Integration der ISE in die Prime-Infrastruktur für Endgeräte-Transparenz

Inhalt

Einleitung

In diesem Dokument wird die Integration der ISE in die Prime-Infrastruktur beschrieben, um mehr Transparenz für authentifizierte Endgeräte zu erhalten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ISE,
- Cisco Prime-Infrastruktur.
- Wireless- oder kabelgebundener AAA-Fluss für Endpunkte, die sich über die ISE authentifizieren.
- SNMP-Konfiguration auf NADs (Network Access Devices) wie Switches und WLCs.

Verwendete Komponenten

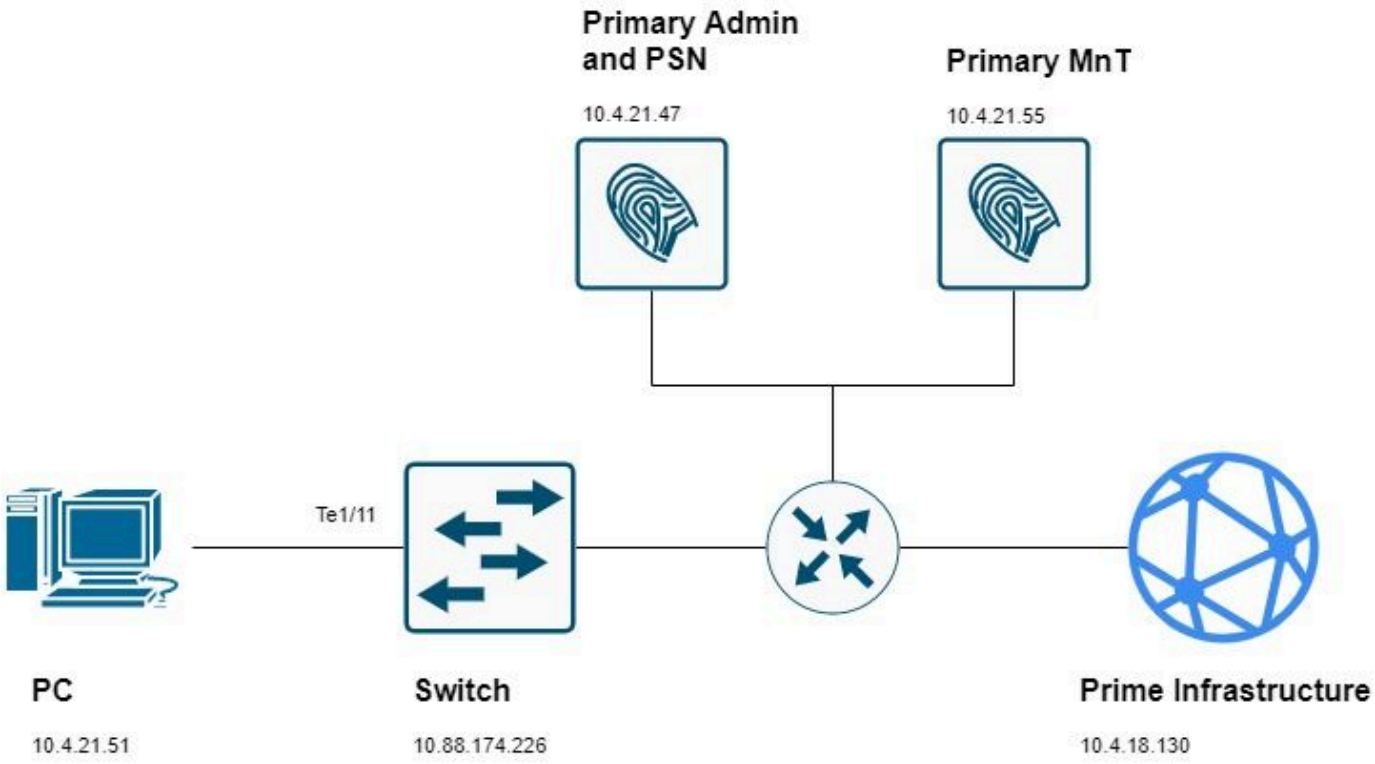
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE 3.1-Bereitstellung.
- Cisco Prime-Infrastruktur 3.8.
- C6816-X-LE mit Cisco IOS® 15.5
- Windows 10-Computer

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Switch-Konfiguration

1. Konfigurieren Sie das Netzwerkzugriffsgerät (NAD) für die AAA-Authentifizierung gegenüber der ISE. In dieser Anleitung verwenden Sie die folgende Konfiguration:

```
aaa new-model

radius server ise31
 address ipv4 10.4.21.47 auth-port 1812 acct-port 1813
 key Cisc0123
```

```
aaa server radius dynamic-author
 client 10.4.21.47 server-key Cisc0123

aaa group server radius ISE
 server name ise31

aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

dot1x system-auth-control
```

2. Konfigurieren Sie die Geräteverfolgung im Switch:

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3. Konfigurieren Sie den Switch-Port für die 802.1x-Authentifizierung, und hängen Sie die Richtlinie für die Geräteverfolgung an:

```
interface TenGigabitEthernet1/11
 device-tracking attach-policy DT1
 authentication host-mode multi-domain
 authentication order dot1x mab webauth
 authentication priority dot1x mab webauth
 authentication port-control auto
 mab
 dot1x pae authenticator
```

4. Konfigurieren Sie RO SNMP-Community und SNMP-Traps entsprechend Ihren Netzwerkanforderungen (Optional können Sie die RW-Community konfigurieren):

