

ISEリダイレクトレスポスチャの実装

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Connectiondata.xml](#)

[Call Homeリスト](#)

[設計](#)

[設定](#)

[ネットワークデバイスグループ \(オプション \)](#)

[ネットワークデバイス](#)

[クライアントプロビジョニング](#)

[手動プロビジョニング \(導入前 \)](#)

[クライアントプロビジョニングポータル \(Web展開 \)](#)

[クライアントプロビジョニングポリシー](#)

[許可](#)

[許可プロファイル](#)

[認可ポリシー](#)

[トラブルシューティング](#)

[Cisco Secure Clientで準拠し、ISEでレスポチャが適用されない \(保留中 \)](#)

[古い/ファントムセッション](#)

[特定](#)

[解決方法](#)

[パフォーマンス](#)

[特定](#)

[解決方法](#)

[アカウントティング](#)

[関連情報](#)

概要

このドキュメントでは、リダイレクトなしのレスポチャフローの使用と設定、およびトラブルシューティングのヒントについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISE でのポスチャ フロー
- ISE でのポスチャ コンポーネントの設定
- ISEポータルへのリダイレクト

後で説明する概念をより深く理解するために、次の手順を実行することをお勧めします。

[以前のISEバージョンとISE 2.2のISEポスチャフローの比較](#) [ISEセッションの管理とポスチャ](#)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 3.1
- Cisco Secureクライアント5.0.01242

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ISEポスチャフローは次の手順で構成されます。

0.認証/許可。通常はポスチャフローが開始される直前に実行されますが、ポスチャ再評価 (PRA)などの特定のユースケースではバイパスできます。認証自体はポスチャディスカバリーをトリガーしないため、これはすべてのポスチャフローに不可欠とは見なされません。

1. ディスカバリー。Secure Client ISEポスチャモジュールによって実行されるプロセスで、現在アクティブなセッションのPSN所有者を検索します。
2. クライアント プロビジョニング。対応するCisco Secure Client（以前のAnyConnect）の ISEポスチャモジュールとコンプライアンスモジュールのバージョンをクライアントにプロビジョニングするためにISEによって実行されるプロセス。この手順では、特定のPSNに含まれ、そのPSNによって署名されたポスチャプロファイルのローカルコピーもクライアントにプッシュされます。
3. システムスキャン。ISEで設定されたポスチャポリシーは、コンプライアンスモジュールによって評価されます。
4. 修復（オプション）。準拠していないポスチャポリシーがある場合に実行されます。
5. CoA。最終的な（準拠または非準拠の）ネットワークアクセスを許可するには、再認証が必要です。

このドキュメントでは、ISEポスチャフローの検出プロセスを中心に説明します。

ディスカバリープロセスではリダイレクションを使用することを推奨しますが、リダイレクションがサポートされていないサードパーティのネットワークデバイスの使用など、リダイレクション

を実装できない特定のケースがあります。このドキュメントの目的は、このような環境でリダイレクトのないポストチャを実装およびトラブルシューティングするための一般的なガイダンスとベストプラクティスを提供することです。

リダイレクトレスフローの詳細については、「[ISE 2.2での以前のISEバージョンとISEポストチャフローの比較](#)」を参照してください。

リダイレクトを使用しないポストチャ検出プローブには、次の2つのタイプがあります。

- 1. Connectiondata.xml
- 2. Call Homeリスト

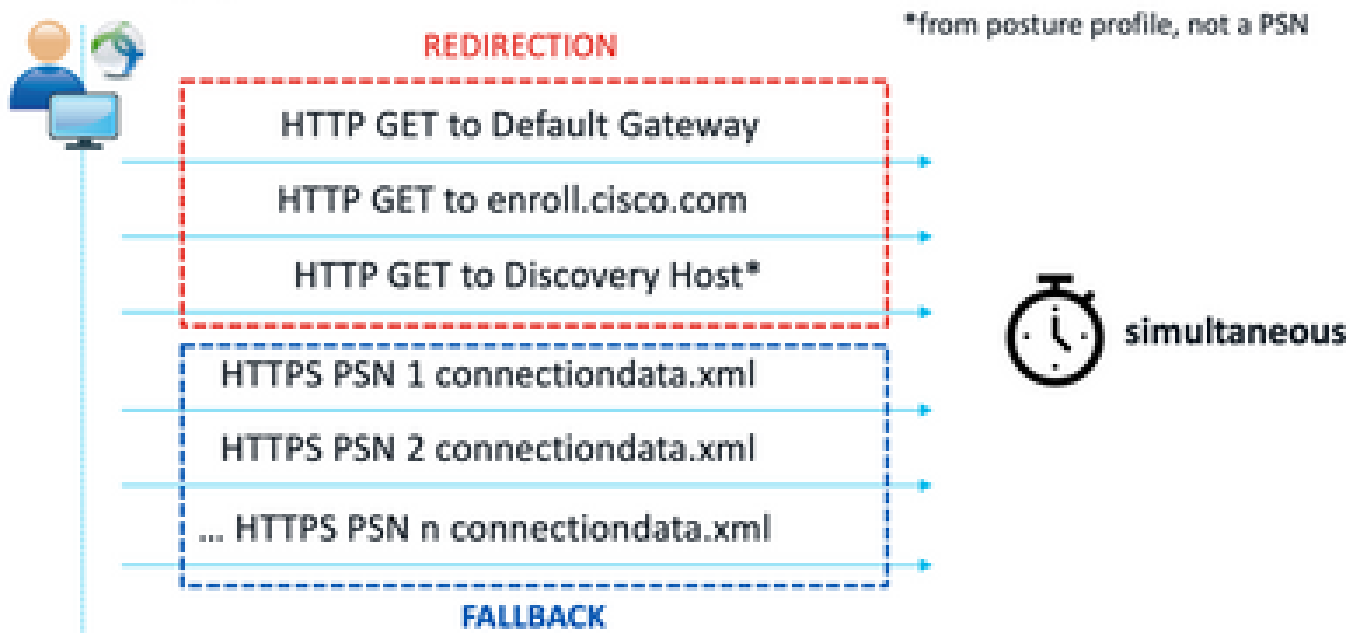
Connectiondata.xml

Connectiondata.xmlは、Cisco Secure Clientによって自動的に作成され、維持されるファイルです。これは、クライアントがポストチャ用に以前に正常に接続したPSNのリストで構成されます。したがって、これはローカルファイルのみであり、その内容はすべてのエンドポイントで永続的ではありません。

connectiondata.xmlの主な目的は、ステージ1とステージ2の両方の検出プローブのバックアップメカニズムとして機能することです。リダイレクションまたはCall HomeリストプローブがアクティブセッションのPSNを検出できない場合、Cisco Secure Clientはconnectiondata.xmlにリストされている各サーバに直接要求を送信します。

