

# TrustSec 認識サービス用の ISE と WSA との統合設定

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク ダイアグラムとトラフィック フロー](#)

[ASA-VPN](#)

[ASA-FW](#)

[ISE](#)

[ステップ 1 : IT およびその他のグループの SGT](#)

[ステップ 2 : SGT を割り当てる VPN アクセスの認可ルール = 2 \( IT \)](#)

[ステップ 3 : ネットワーク デバイスの追加と ASA-VPN の PAC ファイルの生成](#)

[ステップ 4 : pxGrid ロールの有効化](#)

[ステップ 5 : 管理用証明書と pxGrid ロールの生成](#)

[ステップ 6 : pxGrid の自動登録](#)

[WSA](#)

[ステップ 1 : トランスペアレント モードおよびリダイレクション](#)

[ステップ 2 : 証明書の生成](#)

[ステップ 3 : ISE 接続のテスト](#)

[ステップ 4 : ISE 識別プロファイル](#)

[ステップ 5 : SGT タグに基づくポリシーへのアクセス](#)

[確認](#)

[ステップ 1 : VPN セッション](#)

[ステップ 2 : WSA により取得されるセッション情報](#)

[ステップ 3 : WSA へのトラフィック リダイレクション](#)

[トラブルシューティング](#)

[誤った証明書](#)

[正しいシナリオ](#)

[関連情報](#)

## 概要

このドキュメントでは、Web セキュリティ アプライアンス ( WSA ) と Identity Services Engine ( ISE ) を統合する方法について説明します。ISE バージョン 1.3 では、pxGrid と呼ばれる新しい API がサポートされています。認証、暗号化、および特権 ( グループ ) をサポートする

この新しく柔軟なプロトコルにより、他のセキュリティソリューションとの統合が容易になります。

WSA バージョン 8.7 では pxGrid プロトコルがサポートされており、ISE からコンテキスト識別情報を取得できます。その結果、WSA では ISE から取得される TrustSec Security Group Tag ( SGT ) グループに基づいてポリシーを作成できます。

## 前提条件

### 要件

Cisco ISE 構成の経験と、次のトピックに関する基本的な知識があることが推奨されます。

- ISE の導入および認可の設定
- TrustSec と VPN アクセスのための適応型セキュリティ アプライアンス ( ASA ) CLI 設定
- WSA の設定
- TrustSec の導入に関する基本的な知識

### 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くものです。

- Microsoft Windows 7
- Cisco ISE ソフトウェア バージョン 1.3 以降
- Cisco AnyConnect Mobile Security バージョン 3.1 以降
- Cisco ASA バージョン 9.3.1 以降
- Cisco WSA バージョン 8.7 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## 設定

