

Implementieren von ISE Redirectionless Posture

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Connectiondata.xml](#)

[Call Home-Liste](#)

[Design](#)

[Konfigurieren](#)

[Netzwerk-Gerätegruppen \(optional\)](#)

[Netzwerkgerät](#)

[Client-Bereitstellung](#)

[Manuelle Bereitstellung \(Pre-Deployment\)](#)

[Client-Bereitstellungsportal \(Webbereitstellung\)](#)

[Client-Bereitstellungsrichtlinie](#)

[Autorisierung](#)

[Autorisierungsprofil](#)

[Autorisierungsrichtlinie](#)

[Fehlerbehebung](#)

[Konformität mit Cisco Secure Client und Status nicht zutreffend \(ausstehend\) auf ISE](#)

[Veraltete/Phantom-Sitzungen](#)

[Identifizieren](#)

[Lösung](#)

[Leistung](#)

[Identifizieren](#)

[Lösung](#)

[Buchhaltung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Verwendung und Konfiguration eines umleitungslosen Statusflusses und Tipps zur Fehlerbehebung beschrieben.

Voraussetzungen

Anforderungen

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

- Statusüberprüfung für ISE
- Konfiguration von Statuskomponenten auf der ISE
- Umleitung zu ISE-Portalen

Für ein besseres Verständnis der später beschriebenen Konzepte wird empfohlen, folgende Schritte durchzuführen:

Verwendete Komponenten

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

- Cisco ISE Version 3.1
- Cisco Secure Client 5.0.01242

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.

Hintergrundinformationen

Der ISE-Statusflow besteht aus den folgenden Schritten:

0. Authentifizierung/Autorisierung Wird in der Regel unmittelbar vor Beginn des Statusflusses durchgeführt, kann aber in bestimmten Anwendungsfällen wie der Statusüberprüfung (PRA) umgangen werden. Da die Authentifizierung selbst keine Staterkennung auslöst, wird dies nicht bei jedem Statusfluss als wesentlich erachtet.

1. Erkennung. Prozess, der vom Secure Client ISE Posture-Modul ausgeführt wird, um den PSN-Besitzer der **aktuellen aktiven Sitzung** zu finden.
2. Client-Bereitstellung. Von der ISE durchgeführter Prozess zur Bereitstellung des entsprechenden Cisco Secure Client (ehemals AnyConnect) ISE Posture-Moduls und der Versionen des Compliance-Moduls für den Client. In diesem Schritt wird die lokale Kopie des Statusprofils, das in dem jeweiligen PSN enthalten und von diesem signiert ist, ebenfalls an den Client gesendet.
3. Systemscan. Auf der ISE konfigurierte Statusrichtlinien werden vom Compliance-Modul bewertet.
4. Problembeseitigung (optional). Wird bei nicht konformen Statusrichtlinien ausgeführt.
5. CoA Eine erneute Autorisierung ist erforderlich, um den endgültigen (konformen oder nicht konformen) Netzwerkzugriff zu gewähren.

Dieses Dokument konzentriert sich auf den Erkennungsprozess des ISE-Statusflusses.

Cisco empfiehlt, die Umleitung für den Erkennungsprozess zu verwenden. In einigen Fällen ist jedoch eine Umleitung nicht möglich, z. B. bei Netzwerkgeräten von Drittanbietern, bei denen die Umleitung nicht unterstützt wird. Dieses Dokument bietet eine allgemeine Anleitung und Best Practices für die Implementierung und Fehlerbehebung von umleitungslosen Zuständen in solchen Umgebungen.

Eine vollständige Beschreibung des umleitungslosen Datenflusses finden Sie unter [Frühere ISE-Versionen vergleichen mit ISE-Statusfluss in ISE 2.2](#).

Es gibt zwei Arten von Statermittlungssonden, die keine Umleitung verwenden:

1. Connectiondata.xml
2. Call Home-Liste

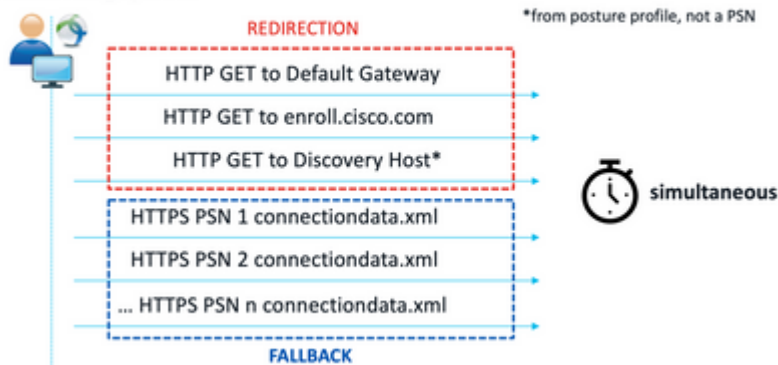
Connectiondata.xml

Connectiondata.xml ist eine Datei, die vom Cisco Secure Client automatisch erstellt und verwaltet wird. Es besteht aus einer Liste von PSNs, mit denen der Client zuvor eine Verbindung für Statusfragen hergestellt hat. Daher handelt es sich hierbei nur um eine lokale Datei, deren Inhalt nicht auf allen Endpunkten dauerhaft ist.

Der Hauptzweck von connectionData.xml besteht darin, als Sicherungsmechanismus für Erkennungssonden der Phasen 1 und 2 zu fungieren. Falls die Weiterleitungs- oder Call Home List-Diagnosetools ein PSN mit einer aktiven Sitzung nicht finden können, sendet der Cisco Secure Client eine direkte Anforderung an jeden der in connectionData.xml aufgeführten Server.

Stage 1 discovery probes

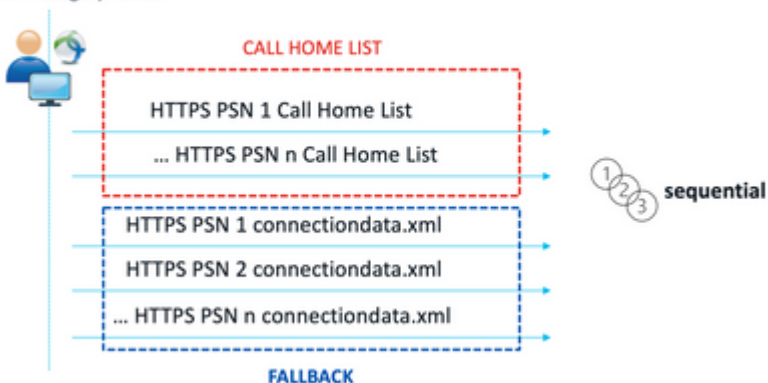
No-MnT stage probes



Erkennungssonden der Stufe 1

Stage 2 discovery probes

MnT stage probes



Erkennungssonden der Stufe 2

Ein häufiges Problem, das durch die Verwendung von connectionData.xml-Tests verursacht wird, ist eine Überlastung der ISE-Bereitstellung aufgrund einer großen Anzahl von HTTPS-Anforderungen, die von den Endpunkten gesendet werden. Es ist wichtig zu berücksichtigen, dass connectionData.xml zwar als Backup-Mechanismus wirksam ist, um vollständige Ausfälle sowohl für Umleitungs- als auch für umleitungslose Statusmechanismen zu vermeiden, jedoch keine nachhaltige Lösung für eine Statusumgebung darstellt. Daher ist es erforderlich, die Design- und Konfigurationsprobleme zu diagnostizieren und zu beheben, die den Ausfall der Haupterkennungssonden verursachen und zu Erkennungsproblemen führen.

