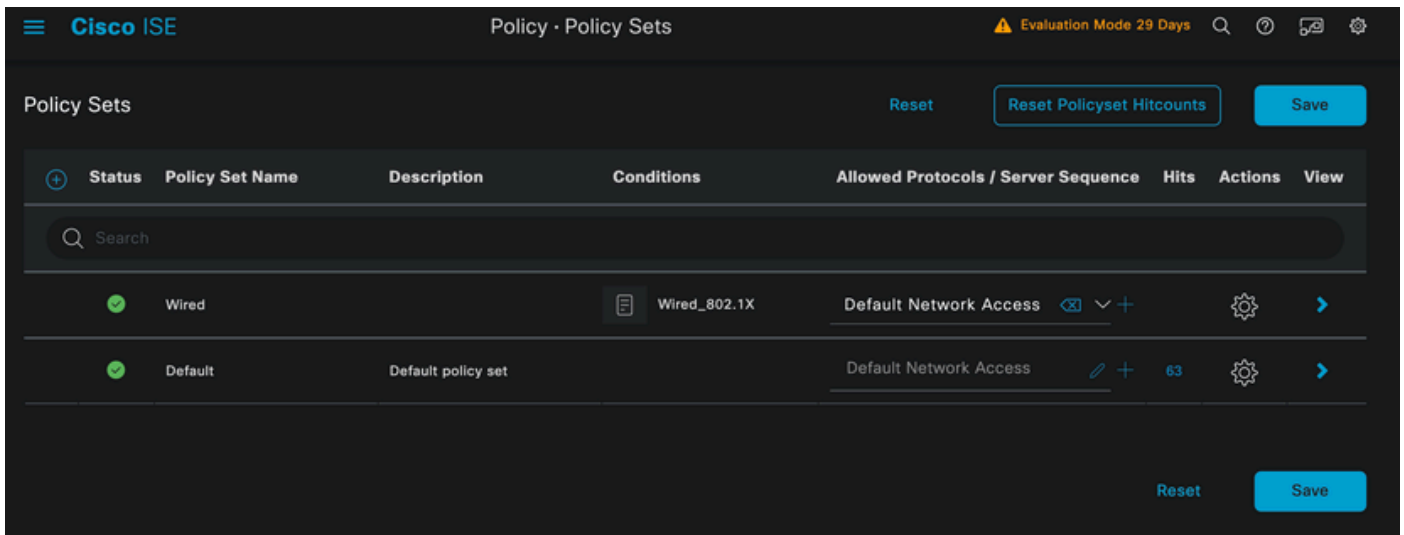
Creazione criteri

La condizione configurata in questo esempio è Wired 802.1x, una condizione preconfigurata nelle nuove distribuzioni ISE. Trascinarlo, quindi fare clic su Usa.



Condition Studio

Infine, selezionare il servizio Protocolli consentiti preconfigurati di Accesso alla rete predefiniti.

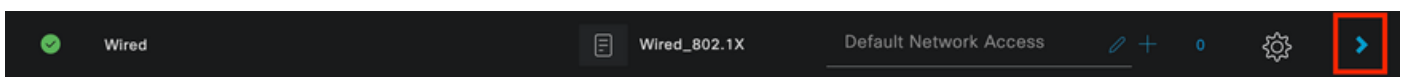


Visualizzazione set di criteri

Fare clic su Save (Salva).

2. d. Configurare i criteri di autenticazione e autorizzazione.

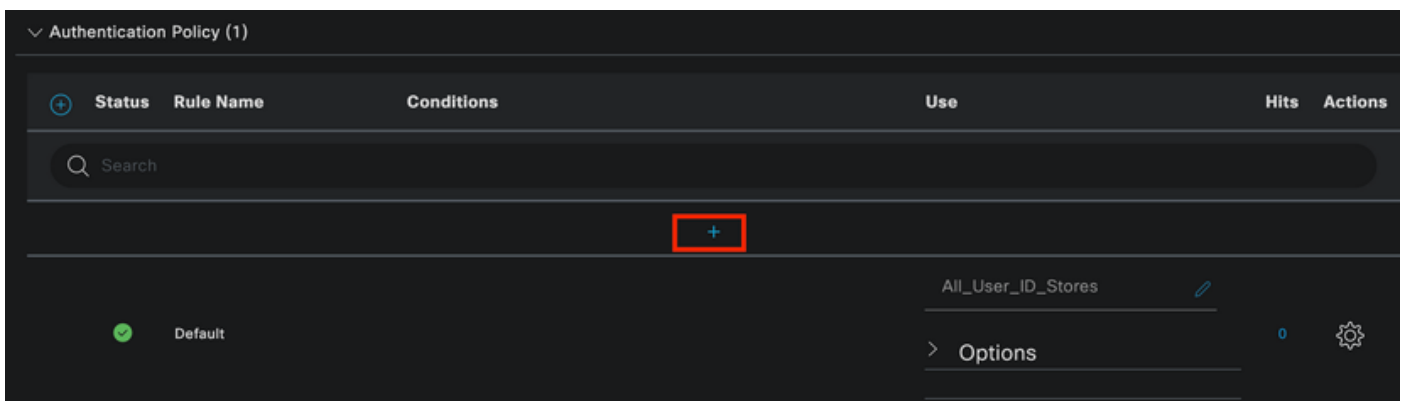
Fare clic sulla freccia a destra del set di criteri appena creato.



Set di criteri per reti cablate

Espandere il criterio di autenticazione

Fare clic sull'icona +.



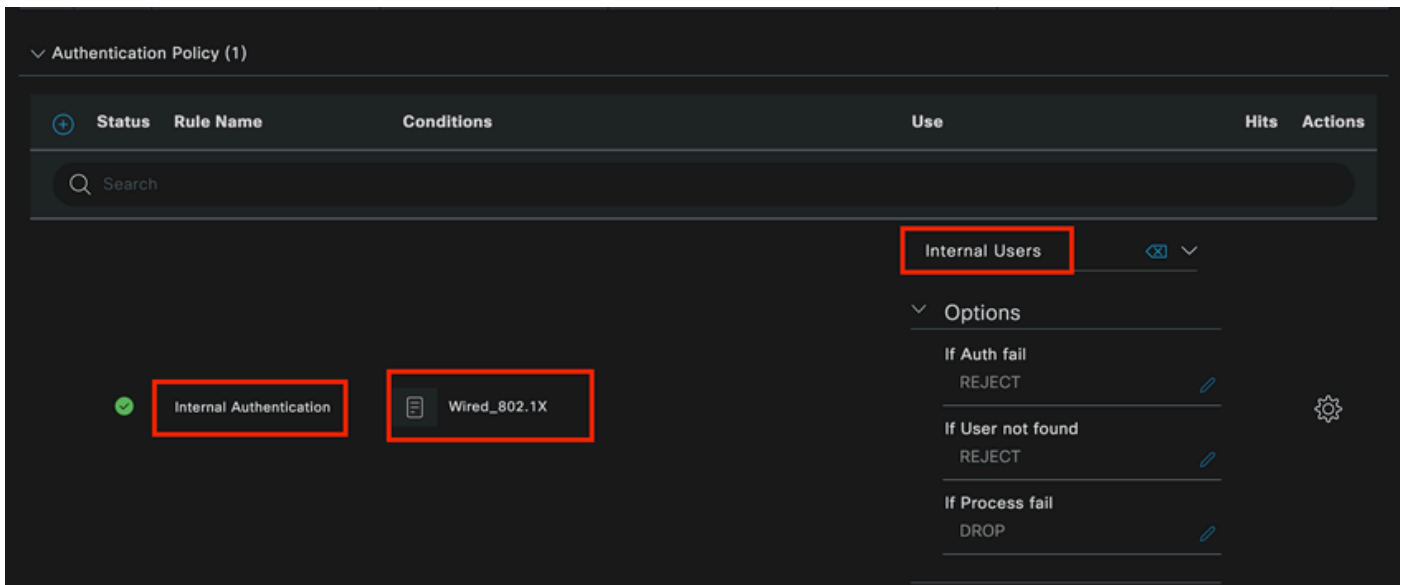
Aggiungi criterio di autenticazione

Assegnare un nome al criterio di autenticazione. In questo esempio viene utilizzata l'autenticazione interna.

Fare clic sull'icona + nella colonna Condizioni per questo nuovo criterio di autenticazione.

È possibile utilizzare la condizione preconfigurata Wired Dot1x ISE fornita con.

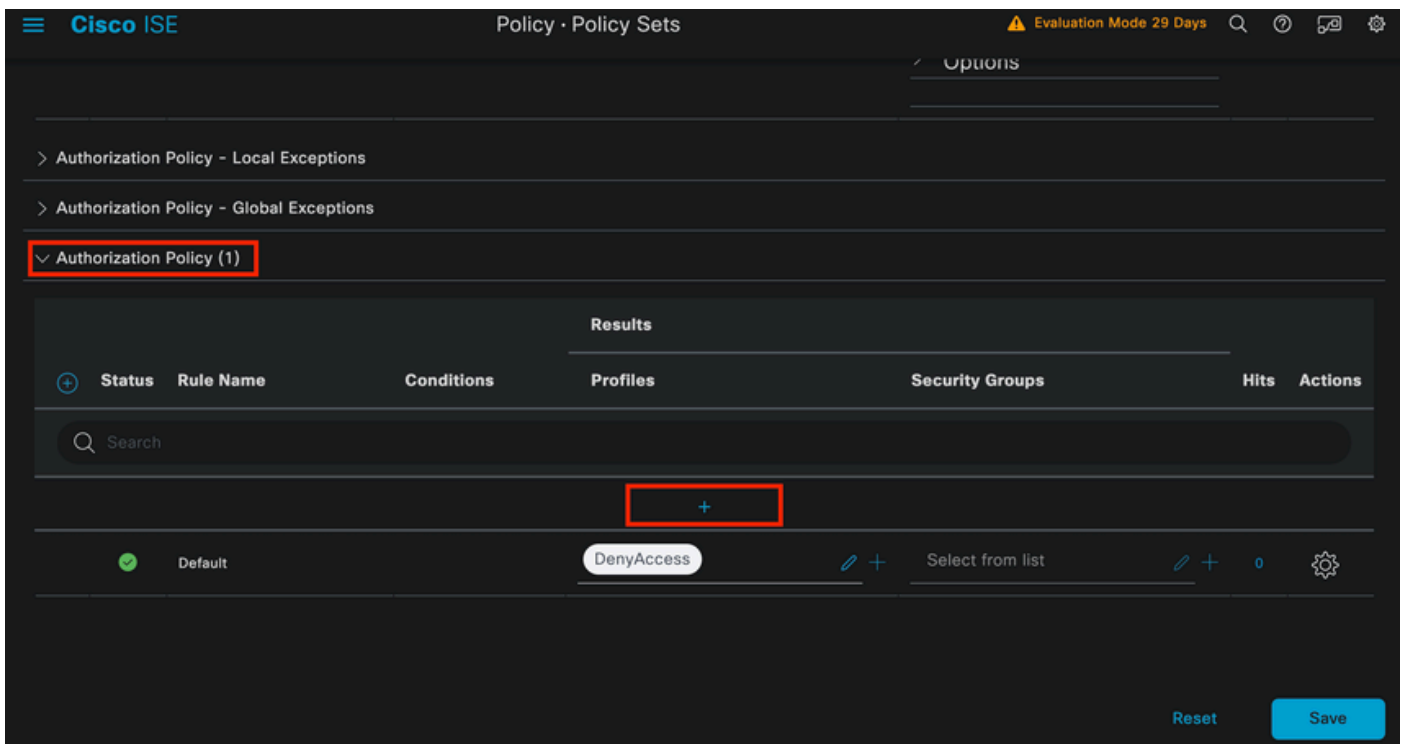
Infine, nella colonna Utilizza selezionare Utenti interni dall'elenco a discesa.



Criteria di autenticazione

Criteria di autorizzazione

La sezione Criteria di autorizzazione si trova nella parte inferiore della pagina. Espanderlo e fare clic sull'icona +.



Criteria di autorizzazione

Assegnare un nome al criterio di autorizzazione appena aggiunto. Nell'esempio di configurazione che segue viene utilizzato il nome Internal ISE Users.

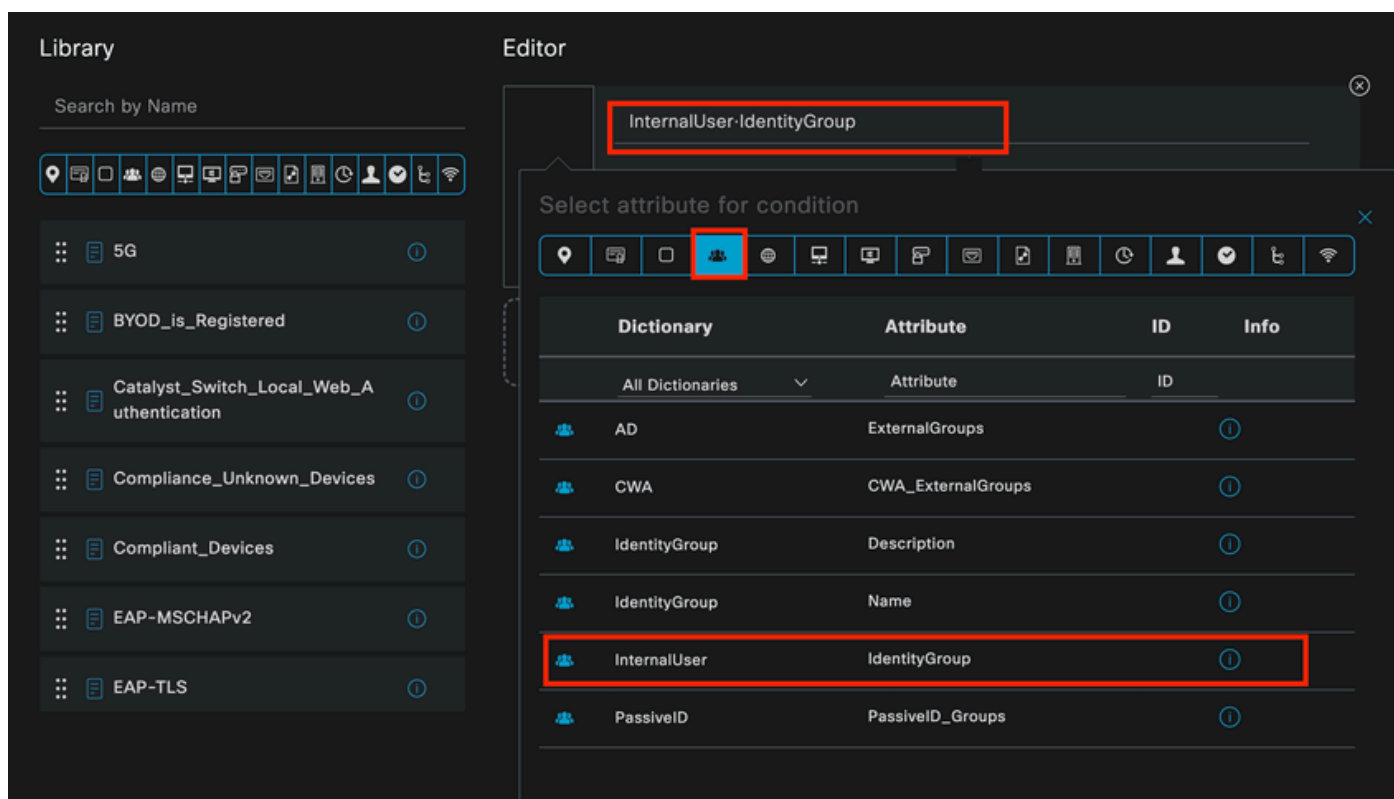
Per creare una condizione per questo criterio di autorizzazione, fare clic sull'icona + nella colonna Condizioni.