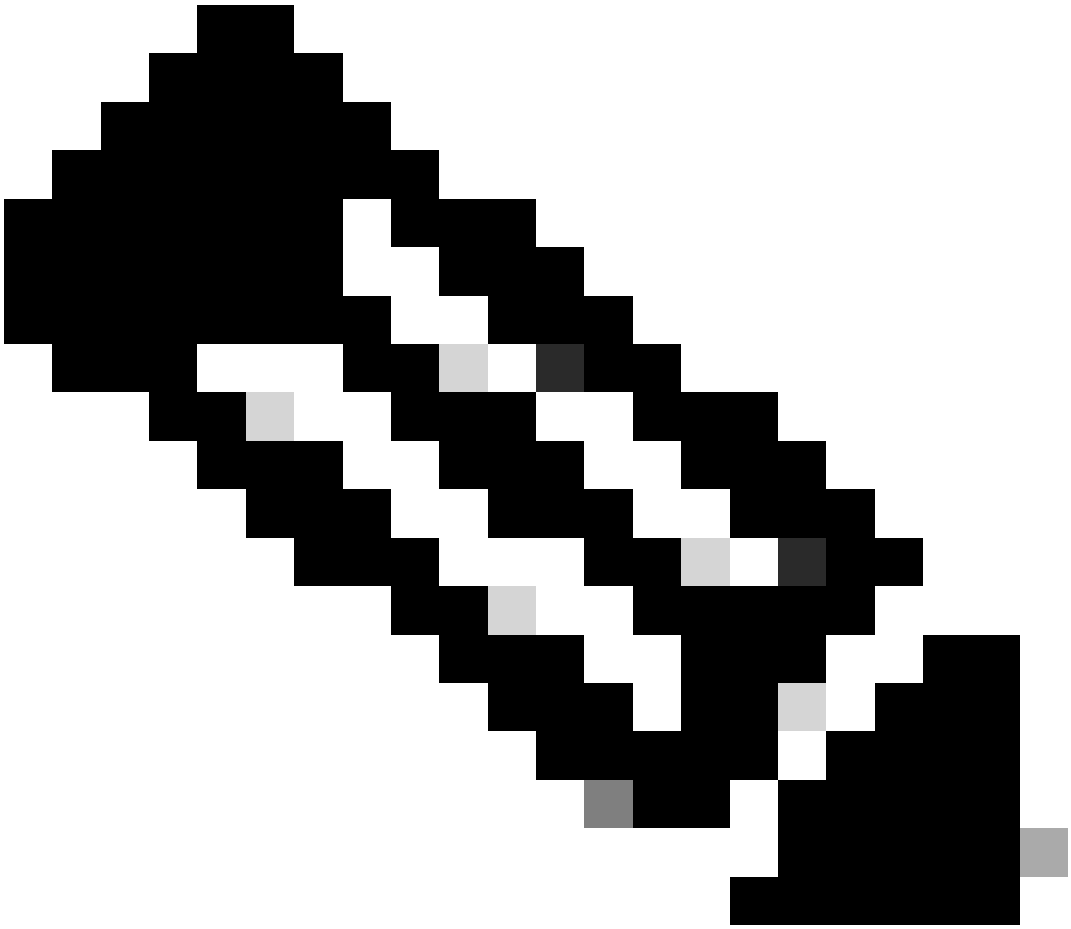
```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server enable traps trustsec authz-file-error
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps port-security
snmp-server enable traps event-manager
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.4.18.130 version 2c public udp-port 161
```

5. Konfigurieren Sie entweder einen Telnet- oder SSH-Zugriff, sodass Prime das Gerät verwalten kann:

```
username admin password 0 cisco!123
aaa authentication login default local

line vty 0 4
 transport input ssh
 login authentication default
```

6. (Optional) Für SSH-Verbindungen ist ein RSA-Schlüssel erforderlich. Wenn die NAD keine besitzt, können Sie sie mit diesen Schritten generieren.

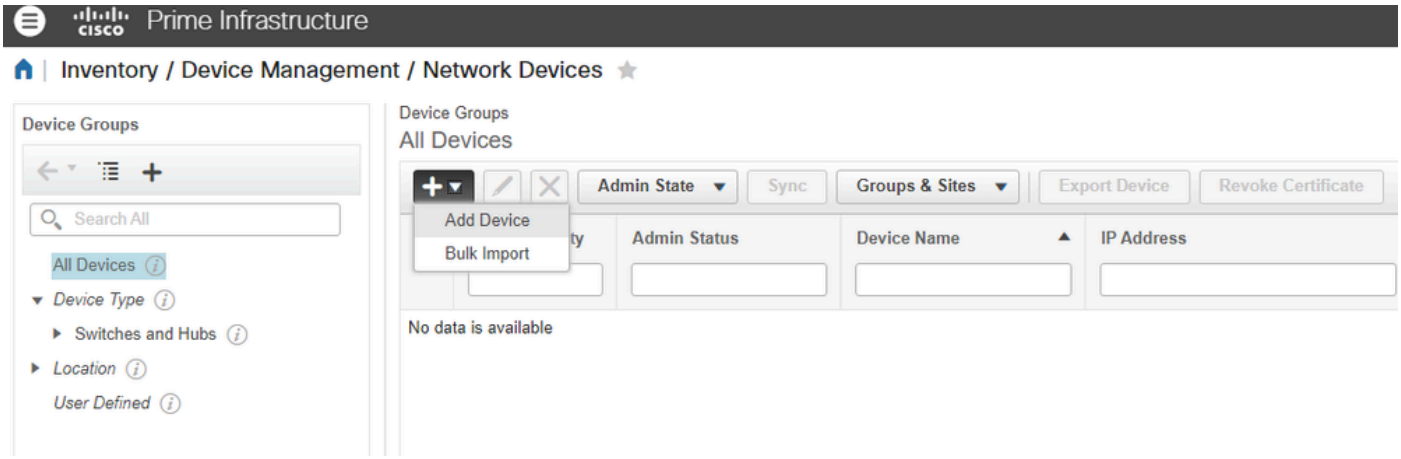


Anmerkung: Einige Geräte erfordern eine konfigurierte Domäne, bevor die RSA generiert wird. Überprüfen Sie, ob auf Ihrem Gerät eine Domäne konfiguriert ist, sodass Sie die vorhandene Domäne nicht überschreiben.

```
ip domain-name cisco.com
crypto key generate rsa
```

Konfiguration der Cisco Prime-Infrastruktur

7. Fügen Sie das Netzwerkgerät in Inventar > Gerätemanagement > Netzwerkgeräte > Pluszeichen (+) > Gerät hinzufügen hinzu:



Pflichtfelder für die Fertigstellung des Bestands:

Für kabelgebundene Geräte:

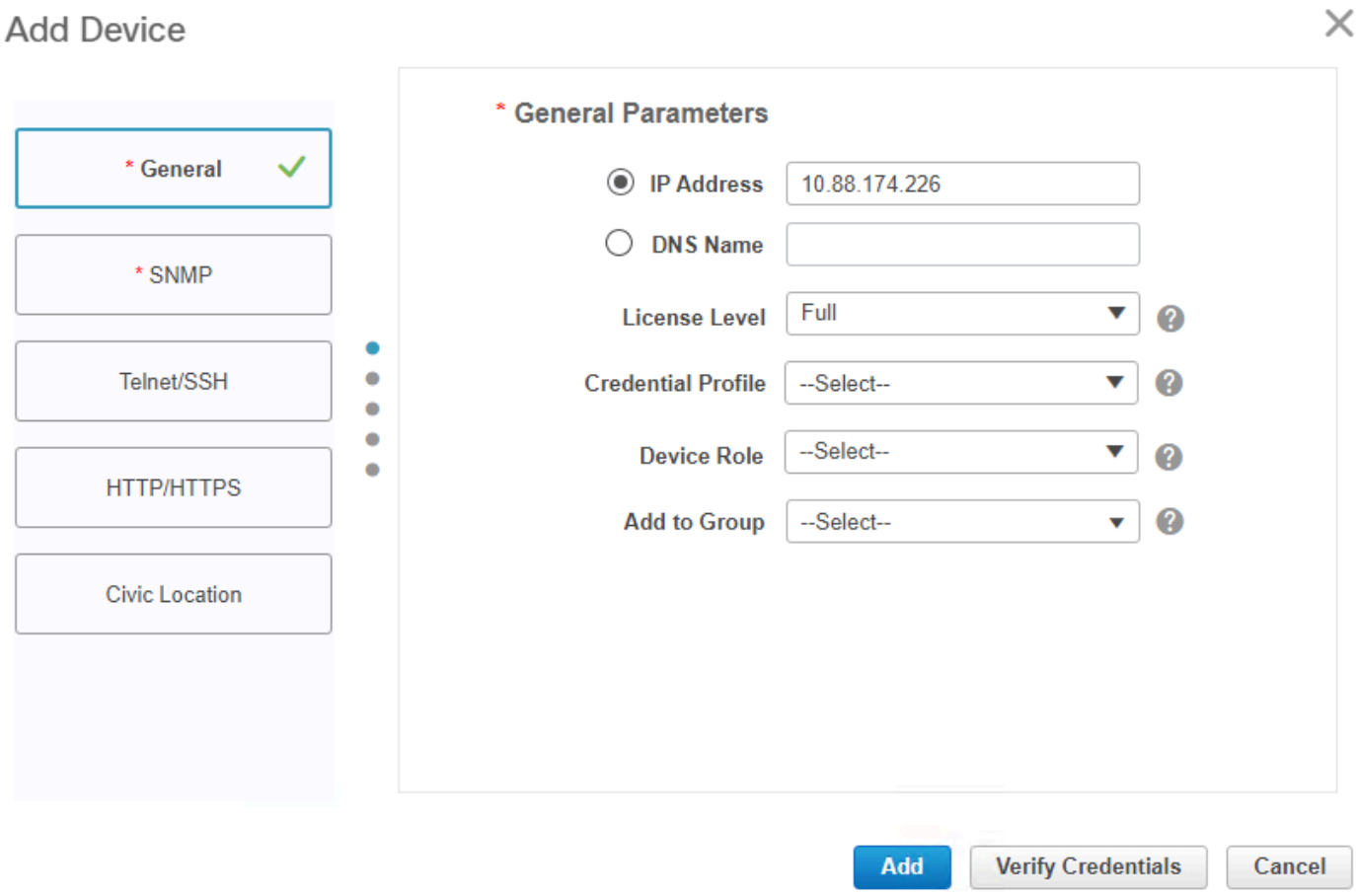
- Allgemein: entweder IP oder DNS.
- SNMP: RO-Community erforderlich - stellen Sie sicher, dass sie auch im Switch/WLC konfiguriert ist.
- Telnet/SSH: Exec-Modus und Anmeldeinformationen zum Aktivieren des Modus.

Für WLC:

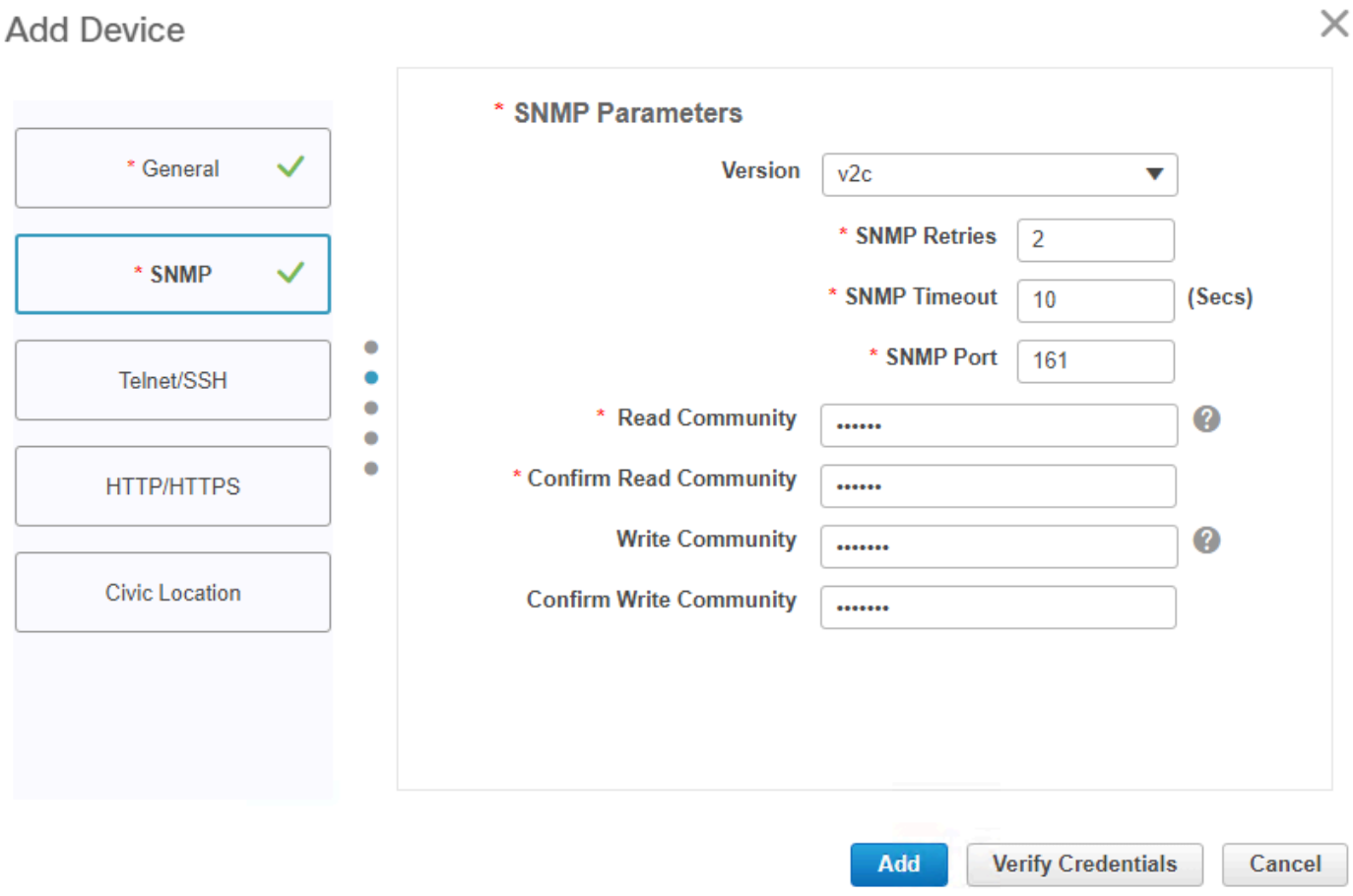
- Allgemein: entweder IP oder DNS.
- SNMP: RO-Community erforderlich - stellen Sie sicher, dass sie auch im Switch/WLC konfiguriert ist.