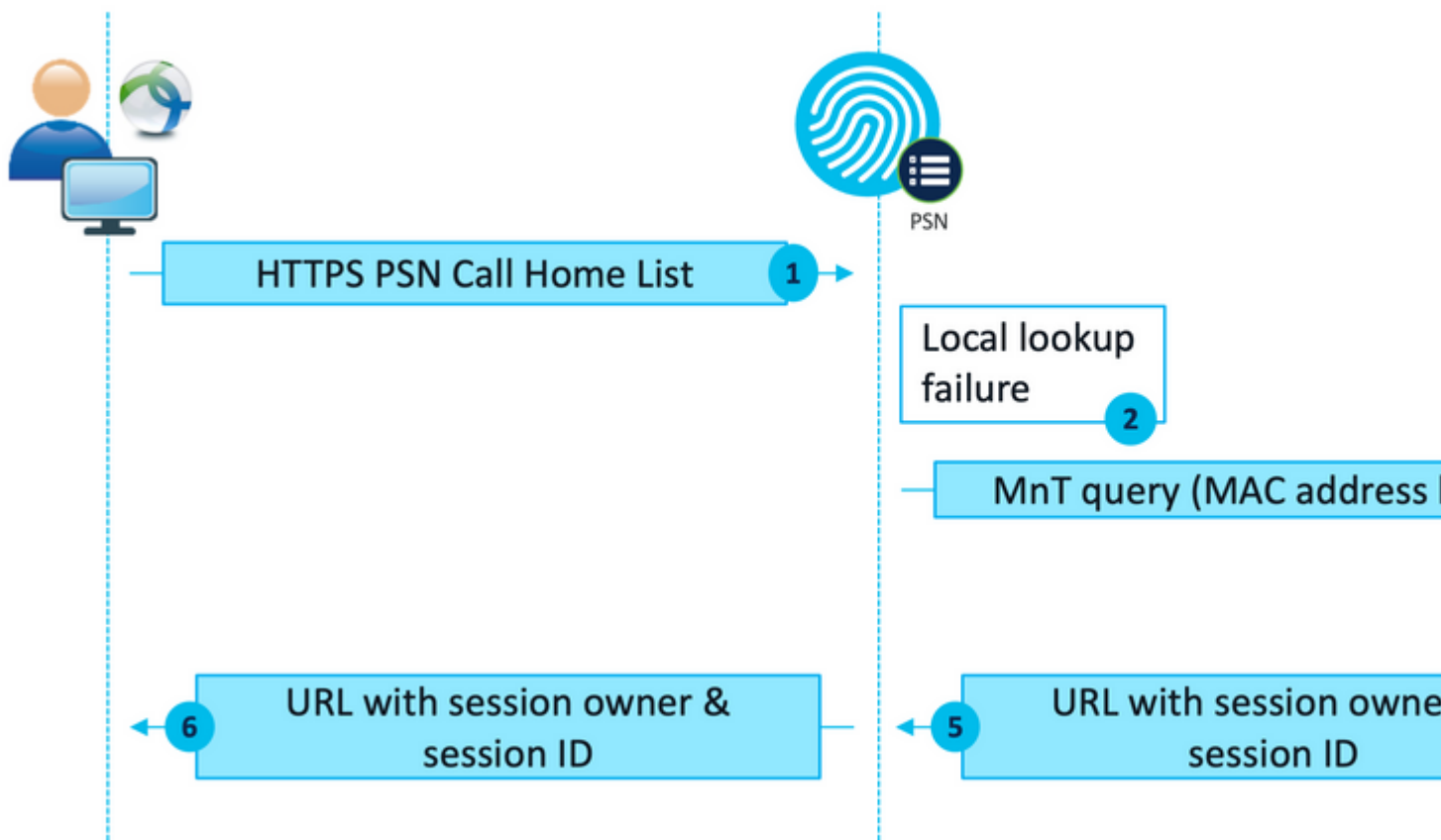
Call Home-Liste

Die Call Home List (Liste der Anrufer-Standorte) ist ein Abschnitt des Statusprofils, in dem eine Liste von PSNs zur Verwendung für die Statusanzeige festgelegt ist. Im Gegensatz zu connectiondata.xml wird diese Datei von einem ISE-Administrator erstellt und verwaltet und erfordert möglicherweise eine Entwurfsphase

für die optimale Konfiguration. Die Liste der PSNs in der Call Home-Liste muss mit der Liste der Authentifizierungs- und Abrechnungsserver übereinstimmen, die im Netzwerkgerät oder Load Balancer für RADIUS konfiguriert ist.

Call Home List-Tests ermöglichen die Verwendung einer MnT-Suche während der aktiven Sitzungssuche, falls die lokale Suche in einem PSN fehlschlägt. Dieselbe Funktion gilt nur für die Prüfpunkte `connectionData.xml`, wenn diese während der Erkennung in Phase 2 verwendet werden. Aus diesem Grund werden alle Sonden der Stufe 2 auch als Sonden der neuen Generation bezeichnet.

MnT lookup



MnT-Suchablauf

Design

Da ein umleitungsloser Erkennungsprozess häufig einen komplexeren Datenfluss und eine höhere Verarbeitungsleistung auf PSNs und MnT im Vergleich zu einem Umleitungsfluss erfordert, können sich bei der Implementierung zwei allgemeine Herausforderungen ergeben:

1. Effektive Erkennung
2. Leistung der ISE-Bereitstellung

Um diese Herausforderungen zu bewältigen, wird empfohlen, die Call Home-Liste so zu entwerfen, dass die Anzahl der PSNs, die ein Endgerät für den Status verwenden kann, begrenzt wird. Bei mittleren und großen Bereitstellungen muss die Bereitstellung verteilt werden, damit mehrere Call Home-Listen mit einer reduzierten Anzahl von PSNs erstellt werden können. Daher sollte die Liste der PSNs, die für die RADIUS-Authentifizierung für ein bestimmtes Netzwerkgerät verwendet werden, auf die gleiche Weise begrenzt werden, damit sie mit der entsprechenden Call Home-Liste übereinstimmen.

Die folgenden Aspekte können bei der Entwicklung der PSN-Verteilungsstrategie berücksichtigt werden, um die maximale Anzahl von PSNs in jeder Call Home-Liste zu bestimmen:

- Anzahl der PSNs in der Bereitstellung
- Hardwarespezifikationen von PSNs und MnT-Knoten
- Maximale Anzahl gleichzeitiger Statussitzen in der Bereitstellung
- Anzahl der Netzwerkgeräte
- Hybride Umgebungen (gleichzeitige Umleitung und umleitungslose Implementierung des Status)
- Anzahl der von den Endpunkten verwendeten Adapter
- Standort von Netzwerkgeräten und PSNs
- Für Statusservices verwendete Netzwerkverbindungstypen (kabelgebunden, Wireless, VPN)

, um eine neue Gruppe hinzuzufügen, einen Namen anzugeben und ggf. die übergeordnete Gruppe auszuwählen.

3. Wiederholen Sie Schritt 2, um alle erforderlichen Gruppen zu erstellen.

In den in diesem Leitfaden verwendeten Beispielen wird die Location Device Group (Standort-Gerätegruppe) verwendet, um die RADIUS-Serverliste und die Call Home List (Anrufleitliste) zu identifizieren, und eine benutzerdefinierte Posture Device Group (Status-Gerätegruppe) wird verwendet, um die Umleitung von umleitungslosen Statusgeräten zu identifizieren.