Stage 1 discovery probes

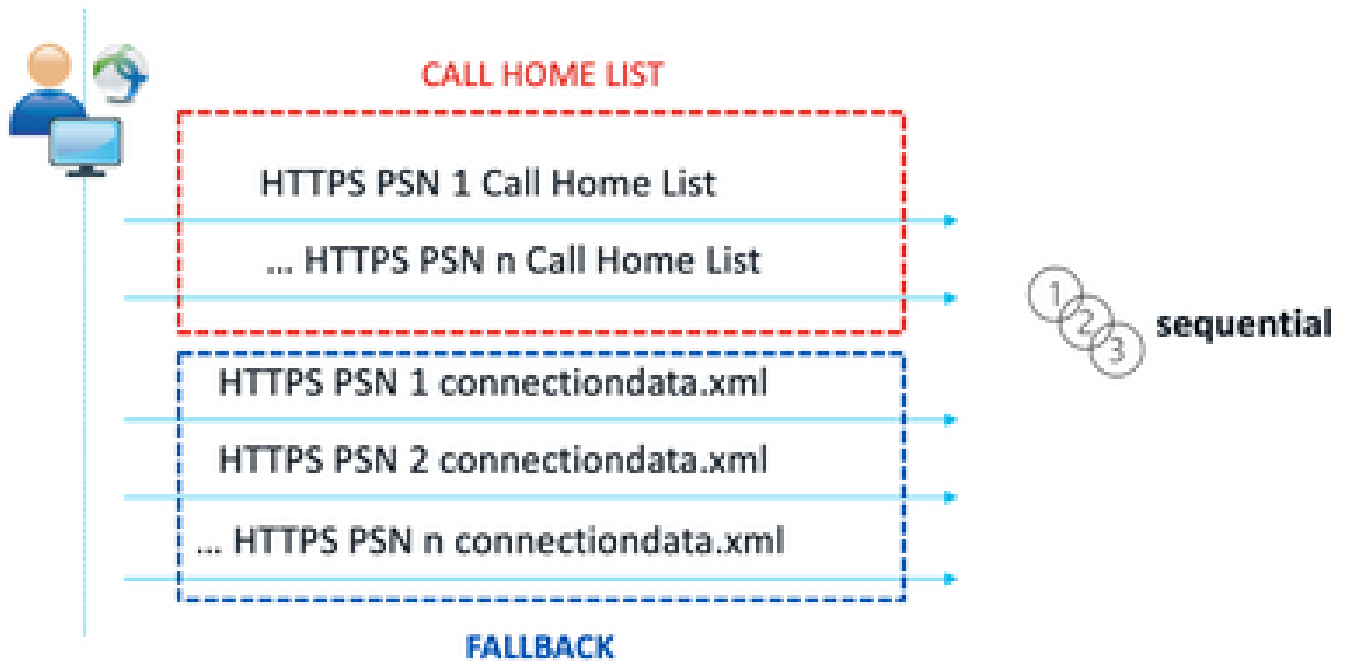
No-MnT stage probes



第1段階の検出プローブ

Stage 2 discovery probes

MnT stage probes



第2段階の検出プローブ

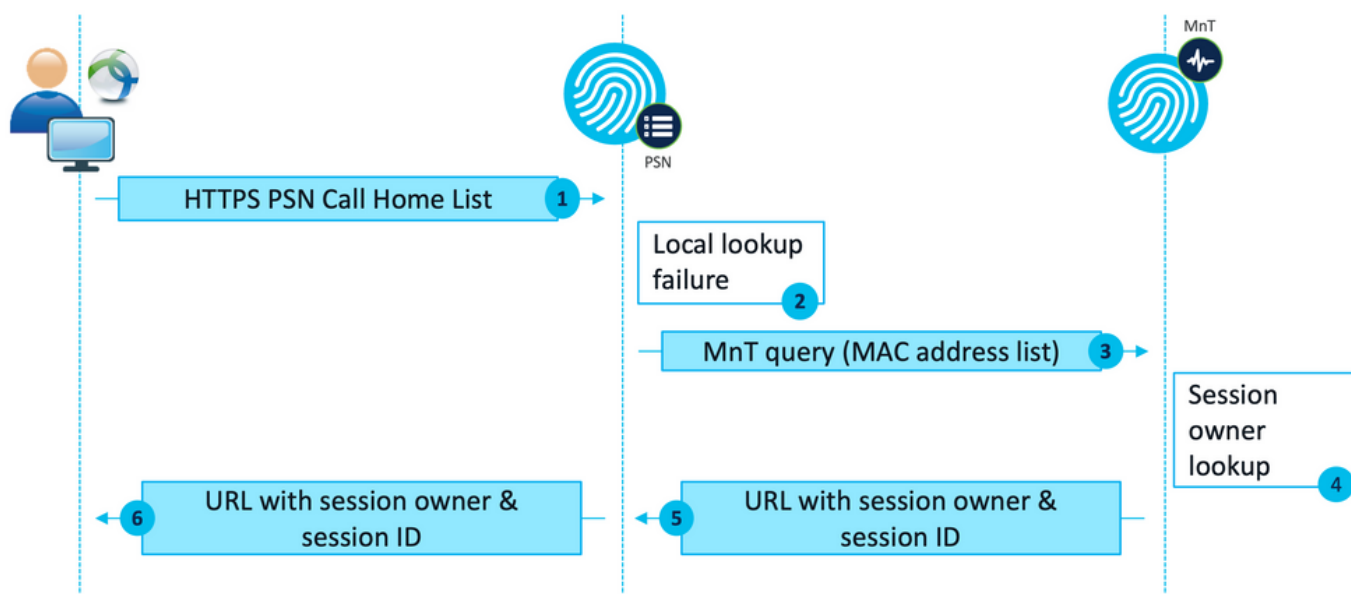
connectiondata.xmlプローブの使用によって引き起こされる一般的な問題は、エンドポイントから送信される多数のHTTPS要求によるISE導入の過負荷です。connectiondata.xmlは、リダイレクトとリダイレクトなしのポスチャメカニズムの両方で完全な停止を回避するためのバックアップメカニズムとして有効ですが、ポスチャ環境の持続可能なソリューションではないため、メインの検出プローブの障害の原因となり、検出の問題を引き起こす設計および設定の問題を診断して解決する必要があることを考慮することが重要です。