L'utente creato in precedenza fa parte del gruppo IseUsers.

Nell'editor, fare clic sulla sezione Fare clic per aggiungere un attributo.

Selezionare l'icona Gruppo di identità.

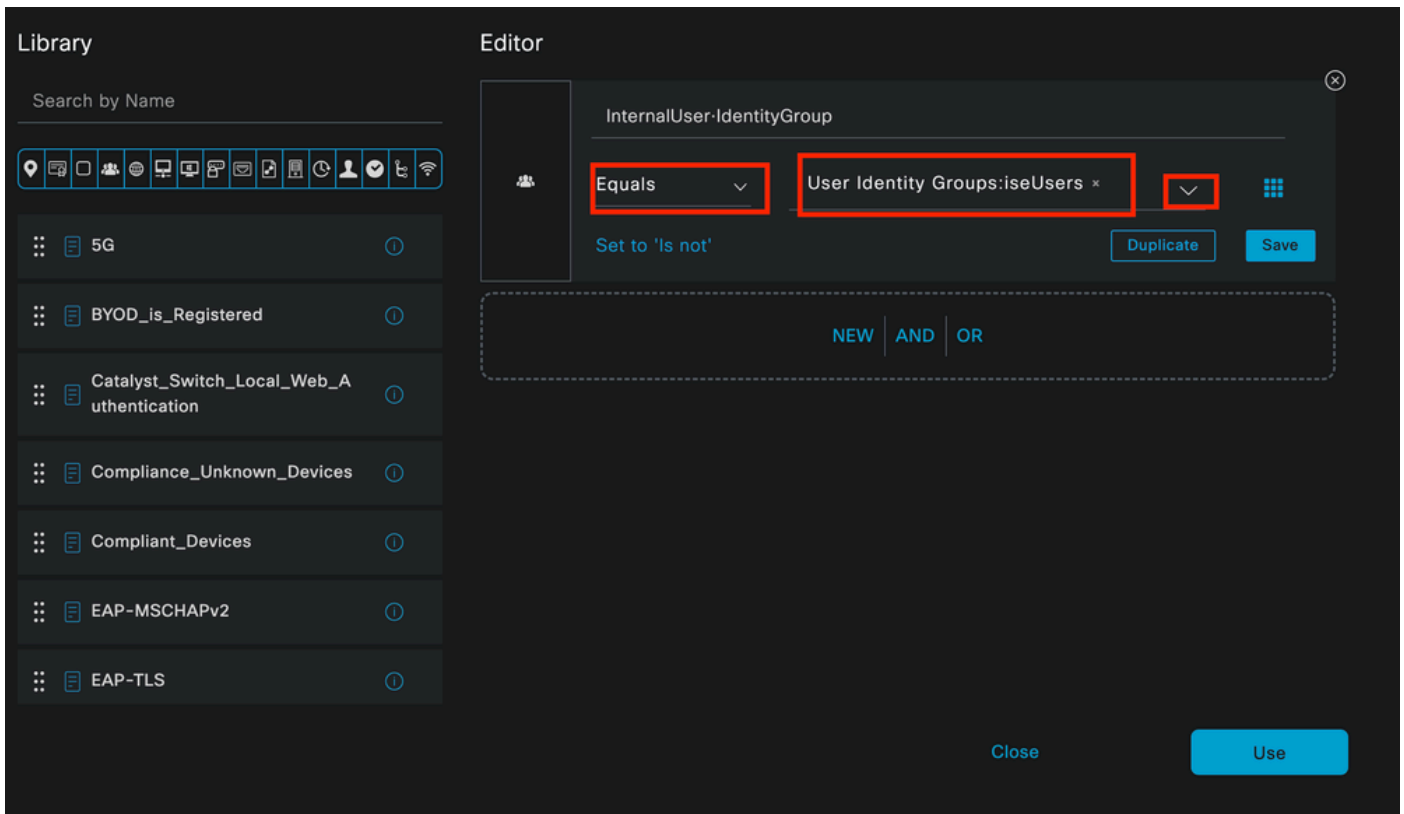
Dal dizionario, selezionare il dizionario InternalUser fornito con l'attributo Identity Group.



Condition Studio per criteri di autorizzazione

Selezionare l'operatore Uguale a.

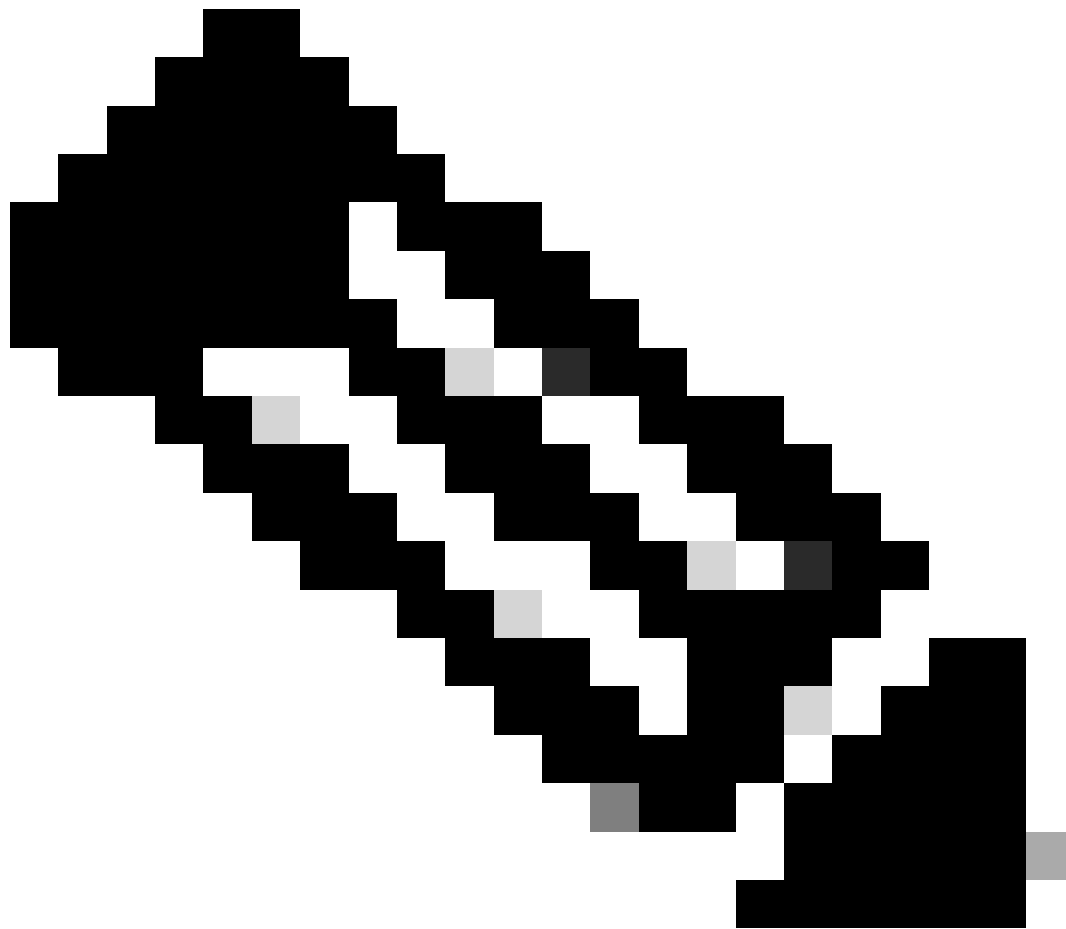
Dall'elenco a discesa Gruppi di identità utente, selezionare il gruppo IseUsers.



Condizione per i criteri di autorizzazione completata

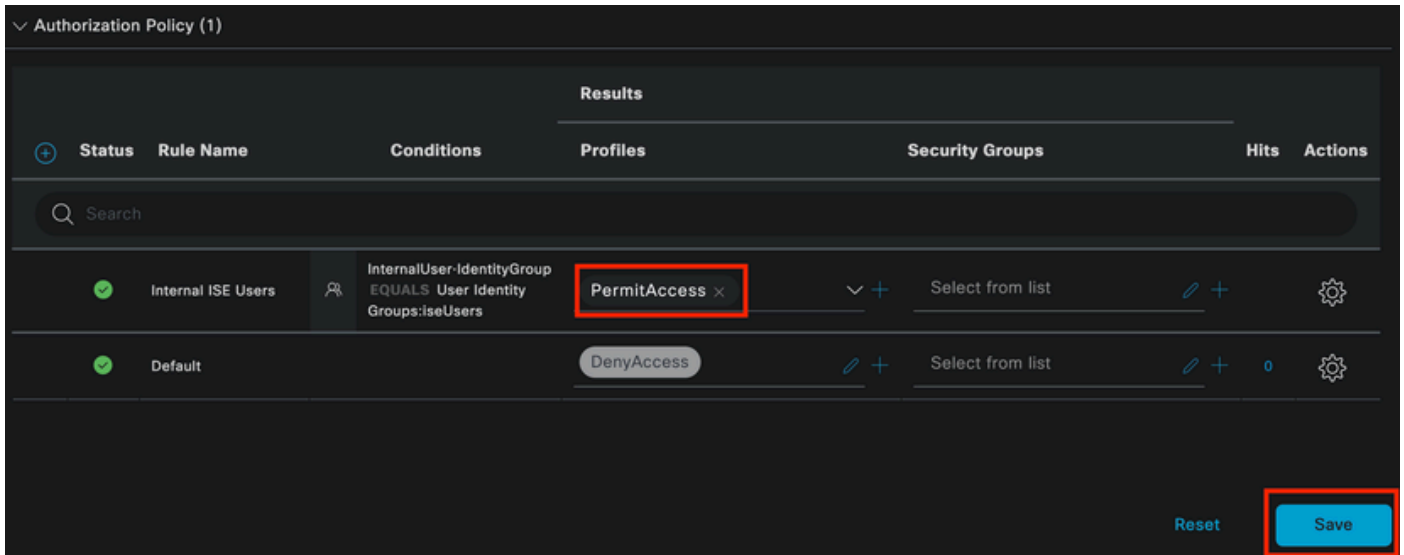
Fare clic su Usa.

Infine, selezionare il profilo di autorizzazione dei risultati che riceve la parte autenticazioni di questo gruppo di identità.



Nota: si noti che le autenticazioni in arrivo ad ISE e che stanno raggiungendo questo set di criteri Dot1x cablato che non fanno parte del gruppo di identità utenti ISEUsers, ora hanno raggiunto il criterio di autorizzazione predefinito. Questo ha il risultato del profilo DenyAccess.

ISE è preconfigurata con il profilo Permit Access. Selezionatelo.



Criteri di autorizzazione completati

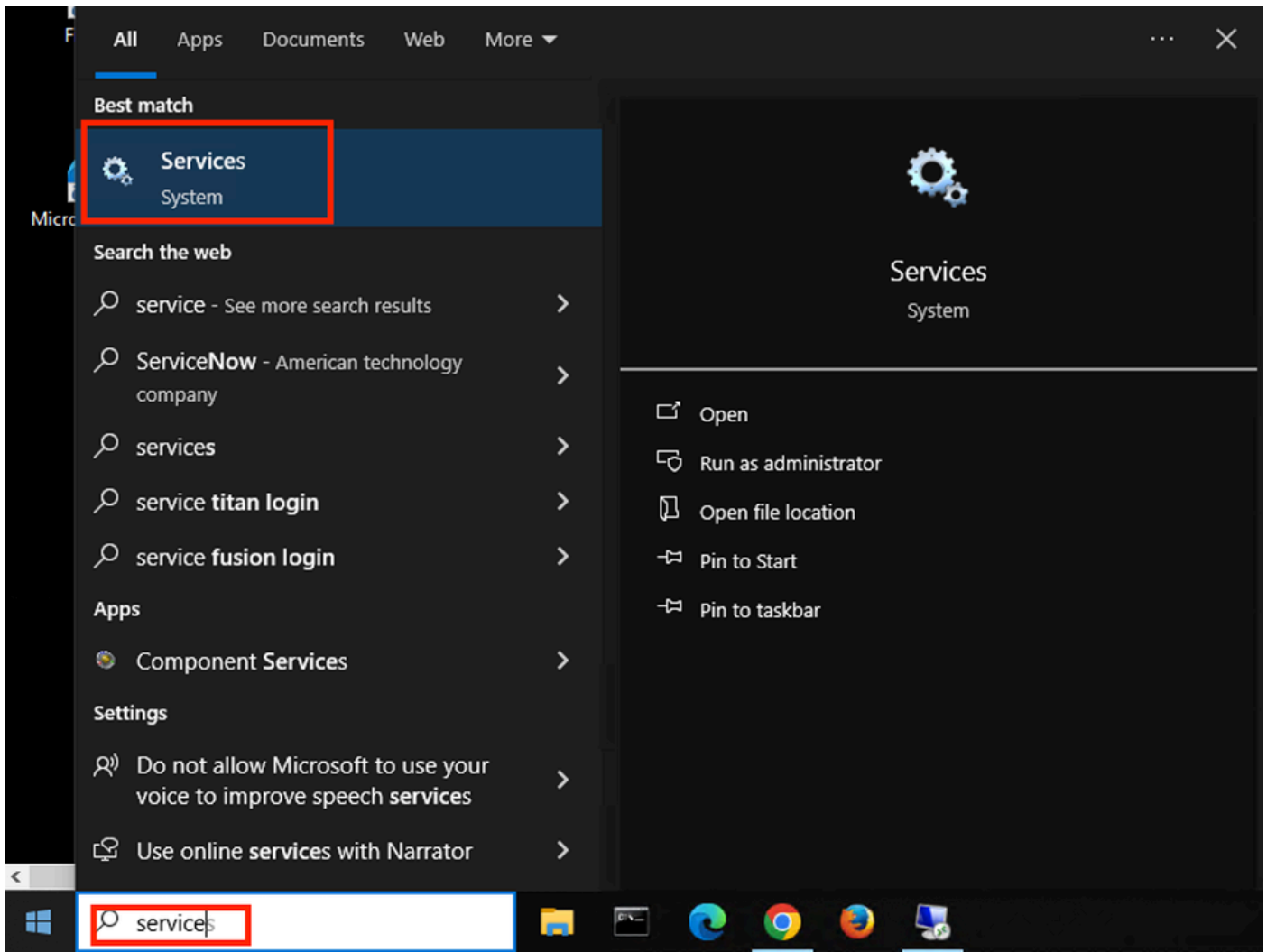
Fare clic su Save (Salva).