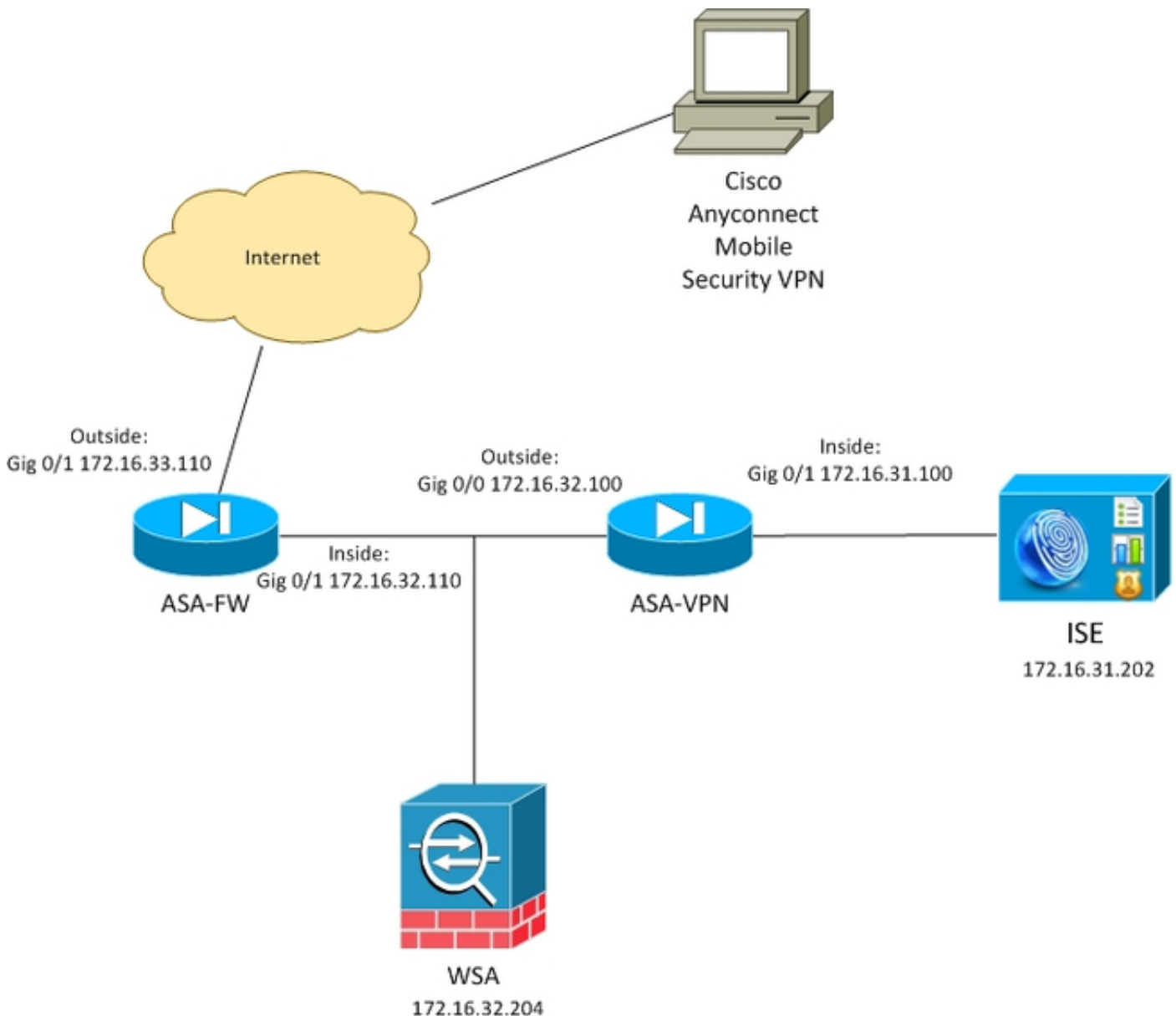
注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録](#) ユーザ専用 ) を使用してください。

### ネットワーク ダイアグラムとトラフィック フロー

TrustSec SGT タグは、社内ネットワークにアクセスするすべてのタイプのユーザに対し、認証サーバとして使用されている ISE により割り当てられます。これには、802.1x または ISE ゲストポータルで認証される有線/ワイヤレス ユーザが含まれます。また、認証に ISE を使用するリモート VPN ユーザも含まれます。

WSA では、ユーザがどのようにネットワークにアクセスしているかは重要ではありません。

この例では、ASA-VPN でセッションを終了するリモート VPN ユーザを使用します。これらのユーザには、特定の SGT タグが割り当てられています。インターネットへの HTTP トラフィックはすべて ASA-FW (ファイアウォール) によりインターセプトされ、検査のため WSA にリダイレクトされます。WSA は識別プロファイルを使用します。これにより、SGT タグに基づいてユーザを分類し、この分類に基づきアクセス ポリシーまたは復号ポリシーを作成できます。



詳細なフローは次のとおりです。

1. AnyConnect VPN ユーザが ASA-VPN 上でセキュア ソケット レイヤ (SSL) セッションを終了します。ASA-VPN が TrustSec に対応して設定され、VPN ユーザの認証に ISE を使用します。認証されたユーザには SGT タグ値 = 2 (名前 = IT) が割り当てられます。ユーザが 172.16.32.0/24 ネットワークから IP アドレス (この例では 172.16.32.50) を受け取ります。
2. ユーザはインターネットの Web ページへのアクセスを試行します。Web Cache Communication Protocol (WCCP) に対応して ASA-FW が設定されます。これにより、トラフィックが WSA にリダイレクトされます。
3. ISE 統合に対応して WSA が設定されます。これは pxGrid を使用して ISE から情報をダウ

- ンロードします。ユーザ IP アドレス 172.16.32.50 に SGT タグ 2 が割り当てられます。
4. WSA はユーザからの HTTP 要求を処理し、アクセス ポリシー PolicyForIT に一致します。このポリシーは、スポーツ サイトへのトラフィックをブロックするように設定されています。SGT 2 に属していないその他のユーザはすべて、デフォルトのアクセス ポリシーに一致し、スポーツ サイトに完全にアクセスできます。