<input type="checkbox"/>	Name	Description	No. of Network
<input type="checkbox"/>	> All Device Types	All Device Types	--
<input type="checkbox"/>	∨ All Locations	All Locations	--
<input type="checkbox"/>	∨ US		0
<input type="checkbox"/>	CENTRAL		0
<input type="checkbox"/>	EST		1
<input type="checkbox"/>	WEST		1
<input type="checkbox"/>	> Is IPSEC Device	Is this a RADIUS over IPSEC Device	--
<input type="checkbox"/>	∨ Posture	Posture redirection or redirectionless group	--
<input type="checkbox"/>	Redirection		0
<input type="checkbox"/>	Redirectionless		1

Netzwerk-Gerätegruppen

Netzwerkgerät

1. Das Netzwerkgerät sollte für die RADIUS-Authentifizierung, -Autorisierung und -Abrechnung konfiguriert werden. Die Konfigurationsschritte finden Sie in der Dokumentation des jeweiligen Anbieters. Konfigurieren Sie die Liste der RADIUS-Server entsprechend der entsprechenden Liste Call Home (Call Home).
2. Navigieren Sie auf der ISE zu **Administration > Network Resources > Network Devices**, und klicken Sie auf **Add**. Konfigurieren Sie die Netzwerk-Gerätegruppen entsprechend dem Design, und aktivieren Sie die **RADIUS-Authentifizierungseinstellungen**, um den **gemeinsamen geheimen Schlüssel** zu konfigurieren.

* Device Profile

Cisco

Model Name

Software Version

* Network Device Group

Location WEST

IPSEC No

Device Type All Device Types

Posture Redirectionless

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret

Konfiguration von Netzwerkgeräten

Verwenden Sie ein einzelnes Sternchen (*), um die Verbindung mit einem beliebigen PSN zuzulassen, Platzhalterwerte, um die Verbindung mit einem beliebigen PSN in einer bestimmten Domäne zuzulassen, oder die PSN-FQDNs, um die Verbindung auf bestimmte PSNs zu beschränken.

- Konfigurieren Sie die **Call Home List (Liste der Anrufer nach Hause)**, um die kommasetrennte Liste der PSNs anzugeben. Stellen Sie sicher, dass Sie den Port des Client Provisioning Portals im Format FQDN:port oder IP:port hinzufügen.

The screenshot shows the 'Preferences' window for an 'Untitled' profile in the Cisco Secure Client Profile Editor. The 'Agent Behaviour' section includes several checkboxes, with 'Enable Posture Non-Redirection Flow' checked. Below this, there are input fields for 'BackOff Timer Limit' (30 Sec), 'Log file size' (5 MB), 'Remediation timer' (Min), 'Automated DART Count' (3), 'Periodic Probe Interval' (30 x 10 min), 'Posture State Synchronisation Interval' (0 Sec), 'Posture State Synchronisation Probe List' (empty), 'Maximum time for CWA/BYOD probing' (90 Sec), and 'Interval of CWA/BYOD probing' (5 Sec). The 'Posture Protocol' section includes 'Discovery host' (empty), 'Server name rules' (set to '* . aaamex . com'), 'Call Home List' (set to 'ise30baaamex.aaamex.com:8443,ise30cmexaa:'), and 'PRA retransmission time' (120 Sec). A 'Help' button is located at the bottom right.

Statusprofilkonfiguration mit dem Profil-Editor

Hinweis: In Schritt 4 des Abschnitts für die Client-Bereitstellungsrichtlinie finden Sie Anweisungen zum Überprüfen des Ports im Client-Bereitstellungsportal, falls erforderlich.

3. Wiederholen Sie Schritt 2 für jede verwendete Call Home-Liste.
4. Laden Sie das Cisco Secure Client-Paket vor der Bereitstellung von [Cisco Software Download herunter](#).

cisco-secure-client-win-5.0.01242-predeploy-k9.zip

[Advisories](#) 

Cisco Secure Client-Paket vor der Bereitstellung

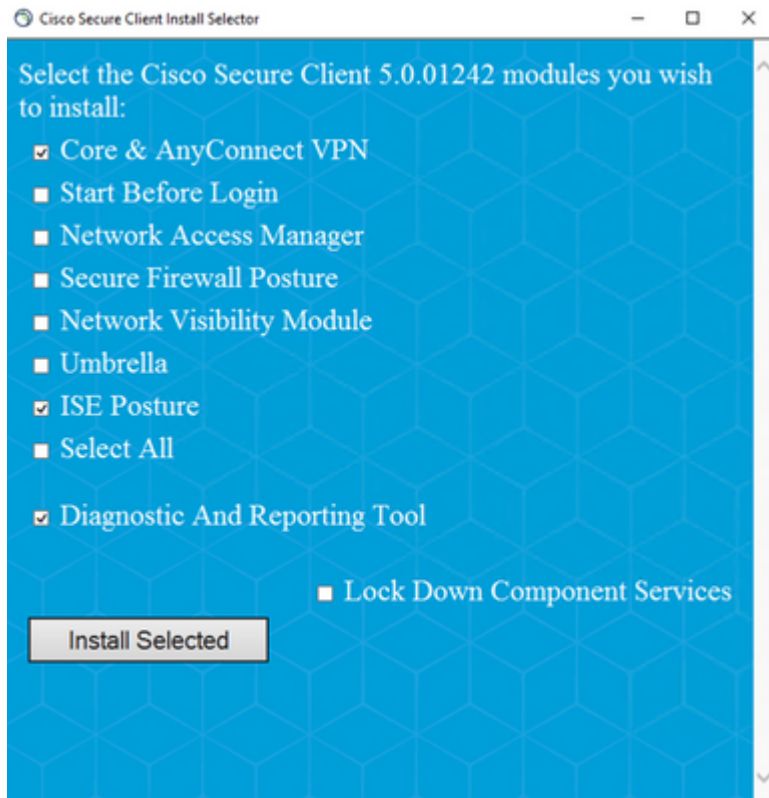
- Speichern Sie das Profil als ISEPostureCFG.xml.
- Verteilen Sie die Profil- und Installationsdateien in einer Archivdatei, oder kopieren Sie die Dateien auf die Clients.

Warnung: Stellen Sie sicher, dass sich die gleichen Cisco Secure Client-Dateien auch auf den Headends befinden, mit denen Sie eine Verbindung herstellen möchten: Secure Firewall ASA, ISE usw. Selbst bei Verwendung der manuellen Bereitstellung muss die ISE für die Client-Bereitstellung mit der entsprechenden Softwareversion konfiguriert werden. Detaillierte Anweisungen finden Sie im Abschnitt Konfiguration der Client-Bereitstellungsrichtlinie.

- Öffnen Sie auf dem Client die ZIP-Datei, und führen Sie Setup aus, um die Core- und ISE Posture-Module zu installieren. Alternativ können die einzelnen msi-Dateien verwendet werden, um jedes Modul zu installieren. In diesem Fall müssen Sie sicherstellen, dass das Core-VPN-Modul zuerst installiert wird.