La configurazione di ISE è completa.

Passaggio 3. Configurazione supplicant nativo di Windows

3. a. Abilitare Wired dot1x su Windows.

Dalla barra di ricerca di Windows aprire Servizi.



Barra di ricerca di Windows

Nella parte inferiore dell'elenco dei servizi, individuare Wired Autoconfig.

Fare clic con il pulsante destro del mouse su Wired AutoConfig e selezionare Properties.

Wired AutoConfig Properties (Local Computer)



General Log On Recovery Dependencies

Service name: dot3svc

Display name: Wired AutoConfig

Description: responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X

Path to executable:

C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p

Startup type: Manual

Service status: Stopped

Start

Stop

Pause

Resume

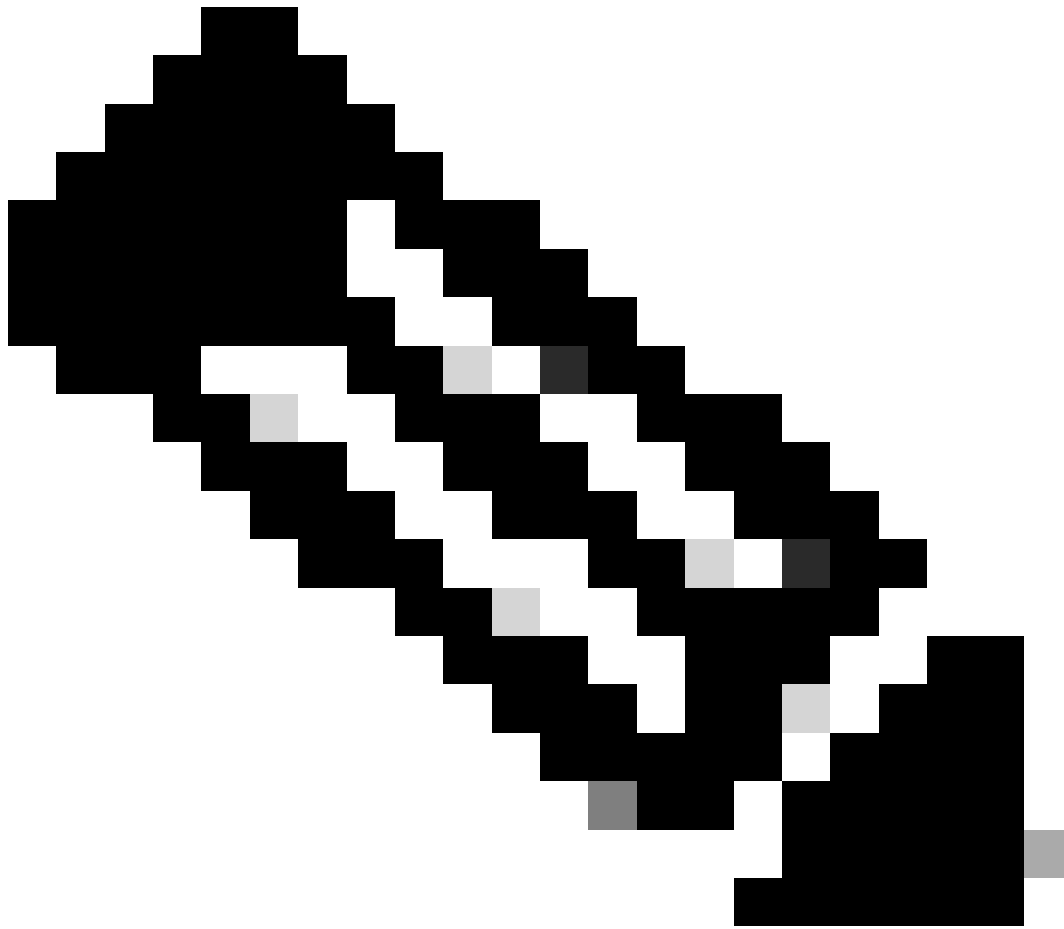
You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK

Cancel

Apply



Nota: il servizio Configurazione automatica reti cablate (DOT3SVC) è responsabile dell'autenticazione IEEE 802.1X sulle interfacce Ethernet.

È selezionato il tipo di avvio Manuale.

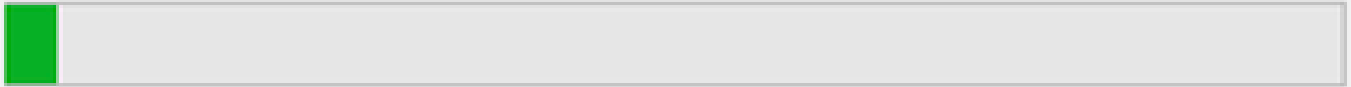
Lo stato del servizio è Arrestato. Fare clic su Start.

Service Control



Windows is attempting to start the following service on Local Computer...

Wired AutoConfig



Close

Controllo servizi

Fare quindi clic su OK.

Il servizio è in esecuzione.

| | | | | |
|--|------------------|---------|-----------------|----------------|
| Windows Update | Enables the ... | Running | Manual (Trig... | Local Syste... |
| Windows Update Medic Service | Enables rem... | | Manual | Local Syste... |
| WinHTTP Web Proxy Auto-Discovery Service | WinHTTP i... | Running | Manual | Local Service |
| Wired AutoConfig | The Wired A... | Running | Manual | Local Syste... |
| WLAN AutoConfig | The WLANS... | | Manual | Local Syste... |
| WMI Performance Adapter | Provides pe... | | Manual | Local Syste... |
| Work Folders | This service ... | | Manual | Local Service |

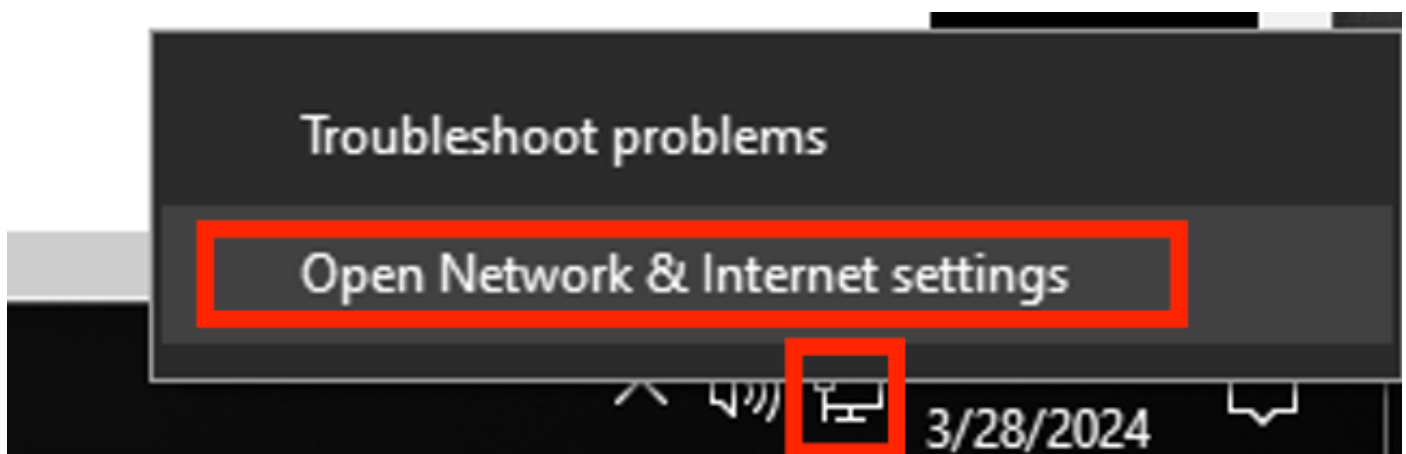
Servizio configurazione automatica reti cablate

3. b. Configurare l'interfaccia del laptop Windows collegata all'autenticatore NAD (ISR 1100).

Dalla barra delle applicazioni, individuare l'angolo a destra, quindi utilizzare l'icona del computer.

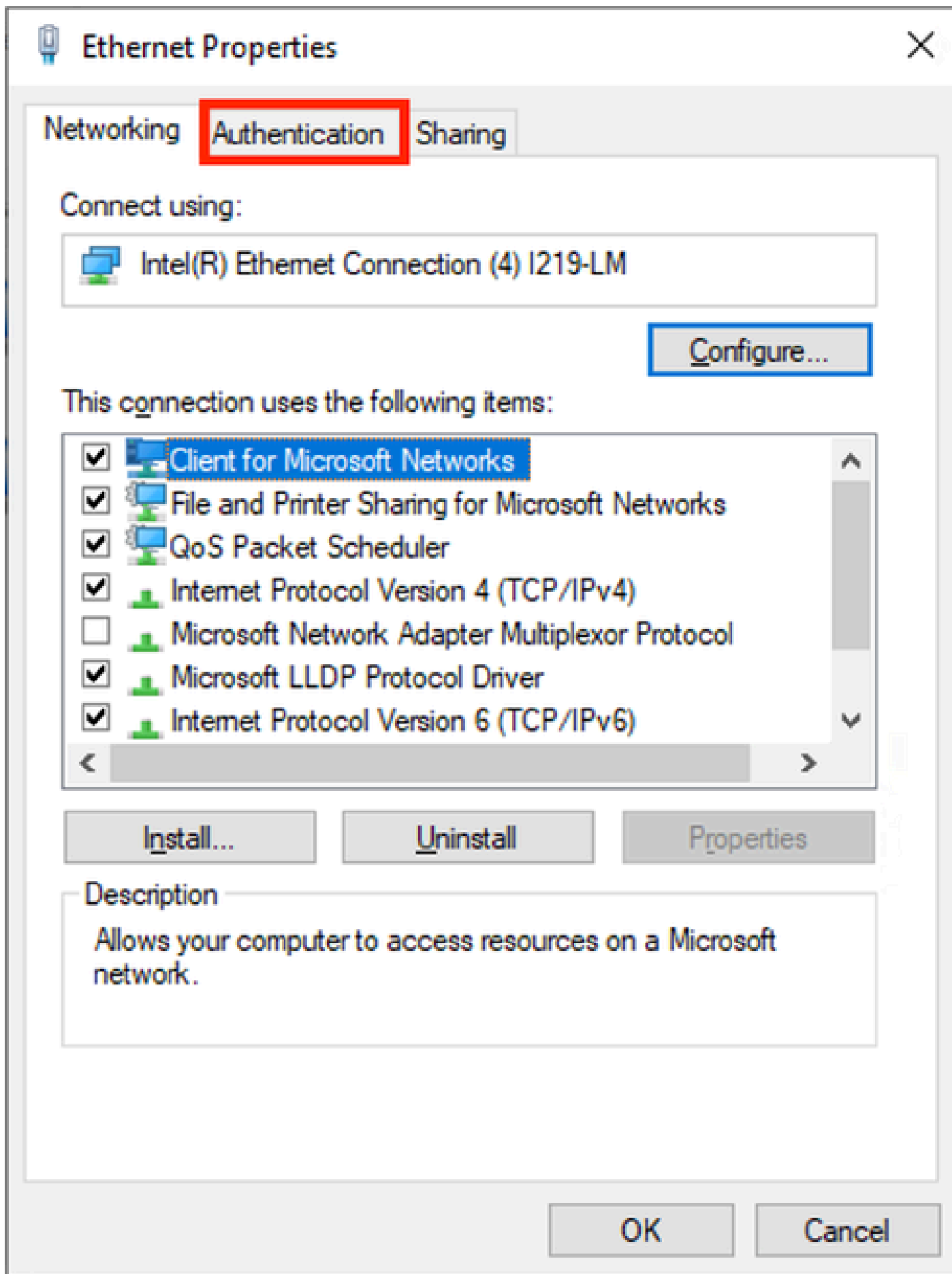
Fare doppio clic sull'icona del computer.

Selezionare Apri impostazioni Rete e Internet.



Una volta aperta la finestra Connessioni di rete, fare clic con il pulsante destro del mouse sull'interfaccia Ethernet collegata a ISR Gig 0/1/0. Fare clic sull'opzione Proprietà.

Fare clic sulla scheda Autenticazione.



Proprietà Ethernet interfaccia

Selezionare la casella di controllo Abilita autenticazione IEEE 802.1X.



Ethernet Properties



Networking

Authentication

Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) ▾

Settings

Remember my credentials for this connection each time I'm logged on

Fallback to unauthorized network access

Additional Settings...