## ASA-VPN

これは、TrustSec に対応して設定されている VPN ゲートウェイです。詳細な設定についてはこのドキュメントでは説明しません。次の例を参照してください。

- [ASA および Catalyst 3750X シリーズ スイッチ TrustSec の設定例およびトラブルシューティングガイド](#)
- [ASA バージョン 9.2 の VPN SGT の分類と適用の設定例](#)

## ASA-FW

ASA ファイアウォールは、WSA への WCCP リダイレクションを処理します。このデバイスは TrustSec を認識しません。

```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.110 255.255.255.0

access-list wccp-routers extended permit ip host 172.16.32.204 any
access-list wccp-redirect extended deny tcp any host 172.16.32.204
access-list wccp-redirect extended permit tcp any any eq www
access-list wccp-redirect extended permit tcp any any eq https

wccp 90 redirect-list wccp-redirect group-list wccp-routers
wccp interface inside 90 redirect in
```

## ISE

ISE は TrustSec 導入環境の中心となります。ネットワークにアクセスして認証するすべてのユーザに対して SGT タグが割り当てられます。ここでは基本設定に必要な手順を説明します。

### ステップ 1 : IT およびその他のグループの SGT

[Policy] > [Results] > [Security Group Access] > [Security Groups] を選択して、SGT を作成します。

**Results**

Search:

← ▾ ▸ [List Icon] [Settings Icon]

- Authentication
- Authorization
- Profiling
- Posture
- Client Provisioning
- TrustSec
  - Security Group ACLs
  - Security Groups**
    - IT
    - Marketing
    - Unknown
  - Security Group Mappings

**Security Groups**  
For Policy Export go to [Administration > System](#)

Edit Add Import Export ▾

	Name	SGT (Dec / Hex)
<input type="checkbox"/>	IT	2/0002
<input type="checkbox"/>	Marketing	3/0003
<input type="checkbox"/>	Unknown	0/0000

## ステップ 2 : SGT を割り当てる VPN アクセスの認可ルール = 2 ( IT )

[Policy] > [Authorization] を選択し、リモート VPN アクセスのルールを作成します。ASA-VPN を介して確立されたすべての VPN 接続にはフル アクセス ( PermitAccess ) が付与され、SGT タグ 2 ( IT ) が割り当てられます。

**Authorization Policy**

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies ▾

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	ASA-VPN	if DEVICE.Device Type EQUALS All Device Types#ASA-VPN	then PermitAccess AND IT