In dieser Anleitung verwenden Sie einen Cisco Switch:

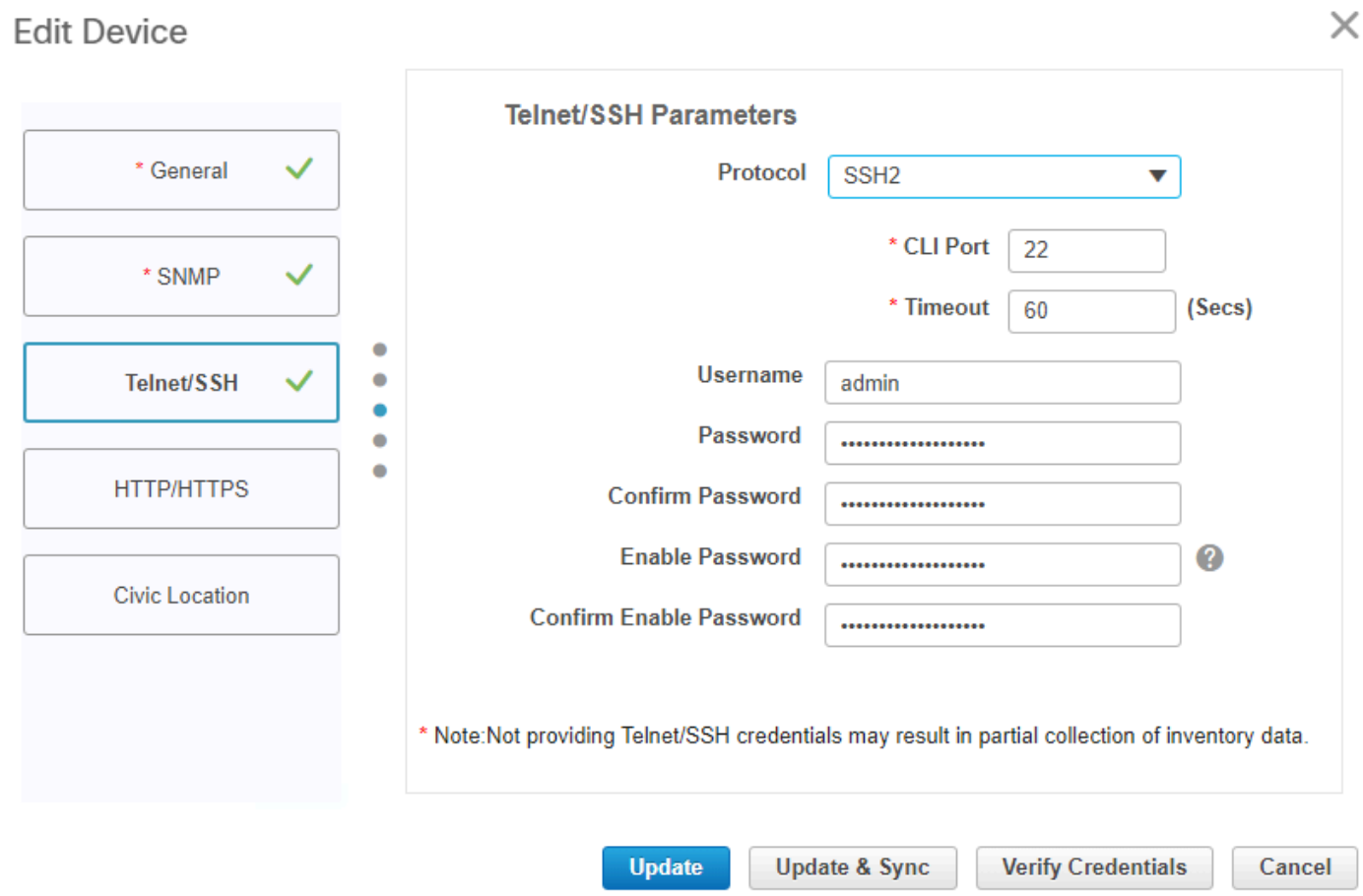
i. Allgemeiner Abschnitt:



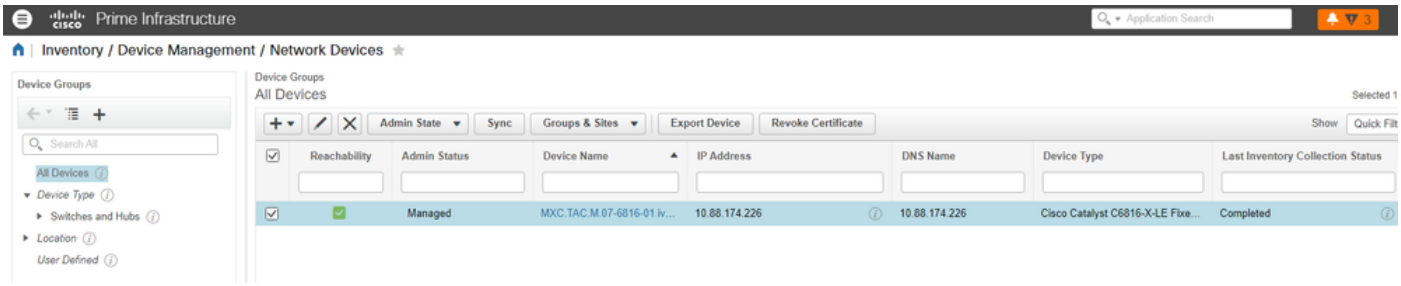
ii) SNMP-Abschnitt:



iii. Telnet/SSH-Abschnitt:



8. Wenn alle erforderlichen Felder ausgefüllt sind, stellen Sie sicher, dass die Status Erreichbarkeit und Erfassung grün bzw. abgeschlossen sind:

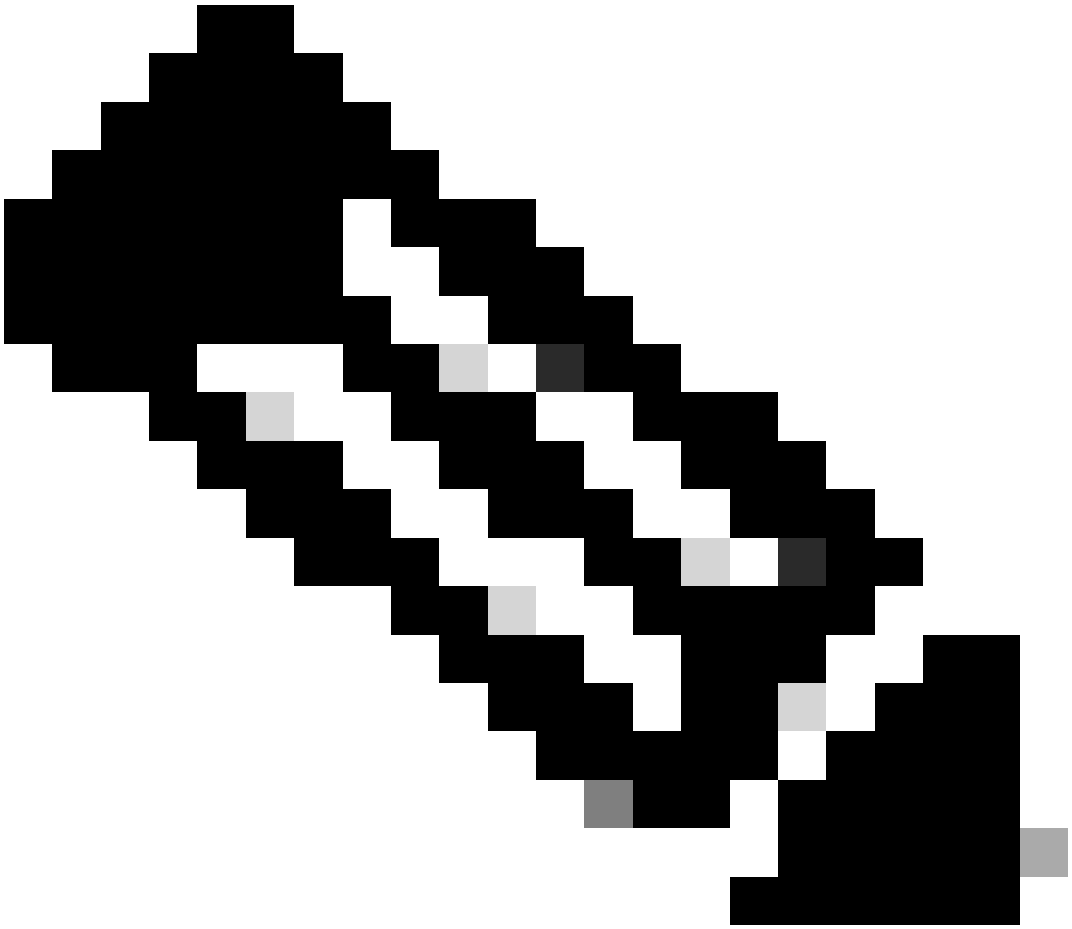


9. Prime in die ISE integrieren.

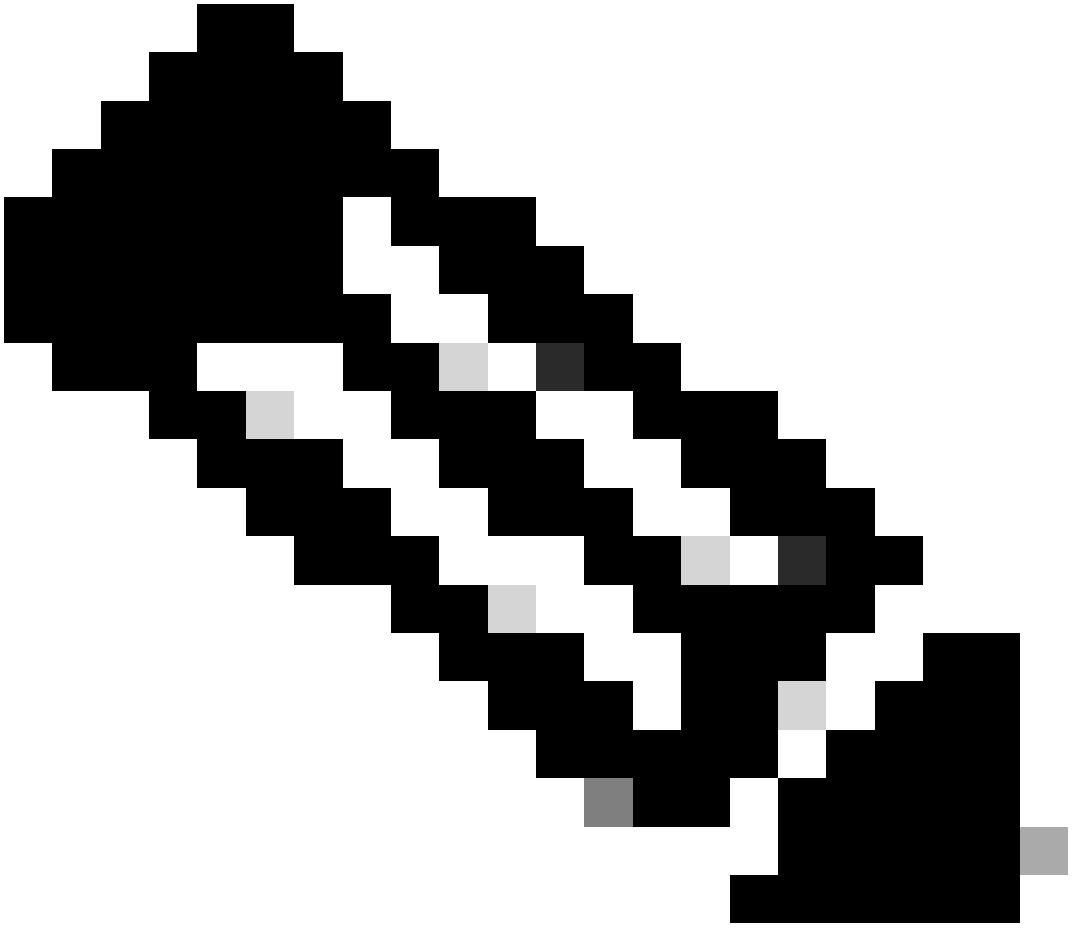
i. Navigieren Sie zu Administration > Servers > ISE Servers.

ii) Wählen Sie im Dropdown-Menü die Option ISE-Server hinzufügen aus, und klicken Sie dann auf Los:

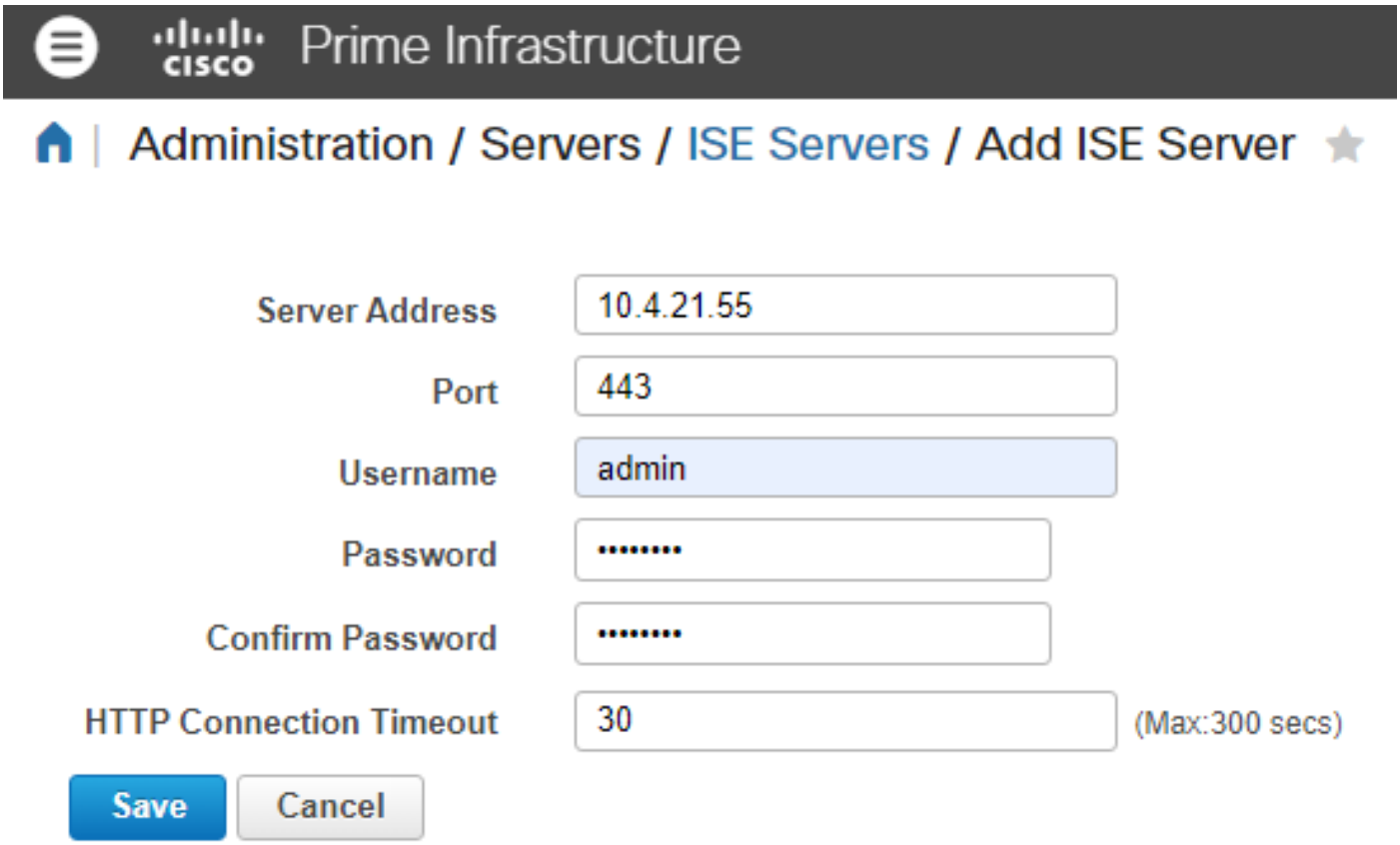
iii. Füllen Sie alle Felder aus, und klicken Sie auf Speichern.



Anmerkung: Die Verbindung muss zu den primären und sekundären (ggf.) ISE-Überwachungsknoten aufgebaut werden.



Anmerkung: Der Standardport ist auf 443 gesetzt, Sie können jedoch jeden anderen offenen Port in der ISE verwenden, um die Verbindung herzustellen.



iv. Navigieren Sie zurück zur Seite ISE-Server. Der Serverstatus lautet "Reachable" (Erreichbar), und die Rolle wird angezeigt (Standalone, Primary [MnT] oder Secondary [MnT]):

Endgerätekonfiguration

10. Der Endpunkt muss für die dot1x (RFC 3850)-Authentifizierung konfiguriert sein. Dies kann entweder durch die Konfiguration des Cisco Network Access Manager (NAM) oder durch die Nutzung der Native Betriebssystemkomponente erreicht werden. Es gibt zahlreiche Leitfäden zu dieser Konfiguration, daher werden diese Schritte in diesem Leitfaden nicht behandelt.

Überprüfung

ISE überprüfen

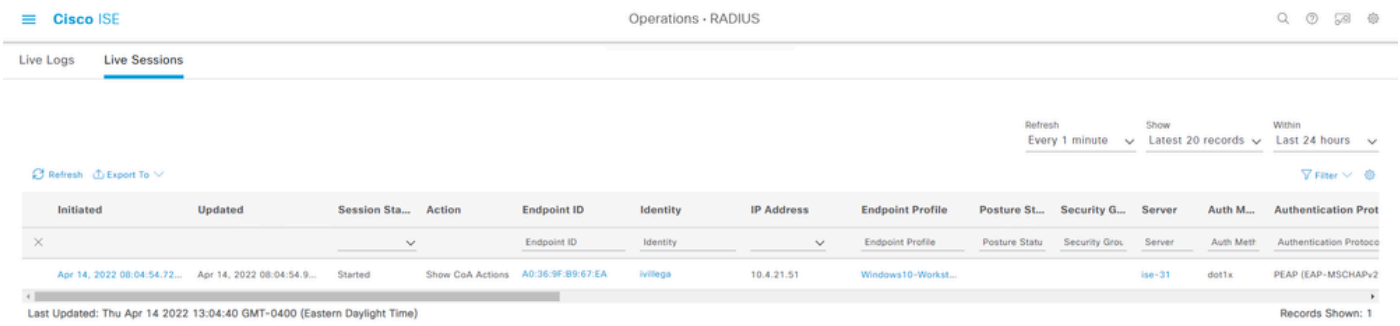
Die ISE empfängt die RADIUS-Anforderung von der NAD und authentifiziert den Benutzer erfolgreich.