Name	Type
Profiles	File folder
Setup	File folder
cisco-secure-client-win-5.0.01242-core-vpn-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-dart-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-iseposture-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-nam-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-nvm-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-posture-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-sbl-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-umbrella-predeploy-k9	Windows Installer Package
Setup	Application
setup	HTML Application

Paketinhalt vor der Bereitstellung mit Cisco Secure Client



Cisco Secure Client-Installationsprogramm

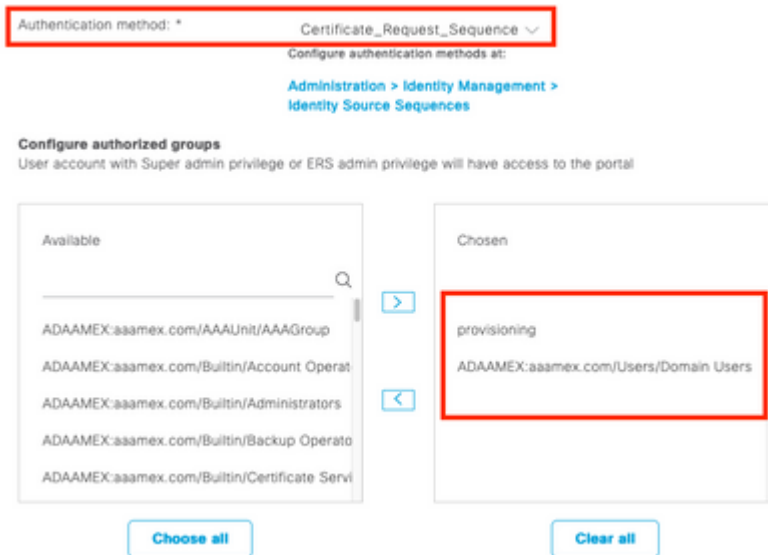
Tipp: Installieren Sie das Diagnose- und Reporting-Tool, das zur Fehlerbehebung verwendet werden soll.

8. Kopieren Sie nach Abschluss der Installation die Statusprofil-XML an die folgenden Speicherorte:
- Windows: %ProgramData%\Cisco\Cisco Secure Client\ISE - Status
 - macOS: /opt/cisco/secureclient/iseposture/

Client-Bereitstellungsportal (Webbereitstellung)

Das ISE Client Provisioning Portal kann zur Installation des Cisco Secure Client ISE Posture-Moduls und des Statusprofils von der ISE verwendet werden. Es kann auch verwendet werden, um das Statusprofil alleine zu übertragen, wenn das ISE Posture-Modul bereits auf dem Client installiert ist.

1. Navigieren Sie zu **Work Centers > Posture > Client Provisioning > Client Provisioning Portal**, um die Portalkonfiguration zu öffnen. Erweitern Sie den Abschnitt **Portal Settings**, und suchen Sie das Feld **Authentication method (Authentifizierungsmethode)**, wählen Sie die **Identity Source Sequence aus**, die für die Authentifizierung im Portal verwendet werden soll.
2. Konfigurieren Sie interne und externe Identitätsgruppen, die zur Verwendung des Client-Bereitstellungsportals autorisiert sind.



Authentifizierungsmethode und autorisierte Gruppen in Portaleinstellungen

3. Konfigurieren Sie im Feld **Fully qualified Domain Name (FQDN)** die URL, die von den Clients für den Zugriff auf das Portal verwendet wird. Um mehrere FQDNs zu konfigurieren, geben Sie die durch Kommas getrennten Werte ein.

Fully qualified domain name (FQDN):

Idle timeout:
1-30 (minutes)

Display language: Use browser locale

Fallback language:

Always use:

4. Konfigurieren Sie den bzw. die DNS-Server, um die Portal-URL in die PSNs der entsprechenden Call Home List aufzulösen.
5. Stellen Sie den Endbenutzern den FQDN für den Zugriff auf das Portal bereit, um die ISE Posture-Software zu installieren.

Hinweis: Um den Portal-FQDN nutzen zu können, müssen die Clients sowohl die PSN-Admin-Zertifikatkette als auch die Portal-Zertifikatkette im vertrauenswürdigen Speicher installiert haben, und das Admin-Zertifikat muss den Portal-FQDN im SAN-Feld enthalten.

Client-Bereitstellungsrichtlinie

Die Client-Bereitstellung muss auf der ISE konfiguriert werden, und zwar unabhängig von der Art der Bereitstellung (Pre-Deployment oder Web Deployment), mit der Cisco Secure Client auf den Endpunkten installiert wird.

1. Laden Sie das Cisco Secure Client Webdeploy-Paket von [Cisco Software Download herunter](#).

Cisco Secure Client Headend Deployment Package (Windows) 

19-Dec-2022

91.38

cisco-secure-client-win-5.0.01242-webdeploy-k9.pkg



[Advisories](#) 

Cisco Secure Client WebDeployment-Paket

2. Laden Sie das neueste webdeploy-Paket von [Cisco Software Download](#) herunter.



The screenshot shows the Cisco Software Download interface. On the left, a navigation menu is visible with categories: All Release, SecureFWPosture, ISEComplianceModule (highlighted with a red box), Android, NVM, and 5.0. The ISEComplianceModule category is expanded, showing a sub-item also labeled ISEComplianceModule. On the right, a table displays file information for the selected package. The table has two columns: File Information and Release Date. The file information includes the package name, version, and a description. The release date is 30-Jan-2023. A warning banner at the top right states: 'AnyConnect 4.x & Secure Client 5.x is available to customers with AnyConnect Plus or AnyConnect Enterprise. For migration, please see the AnyConnect ordering guide at: http://www.cisco.com/c/dam/en/...'

File Information	Release Date
ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later. 	30-Jan-2023
cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg	
Advisories 	

ISE Compliance Module webdeploy-Paket

3. Navigieren Sie auf der ISE zu Work Centers > Posture > Client Provisioning > **Resources** und klicken Sie auf **Add** > Agent resources from local disk (**Hinzufügen** > **Agent-Ressourcen von der lokalen Festplatte**). Wählen Sie **Cisco Provided Packages** aus dem Dropdown-Menü Kategorie aus, und laden Sie das zuvor heruntergeladene Cisco Secure Client WebDeployment-Paket hoch. Wiederholen Sie den gleichen Vorgang, um das Compliance-Modul hochzuladen.

Agent Resources From Local Disk

Category

Cisco Provided Packages



cisco-secure-client-win-5.0.01242-webdeploy-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 5.0...	AnyConnectDesktopWind...	5.0.1242.0	Cisco S

Von Cisco bereitgestellte Pakete auf die ISE hochladen

4. Klicken Sie auf der Registerkarte "**Ressourcen**" auf **Hinzufügen** > **AnyConnect Posture Profile**. Im Profil:
 - Konfigurieren Sie einen **Namen**, mit dem das Profil in der ISE identifiziert werden kann.
 - Konfigurieren Sie die **Servernamen-Regeln** getrennt durch Kommas. Verwenden Sie ein einzelnes Sternchen (*), um die Verbindung mit einem beliebigen PSN zuzulassen, Platzhalterwerte, um die Verbindung mit einem beliebigen PSN in einer bestimmten Domäne zuzulassen, oder die PSN-FQDNs, um die Verbindung auf bestimmte PSNs zu beschränken.
 - Konfigurieren Sie die **Call Home List (Liste der Anrufer nach Hause)**, um die kommagetrennte Liste der PSNs anzugeben. Stellen Sie sicher, dass Sie den Port des Client Provisioning Portals im Format FQDN:port oder IP:port hinzufügen.