Call Homeリスト

Call Homeリストは、ポスチャプロファイルのセクションで、ポスチャに使用するPSNのリストが指定されます。connectiondata.xmlとは異なり、これはISE管理者によって作成および維持され、最適な設定のために設計フェーズが必要になる場合があります。Call HomeリストのPSNのリストは、RADIUSのネットワークデバイスまたはロードバランサに設定されている認証およびアカウントサーバーのリストと一致している必要があります。

Call Homeリストプローブを使用すると、PSNでローカルルックアップが失敗した場合に、アクティブセッションの検索中にMnTルックアップを使用できます。同じ機能がconnectiondata.xmlプローブに拡張されるのは、それらがステージ2の検出中に使用された場合だけです。このため、すべてのステージ2プローブは、新世代プローブとも呼ばれます。

MnT lookup



MnTルックアップフロー

設計

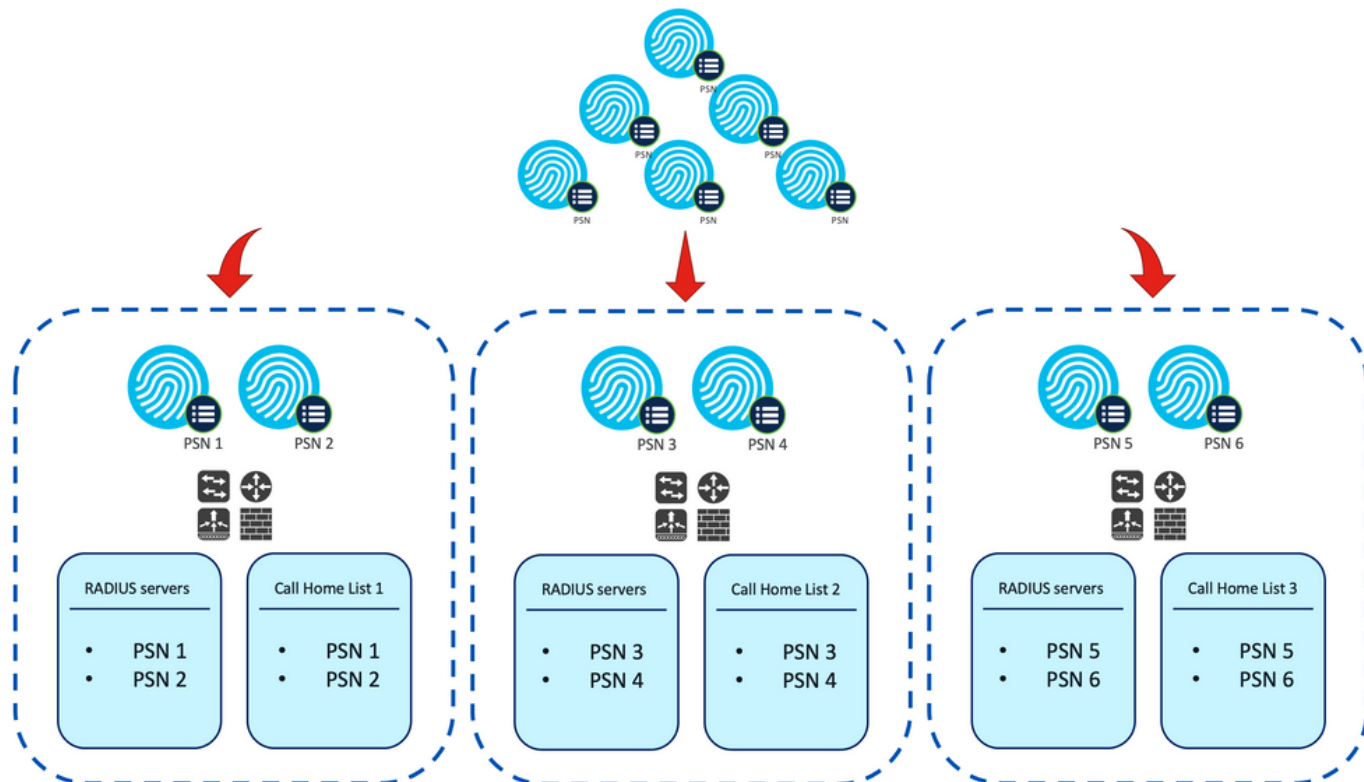
リダイレクトレス検出プロセスは、多くの場合、リダイレクトフローよりも複雑なフローを伴い、PSNおよびMnT上で大量の処理を行うため、実装時に発生する可能性がある一般的な課題が2つあります。

1. 効果的な検出
2. ISE導入のパフォーマンス

これらの課題に対処するには、Call Homeリストを設計して、特定のエンドポイントがポスチャに使用できるPSNの数を制限することをお勧めします。中規模および大規模の導入では、複数のCall Homeリストを作成するために少数のPSNで導入を分散する必要があります。結果として、特定のネットワークデバイスのRADIUS認証に使用されるPSNのリストは、対応するCall Homeリストに一致するように制限する必要があります。

各Call Homeリスト内のPSNの最大数を決定するPSN分散戦略を作成する際には、次の点を考慮できます。

- 展開内のPSNの数
- PSNおよびMnTノードのハードウェア仕様
- 展開での同時ポスチャセッションの最大数
- ネットワークデバイスの数
- ハイブリッド環境（同時リダイレクトおよびリダイレクトなしのポスチャ実装）
- エンドポイントが使用するアダプタの数
- ネットワークデバイスとPSNの場所
- ポスチャに使用されるネットワーク接続タイプ（有線、ワイヤレス、VPN）



例：リダイレクトなしのポストチャのためのPSN配布

ヒント:[ネットワークデバイスグループ](#)を使用して、設計に従ってネットワークデバイスを分類します。

設定

ネットワークデバイスグループ (オプション)

ネットワークデバイスグループを使用すると、ネットワークデバイスを特定し、対応するRADIUSサーバリストおよびCall Homeリストと照合できます。ハイブリッド環境の場合は、それらを使用して、リダイレクトをサポートしないデバイスからのリダイレクトをサポートするデバイスを特定することもできます。

設計フェーズで作成された配布戦略がネットワークデバイスグループに依存する場合は、次の手順に従ってISE上でそれらを設定します。

1. Administration > Network Resources Network Resource Groupsの順に移動します。
2. Addをクリックして新しいグループを追加し、名前を指定して、必要に応じて親グループを選択します。
3. 手順2を繰り返して、必要なグループをすべて作成します。