Das NAD wird für RADIUS unter ISE > Administration > Network Resources > Network Devices

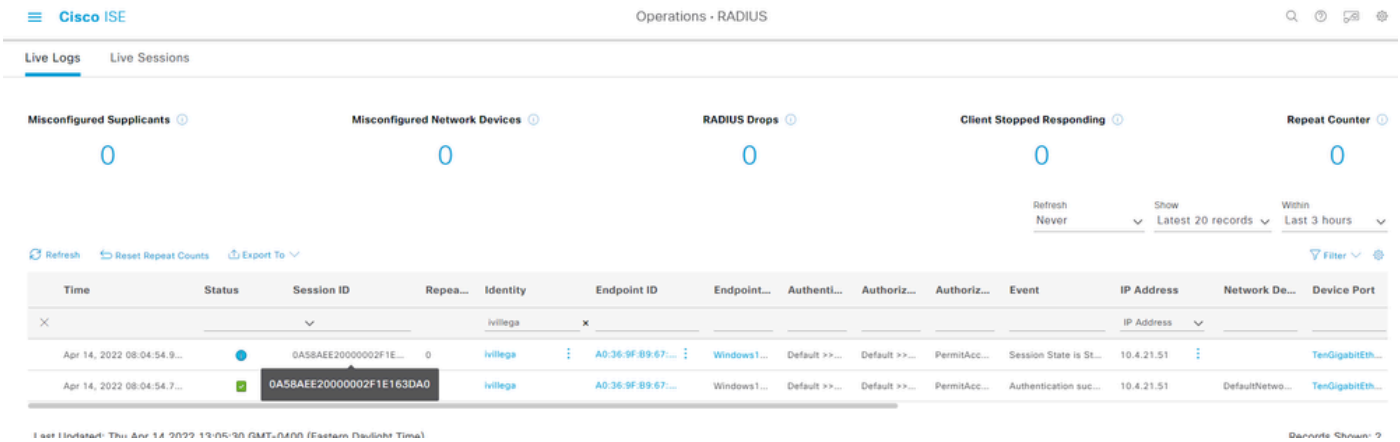
(ISE > Verwaltung > Netzwerkressourcen > Netzwerkgeräte) hinzugefügt und konfiguriert.

1. Navigieren Sie zu Operations > RADIUS > Live Sessions.

Vergewissern Sie sich, dass die Benutzer-Live-Sitzung auf dieser Seite aufgeführt ist. Die Sitzungsinformationen werden an die Prime-Infrastruktur weitergegeben.



2. Überprüfen Sie die Sitzungs-ID unter Operations > RADIUS > Live Logs:



Überprüfung der Netzwerkkarte

3. Überprüfen Sie die Sitzungsdetails im NAD. Die Sitzungs-ID stimmt mit der Sitzungs-ID in der ISE überein:

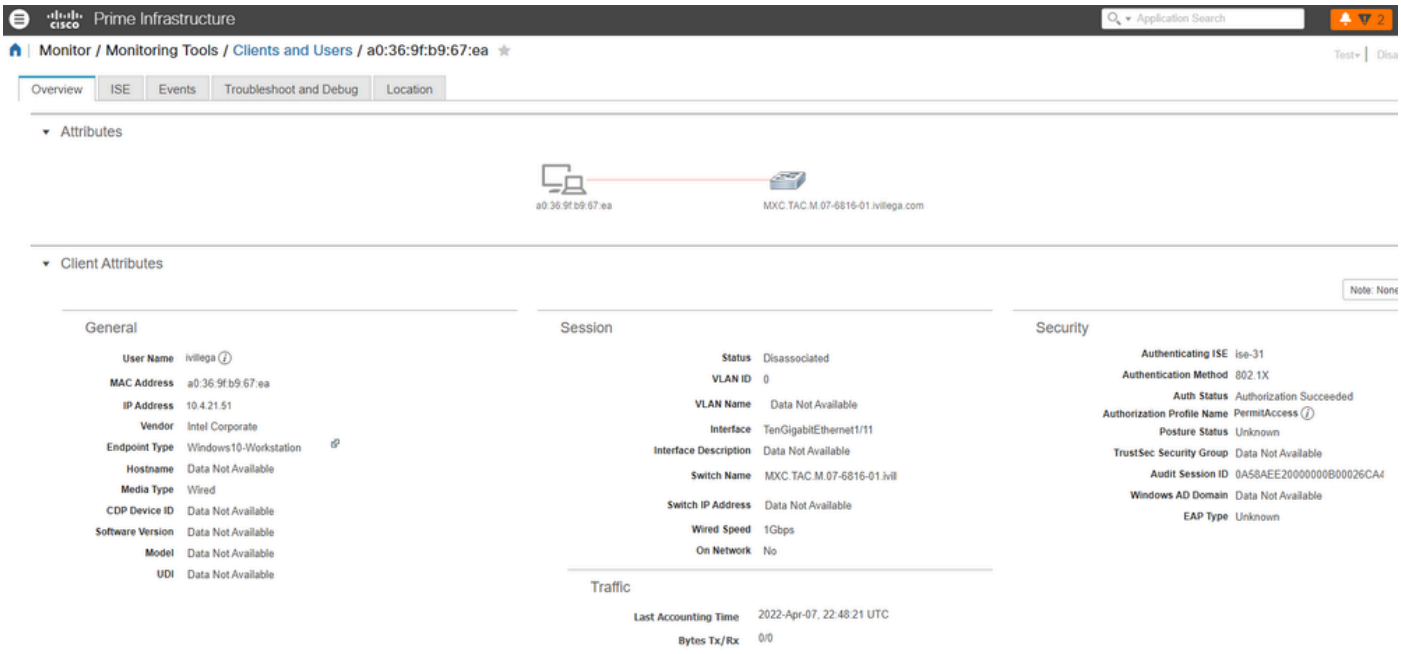
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: multi-domain
 Oper control dir: both
  Session timeout: N/A
Common Session ID: 0A58AEE20000002F1E163DA0
  Acct Session ID: 0x00000023
           Handle: 0xD9000001
   Current Policy: POLICY_Te1/11
```

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

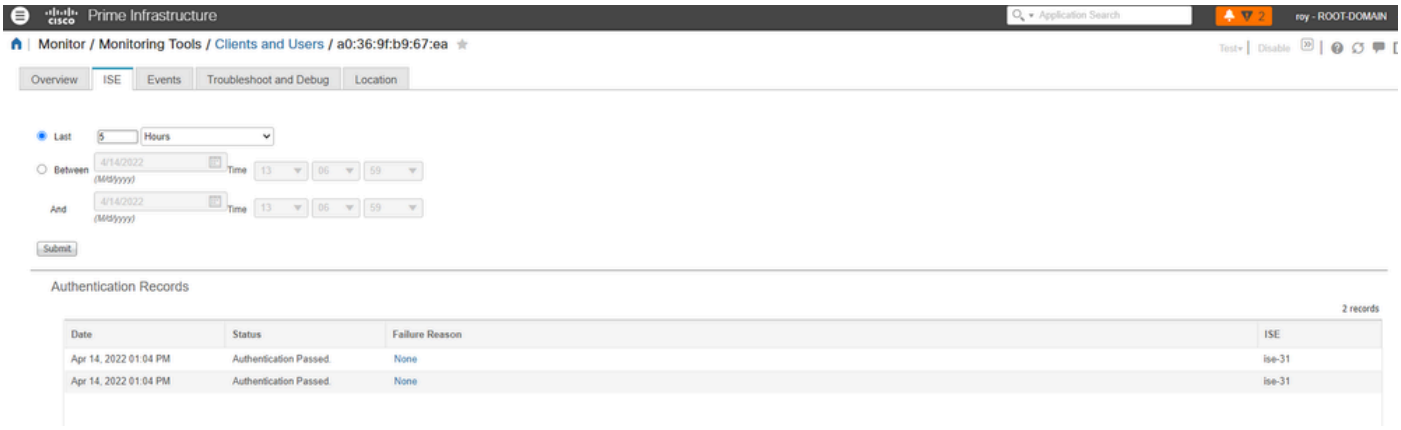
Prime-Infrastruktur verifizieren

4. Navigieren Sie zu Überwachen > Überwachungstools > Clients und Benutzer. Die MAC-Adresse des Endpunkts wird angezeigt:

5. Wenn Sie darauf klicken, werden die Details der Benutzersitzung und die ISE-Serverinformationen angezeigt:



6. Es gibt auch eine Registerkarte mit der Bezeichnung ISE zum Abrufen der Sitzungsereignisse für diesen Endpunkt. Sie können einen Zeitrahmen auswählen, den die Prime-Infrastruktur zum Abrufen von Ereignissen von der ISE verwendet:



Fehlerbehebung

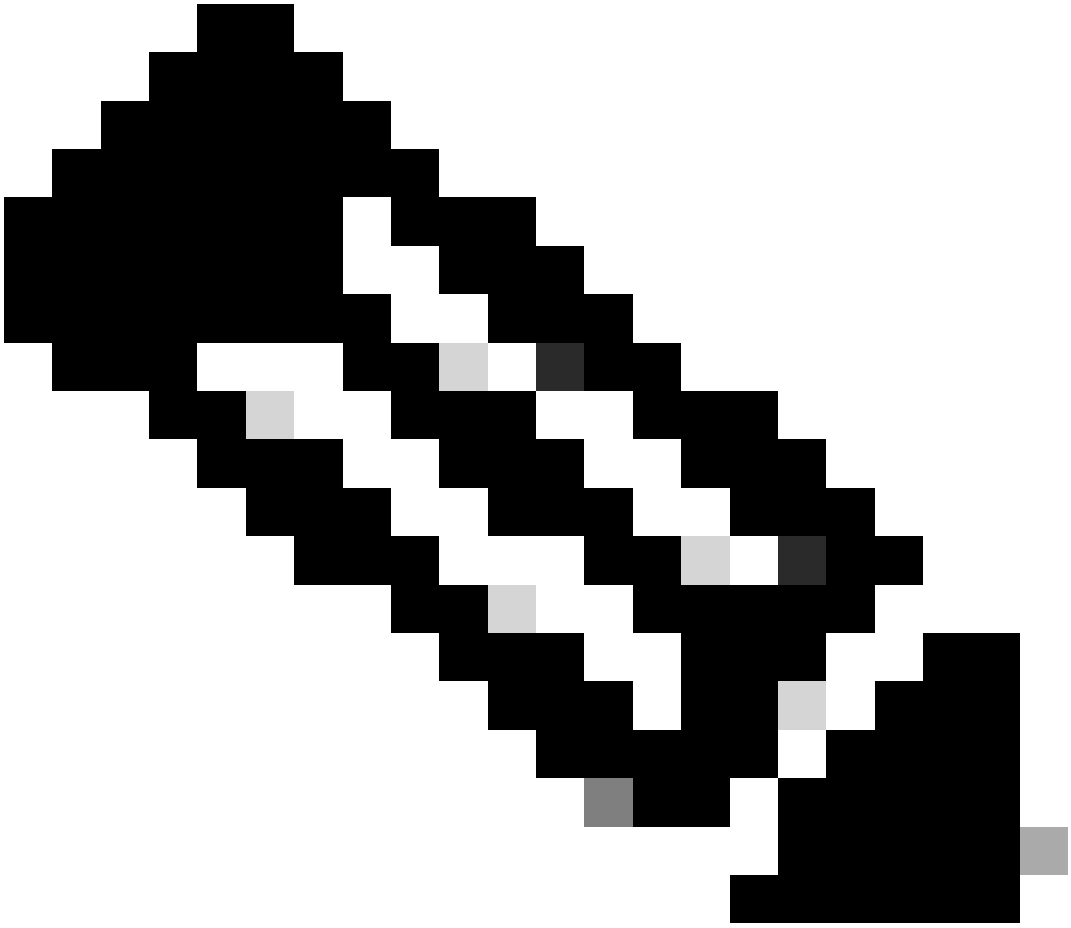
1. Testen Sie die Verbindung zwischen ISE und der Prime-Infrastruktur mit Pings. Wenn keine Verbindung besteht, können Sie das Problem mithilfe von Tracerouten entweder von der ISE oder der PI lokalisieren.

2. Überprüfen Sie, ob der in Schritt 9 konfigurierte Port im ISE MnT-Knoten geöffnet ist (der Standardport lautet 443):

```
ise-31-1/admin# show ports | include :443
     tcp: 0.0.0.0:80, 0.0.0.0:19444, 0.0.0.0:19001, 0.0.0.0:443
```

Wenn der Port in der Ausgabe aufgeführt ist, bedeutet dies, dass der Port für ISE MnT geöffnet ist.

Wenn kein Ausgang vorhanden oder der Port nicht aufgeführt ist, bedeutet dies, dass der Port für ISE MnT geschlossen ist. In diesem Fall können Sie einen anderen Port verwenden oder ein TAC-Ticket beim ISE-Team erstellen, um zu überprüfen, warum der Port nicht geöffnet ist.



Anmerkung: Der ISE MnT-Knoten verwendet nur einige Ports. Es ist nicht möglich, Ports im ISE MnT-Knoten zu öffnen, die nicht im ISE-Installationshandbuch, Port-Referenzabschnitt, aufgeführt sind.

---

3. Testen Sie den in Schritt 9 konfigurierten Port mit Telnet von der Prime-Infrastruktur:

```
prime-testcom/admin# telnet 10.4.21.55 port 443
Trying 10.4.21.55...
Connected to 10.4.21.55.
```

Wenn die Ausgabe des Telnet-Tests mit <ISE MnT IP/FQDN> verbunden ist, bedeutet dies, dass der Test erfolgreich war.

Wenn die Ausgabe des Telnet-Tests bei Trying <ISE MnT IP/FQDN> feststeckt, bedeutet dies, dass der Test fehlgeschlagen ist. Dies kann mit ACLs in zwischengeschalteten Netzwerkgeräten

oder mit Firewall-Regeln zusammenhängen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.