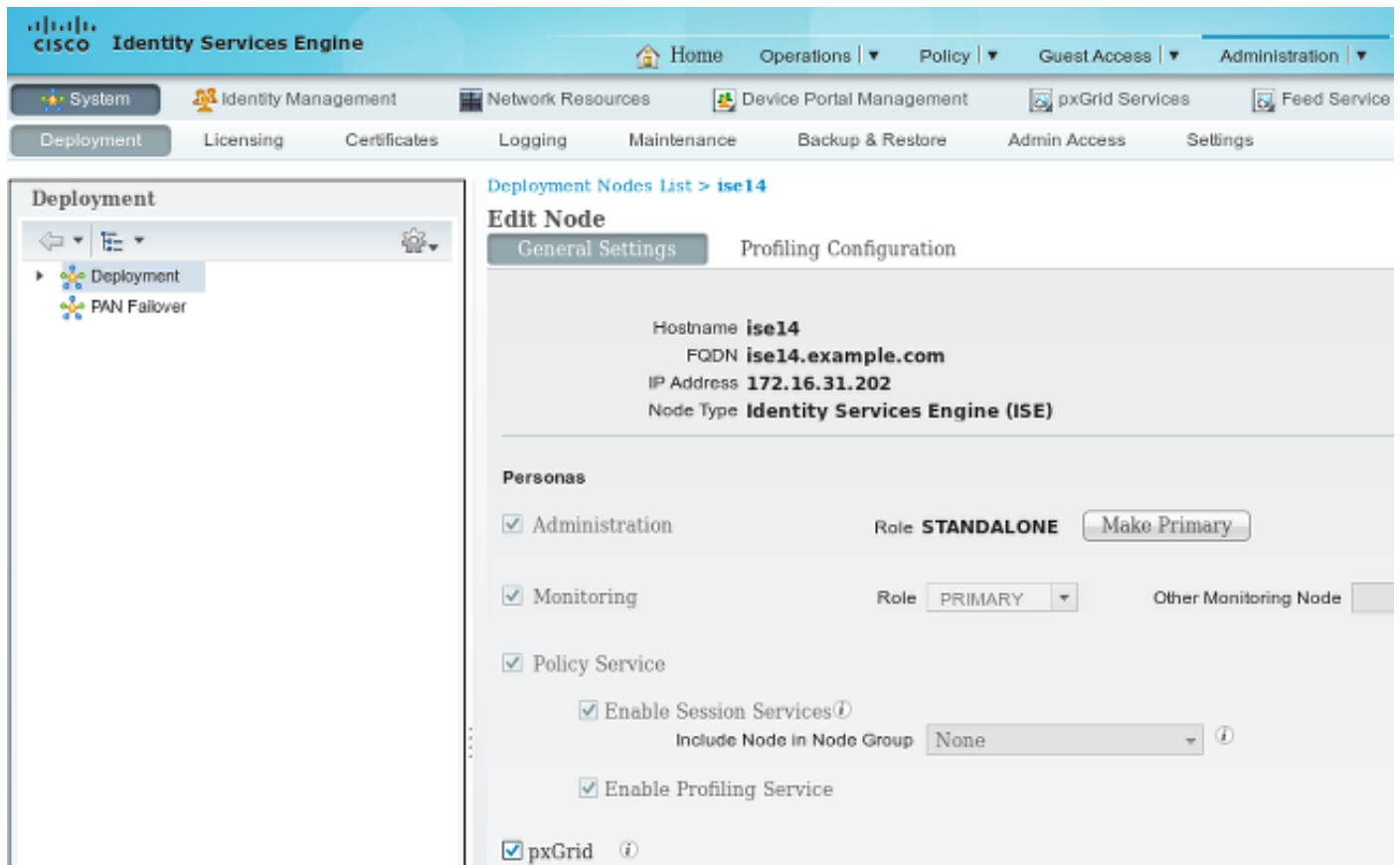
## ステップ 3 : ネットワーク デバイスの追加と ASA-VPN の PAC ファイルの生成

TrustSec ドメインに ASA-VPN を追加するには、プロキシ自動設定 ( PAC ) ファイルを手動で生成する必要があります。このファイルは ASA にインポートされます。

これは [Administration] > [Network Devices] から設定できます。ASA の追加後に、TrustSec 設定まで下にスクロールし、PAC ファイルを生成します。この詳細については、別の ( 参照 ) ドキュメントで説明します。

## ステップ 4 : pxGrid ロールの有効化

[Administration] > [Deployment] を選択し、pxGrid ロールを有効にします。



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The main menu has 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Service'. The 'Deployment' section is expanded, showing 'Deployment' and 'PAN Failover'. The 'Edit Node' page for 'ise14' is displayed, with the 'General Settings' tab selected. The node details are: Hostname 'ise14', FQDN 'ise14.example.com', IP Address '172.16.31.202', and Node Type 'Identity Services Engine (ISE)'. Under 'Personas', 'Administration' is checked with a role of 'STANDALONE', 'Monitoring' is checked with a role of 'PRIMARY', and 'Policy Service' is checked. Below these, 'Enable Session Services' is checked with 'Include Node in Node Group' set to 'None', and 'Enable Profiling Service' is checked. At the bottom, the 'pxGrid' checkbox is checked.