OK

Cancel

Proprietà Ethernet autenticazione

Selezionare PEAP (Protected EAP).

Deselezionare l'opzione Memorizza credenziali per questa connessione ogni volta che si accede.

Fare clic su Impostazioni.

Protected EAP Properties



When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1;srv2;. *\.srv3\.com):

Trusted Root Certification Authorities:

- AAA Certificate Services
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert Global Root G2

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

Enable Identity Privacy

OK

Cancel

Interface: GigabitEthernet0/1/0
IIF-ID: 0x08767C0D
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool <----- The username configured for Windows Native Supplicant
Status: Authorized <----- An indication that this session was authorized by the PSN
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A0000000C83E28461
Acct Session ID: 0x00000003
Handle: 0xc6000002
Current Policy: POLICY_Gi0/1/0

Local Policies:

Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Server Policies:

Method status list:

| Method | State |
|--------|---|
| dot1x | Authc Success <----- An indication that dot1x is used for this authentication |

Router#

Log ISE

Passare alla scheda Operazioni > Raggio >Live Log.

filtrare in base all'identità del nome utente; nell'esempio viene utilizzato il nome utente iseiscool;

Operations · RADIUS

Live Logs Live Sessions

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

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To Filter

| Time | Status | Details | Repea... | Identity | Endpoint ID | Endpoint... | Authentication Policy | Authc |
|----------------------------|--------|---------|----------|-----------|--------------------|-------------|----------------------------------|-------|
| × | | | | iseiscool | Endpoint ID | Endpoint Pr | Authentication Policy | Authc |
| Mar 28, 2024 07:04:35.4... | | | 0 | iseiscool | 8C:16:45:0D:F4:... | Unknown | Wired >> Internal Authentication | Wired |
| Mar 28, 2024 07:04:35.3... | | | | iseiscool | 8C:16:45:0D:F4:... | Unknown | Wired >> Internal Authentication | Wired |

Last Updated: Thu Mar 28 2024 01:29:12 GMT-0600 (Central Standard Time) Records Shown: 2

ISE Live Log

Operations · RADIUS

Live Logs Live Sessions

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

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To Filter

| Authorization Policy | Authoriz... | IP Address | Network De... | Device Port | Identity Group | Posture ... | Server |
|----------------------|-----------------------------|--------------|---------------|----------------------|-------------------------------|-------------|--------|
| n | Wired >> Internal ISE Users | PermitAcc... | | GigabitEthernet0/1/0 | | | PSN01 |
| n | Wired >> Internal ISE Users | PermitAcc... | ISR1100 | GigabitEthernet0/1/0 | User Identity Groups:iseUsers | | PSN01 |

Last Updated: Thu Mar 28 2024 01:34:19 GMT-0600 (Central Standard Time) Records Shown: 2

ISE Live Log

Da questa rapida visualizzazione, i log attivi forniscono le informazioni principali:

- Timestamp dell'autenticazione.
- Identità utilizzata.
- Indirizzo MAC endpoint.
- Criterio impostato e criterio di autenticazione raggiunto.
- Criterio impostato e Criterio di autorizzazione raggiunto.
- Risultato profilo autorizzazione.
- Il dispositivo di rete che invia la richiesta Radius all'ISE.
- Interfaccia a cui è collegato l'endpoint.
- Gruppo di identità dell'utente autenticato.
- Il PSN (Policy Server Node) che ha gestito l'autenticazione.

Risoluzione dei problemi

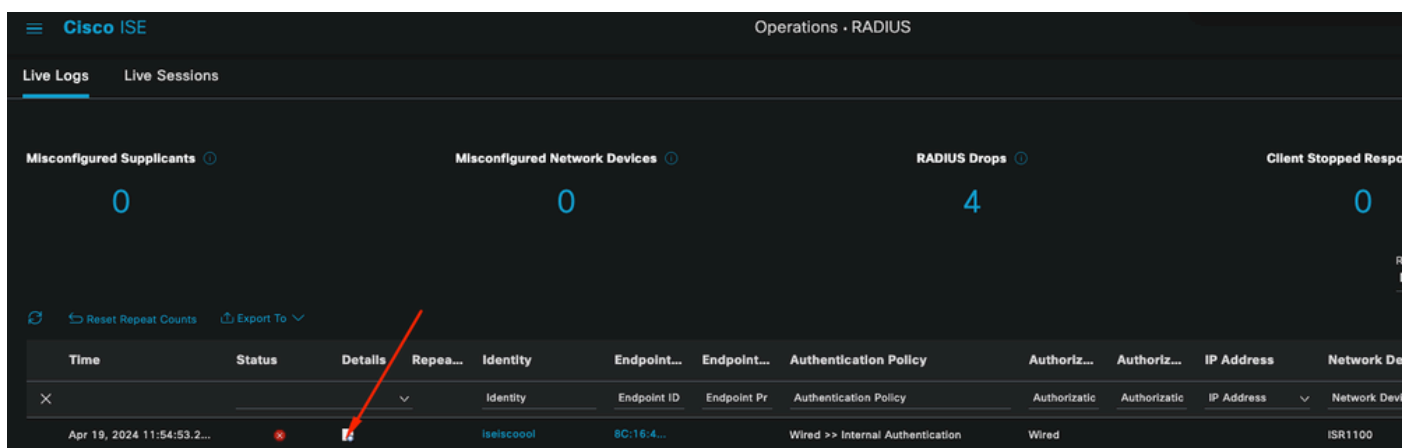
1 - Lettura dei dettagli del log di ISE Live

Selezionare Operazioni > Raggio > scheda Live Log, filtrare in base allo stato di autenticazione: Non riuscito OPPURE in base al nome utente utilizzato OPPURE in base all'indirizzo MAC OPPURE in base al dispositivo di accesso alla rete utilizzato.

Accedere a Operazioni > Raggio > Registri attivi > Autenticazione desiderata > Dettagli registro attivo.

Nella stessa pagina, dopo aver filtrato l'autenticazione, fare clic sull'icona Cerca.

Primo scenario: l'utente immette il proprio nome utente con un errore di battitura.



The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are four summary cards: Misconfigured Suppllicants (0), Misconfigured Network Devices (0), RADIUS Drops (4), and Client Stopped Responses (0). Below these are buttons for 'Reset Repeat Counts' and 'Export To'. A table of active logs is displayed with the following columns: Time, Status, Details, Repea..., Identity, Endpoint..., Endpoint..., Authentication Policy, Authoriz..., Authoriz..., IP Address, and Network De. A red arrow points to the 'Details' column header. The first row of the table shows a log entry with a red 'X' in the Status column, a red 'X' in the Details column, the identity 'iselscoool', endpoint ID '8C:16:4...', authentication policy 'Wired >> Internal Authentication', authorization 'Wired', IP address, and network device 'ISR1100'.

Apertura dei dettagli dei log in tempo reale

Una volta aperti i dettagli del registro attivo, è possibile verificare che l'autenticazione non è riuscita ed è elencato anche il nome utente utilizzato.

Overview

| | |
|-----------------------|----------------------------------|
| Event | 5400 Authentication failed |
| Username | iseiscoool |
| Endpoint Id | <ENDPOINT MAC ADDRESS># |
| Endpoint Profile | |
| Authentication Policy | Wired >> Internal Authentication |
| Authorization Policy | Wired |
| Authorization Result | |

Sezione Panoramica

Nello stesso dettaglio di registro attivo, nella sezione Dettagli autenticazione, è possibile trovare il motivo dell'errore, la causa principale e la risoluzione dell'errore.

| | |
|----------------|--|
| Event | 5400 Authentication failed |
| Failure Reason | 22056 Subject not found in the applicable identity store(s) |
| Resolution | Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resolution settings or if they do not support the current authentication protocol. |
| Root cause | Subject not found in the applicable identity store(s). |
| Username | iseiscoool |

Dettagli autenticazione

In questo scenario, il motivo per cui l'autenticazione non riesce è che il nome utente ha un errore di battitura. Tuttavia, lo stesso errore verrebbe visualizzato se l'utente non è stato creato in ISE o se ISE non è stato in grado di convalidare l'esistenza dell'utente in altri archivi identità, ad esempio LDAP o AD.

Sezione Passi

15041 Evaluating Identity Policy

15013 Selected Identity Source - Internal Users ←

24210 Looking up User in Internal Users IDStore - iseiscoool ←

24216 The user is not found in the internal users identity store ←

22056 Subject not found in the applicable identity store(s) ←

22058 The advanced option that is configured for an unknown user is used

22061 The 'Reject' advanced option is configured in case of a failed authentication request ←

11815 Inner EAP-MSCHAP authentication failed ←

11520 Prepared EAP-Failure for inner EAP method

22028 Authentication failed and the advanced options are ignored

12305 Prepared EAP-Request with another PEAP challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12304 Extracted EAP-Response containing PEAP challenge-response

61025 Open secure connection with TLS peer

12307 PEAP authentication failed ←

11504 Prepared EAP-Failure

11003 Returned RADIUS Access-Reject ←

Sezione passaggio Dettagli registro dinamico

La sezione step descrive in dettaglio il processo ISE eseguito durante la conversazione RADIUS.

Qui puoi trovare informazioni come:

- Come è iniziata la conversazione.
- Processo di handshake SSL.
- Metodo EAP negoziato.
- Processo del metodo EAP.

Nell'esempio, è possibile notare che ISE ha appena archiviato le identità interne per questa autenticazione. L'utente non è stato trovato e per questo motivo ISE ha inviato come risposta un messaggio di rifiuto di accesso.

Secondo scenario: l'amministratore ISE ha disabilitato PEAP dai protocolli Policy Set Allowed.

2 - PEAP disabilitato

Una volta aperti i dettagli del log in tempo reale dalla sessione in cui si è verificato l'errore, viene visualizzato il messaggio di errore "PEAP is not allowed in the Allowed Protocols" (PEAP non consentito nei protocolli consentiti).

| | |
|----------------|--|
| Event | 5400 Authentication failed |
| Failure Reason | 12303 Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols |
| Resolution | Ensure that the PEAP protocol is allowed by ISE in Allowed Protocols. |
| Root cause | The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use PEAP instead. However, PEAP is not allowed in Allowed Protocols. |
| Username | iseiscool |

Rapporto dettagliato registro dinamico

Questo errore è facile da risolvere. Per risolvere il problema, passare a Criteri > Elementi criterio > Autenticazione > Protocolli consentiti. Verificare se l'opzione Allow PEAP (Consenti PEAP) è disabilitata.

The screenshot shows the Cisco ISE configuration interface for a policy element named "Allow EAP-TLS". The left sidebar contains a navigation menu with categories: Authentication, Allowed Protocols, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled "Results" and shows the configuration for the "Allow EAP-TLS" policy element. The configuration includes several options: "Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy" (unchecked), "Enable Stateless Session Resume" (unchecked), "Session ticket time to live" set to 2 Hours, and "Proactive session ticket update will occur after 90 % of Time To Live has expired". Under the "PEAP Inner Methods" section, "Allow EAP-MS-CHAPv2" is checked, and "Allow Password Change" is checked with 1 Retries (Valid Range 0 to 3). "Allow EAP-GTC" is checked, and "Allow Password Change" is checked with 1 Retries (Valid Range 0 to 3). "Allow EAP-TLS" is checked, and "Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy" is unchecked. "Require cryptobinding TLV" is unchecked, and "Allow PEAPv0 only for legacy clients" is unchecked. The "Allow PEAP" checkbox is highlighted with a red box.

Sezione Protocolli consentiti

Terzo scenario: l'autenticazione non riesce perché l'endpoint non considera attendibile il certificato ISE.

Passare ai dettagli del registro attivo. Individuare il record per l'autenticazione non riuscita e controllare i dettagli del registro attivo.

Authentication Details

Source Timestamp 2024-04-20 04:37:42.007

Received Timestamp 2024-04-20 04:37:42.007

Policy Server ISE PSN

Event 5411 Supplicant stopped responding to ISE

Failure Reason 12934 Supplicant stopped responding to ISE during PEAP tunnel establishment

Resolution
Check whether the proper server certificate is installed and configured for EAP in the Local Certificates page (Administration > System > Certificates > Local Certificates). Also ensure that the certificate authority that signed this server certificate is correctly installed in client's supplicant. Check the previous steps in the log for this EAP-TLS conversation for a message indicating why the handshake failed. Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information.

Root cause PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

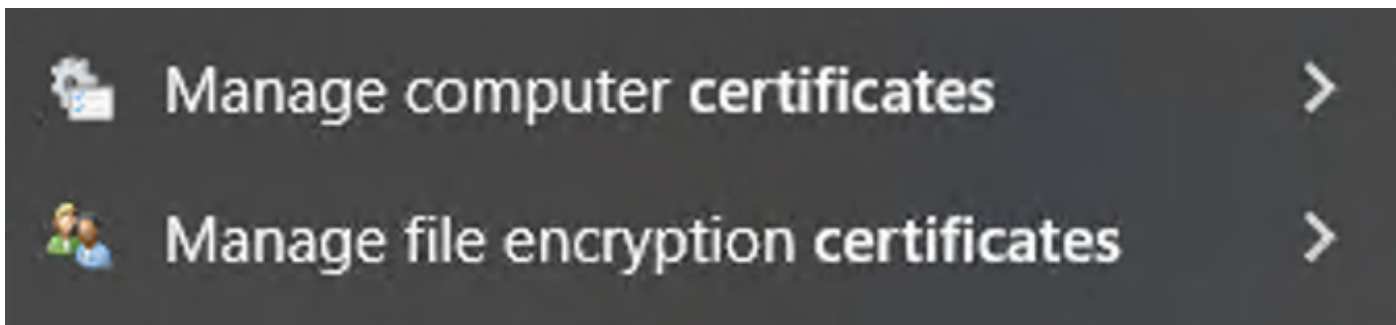
Username iseiscool

Dettagli registro dinamico

L'endpoint rifiuta il certificato utilizzato per la definizione del tunnel PEAP.

Per risolvere il problema, nell'endpoint di Windows in cui si verifica il problema verificare che la catena di CA che ha firmato il certificato ISE si trovi nella sezione Gestione certificati utente > Autorità di certificazione radice attendibili OPPURE Gestione certificati computer > Autorità di certificazione radice attendibili.