このガイド全体で使用されている例では、ロケーションデバイスグループを使用してRADIUSサーバリストとCall Homeリストを識別し、カスタムポストチャデバイスグループを使用してリダイレクトなしのポストチャデバイスからのリダイレクトを識別します。

<input type="checkbox"/> Name	Description	No. of Network Devices
<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

ネットワーク デバイス グループ

ネットワークデバイス





1. ネットワークデバイスはRADIUS認証、許可、アカウントリング用に設定する必要があります。設定手順については、各ベンダーのドキュメントを参照してください。対応するCall Homeリストに従って、RADIUSサーバリストを設定します。
2. ISEで、Administration > Network Resources > Network Devicesの順に移動し、Addをクリックします。設計に従ってネットワークデバイスグループを設定し、RADIUS認証設定を有効にして共有秘密を設定します。

Device Profile  Cisco  

Model Name 

Software Version 

Network Device Group

Location	WEST 	Set To Default
IPSEC	No 	Set To Default
Device Type	All Device Types 	Set To Default
Posture	Redirectionless 	Set To Default

 RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret [Show](#)

ネットワークデバイスの設定

クライアント プロビジョニング

クライアントに適切なソフトウェアとプロファイルをプロビジョニングして、リダイレクトのない環境でポスチャを実行するには、次の2つの方法があります。

1. 手動プロビジョニング (導入前)
2. クライアントプロビジョニングポータル (Web展開)

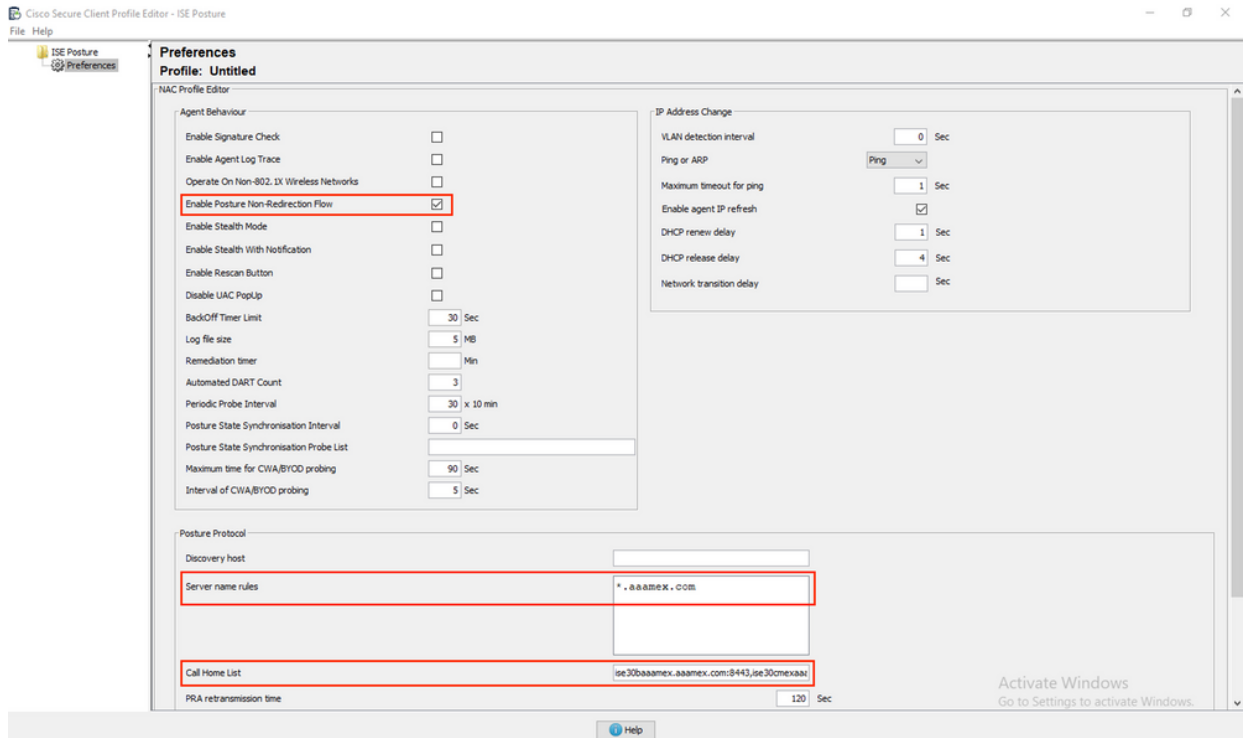
手動プロビジョニング (導入前)

1. [Ciscoソフトウェアダウンロード](#)からCisco Secure Client Profile Editorをダウンロードして



2. ISEポスタチャプロファイルエディタを開きます。

- Enable Posture Non-Redirection Flowが有効になっていることを確認します。
- サーバ名ルールをカンマで区切って設定します。アスタリスク(*)を1つ使用して任意のPSNへの接続を許可するか、ワイルドカード値を使用して特定のドメイン内の任意のPSNへの接続を許可するか、PSN FQDNを使用して特定のPSNへの接続を制限します。
- PSNのカンマ区切りリストを指定するようにCall Home Listを設定します。必ず、FQDN:portまたはIP:portの形式でクライアントプロビジョニングポータルポートを追加してください。



プロファイルエディタによるポスタチャプロファイルの設定

注：必要に応じてクライアントプロビジョニングポータルポートを確認する方法については、「クライアントプロビジョニングポリシー」セクションのステップ4を参照してください。

3. 使用中のCall Homeリストごとにステップ2を繰り返します。

4. [Ciscoソフトウェアダウンロード](#)からCisco Secure Client導入前パッケージをダウンロードします。

Cisco Secure Client導入前パッケージ

5. プロファイルをISEPostureCFG.xmlとして保存します。
6. プロファイルとインストールファイルをアーカイブファイルに配布するか、クライアントにコピーします。

警告：接続しようとしているヘッドエンドに、同じCisco Secure Clientファイル（Secure Firewall ASA、ISEなど）があることを確認してください。手動プロビジョニングを使用する場合でも、対応するソフトウェアバージョンでクライアントプロビジョニング用にISEを設定する必要があります。詳細な手順については、「クライアントプロビジョニングポリシーの設定」セクションを参照してください。

7. クライアントで、zipファイルを開き、セットアップを実行してコアおよびISEポスチャモジュールをインストールします。あるいは、個々のmsiファイルを使用して各モジュールをインストールすることもできます。この場合は、最初にcore-vpnモジュールがインストールされていることを確認する必要があります。

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

Cisco Secure Client導入前パッケージの内容

Select the Cisco Secure Client 5.0.01242 modules you wish to install:

- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- Select All

- Diagnostic And Reporting Tool

- Lock Down Component Services

Install Selected

Cisco Secure Clientインストーラ

ヒント：トラブルシューティングに使用する診断およびレポートツールをインストールします。

8. インストールが完了したら、ポスチャプロファイルxmlを次の場所にコピーします。
 - Windows: %ProgramData%\Cisco\Cisco Secure Client\ISE Posture
 - MacOS:/opt/cisco/secureclient/iseposture/

クライアントプロビジョニングポータル (Web展開)

ISEクライアントプロビジョニングポータルを使用して、Cisco Secure Client ISEポスチャモジュールとISEからのポスチャプロファイルをインストールできます。ISEポスチャモジュールがすで

にクライアントにインストールされている場合は、ポスチャプロファイルをプッシュするためにも使用できます。

1. Work Centers > Posture > Client Provisioning > Client Provisioning Portalの順に移動し、ポータル設定を開きます。Portal Settingsセクションを展開し、Authentication methodフィールドを見つけて、ポータルでの認証に使用するIdentity Source Sequenceを選択します。
2. クライアントプロビジョニングポータルの使用を許可された内部および外部IDグループを設定します。

Authentication method: * Certificate_Request_Sequence

Configure authentication methods at:

[Administration > Identity Management > Identity Source Sequences](#)

Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal

Available	Chosen
ADAAMEX:saamex.com/AAAUUnit/AAAGroup	provisioning
ADAAMEX:saamex.com/Builtin/Account Operat	ADAAMEX:saamex.com/Users/Domain Users
ADAAMEX:saamex.com/Builtin/Administrators	
ADAAMEX:saamex.com/Builtin/Backup Operato	
ADAAMEX:saamex.com/Builtin/Certificate Servi	

[Choose all](#) [Clear all](#)

ポータル設定での認証方法と承認されたグループ

3. Fully Qualified Domain Name (FQDN ; 完全修飾ドメイン名) フィールドで、クライアントがポータルにアクセスするために使用するURLを設定します。複数のFQDNを設定するには、値をカンマで区切って入力します。

Fully qualified domain name (FQDN): clientprovisioning.aaamex

Idle timeout: 10
1-30 (minutes)

Display language: Use browser locale

Fallback language: English - English ▾

Always use: English - English ▾

4. ポータルURLを対応するCall HomeリストのPSNに解決するようにDNSサーバを設定します。
5. ISEポスチャソフトウェアをインストールするために、ポータルにアクセスするためのFQDNをエンドユーザに提供します。

注：ポータルFQDNを使用するには、クライアントのPSN Admin証明書チェーンおよびポータル証明書チェーンが信頼ストアにインストールされている必要があります。また、管理証明書のSANフィールドにポータルFQDNが含まれている必要があります。

クライアントプロビジョニングポリシー

クライアントプロビジョニングは、エンドポイントにCisco Secure Clientをインストールするために使用するプロビジョニングのタイプ（導入前またはWeb導入）に関係なく、ISEで設定する必要があります。

1. シスコのソフトウェアダウンロードからCisco Secure Client webdeployパッケージを[ダウンロード](#)

Cisco Secure Client Headend Deployment Package (Windows) 19-Dec-2022 91.38 MB [↓](#) [🛒](#)
cisco-secure-client-win-5.0.01242-webdeploy-k9.pkg
[Advisories](#) [🔗](#)

[ロードします。](#)

Cisco Secure Client WebDeployパッケージ

2. [シスコソフトウェアダウンロード](#)から最新のコンプライアンスモジュールwebdeployパッケージをダウンロードします。

All Release ▾

SecureFWPosture >


ISEComplianceModule ▾

ISEComplianceModule

Android >

NVM >

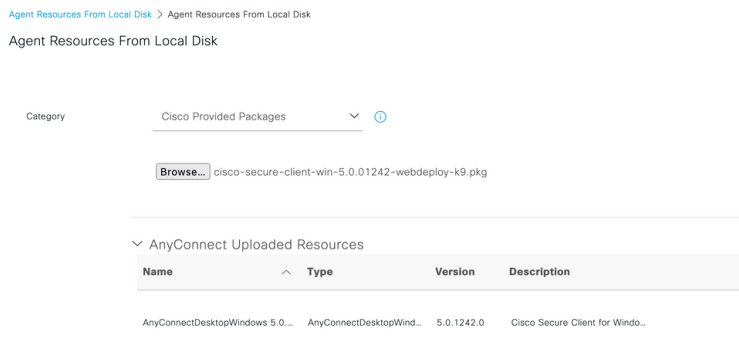
5.0 >

 AnyConnect 4.x & Secure Client 5.x is available to customers with AnyConnect Plus or Apex licenses. For information on Plus/Apex licenses and migration, please see the AnyConnect ordering guide at: <http://www.cisco.com/cj/dam/en/us/products/security/anyconnect-og.pdf>

File Information	Release Date	Size	
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	19.59 MB	↓ 🛒
cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg Advisories 🔗			

ISEコンプライアンスモジュールWebDeployパッケージ

3. ISEで、Work Centers > Posture > Client Provisioning > Resourcesの順に移動し、Add > Agent resources from local diskの順にクリックします。CategoryドロップダウンメニューからCisco Provided Packagesを選択し、以前にダウンロードしたCisco Secure Client webdeployパッケージをアップロードします。同じプロセスを繰り返して、コンプライアンス



スモジュールをアップロードします。

Submit Cancel

シスコが提供するパッケージのISEへのアップロード

4. Resourcesタブに戻り、Add > AnyConnect Posture Profileの順にクリックします。プロファイル:

- ISE内でプロファイルを識別するために使用できる名前を設定します。
- サーバ名ルールをカンマで区切って設定します。アスタリスク(*)を1つ使用して任意のPSNへの接続を許可するか、ワイルドカード値を使用して特定のドメイン内の任意のPSNへの接続を許可するか、PSN FQDNを使用して特定のPSNへの接続を制限します。
- PSNのカンマ区切りリストを指定するようにCall Home Listを設定します。FQDN:portまたはIP:portの形式を使用して、クライアントプロビジョニングポータル

* Name: CSC Redirectionless

Description: Redirectionless Posture LAB - 2 PSNs

ポートを追加します。

ISEポスチャプロファイルの設定I

Posture Protocol

Parameter	Value	Notes	Description
PRA 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	*.saames.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. "*.psia.com"
Call Home List	rix.saames.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 this max time limit is reached