* Name: CSC Redirectionless

Description: Redirectionless Posture LAB - 2 PSNs

ISE-Statusprofil-Konfiguration I

Posture Protocol

Parameter	Value	Notes	Description
PSA retransmission time	120 secs		This is the agent retry period if there is a Passive Assessment communication failure.
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Server name rules	*.asamex.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cscc.com"
Call Home List	vix.asamex.com:8443	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till the max time limit is reached

ISE-Statusprofil-Konfiguration II

Um den Port zu finden, der in der Call Home-Liste verwendet werden soll, navigieren Sie zu **Work Centers > Posture > Client Provisioning > Client Provisioning Portal**, wählen Sie das verwendete Portal aus, und erweitern Sie Portal Settings (Porteinstellungen).

Portals Settings and Customization

Portal Name: Client Provisioning Portal (default) Description: Default portal and user experience user

Language File 

[Portal test URL](#)

Portal Behavior and Flow Settings Portal Page Customization

Portal & Page Settings

Portal Settings

HTTPS port:* 8443 (8000 - 8999)


5. Klicken Sie auf der Registerkarte "**Ressourcen**" auf **Hinzufügen** > **AnyConnect-Konfiguration**. Wählen Sie das Cisco Secure Client-Paket und das Kompatibilitätsmodul aus, die verwendet werden sollen.

Warnung: Wenn Cisco Secure Client bereits auf den Clients bereitgestellt wurde, stellen Sie sicher, dass die ISE-Version mit der Version auf den Endgeräten übereinstimmt. Wenn ASA oder FTD für die Web-Bereitstellung verwendet wird, sollte auch die Version auf diesem Gerät übereinstimmen.

6. Blättern Sie nach unten zum Abschnitt **Statusauswahl**, und wählen Sie das Profil aus, das in Schritt 1 erstellt wurde. Klicken Sie unten auf der Seite auf **Senden**, um die Konfiguration zu speichern.

* Select AnyConnect Package: CiscoSecureClientDesktopWindows 5.0▼

* Configuration Name: AnyConnect Configuration Redirectionless

Description: 

Description Value Notes

* Compliance Module: ComplianceModuleWindows 4.3.3335.6146▼

Cisco Secure Client Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Secure Firewall Posture
- Network Visibility
- Umbrella
- Start Before Logon
- Diagnostic and Reporting Tool

AnyConnect-Konfiguration

Profile Selection

* ISE Posture: CSC Redirectionless ▼

VPN: ▼

Profilauswahl

7. Navigieren Sie zu **Work Centers** > **Posture** > **Client Provisioning** > **Client provisioning policy**. Suchen Sie die Richtlinie, die für das erforderliche Betriebssystem verwendet wird, und klicken Sie auf **Bearbeiten**. Klicken Sie in der Spalte **Ergebnisse** auf +, und wählen Sie im Abschnitt **Agentenkonfiguration** aus Schritt 5 die AnyConnect-Konfiguration aus.

Hinweis: Verwenden Sie bei mehreren Call Home-Listen das Feld **Andere Bedingungen**, um das richtige Profil an die entsprechenden Clients weiterzuleiten. In diesem Beispiel wird die Device Location Group verwendet, um das Statusprofil zu identifizieren, das in die Richtlinie eingefügt wird.

Tipp: Wenn mehrere Client-Bereitstellungsrichtlinien für dasselbe Betriebssystem konfiguriert sind, wird empfohlen, sie sich gegenseitig auszuschließen, d. h., ein Client sollte jeweils nur eine Richtlinie erreichen können. RADIUS-Attribute können in der Spalte **Other Conditions (Andere Bedingungen)** verwendet werden, um eine Richtlinie von einer anderen zu unterscheiden.

Agent Configuration

ect Configuration Redirectionless[▼] Is Upgrade Mandatory

Native Supplicant Configuration

Choose a Config Wizard [▼]

Choose a Wizard Profile [▼]

Konfiguration des Client-Bereitstellungsrichtlinien-Agents

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.



	Rule Name	Identity Groups	Operating Systems	Other Conditions
☰ <input checked="" type="checkbox"/>	IOS	If Any	and Apple iOS All	and Condition(s)
☰ <input checked="" type="checkbox"/>	Android	If Any	and Android	and Condition(s)
☰ <input checked="" type="checkbox"/>	Windows	If Any	and Windows All	and DEVICE:Location EQUALS All Locations#US#WEST
☰ <input checked="" type="checkbox"/>	MAC OS	If Any	and Mac OSX	and Condition(s)
☰ <input checked="" type="checkbox"/>	Chromebook	If Any	and Chrome OS All	and Condition(s)

Client-Bereitstellungsrichtlinie

8. Wiederholen Sie die Schritte 4 bis 7 für jede verwendete Call Home-Liste und das entsprechende Statusprofil. In Hybrid-Umgebungen können die gleichen Profile für Umleitungs-Clients verwendet werden.

Autorisierung

Autorisierungsprofil

1. Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > **Autorisierung** > **Herunterladbare ACLs**, und klicken Sie auf **Hinzufügen**.
2. Erstellen Sie eine DACL, um den Datenverkehr zu DNS, DHCP (falls verwendet), ISE-PSNs zuzulassen und anderen Datenverkehr zu blockieren. Stellen Sie sicher, dass Sie allen anderen Datenverkehr zulassen, der für den Zugriff erforderlich ist, bevor Sie den endgültigen konformen Zugriff zulassen.

* Name: redirectionless_posture

Description: DACL used for posture with ise30baaamex and ise30cmexaaa

IP version: IPv4 IPv6 Agnostic

* DACL Content:

1234567	permit udp any any eq domain
8910111	permit udp any any eq bootps
2131415	permit ip any host <pin 1 IP address>
1617181	permit ip any host <pin 2 IP address>
9202122	permit icmp any any
2324252	deny ip any any
6272629	
3031323	
3343536	
3738394	
0414243	

Check DACL Syntax

DACL is valid

DACL-Konfiguration

permit udp any any eq domain
 permit udp any any eq bootps
 permit ip any host

permit ip any host

deny ip any any

Achtung: Einige Geräte von Drittanbietern unterstützen möglicherweise keine DACLs. In diesem Fall müssen Sie eine Filter-ID oder andere anbieterspezifische Attribute verwenden. Weitere Informationen finden Sie in der Herstellerdokumentation. Wenn keine DACLs verwendet werden, müssen Sie die entsprechende ACL im Netzwerkgerät konfigurieren.

3. Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > **Autorisierung** > **Autorisierungsprofile**, und klicken Sie auf **Hinzufügen**. Geben Sie dem Autorisierungsprofil einen Namen, und wählen Sie **DACL-Namen** aus **Allgemeine Aufgaben aus**. Wählen Sie aus dem Dropdown-Menü die in Schritt 2 erstellte DACL aus.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name

Autorisierungsprofil

Hinweis: Wenn keine DACLs verwendet werden, verwenden Sie **Filter-ID** aus **Common Tasks** oder den **erweiterten Attributeinstellungen**, um den entsprechenden ACL-Namen zu übertragen.

4. Wiederholen Sie die Schritte 1 bis 3 für jede verwendete Call Home-Liste. In Hybrid-Umgebungen ist nur ein einziges Autorisierungsprofil für die Umleitung erforderlich. Die Konfiguration des Autorisierungsprofils für die Umleitung wird in diesem Dokument nicht behandelt.