È possibile accedere a questa sezione di configurazione nel dispositivo Windows eseguendo una ricerca nella barra di ricerca di Windows.

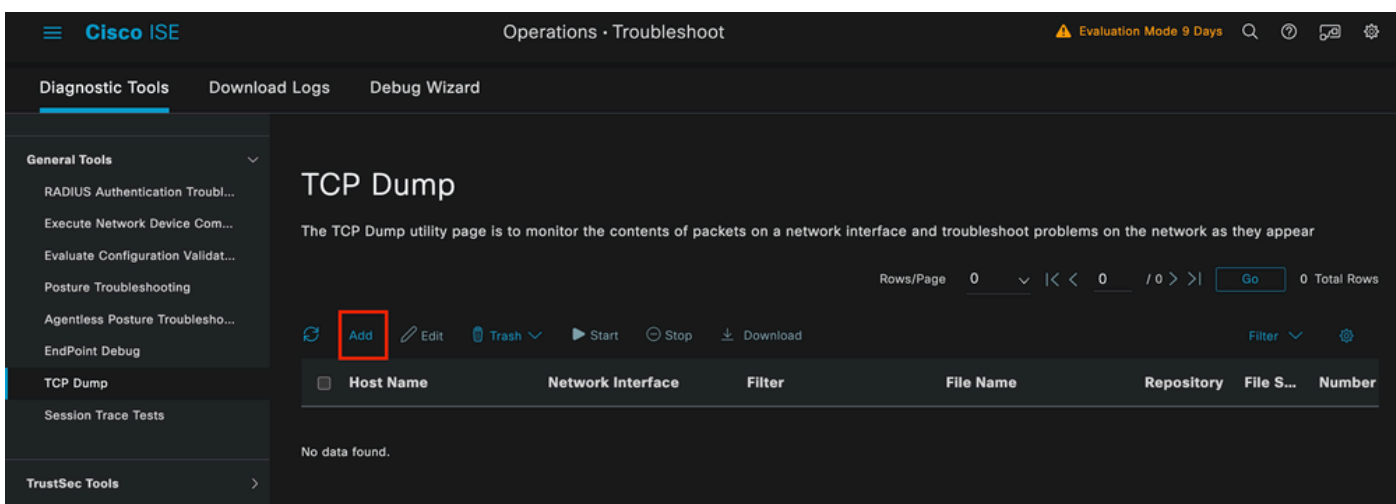


Risultati della barra di ricerca di Windows

3 - ISE TCP Dump Tool (acquisizione pacchetti)

L'analisi dell'acquisizione dei pacchetti è essenziale per la risoluzione dei problemi. Direttamente dalle acquisizioni di pacchetti ISE, è possibile acquisire i pacchetti su tutti i nodi e su qualsiasi interfaccia dei nodi.

Per accedere a questo strumento, selezionare Operazioni > Strumenti diagnostici > Strumenti generali > Dump TCP.



Sezione dump TCP

Fare clic sul pulsante Add (Aggiungi) per avviare la configurazione di un pcap.

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*

ISE PSN



Network Interface*

GigabitEthernet 0 [Up, Running]



Filter



E.g: ip host 10.77.122.123 and not
10.177.122.119

File Name

ISEPCAP

Creazione dump TCP

Repository

File Size
10
Mb

Limit to
1
File(s)

Time Limit
5
Minute(s)

Promiscuous Mode

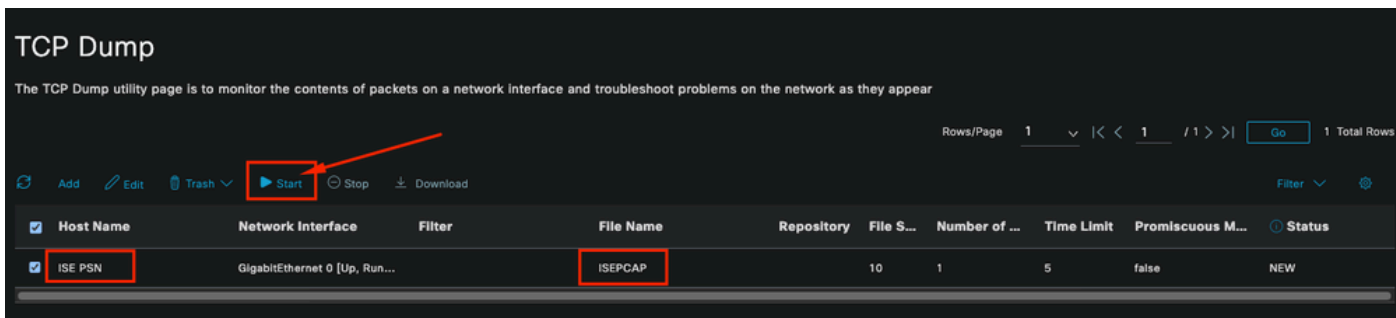
Cancel Save Save and Run

Sezione dump TCP

Per creare una cuffia in ISE, immettere i seguenti dati:

- Selezionare il nodo in cui è necessario prendere il pcap.
- Selezionare l'interfaccia del nodo ISE utilizzata per il pcap.
- Se è necessario catturare un certo traffico, usare i filtri, ISE offre alcuni esempi.
- Assegnate un nome alla pcap. In questo scenario è stato utilizzato ISEPCAP.
- Selezionare il repository; se non è selezionato alcun repository, l'acquisizione viene salvata sul disco locale ISE e può essere scaricata dalla GUI.
- Inoltre, se necessario, modificare le dimensioni del file pcap.
- Se necessario, utilizzare più di un file, in modo che se le dimensioni del file superano quelle del file, verrà creato un nuovo file.
- Se necessario, prolungare il tempo di acquisizione del traffico per il pcap.

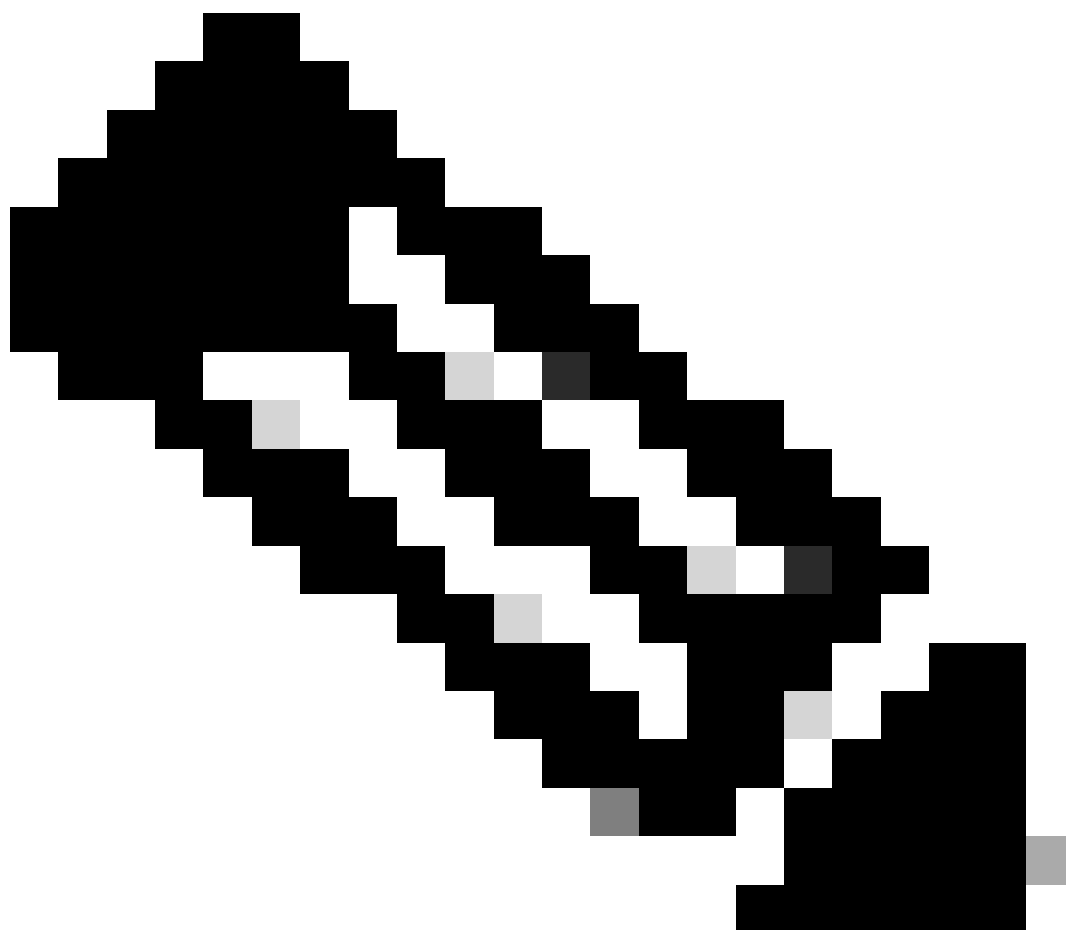
Infine, fare clic sul pulsante Salva.



Sezione dump TCP

Quindi, quando pronti, selezionare il pcap e fare clic sul pulsante Start.

Dopo aver fatto clic su Avvia, la colonna Stato (Status) viene impostata su IN ESECUZIONE (RUNNING).



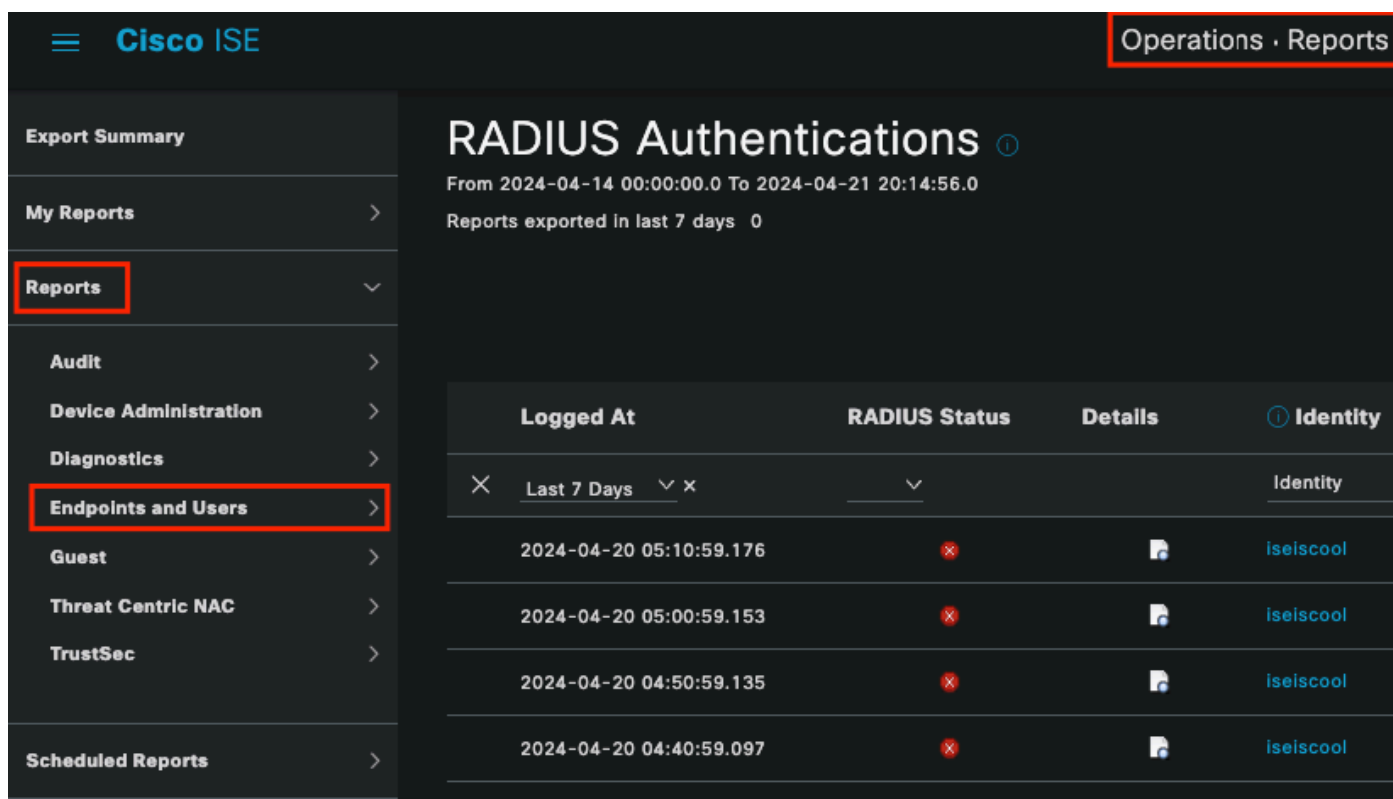
Nota: quando PCAP è in stato RUNNING, replicare lo scenario di errore o il comportamento da acquisire. Una volta completate le operazioni, i dettagli della conversazione RADIUS sono visibili nel PCAP.

Dopo aver acquisito i dati necessari durante l'esecuzione di PCAP, completare la raccolta pcap. Selezionarla nuovamente e fare clic su Stop.

3 - 1 Report ISE

Nel caso in cui sia necessaria un'analisi più approfondita, ISE offre report utili per analizzare eventi passati.

Per individuarli, passare a Operazioni > Report > Report > Endpoint e utenti



The screenshot shows the Cisco ISE interface. The top navigation bar includes the Cisco ISE logo and a 'Reports' link highlighted with a red box. The left sidebar contains a menu with 'Reports' highlighted in red, and 'Endpoints and Users' also highlighted in red. The main content area displays the 'RADIUS Authentications' report for the period from 2024-04-14 00:00:00.0 to 2024-04-21 20:14:56.0. The report shows 0 reports exported in the last 7 days. Below the header, there is a table with the following data:

| Logged At | RADIUS Status | Details | Identity |
|-------------------------|---------------|---------|-----------|
| × Last 7 Days × | ↓ | | Identity |
| 2024-04-20 05:10:59.176 | × | | iseiscool |
| 2024-04-20 05:00:59.153 | × | | iseiscool |
| 2024-04-20 04:50:59.135 | × | | iseiscool |
| 2024-04-20 04:40:59.097 | × | | iseiscool |

Sezione Report ISE

Endpoints and Users



Agentless Posture

Authentication Summary

Client Provisioning

Current Active Sessions

Endpoint & Logical Profi...