ISEポスチャプロファイルの設定II

Call Homeリストで使用するポートを検索するには、Work Centers > Posture > Client Provisioning > Client Provisioning Portalの順に移動し、使用中のポータルを選択してPortal Settingsを展開します。

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)

クライアントプロビジョニングポータルポート

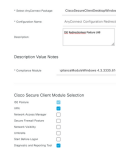
- Resourcesタブに戻り、Add > AnyConnect Configurationの順にクリックします。使用するCisco Secure Clientパッケージとコンプライアンスモジュールを選択します。

警告：クライアントにCisco Secure Clientが事前に導入されている場合は、ISEのバージョンがエンドポイントのバージョンと一致していることを確認してください。Web展開にASAまたはFTDを使用する場合、このデバイスのバージョンも一致する必要があります。

- Posture Selectionセクションまでスクロールダウンして、ステップ1で作成したプロファイ

ルを選択します。ページの下部にあるSubmitをクリックして、設定を保存します。

AnyConnectの設定



Profile Selection

* ISE Posture	CSC Redirectionless	▼
VPN		▼

プロファイル選択

7. Work Centers > Posture > Client Provisioning > Client provisioning policyの順に移動します。必要なオペレーティングシステムに使用されているポリシーを探し、Editをクリックします。Results列で+記号をクリックし、Agent Configurationセクションのステップ5でAnyConnect設定を選択します。

注：複数のCall Homeリストがある場合は、Other Conditionsフィールドを使用して、対応するクライアントに正しいプロファイルをプッシュします。この例では、デバイスロケーショングループを使用して、ポリシーにプッシュされるポスチャプロファイルを特定します。

ヒント：同じOSに対して複数のクライアントプロビジョニングポリシーが設定されている場合は、これらを相互に排他的にすることをお勧めします。つまり、特定のクライアントが一度に1つのポリシーしかヒットできないようにする必要があります。RADIUS属性をOther Conditions列で使用すると、1つのポリシーを別のポリシーと区別できます。

Agent Configuration

ect Configuration Redirectionless



Is Upgrade Mandatory

Native Supplicant Configuration

Choose a Config Wizard



Choose a Wizard Profile



クライアントプロビジョニングポリシーエージェントの設定

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	Results	
	<input checked="" type="checkbox"/> IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP	Edit
	<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP	Edit
	<input checked="" type="checkbox"/> Windows	If Any	and Windows All	and DEVICE-Location EQUALS All Locations#USHWEST	then AnyConnect Configuration Redirectionless	Edit
	<input checked="" type="checkbox"/> MAC OS	If Any	and Mac OSX	and Condition(s)	then MacOS Configuration And MacOSXSPWizard 2.7.0.1 And Cisco-ISE-NSP	Edit
	<input checked="" type="checkbox"/> Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP	Edit

Save

Reset

クライアントプロビジョニングポリシー

- 使用中の各Call Homeリストと対応するポスチャプロファイルについて、ステップ4 ~ 7を繰り返します。ハイブリッド環境では、同じプロファイルのリダイレクトクライアントに使用できません。

許可

許可プロファイル

1. Policy > Policy Elements > Results > Authorization > Downloadable ACLsの順に移動し、Addをクリックします。
2. DACLを作成して、DNS、DHCP (使用されている場合)、ISE PSNへのトラフィックを許可し、他のトラフィックをブロックします。最終的に準拠したアクセスを行う前に、アクセスに必要な他のトラフィックをすべて許可してください。

* Name

Description

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 <ip 1 IP address>
1617181	permit ip any host <ip 2 IP address>
9202132	permit icmp any any
2324252	deny ip any any
6272829	
3031323	
3343838	
3738394	
0414343	

Check DACL Syntax

DACL is valid

DACLの設定

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

```
permit ip any host
```

deny ip any any

注意：一部のサードパーティデバイスはDACLをサポートしていない可能性があります。このような場合は、Filter-IDまたはその他のベンダー固有属性を使用する必要があります。詳細については、ベンダーのマニュアルを参照してください。DACLを使用しない場合は、ネットワークデバイスで対応するACLを設定してください。

3. Policy > Policy Elements > Results > Authorization > Authorization profilesの順に移動し、Addをクリックします。認可プロファイルに名前を付け、Common TasksからDACL名を選

択します。ドロップダウンメニューから、手順2で作成したDACLを選択します。



許可プロファイル

注: DACLを使用しない場合は、Common TasksのFilter-IDまたはAdvanced Attribute Settingsを使用して、対応するACL名をプッシュします。

4. 使用中のCall Homeリストごとにステップ1 ~ 3を繰り返します。ハイブリッド環境では、リダイレクションに必要な認証プロファイルは1つだけです。リダイレクションの許可プロファイルの設定は、このドキュメントの範囲外です。

認可ポリシー

1. Policy > Policy Setsの順に移動し、使用中のポリシーセットを開くか、または新しいポリシーセットを作成します。
2. Authorization Policyセクションまでスクロールします。Session Posture Status NOT_EQUALS Compliantを使用して認可ポリシーを作成し、前のセクションで作成した認可プロファイルを選択します。

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
Compliant		Session-PostureStatus EQUALS Compliant	Compliant access ×	Select from list	0
Redirectionless	AND	DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant	Redirectionless posture ×	Select from list	0
Redirection	AND	Session-PostureStatus NOT_EQUALS Compliant DEVICE-Posture EQUALS Posture#Redirection	Redirection posture ×	Select from list	0
Default			DenyAccess ×	Select from list	0

許可ポリシー

- 対応するCall Homeリストが使用されている各認可プロファイルについて、ステップ2を繰り返します。ハイブリッド環境では、リダイレクションに必要な許可ポリシーは1つだけです。

トラブルシューティング

Cisco Secure Clientで準拠し、ISEでポスチャが適用されない (保留中)

古い/ファントムセッション

展開内に古いセッションやファントムセッションがあると、リダイレクトなしのポスチャ検出で断続的かつランダムな障害が生成される可能性があります。この結果、Cisco Secure Client UIが準拠アクセスを示している間、ユーザはISE上でポスチャ不明または該当しないアクセス状態のままになります。

古いセッションは、アクティブではなくなった古いセッションです。これらは認証要求とアカウントティング開始によって作成されますが、セッションをクリアするためにPSNでアカウントティング停止が受信されません。