## ステップ 5 : 管理用証明書と pxGrid ロールの生成

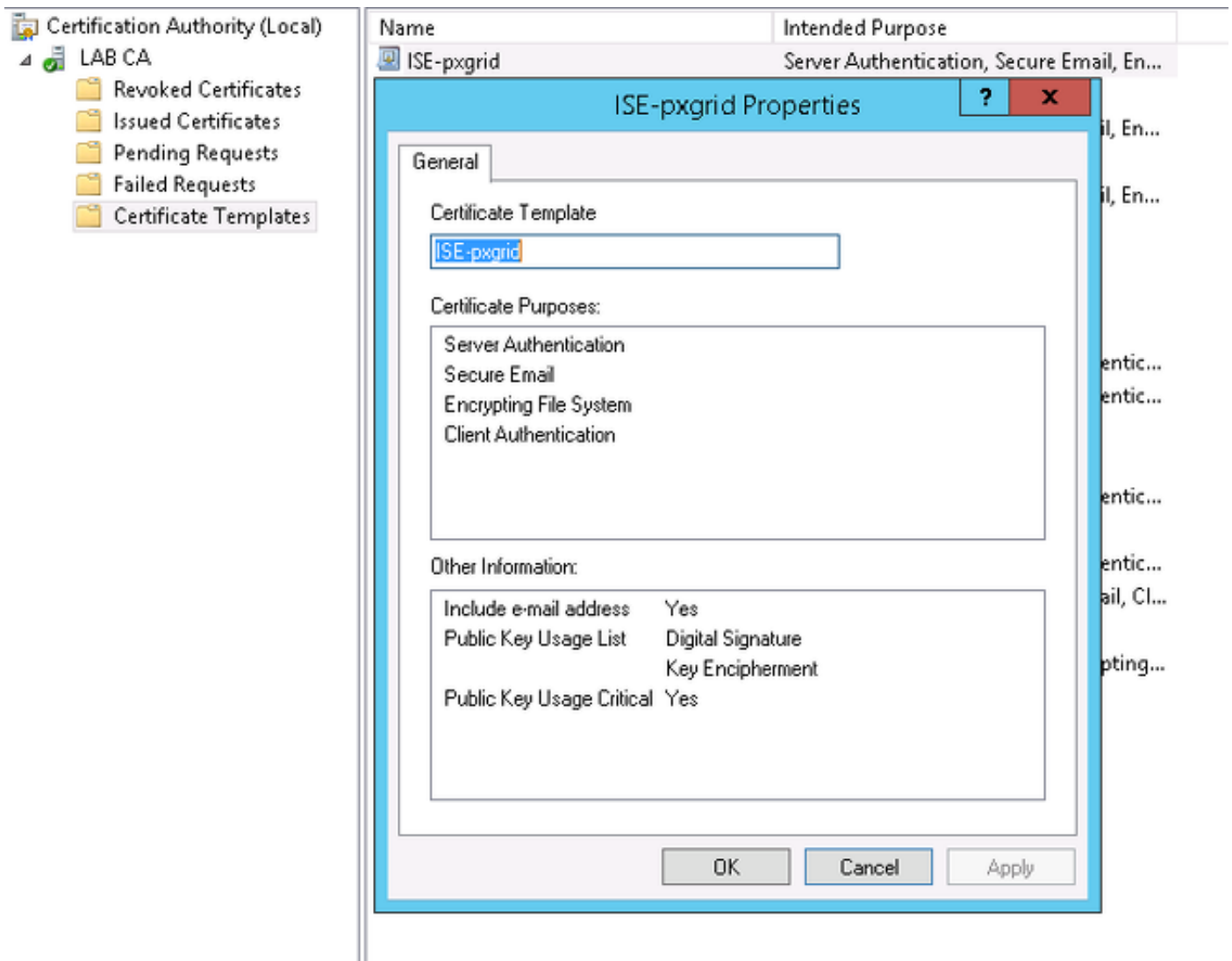
pxGrid プロトコルは、クライアントとサーバの両方に対して証明書認証を使用します。ISE と WSA の両方に正しい証明書を設定することが非常に重要です。両方の証明書では、[Subject] に完全修飾ドメイン名 ( FQDN ) が含まれており、クライアント認証とサーバ認証のための x509 拡張が含まれている必要があります。また、ISE と WSA の両方に対して正しい DNS A レコードが作成され、このレコードが対応する FQDN と一致することを確認してください。