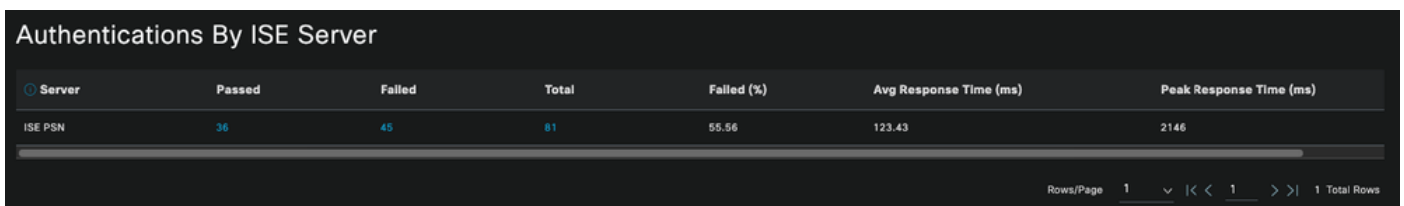
Endpoint Scripts Provisi...

External Mobile Device ...

Manual Certificate Provi...

PassiveID

: nella distribuzione utilizzata per questo documento, è stato utilizzato un solo PSN. Per distribuzioni più grandi, tuttavia, questi dati sono utili per verificare se è necessario il bilanciamento del carico.



| Server | Passed | Failed | Total | Failed (%) | Avg Response Time (ms) | Peak Response Time (ms) |
|---------|--------|--------|-------|------------|------------------------|-------------------------|
| ISE PSN | 36 | 45 | 81 | 55.56 | 123.43 | 2146 |

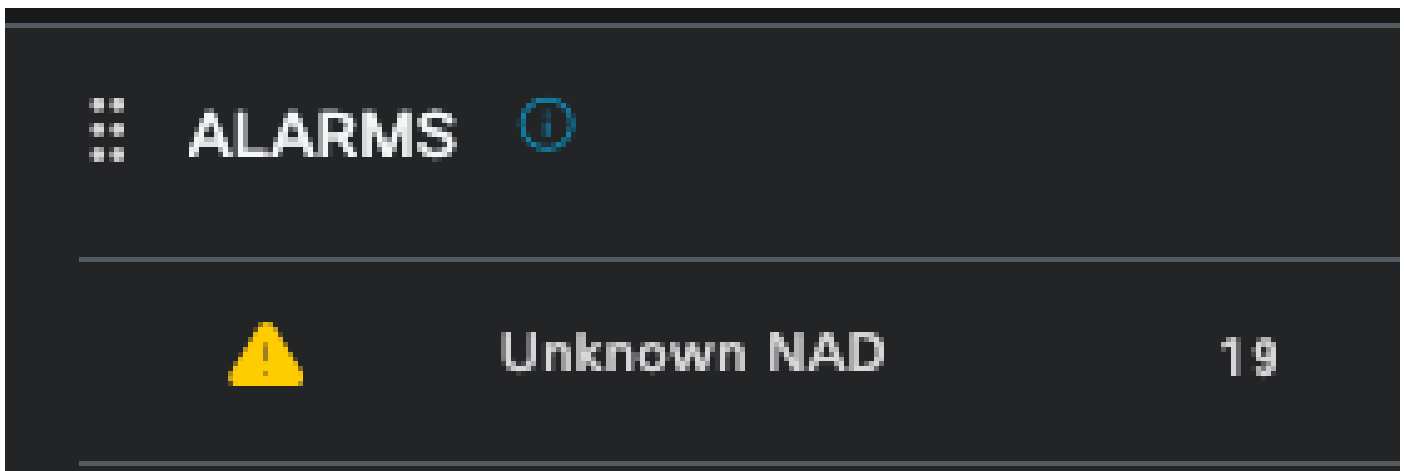
Autenticazioni da parte di ISE Server

4 - Allarmi ISE

Nella sezione Allarmi del dashboard ISE vengono visualizzati i problemi di distribuzione.

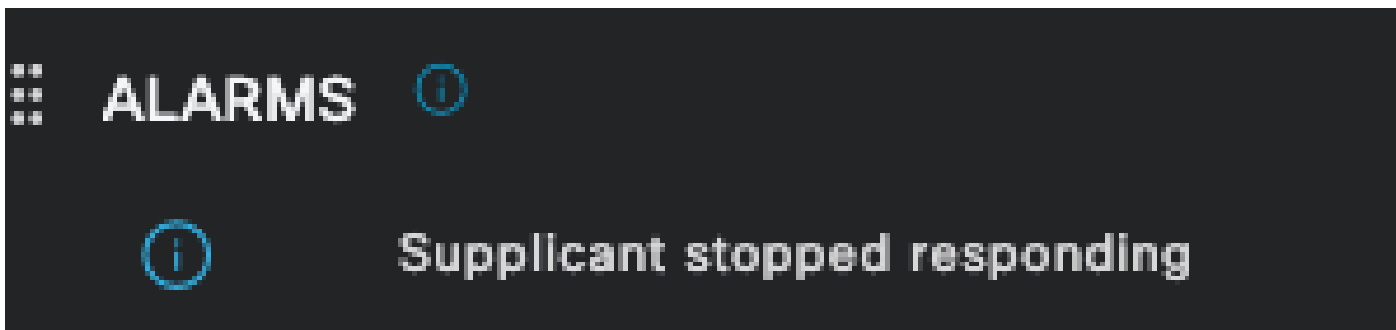
Di seguito sono riportati diversi avvisi ISE che aiutano nella risoluzione dei problemi.

NAD sconosciuto: questo allarme viene visualizzato quando un dispositivo di rete autentica un endpoint e sta raggiungendo ISE. Tuttavia, ISE non si fida di questa tecnologia e interrompe la connessione RADIUS. Il motivo più comune è che il dispositivo di rete non viene creato oppure l'indirizzo IP utilizzato dal dispositivo di rete non corrisponde a quello registrato da ISE.



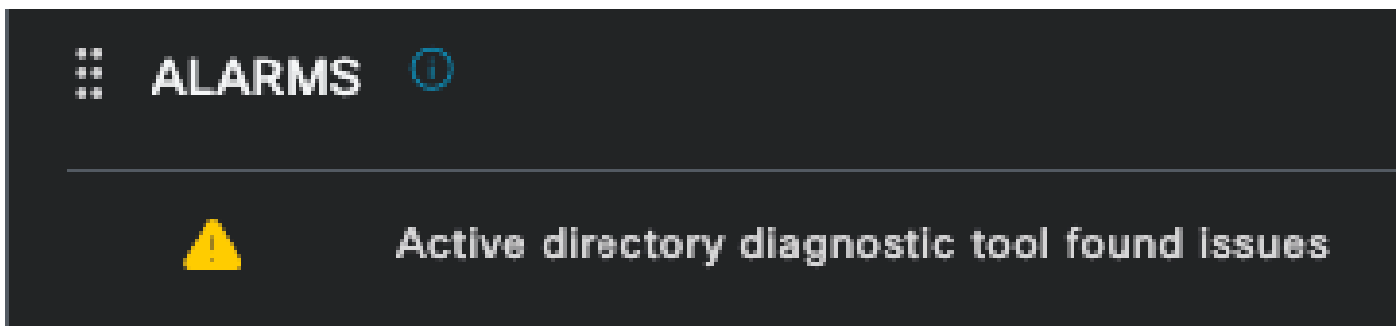
NAD sconosciuto

Supplicant Stopped Responding: questo allarme si verifica quando vi è un problema con la comunicazione del supplicant, la maggior parte del tempo è dovuto a una configurazione errata nel supplicant che deve essere controllato e investigato sul lato endpoint.



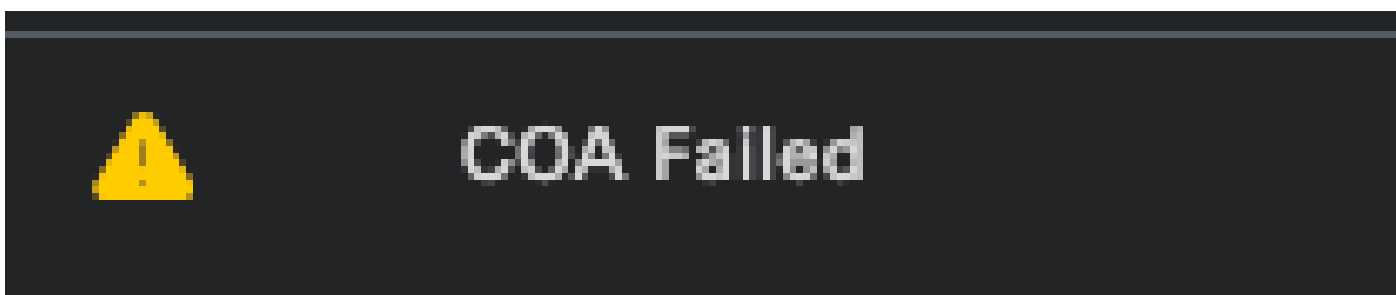
Il richiedente non risponde

Problemi rilevati dallo strumento di diagnostica di Active Directory: questo avviso si verifica quando si utilizza Active Directory per convalidare l'identità dell'utente, se inizia a verificarsi problemi con il processo di comunicazione o se la connessione viene interrotta. In questo modo sarà possibile comprendere il motivo per cui le autenticazioni che identificano l'identità nell'Active Directory non vengono eseguite.



Diagnostica AD non riuscita

COA (Change of Authorization) Failed — Multiple flows in ISE use CoA, questo allarme informa l'utente se si sono verificati problemi durante la comunicazione della porta CoA con qualsiasi dispositivo di rete.



Errore Coa

5 - Configurazione di debug ISE e raccolta dei log

Per continuare con i dettagli del processo di autenticazione, è necessario abilitare i componenti successivi in DEBUG per i problemi mab e dot1x:

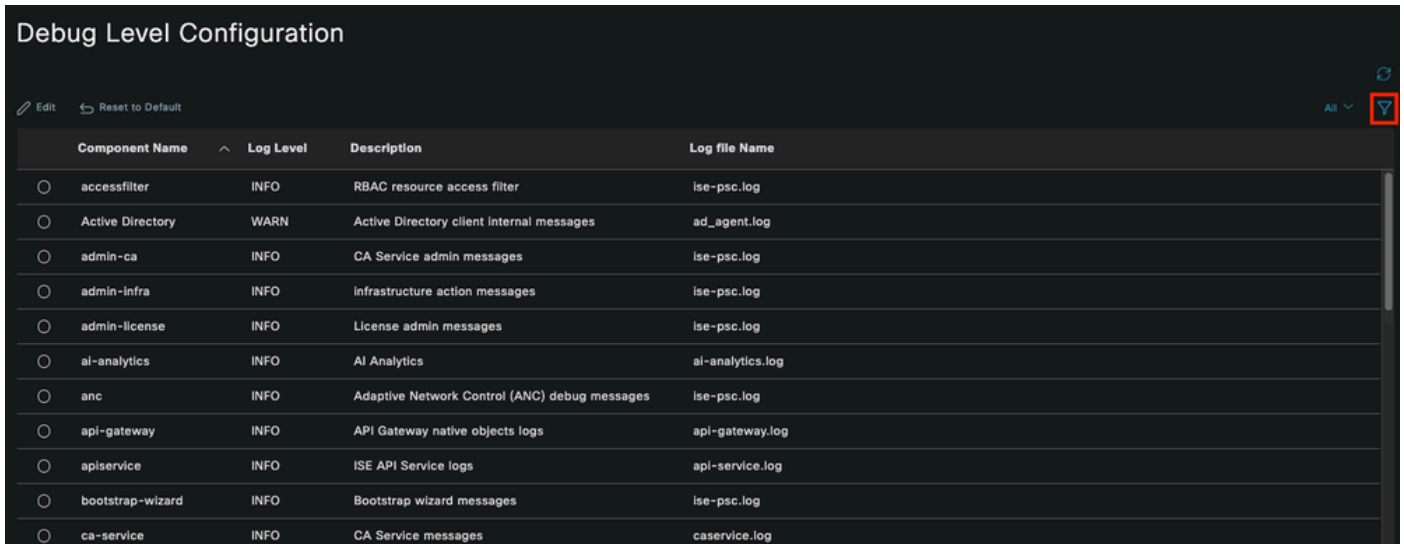
Problema: dot1x/mab

Attributi da impostare sul livello di debug.

- runtime-AAA (prt-server.log)
- nsf (ise-psc.log)
- sessione nsf (ise-psc.log)

Per abilitare i componenti al livello DEBUG, è necessario innanzitutto identificare il PSN che riceve l'autenticazione non riuscita o che deve essere analizzata. È possibile ottenere queste informazioni dai log attivi. Quindi selezionare ISE Menu > Troubleshoot > Debug Wizard > Debug Log Configuration > Select the PSN > Click the Edit Button.