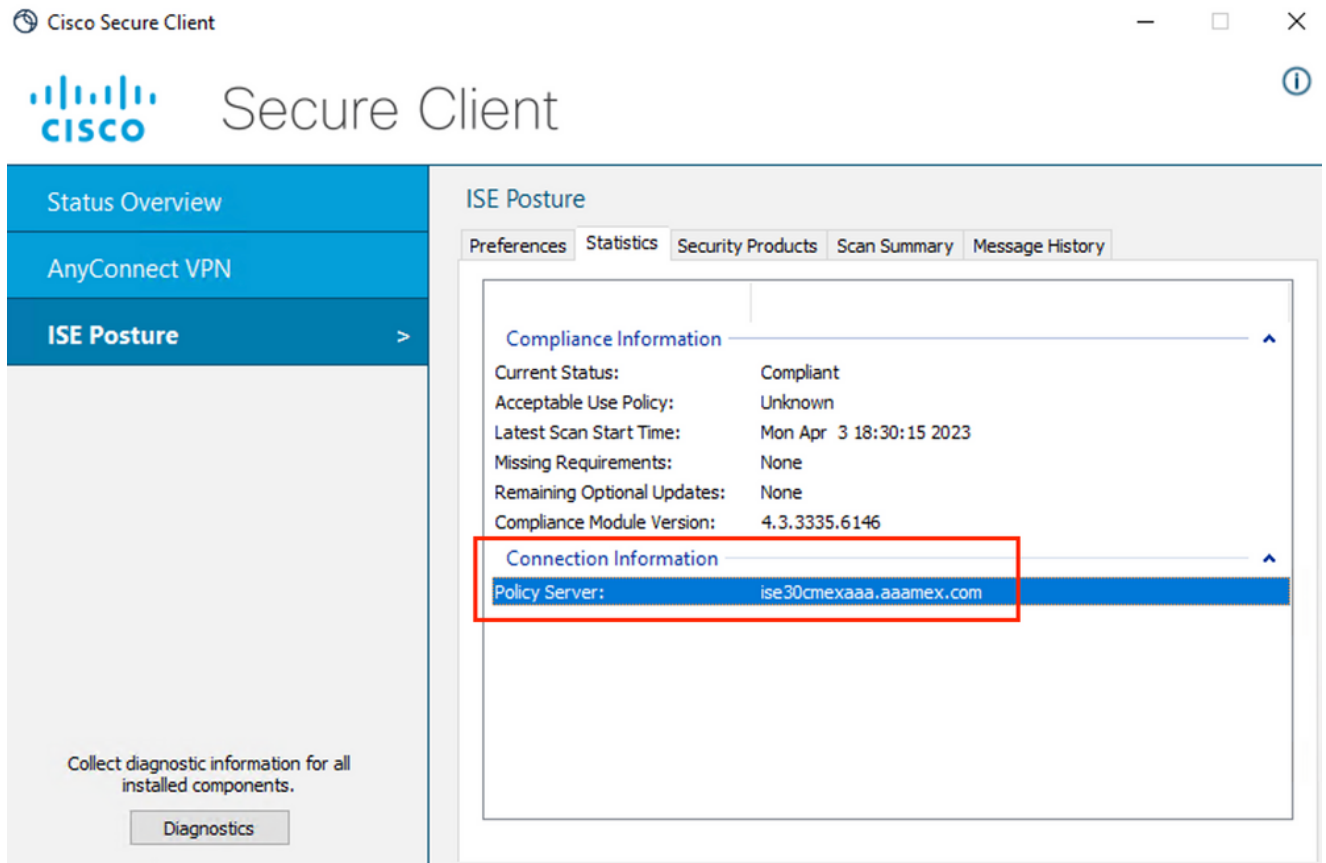
ファントムセッションは、特定のPSNで実際にアクティブではなかったセッションです。これらはアカウントティングの暫定アップデートによって作成されますが、セッションをクリアするためのアカウントティングの停止はPSNで受信されません。

特定

古い/ファントムセッションの問題を特定するには、クライアントのシステムスキャンで使用されるPSNを確認し、認証を実行しているPSNと比較します。

- Cisco Secure Client UIの左下隅にある歯車アイコンをクリックします。左側のメニューから

、ISE Postureセクションを開き、Statisticsタブに移動します。[接続情報]にポリシーサーバを書き留めます。



Cisco Secure ClientのISEポスタチャのポリシーサーバ

2. ISE RADIUSのライブログには、次の点に注意してください。

- ポスチャステータスの変更
- サーバの変更
- 認可ポリシーと認可プロファイルに変更なし
- CoAライブログなし

Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server	Posture Status	Authorization Profiles
Apr 03, 2023 07:32:52.3...	●		0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	Ise30cmexaaa	Compliant	Redirectionless posture
Apr 03, 2023 07:32:40.7...	■			#ACSACL#-IP-...			Ise30baaamex		
Apr 03, 2023 07:32:40.6...	■			redirectionless	00:50:5...	Posture Lab >> Redirectionless	Ise30baaamex	NotApplicable	Redirectionless posture

古い/ファントムセッションのライブログ

3. ライブセッションまたは最後の認証ライブログの詳細を開きます。ポリシーサーバをメモします。ステップ1で確認したサーバと異なる場合は、古い/ファントムセッションの問題を示します。

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	ise30baaamex
---------------	--------------

Event	5200 Authentication succeeded
Username	redirectionless

ライブログの詳細のポリシーサーバー

解決方法

ISE 2.6パッチ6および2.7パッチ3より上位のISEバージョンでは、リダイレクトなしのポスチャフローにおける古い/ファントムセッションシナリオのソリューションとして[RADIUSセッションディレクトリ](#)が実装されています。

1. Administration > System > Settings > Light Data Distributionの順に移動し、Enable RADIUS Session Directoryチェックボックスがオンになっていることを確認します。

The screenshot shows the ISE Settings page with the following structure:

- Navigation tabs: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, **Settings**
- Left sidebar menu: 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**
- Main content area:
 - RADIUS Session Directory**

Enable the RADIUS Session Directory (RSD) feature to store the user session information and replicate it across the 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 connecting to ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling service, disabling this option will use legacy Profiler owners directory.

Enable Endpoint Owner Directory
 - Advanced Settings**

Configure the following options for RSD and EPOD.