Autorisierungsrichtlinie

1. Navigieren Sie zu **Policy > Policy Sets**, und öffnen Sie den verwendeten Policy Set, oder erstellen Sie einen neuen.
2. Blättern Sie nach unten zum Abschnitt **Autorisierungsrichtlinie**. Erstellen Sie eine Autorisierungsrichtlinie mit **Session PostureStatus NOT_EQUALS Compliant**, und wählen Sie das im vorherigen Abschnitt erstellte Autorisierungsprofil aus.

			Results
Status	Rule Name	Conditions	Profiles
✓	Compliant	Session-PostureStatus EQUALS Compliant	Compliant access x
✓	Redirectionless	AND DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant	Redirectionless posture x
✓	Redirection	AND Session-PostureStatus NOT_EQUALS Compliant DEVICE-Posture EQUALS Posture#Redirection	Redirection posture x
✓	Default		DenyAccess x

Autorisierungsrichtlinien

3. Wiederholen Sie Schritt 2 für jedes Autorisierungsprofil mit der entsprechenden verwendeten Call Home-Liste. In Hybrid-Umgebungen ist nur eine einzige Autorisierungsrichtlinie für die Umleitung erforderlich.

Fehlerbehebung

Konformität mit Cisco Secure Client und Status nicht zutreffend (ausstehend) auf ISE

Veraltete/Phantom-Sitzungen

Das Vorhandensein veralteter oder Phantom-Sitzungen in der Bereitstellung kann intermittierende und scheinbar zufällige Fehler mit umleitungsloser Statuserkennung verursachen, die dazu führen, dass Benutzer in einem unbekanntem/nicht anwendbarem Status auf der ISE feststecken, während die Benutzeroberfläche des Cisco Secure Client einen konformen Zugriff aufweist.

[Veraltete Sitzungen](#) sind alte Sitzungen, die nicht mehr aktiv sind. Sie werden durch eine Authentifizierungsanforderung und einen Accounting-Start erstellt, aber auf dem PSN wird kein Accounting-Stopp empfangen, um die Sitzung zu löschen.

[Phantom-Sitzungen](#) sind Sitzungen, die in einem bestimmten PSN nie aktiv waren. Sie werden durch ein Accounting-Interim-Update erstellt, es wird jedoch kein Accounting-Stopp auf dem PSN empfangen, um die Sitzung zu löschen.

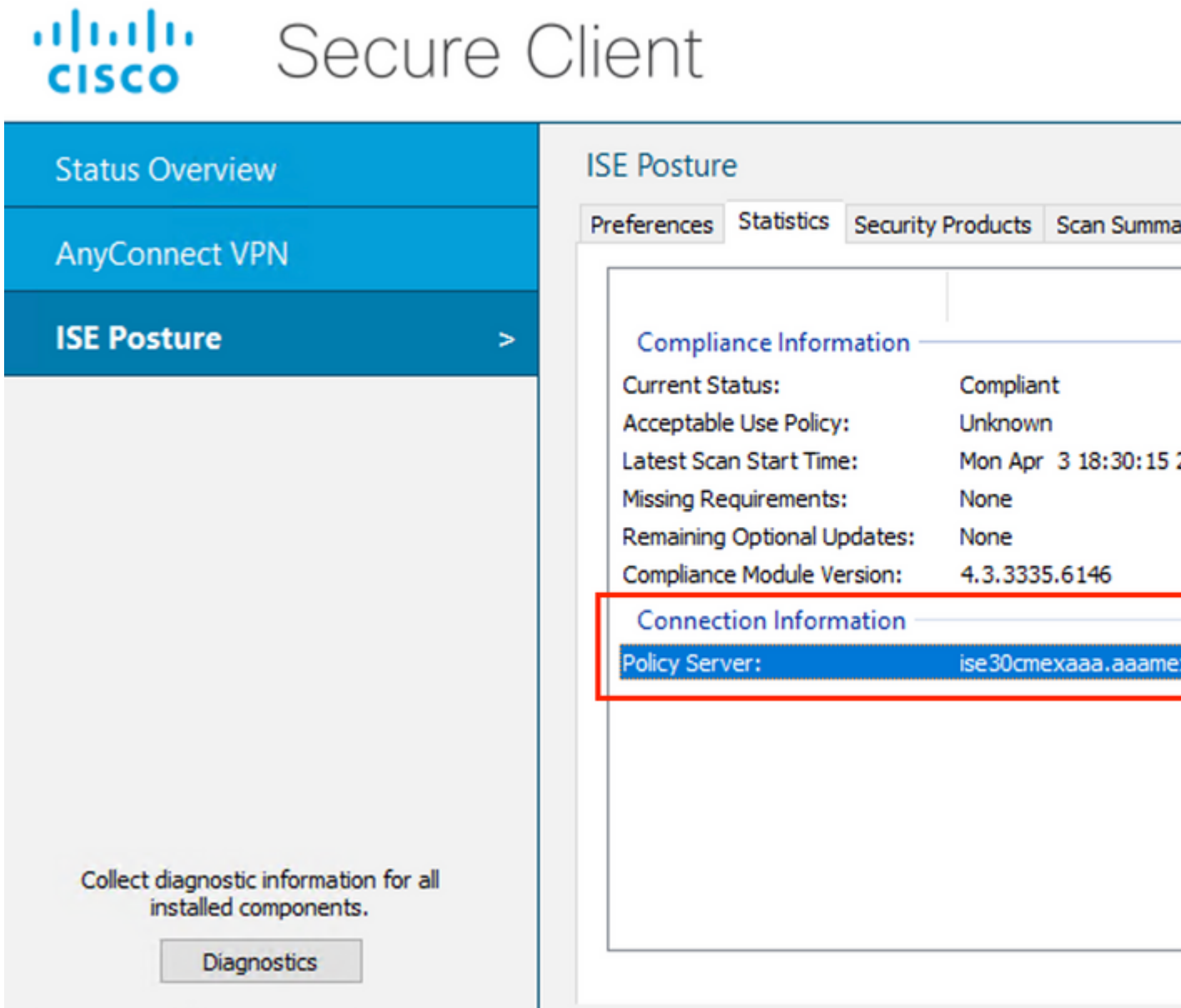
Identifizieren

Um ein veraltetes/Phantom-Sitzungsproblem zu identifizieren, überprüfen Sie das beim Systemscan auf dem

Client verwendete PSN, und vergleichen Sie es mit dem PSN, der die Authentifizierung durchführt:

1. Klicken Sie in der Benutzeroberfläche von Cisco Secure Client auf das **Zahnrad-Symbol** in der linken unteren Ecke. Öffnen Sie im linken Menü den Abschnitt **ISE-Status**, und navigieren Sie zur Registerkarte **Statistik**. Notieren Sie sich den Policy Server unter Verbindungsinformationen.

 Cisco Secure Client



The screenshot displays the Cisco Secure Client interface. The left sidebar contains navigation options: 'Status Overview', 'AnyConnect VPN', and 'ISE Posture' (which is selected and has a right-pointing arrow). Below the sidebar, there is a button labeled 'Diagnostics' with the text 'Collect diagnostic information for all installed components.' above it. The main content area is titled 'ISE Posture' and has four tabs: 'Preferences', 'Statistics', 'Security Products', and 'Scan Summary'. The 'Statistics' tab is active. Under the 'Compliance Information' section, the following details are listed:

Current Status:	Compliant
Acceptable Use Policy:	Unknown
Latest Scan Start Time:	Mon Apr 3 18:30:15 2
Missing Requirements:	None
Remaining Optional Updates:	None
Compliance Module Version:	4.3.3335.6146

Below this, the 'Connection Information' section is visible, with the 'Policy Server' field highlighted in blue and enclosed in a red box. The value for the Policy Server is 'ise30cmexaaa.aaame'.