Viene visualizzato il menu successivo. Fare clic sull'icona del filtro:

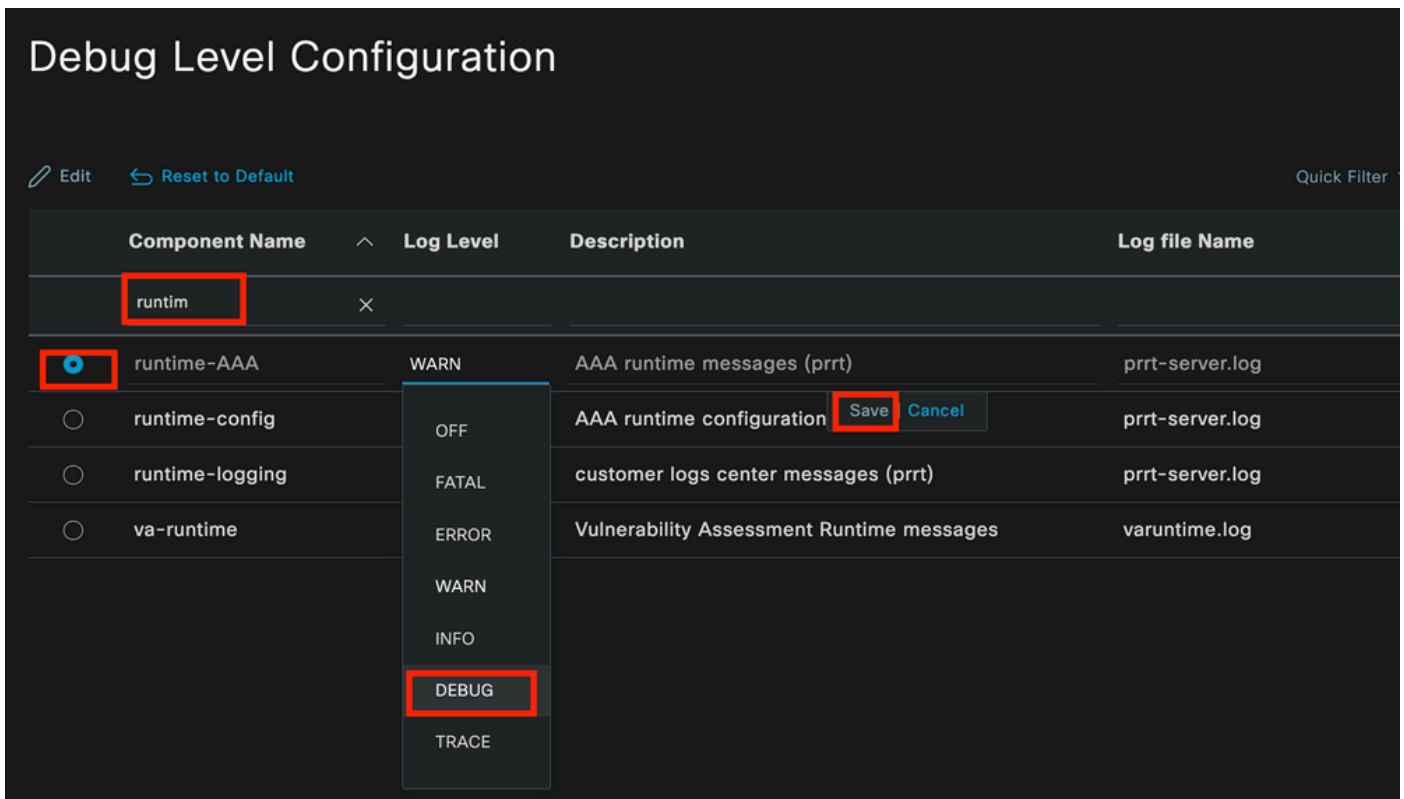


The screenshot shows the 'Debug Level Configuration' page with a table of components. The table has four columns: Component Name, Log Level, Description, and Log file Name. Each row has a radio button in the first column. The current log level for all components is 'INFO'. A red box highlights a filter icon in the top right corner of the table area.

| Component Name | Log Level | Description | Log file Name |
|--|-----------|---|------------------|
| <input type="radio"/> accessfilter | INFO | RBAC resource access filter | ise-psc.log |
| <input type="radio"/> Active Directory | WARN | Active Directory client internal messages | ad_agent.log |
| <input type="radio"/> admin-ca | INFO | CA Service admin messages | ise-psc.log |
| <input type="radio"/> admin-Infra | INFO | Infrastructure action messages | ise-psc.log |
| <input type="radio"/> admin-license | INFO | License admin messages | ise-psc.log |
| <input type="radio"/> ai-analytics | INFO | AI Analytics | ai-analytics.log |
| <input type="radio"/> anc | INFO | Adaptive Network Control (ANC) debug messages | ise-psc.log |
| <input type="radio"/> api-gateway | INFO | API Gateway native objects logs | api-gateway.log |
| <input type="radio"/> apiservice | INFO | ISE API Service logs | api-service.log |
| <input type="radio"/> bootstrap-wizard | INFO | Bootstrap wizard messages | ise-psc.log |
| <input type="radio"/> ca-service | INFO | CA Service messages | caservice.log |

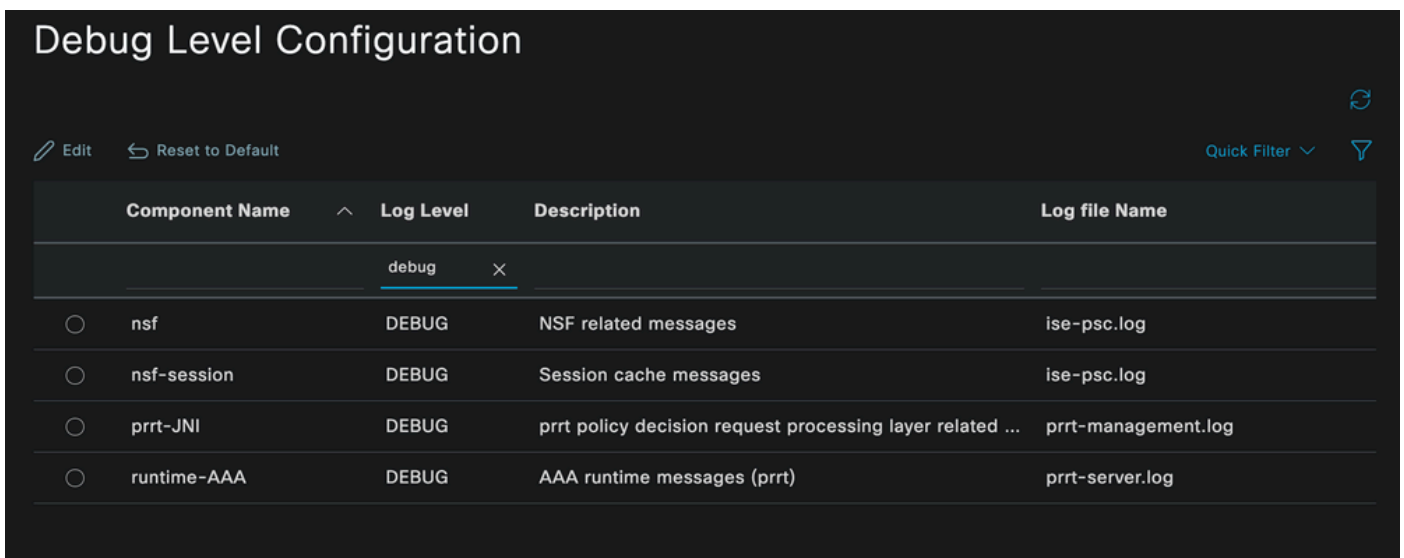
Configurazione registro di debug

Nella colonna Nome componente cercare gli attributi elencati in precedenza. Selezionare ciascun livello di log e modificarlo in DEBUG. Salvare le modifiche.



Configurazione componente AAA runtime

Una volta completata la configurazione di ciascun componente, filtrarlo con DEBUG per verificare che tutti i componenti siano stati configurati correttamente.



Configurazione registro di debug

Se è necessario analizzare immediatamente i log, è possibile scaricarli selezionando il percorso Menu ISE > Operazioni > Risoluzione dei problemi > Log di download > Elenco nodi Accessorio > PSN e abilitando DEBUGS > Debug Log.

In questo caso, è necessario scaricare i file per i problemi dot1x e mab nei file prrt-server.log e ise-psc.log. Il registro da scaricare è quello con la data dell'ultimo test.

È sufficiente fare clic sul file di registro visualizzato in questa immagine e scaricarlo (visualizzato in

blu).

| Debug Log Type | Log File | Description | Size |
|--------------------------|--------------------------|-----------------------------|--------|
| ise-psc (16) (111 MB) | | | |
| <input type="checkbox"/> | ise-psc (all logs) | Main ise debug log messages | 111 MB |
| <input type="checkbox"/> | ise-psc.log | | 5.8 MB |
| <input type="checkbox"/> | ise-psc.log.2024-04-03-1 | | 7.0 MB |
| <input type="checkbox"/> | ise-psc.log.2024-04-04-1 | | 6.9 MB |
| <input type="checkbox"/> | ise-psc.log.2024-04-05-1 | | 6.9 MB |
| <input type="checkbox"/> | ise-psc.log.2024-04-06-1 | | 7.0 MB |
| <input type="checkbox"/> | ise-psc.log.2024-04-07-1 | | 6.9 MB |
| <input type="checkbox"/> | ise-psc.log.2024-04-08-1 | | 6.9 MB |
| <input type="checkbox"/> | ise-psc.log.2024-04-09-1 | | 7.6 MB |
| <input type="checkbox"/> | ise-psc.log.2024-04-10-1 | | 8.0 MB |

Debug dei log dal nodo PSN

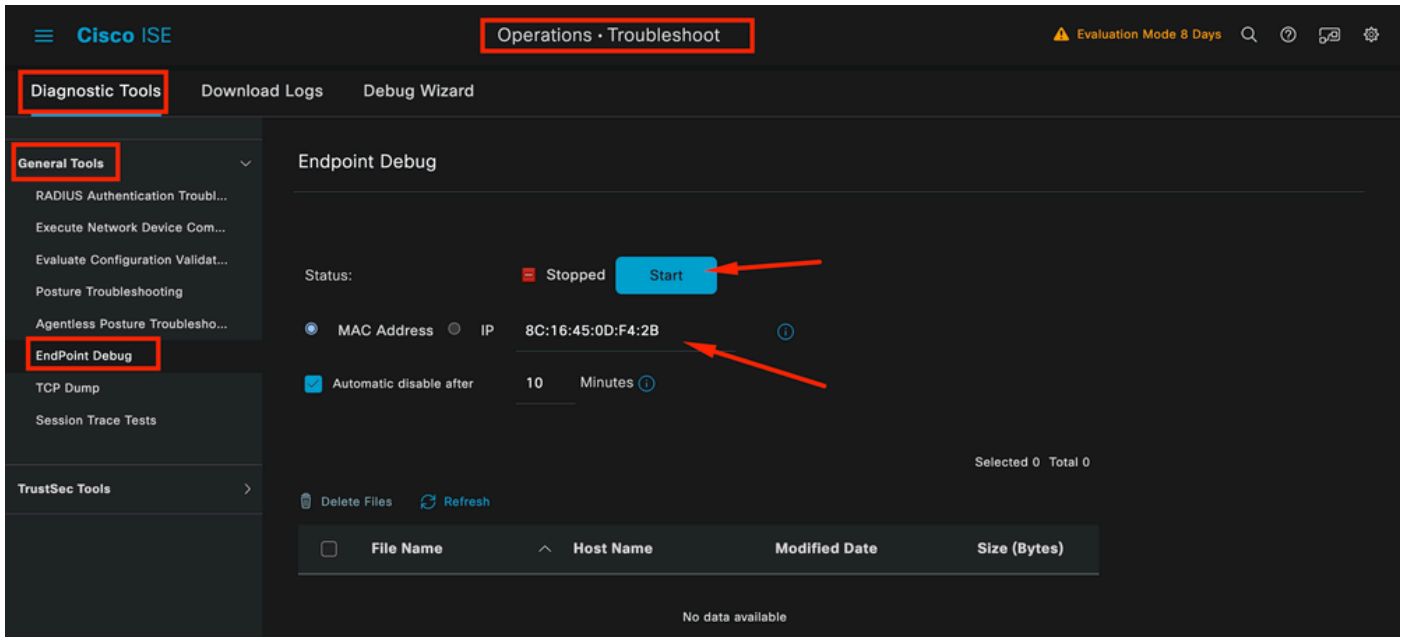
| Debug Log Type | Log File | Description | Size |
|--------------------------|------------------------|--|--------|
| prrt-server (1) (7.8 MB) | | | |
| <input type="checkbox"/> | prrt-server (all logs) | Protocol Runtime runtime configuration, debug and customer logs messages | 7.8 MB |
| <input type="checkbox"/> | prrt-server.log | | 7.8 MB |
| > pxcloud (4) (20 KB) | | | |

Sezione Log di debug

6 - Debug dell'ISE per endpoint

È inoltre disponibile un'altra opzione per ottenere i log di DEBUG, i log di debug per endpoint in base all'indirizzo MAC o all'IP. È possibile utilizzare lo strumento Endpoint Debug ISE.

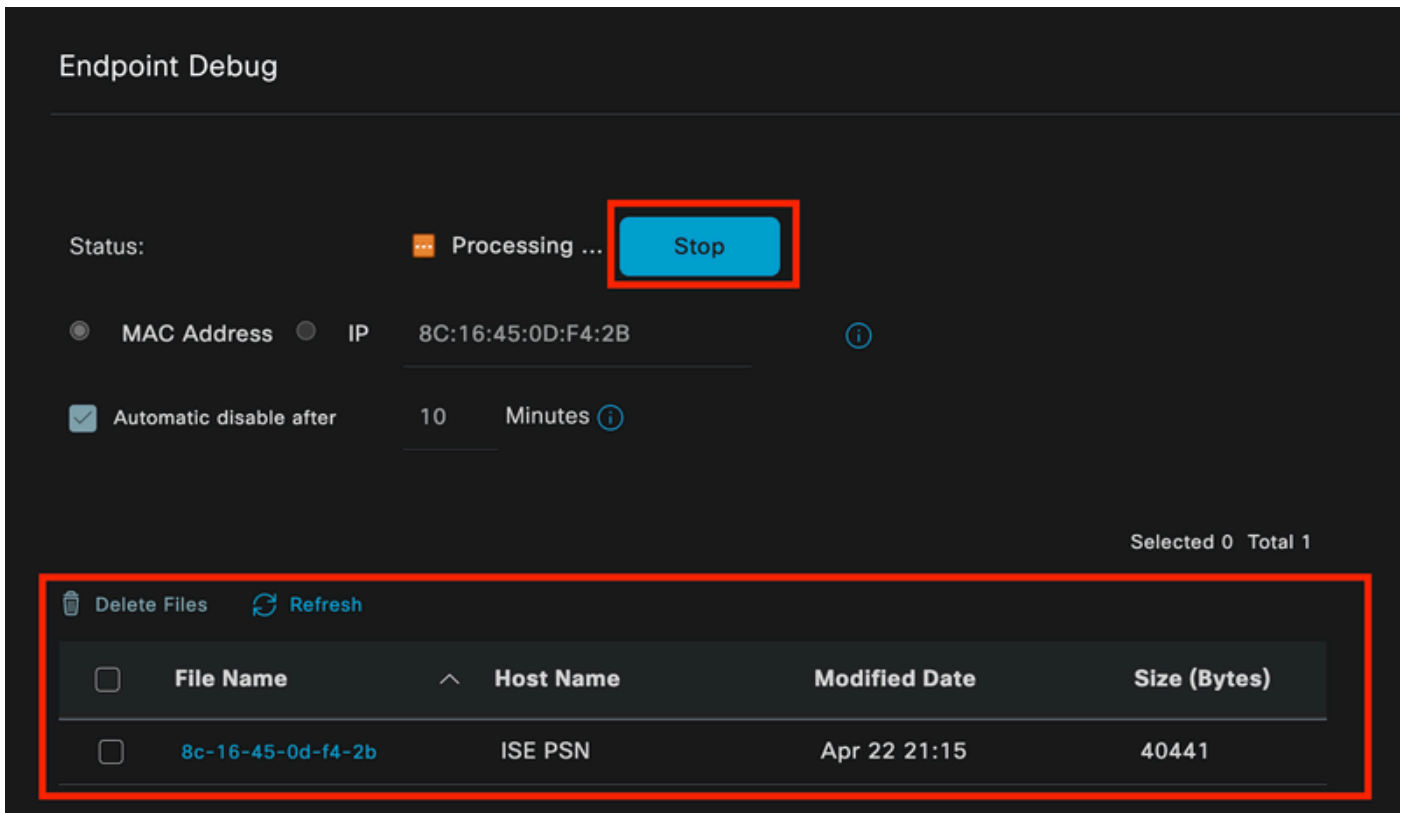
Selezionare ISE Menu > Operations > Troubleshoot > Diagnostic Tools > General Tools > Endpoint Debug.