Batch size: 10 (dropdown menu) Items: 1 (info icon)

RADIUSセッションディレクトリの有効化

2. ISE CLIから、次のコマンドを実行して、ISEメッセージングサービスがすべてのPSNで実行されていることを確認します アプリケーションステータスiseの表示


```
lise30cmexaaa/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	
DNS Server (named)	disabled	
ISE Messaging Service	running	16526
ISE API Gateway Database Service	running	18463
ISE API Gateway Service	running	23052

ISEメッセージングサービス実行中 (自動)

注：このサービスは、PSN間のRSDに使用される通信方法を指し、ISE UIから設定できるsyslogのISEメッセージングサービス設定の状態に関係なく実行される必要があります。

3. ISE Dashboardに移動し、Alarmsダッシュレットを見つけます。Queue Link Errorアラームがあるかどうかを確認します。アラームの名前をクリックすると、詳細が表示されます。

Severity	Name	Occu...	Last Occurred
▼	queue	x	
	Queue Link Error	2143	37 mins ago

Last refreshed: 2023-04-03 14:45:19

キューリンクエラーアラーム

4. ポスチャに使用されるPSN間でアラームが生成されているかどうかを確認します。

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 firewall. Please note that these alarms could occur between nodes, when the nodes 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 / 22 >> Go 2143 Total Rows

Refresh Acknowledge

<input type="checkbox"/>	Time Stamp	Description	Cause= {tts_alert;" unknown Ca"}	Details
<input type="checkbox"/>	Apr 03 2023 21:07:00.977 PM	Queue Link Error: Message=From Ise30cmexaaa.aaamex.com To Ise30baaamex.aaamex.com; Cause={tts_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={tts_alert;" unkno...		

キューリンクエラーアラームの詳細

5. アラームの説明にカーソルを合わせると、詳細が表示され、原因フィールドが書き留められます。キューリンクエラーの最も一般的な原因は次の2つです。

- タイムアウト：ノードからポート8671の別のノードに送信された要求がしきい値内で応答されないことを示します。修復するには、ノード間でTCPポート8671が許可されていることを確認します。
- Unknown CA: ISEメッセージング証明書を署名している証明書チェーンが無効または

不完全であることを示します。このエラーを修復するには、次の手順を実行します。

- a. Administration > System > Certificates > Certificate signing requestsの順に移動します。
- b. Generate Certificate Signing Requests (CSR)をクリックします。
- c. ドロップダウンメニューからISE Root CAを選択し、Replace ISE Root CA Certificate chainをクリックします。
ISEルートCAが使用できない場合は、Certificate Authority > Internal CA settingsの順に移動し、Enable Certificate Authorityをクリックしてから、CSRに戻ってルートCAを再生成します。
- d. 新しいCSRを生成し、ドロップダウンメニューからISE Messaging Serviceを選択します。
- e. 展開からすべてのノードを選択し、証明書を再生成します。

注：証明書の再生成中は、Queue Link Errorアラームで原因不明のCAまたはEconnrefusedが発生することが予想されます。証明書の生成後にアラームを監視して、問題が解決されたことを確認します。

パフォーマンス

特定

リダイレクトなしのポスチャに関連する高いCPU使用率や高い負荷平均などのパフォーマンスの問題は、PSNおよびMnTノードに影響を与える可能性があり、多くの場合、次のイベントが付随または先行します。

- ランダムまたは断続的なNo policy server detectedエラー(Cisco Secure Client)
- ポータルサービススレッドプールがしきい値に達したイベントの最大リソース制限に達したレポート。Operations > Reports > Reports > Audit > Operations Auditの順に移動して、レポートを表示します。
- MNTルックアップへのポスチャエラーは高アラームです。これらのアラームは、ISE 3.1以降のバージョンでのみ生成されます。

解決方法

導入のパフォーマンスがリダイレクトなしのポスチャの影響を受ける場合、これは効果的な実装ではないことが多いことを示します。次の点を修正することをお勧めします。

- Call Homeリストごとに使用されるPSNの数設計に従って、エンドポイントまたはネットワークデバイスごとのポスチャに使用できるPSNの数を減らすことを検討してください。
- Call Homeリストのクライアントプロビジョニングポータルポート。各ノードのIPまたはFQDNの後にポータルポート番号が含まれていることを確認します。

影響を軽減するには、次の手順を実行します。

1. Cisco Secure Clientフォルダからファイルを削除してエンドポイントから connectiondata.xmlをクリアし、ISE PostureサービスまたはCisco Secure Clientを再起動します。サービスを再起動しないと、古いファイルが再生成され、変更は有効になりません。このアクションは、Call Homeリストを修正した後にも実行する必要があります。
2. DACLまたは他のACLを使用して、ISE PSNへのトラフィックをブロックし、関連性のないネットワーク接続を実現します。

- 認可ポリシーでポストチャが適用されていないが、Cisco Secure Client ISEポストチャモジュールがインストールされているエンドポイントに適用される接続の場合、TCPポート8905およびクライアントプロビジョニングポータルポートのすべてのISE PSNに対するクライアントからのトラフィックをブロックします。このアクションは、リダイレクト実装を使用するポストチャにも推奨されます。
- ポストチャが許可ポリシーに適用される接続では、クライアントから認証側PSNへのトラフィックを許可し、展開内の他のPSNへのトラフィックをブロックします。このアクションは、設計の改訂中に一時的に実行できます。

[Authorization Profiles](#) > Redirectionless-PSN1

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

DACL Name

単一のPSNに対するDACLを使用した認証プロファイル

Compliant	Session-PostureStatus EQUALS Compliant	Compliant access
Redirectionless PSN1	DEVICE-Posture EQUALS Posture#Redirectionless	Redirectionless PSN1
	DEVICE-Location EQUALS All Locations#US#WEST	
	Session-PostureStatus NOT_EQUALS Compliant	
	Network Access-ISE Host Name EQUALS ise30baamex.aaamex.com	
Redirectionless PSN2	DEVICE-Posture EQUALS Posture#Redirectionless	Redirectionless PSN2
	DEVICE-Location EQUALS All Locations#US#WEST	
	Session-PostureStatus NOT_EQUALS Compliant	
	Network Access-ISE Host Name EQUALS ise30cmexaaa.aaamex.com	
Redirection	Session-PostureStatus NOT_EQUALS Compliant	Redirection posture
	DEVICE-Posture EQUALS Posture#Redirection	

アカウントティング

RADIUSアカウントティングは、ISEでのセッション管理に不可欠です。ポスチャは実行されるアクティブセッションに依存するため、アカウントティング設定の誤りまたは欠如もポスチャディスカバリとISEのパフォーマンスに影響を与える可能性があります。各セッションの1つのPSNに認証要求、アカウントティング開始、アカウントティング停止、およびアカウントティング更新を送信するように、アカウントティングがネットワークデバイスで正しく構成されていることを確認することが重要です。

ISEで受信したアカウントティングパケットを確認するには、Operations > Reports > Reports > Endpoints and Users > RADIUS Accountingの順に移動します。

関連情報

- [シスコテクニカルサポートおよびダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。