Policy Server für ISE-Status im Cisco Secure Client

2. In ISE-RADIUS-Live-Protokollen werden folgende Punkte berücksichtigt:
 - Statusänderung
 - Änderung im Server
 - Keine Änderung bei Autorisierungsrichtlinie und Autorisierungsprofil
 - Kein CoA-Live-Protokoll

Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server
×		▼		Identity	Endpoint ID	Authorization Policy	Server
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa
Apr 03, 2023 07:32:40.7...				#ACSACL#-IP-...			ise30baamex
Apr 03, 2023 07:32:40.6...				redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baame

Live-Protokolle für veraltete/Phantom-Sitzungen

- Öffnen Sie die Live-Sitzung oder die letzten Details des Authentifizierungs-Live-Protokolls. Beachten Sie, dass der Policy Server, wenn er sich von dem in Schritt 1 beobachteten Server unterscheidet, auf ein Problem mit veralteten/Phantom-Sitzungen hinweist.

Overview

Event: 5200 Authentication succeeded

Username: redirectionless

Endpoint Id: 00:50:56:B3:3E:0E

Endpoint Profile: Windows10-Workstation

Authentication Policy: Posture Lab >> Default

Authorization Policy: Posture Lab >> Redirectionless

Authorization Result: Redirectionless posture

Authentication Details

Source Timestamp: 2023-04-03 19:32:40.691

Received Timestamp: 2023-04-03 19:32:40.691

Policy Server: ise30baamex

Event: 5200 Authentication succeeded

Username: redirectionless


Richtlinienserver in Live-Protokolldetails

Lösung

Die ISE-Versionen oberhalb von ISE 2.6 Patch 6 und 2.7 Patch 3 implementieren [RADIUS Session Directory](#) als Lösung für veraltete/Phantom-Sitzungen im umleitungslosen Statusfluss.

- Navigieren Sie zu Administration > **System** > **Settings** > **Light Data Distribution**, und stellen Sie sicher, dass das Kontrollkästchen **Enable RADIUS Session Directory (RADIUS-Sitzungsverzeichnis aktivieren)** aktiviert ist.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Back

FIPS Mode
Security Settings
Alarm Settings
Posture >
Profiling
Protocols >
Endpoint Scripts >
Proxy
SMTP Server
SMS Gateway
System Time 
ERS Settings
API Gateway Settings
Network Success Diagnostics >
DHCP & DNS Services
Max Sessions
Light Data Distribution

RADIUS Session Directory

Enable the RADIUS Session Directory (RSD) feature to store the user session information and PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.

Enable RADIUS Session Directory



Endpoint Owner Directory

Enable the Endpoint Owner Directory (EPOD) feature to store the PSN FQDN of each MAC address in ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling sessions. The EPOD option will use legacy Profiler owners directory.

Enable Endpoint Owner Directory

Advanced Settings

Configure the following options for RSD and EPOD.

Batch size
10  Items 

RADIUS-Sitzungsverzeichnis aktivieren

- Überprüfen Sie über die ISE CLI, ob **ISE Messaging Service** auf **allen PSNs** ausgeführt wird, indem Sie den Befehl **Anwendungsstatus anzeigen ise**.