Debug dell'endpoint

Immettere quindi le informazioni desiderate sull'endpoint per avviare l'acquisizione dei log. Fare clic su Start.

Quindi fare clic su Continue (Continua) nel messaggio di avviso.



Debug dell'endpoint

Una volta acquisite le informazioni, fare clic su Stop.

Fare clic sul nome del file visualizzato in blu. in questa immagine.

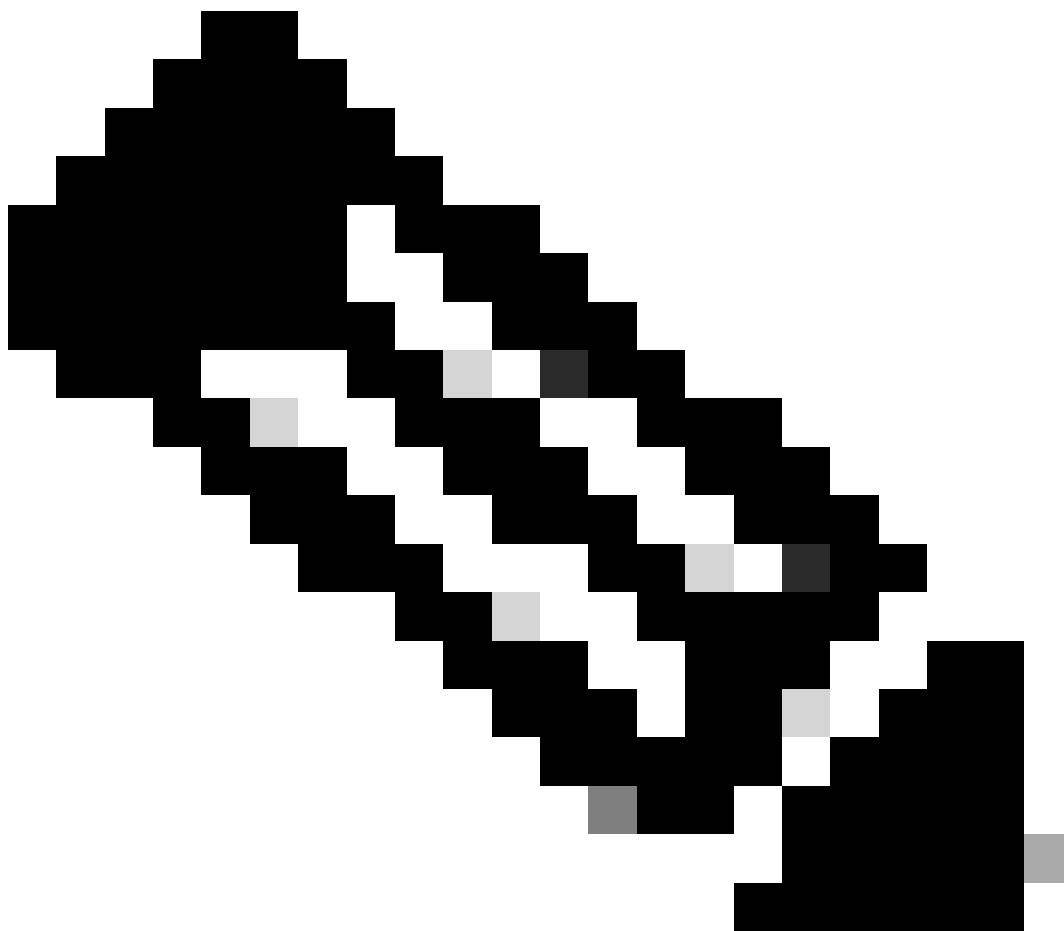
Selected 1 Total 1

Delete Files Refresh

| <input type="checkbox"/> | File Name | Host Name | Modified Date | Size (Bytes) |
|-------------------------------------|-------------------|-----------|---------------|--------------|
| <input checked="" type="checkbox"/> | 8c-16-45-0d-f4-2b | ISE PSN | Apr 22 21:17 | 67959712 |

Debug dell'endpoint

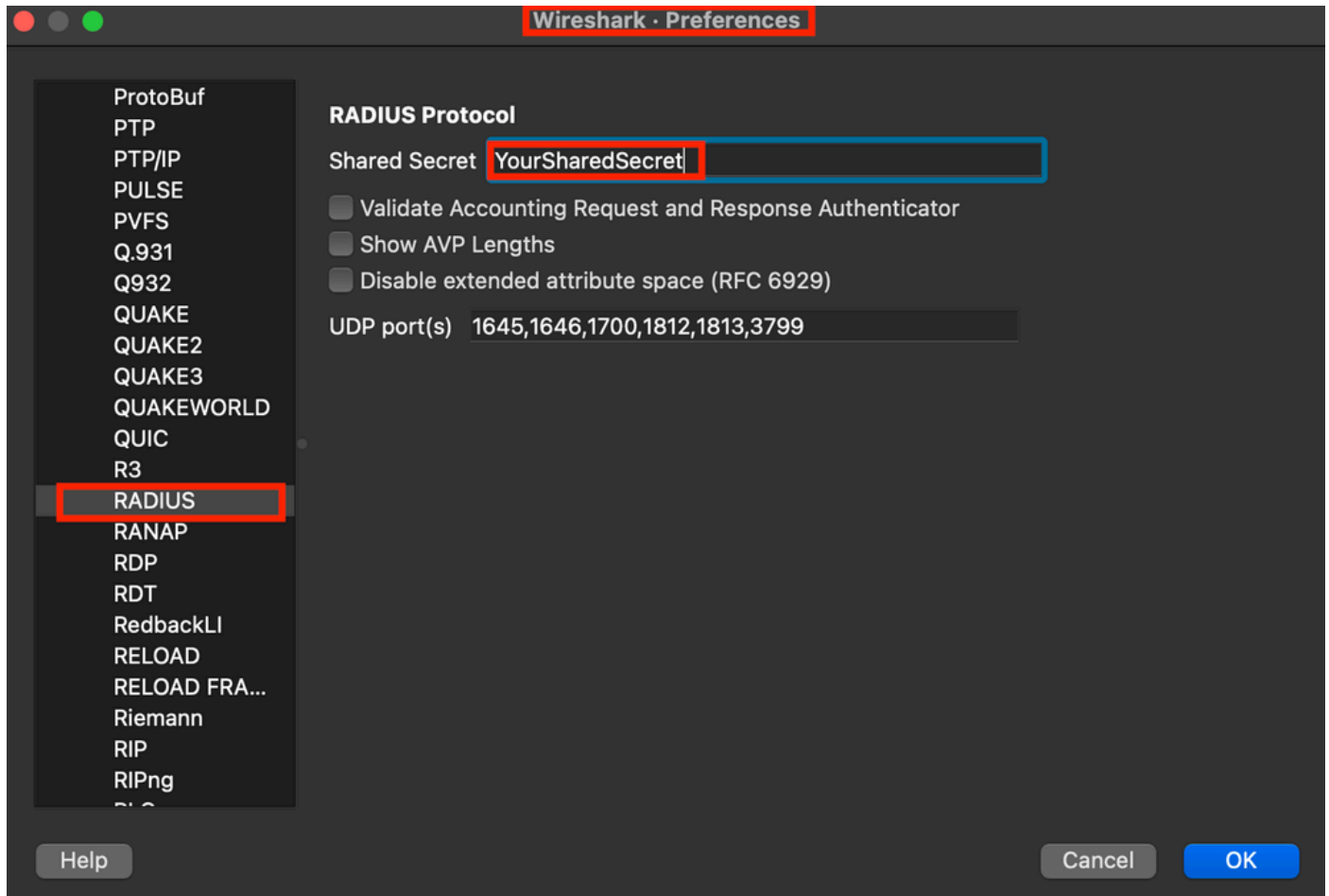
È necessario essere in grado di visualizzare i log di autenticazione con i log di DEBUG senza abilitarli direttamente da Configurazione log di debug.



Nota: poiché alcuni elementi potrebbero essere omessi nell'output di debug dell'endpoint, si otterrebbe un file di log più completo generandolo con la configurazione del log di debug e scaricando tutti i log richiesti da qualsiasi file necessario. Come spiegato nella sezione precedente Configurazione di debug ISE e raccolta dei log.

7 - Decrittografa pacchetti RADIUS

I pacchetti Radius non vengono crittografati ad eccezione del campo della password utente. Tuttavia, è necessario verificare la password inviata. Per visualizzare il pacchetto inviato dall'utente, selezionare Wireshark > Preferenze > Protocolli > RADIUS e quindi aggiungere la chiave condivisa RADIUS utilizzata da ISE e dal dispositivo di rete. Quindi, i pacchetti RADIUS vengono decrittati.



Opzioni raggio Wireshark

8 - Comandi per la risoluzione dei problemi dei dispositivi di rete

Il comando successivo consente di risolvere i problemi relativi a ISR 1100 o a dispositivi Wired AND.

8 - 1 Per verificare se il server AAA o ISE è disponibile e raggiungibile dal dispositivo di rete, usare show aaa server.

```
Router>show aaa servers
```

```
RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname  
State: current UP, duration 2876s, previous duration 0s  
Dead: total time 0s, count 0
```

```
Platform State from SMD: current UP, duration 2876s, previous duration 0s  
SMD Platform Dead: total time 0s, count 0
```

Platform State from WNCN (1) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (2) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (3) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (4) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (5) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (6) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (7) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (8) : current UP, duration 3015s, previous duration 0s

WNCN Platform Dead: total time 0s, count 0UP

Quarantined: No

Authn: request 11, timeouts 0, failover 0, retransmission 0

Response: accept 1, reject 0, challenge 10
Response: unexpected 0, server error 0, incorrect 0, time 33ms
Transaction: success 11, failure 0
Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0
Dot1x transactions:

Response: total responses: 11, avg response time: 33ms
Transaction: timeouts 0, failover 0
Transaction: total 1, success 1, failure 0

MAC auth transactions:
Response: total responses: 0, avg response time: 0ms
Transaction: timeouts 0, failover 0
Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0

Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0
MAC author transactions:

Response: total responses: 0, avg response time: 0ms
Transaction: timeouts 0, failover 0
Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3
Request: start 1, interim 0, stop 0
Response: start 1, interim 0, stop 0

Response: unexpected 0, server error 0, incorrect 0, time 27ms
Transaction: success 2, failure 1
Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0

Elapsed time since counters last cleared: 47m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0

```
Consecutive Response Failures: total 0
    SMD Platform : max 0, current 0 total 0
    WNCN Platform: max 0, current 0 total 0
    IOSN Platform : max 0, current 0 total 0

Consecutive Timeouts: total 3
    SMD Platform : max 0, current 0 total 0
    WNCN Platform: max 0, current 0 total 0
    IOSN Platform : max 3, current 0 total 3

Requests per minute past 24 hours:
    high - 0 hours, 47 minutes ago: 4
    low  - 0 hours, 45 minutes ago: 0
    average: 0
```

Router>

8-2 Per verificare lo stato della porta, i dettagli, gli ACL applicati alla sessione, il metodo di autenticazione e altre informazioni utili, usare il comando `show authentication sessions interface <interface where the laptop is attached>`.

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A00000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0
```

```
Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
```

```
Server Policies:
```

```
Method status list:
Method State
dot1x Authc Success
```

Router#

8-3 Per verificare di avere tutti i comandi richiesti per aaa nella configurazione globale, eseguire `show running-config aaa`.


```

Router#sh run aaa
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
client <A.B.C.D> server-key Cisc0123
!
!
radius server COHVSRAISE01-NEW
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646
timeout 15
key Cisc0123
!
!
aaa group server radius ISE-CLUSTER
server name COHVSRAISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#

```

8-4 Un altro comando utile è quello di testare `aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy`.

```

Router#test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy
User was successfully authenticated.

Router#

```

9 - Debug relativi ai dispositivi di rete

- `debug dot1x all`: visualizza tutti i messaggi EAP dot1x
- `debug aaa authentication`: visualizza le informazioni di debug dell'autenticazione provenienti dalle applicazioni AAA
- `debug aaa authorization` - Visualizza le informazioni di debug per l'autorizzazione AAA
- `debug radius authentication`: fornisce informazioni dettagliate sulle attività a livello di protocollo solo per l'autenticazione
- `debug radius`: fornisce informazioni dettagliate sulle attività a livello di protocollo

Informazioni correlate

- [Supporto tecnico Cisco e download](#)

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).