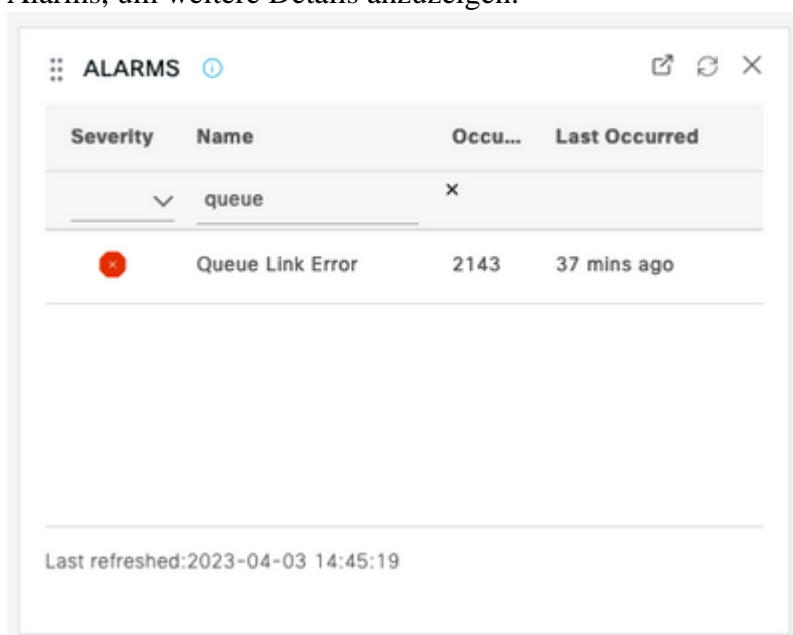
```
ise30cmexaaa/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	12434
Database Server	running	112 PROCESSES
Application Server	running	33093
Profiler Database	running	19622
ISE Indexing Engine	running	42923
AD Connector	running	60317
M&T Session Database	running	19361
M&T Log Processor	running	33283
Certificate Authority Service	disabled	
EST Service	disabled	
SXP Engine Service	disabled	
Docker Daemon	running	14791
TC-NAC MongoDB Container	running	18594
TC-NAC Core Engine Container	running	18981
VA Database	running	53465
VA Service	running	53906
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID WMI Service	running	55480
PassiveID Syslog Service	running	56312
PassiveID API Service	running	57153
PassiveID Agent Service	running	58079
PassiveID Endpoint Service	running	59138
PassiveID SPAN Service	running	60059
DHCP Server (dhcpd)	disabled	
DNF Service (dnf)	disabled	
ISE Messaging Service	running	16526
ISE API Gateway Database Service	running	18463
ISE API Gateway Service	running	23052

ISE Messaging Service wird ausgeführt

Hinweis: Dieser Service bezieht sich auf die Kommunikationsmethode, die für RSD zwischen PSNs verwendet wird und unabhängig vom Status der ISE Messaging Service-Einstellung für Syslog ausgeführt werden sollte, die über die ISE-Benutzeroberfläche festgelegt werden kann.

3. Navigieren Sie zum ISE **Dashboard**, und suchen Sie das **Alarms**-Dashlet. Überprüfen Sie, ob Warnungen zu **Warteschlangenverbindungsfehlern** vorliegen. Klicken Sie auf den Namen des Alarms, um weitere Details anzuzeigen.



Warnungen zu Verbindungsfehlern in Warteschlange

4. Überprüfen Sie, ob zwischen den für den Status verwendeten PSNs Alarmer generiert werden.

✖ Alarms: Queue Link Error

Description

The queue link between two nodes in the ISE deployment is down.

Suggested Actions

Please check and restore connectivity between the nodes. Ensure that the nodes and the ISE Messaging Service are up and running. Ensure that ISE Messaging Service ports are not blocked by firewalls or are being registered to deployment or manually-synced from PSPAN or when the nodes are in out-of-sync state or when the nodes are getting restarted.

Rows/Page 100 < > 1

Refresh Acknowledge

<input type="checkbox"/> Time Stamp	Description	Cause={tls_alert;* unknown Ca* }
<input type="checkbox"/> Apr 03 2023 21:07:00.977 PM	Queue Link Error: Message=From ise30cmexaaa.aaamex.com To ise30baaamex.aaamex.com; Cause={tls_alert;* unkno...	
<input type="checkbox"/> Apr 03 2023 21:07:00.959 PM	Queue Link Error: Message=From ise30baaamex.aaamex.com To ise30cmexaaa.aaamex.com; Cause={tls_alert;* unkno...	

Alarmdetails für Warteschlangenverbindungsfehler

5. Bewegen Sie den Mauszeiger über die Beschreibung der Erinnerung, um alle Details anzuzeigen und das Feld Ursache zu notieren. Die zwei häufigsten Ursachen für Warteschlangenverbindungsfehler sind:

- Timeout: gibt an, dass die Anforderungen, die von einem Knoten an einen anderen Knoten auf Port 8671 gesendet werden, nicht innerhalb des Grenzwerts beantwortet werden. Überprüfen Sie, ob der TCP-Port 8671 zwischen den Knoten zulässig ist, um die Ursache zu beheben.
- Unbekannte Zertifizierungsstelle: gibt an, dass die Zertifikatskette, die das ISE-Messaging-Zertifikat signiert, ungültig oder unvollständig ist. So beheben Sie diesen Fehler:
 - a. Navigieren Sie zu **Administration > System > Certificates > Certificate Signing Requests**.
 - b. Klicken Sie auf **CSR (Certificate Signing Requests) generieren**.
 - c. Wählen Sie im Dropdown-Menü die Option **ISE Root CA** aus, und klicken Sie auf **Replace ISE Root CA Certificate chain**.
Wenn die ISE-Stammzertifizierungsstelle nicht verfügbar ist, navigieren Sie zu **Zertifizierungsstelle > Interne Zertifizierungsstelleneinstellungen**, und klicken Sie auf **Zertifizierungsstelle aktivieren**, kehren Sie zum CSR zurück, und generieren Sie die Stammzertifizierungsstelle neu.
 - d. Erstellen Sie einen neuen CSR, und wählen Sie **ISE Messaging Service** aus dem Dropdown-Menü aus.
 - e. Wählen Sie alle Knoten aus der Bereitstellung aus, und generieren Sie das Zertifikat neu.

Hinweis: Es wird erwartet, dass während der Neugenerierung der Zertifikate Warnungen aufgrund von Warteschlangenverbindungsfehlern mit der Ursache Unbekannte Zertifizierungsstelle oder Nicht verweigert beobachtet werden. Überwachen Sie die Warnungen nach der Zertifikatgenerierung, um zu bestätigen, dass das Problem behoben wurde.

Leistung

Identifizieren

Leistungsprobleme wie eine hohe CPU-Auslastung und ein hoher Lastdurchschnitt im Zusammenhang mit einem umleitungslosen Status können sich auf PSN- und MnT-Knoten auswirken und werden häufig von

den folgenden Ereignissen begleitet oder ihnen vorangehen:

- Zufällig oder zeitweilig *Kein Policy Server* im Cisco Secure Client *erkannt*
- *Der maximale Ressourcengrenzwert hat Berichte für den Threadpool des Portaldiensts erreicht, die Schwellenwertereignisse erreicht haben.* Navigieren Sie zu Vorgänge > **Berichte** > **Berichte** > **Audit** > **Operations Audit** (Betriebsprüfung), um die Berichte anzuzeigen.
- *Statusabfrage nach MNT-Suche enthält hohe Alarme.* Diese Alarme werden nur für ISE 3.1 und höher generiert.

Lösung





Wenn die Leistung der Bereitstellung durch einen umleitungslosen Status beeinträchtigt wird, ist dies häufig ein Hinweis auf eine ineffektive Implementierung. Es wird empfohlen, die folgenden Aspekte zu überarbeiten:

- Anzahl der pro Call Home-Liste verwendeten PSNs Erwägen Sie, die Anzahl der PSNs, die je nach Design für den Status pro Endgerät oder Netzwerkgerät verwendet werden können, zu reduzieren.
- Port des Clientbereitstellungsportals in der Liste der Call Home-Geräte. Vergewissern Sie sich, dass die Portalportnummer hinter der IP- oder FQDN-Nummer jedes Knotens steht.

So reduzieren Sie die Auswirkungen:

1. Löschen Sie "connectiondata.xml" aus den Endpunkten, indem Sie die Datei aus dem Ordner "Cisco Secure Client" entfernen und den ISE Posture-Dienst oder Cisco Secure Client neu starten. Wenn die Dienste nicht neu gestartet werden, wird die alte Datei neu generiert, und die Änderungen werden nicht übernommen. Diese Aktion sollte auch nach der Überarbeitung und Änderung der Call Home-Listen durchgeführt werden.
2. Verwenden Sie DACLs oder andere ACLs, um Datenverkehr zu ISE-PSNs für Netzwerkverbindungen zu blockieren, wenn dies nicht relevant ist:
 - Für Verbindungen, bei denen der Status in den Autorisierungsrichtlinien nicht erzwungen wird, die aber für Endpunkte mit installiertem Cisco Secure Client ISE Posture-Modul gelten, blockieren Sie den Datenverkehr von den Clients zu allen ISE-PSNs für die TCP-Ports 8905 und den Client Provisioning Portal-Port. Diese Aktion wird auch für den Status mit Umleitungsimplementierung empfohlen.
 - Bei Verbindungen, bei denen der Status in den Autorisierungsrichtlinien erzwungen wird, Datenverkehr von den Clients zum authentifizierenden PSN zulassen und Datenverkehr zu anderen PSNs in der Bereitstellung blockieren. Diese Aktion kann vorübergehend ausgeführt werden, während das Design überarbeitet wird.

Authorization Profile

* Name	Redirectionless PSN1
Description	Authorization profile for redirectionless posture with DACL allowing traffic only to PSN1, DNS and DHCP
* Access Type	ACCESS_ACCEPT
Network Device Profile	 Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> 
Agentless Posture	<input type="checkbox"/> 
Passive Identity Tracking	<input type="checkbox"/> 

Common Tasks

<input checked="" type="checkbox"/> DACL Name	redirectionless_posture_psn1
---	------------------------------

Autorisierungsprofil mit DACL für ein PSN

✓	Compliant		Session-PostureStatus EQUALS Compliant
✓	Redirectionless PSN1	AND	DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant Network Access-ISE Host Name EQUALS Ise30baaamex.aaam
✓	Redirectionless PSN2	AND	DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant Network Access-ISE Host Name EQUALS Ise30cmexaaa.aaam
✓	Redirection	AND	Session-PostureStatus NOT_EQUALS Compliant DEVICE-Posture EQUALS Posture#Redirection

Autorisierungsrichtlinien pro PSN

Buchhaltung

RADIUS-Accounting ist für das Sitzungsmanagement auf der ISE unverzichtbar. Da der Status von einer aktiven Sitzung abhängt, kann sich eine falsche oder fehlende Accounting-Konfiguration auch auf die Staterkennung und die ISE-Leistung auswirken. Es ist wichtig zu überprüfen, ob die Abrechnung auf dem Netzwerkgerät korrekt konfiguriert ist, um Authentifizierungsanforderungen, Abrechnungsstart, Abrechnungsstopp und Abrechnungsaktualisierungen für jede Sitzung an einen einzigen PSN zu senden.

Um die auf der ISE empfangenen Abrechnungspakete zu überprüfen, navigieren Sie zu **Operations > Reports > Reports > Endpoints and Users > RADIUS Accounting**.

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

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.