両方の証明書が異なる認証局 ( CA ) により署名される場合は、これらの CA を信頼できるストアに格納することが重要です。

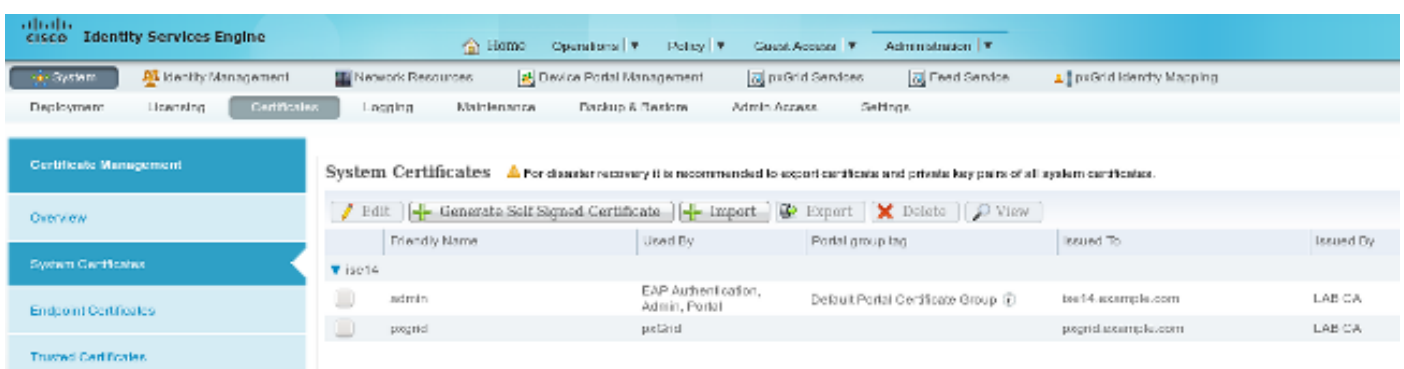
証明書を設定するには、[Administration] > [Certificates] を選択します。

ISE は、各ロールの証明書署名要求 ( CSR ) を生成できます。pxGrid ロールの場合、CSR をエクスポートし、外部 CA により署名します。

この例では、Microsoft CA が次のテンプレートに使用されています。



最終的な結果は次のようになります。



ise14.example.com と pxgrid.example.com の DNS A レコード ( 172.16.31.202. をポイントする ) を必ず作成してください。

## ステップ 6 : pxGrid の自動登録

デフォルトの場合、ISE は pxGrid サブスクリバを自動的に登録しません。管理者がこれを手動で承認する必要があります。WSA 統合のためにその設定を変更する必要があります。

[Administration] > [pxGrid Services] を選択し、[Enable Auto-Registration] を設定します。

[View By Capabilities](#)

[Enable Auto-Registration](#) [Disable Auto-Registration](#)

## WSA

### ステップ 1：トランスペアレント モードおよびリダイレクション

この例では、WSA で、管理インターフェイス、トランスペアレント モード、および ASA からのリダイレクションだけが設定されています。

The screenshot shows the Cisco S000V Web Security Virtual Appliance interface. The top navigation bar includes: Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Transparent Redirection".

**Transparent Redirection Device**

Type: WCCP v2 Router [Edit Device...](#)

**WCCP v2 Services**

[Add Service...](#)

Service Profile Name	Service ID	Router IP Addresses	Ports	Delete
wccp90	90	172.16.32.110, 172.16.33.110	80,443	

### ステップ 2：証明書の生成

WSA は、すべての証明書を署名するため CA を信頼する必要があります。[Network] > [Certificate Management] を選択し、CA 証明書を追加します。



Cisco S000V  
Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

## Manage Trusted Root Certificates

Custom Trusted Root Certificates

Import...

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Certificate	Expiration Date	On Cisco List	Delete
LAB CA	Feb 12 07:48:12 2025 GMT	No	

Cancel Submit

また、WSA が pxGrid の認証に使用する証明書を生成する必要もあります。[Network] > [Identity Services Engine] > [WSA Client certificate] を選択し、CSR を生成し、正しい CA テンプレート ( ISE-pxgrid ) を使用して CSR に署名し、再びインポートします。

また「ISE Admin Certificate」と「ISE pxGrid Certificate」では、CA 証明書をインポートします ( ISE により提示される pxGrid 証明書を信頼するため ) 。

Cisco S000V  
Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

## Identity Services Engine

Identity Services Engine Settings

ISE Server:	172.16.31.202
WSA Client Certificate:	Using Generated Certificate: Common name: wsa.example.com Organization: TAC Organizational Unit: Krakow Country: PL Expiration Date: May 5 15:57:36 2016 GMT Basic Constraints: Not Critical
ISE Admin Certificate:	Common name: LAB CA Organization: Organizational Unit: Country: Expiration Date: Feb 12 07:48:12 2025 GMT Basic Constraints: Critical
ISE PxGrid Certificate:	Common name: LAB CA Organization: Organizational Unit: Country: Expiration Date: Feb 12 07:48:12 2025 GMT Basic Constraints: Critical

Edit Settings...

ステップ 3 : ISE 接続のテスト

[Network] > [Identity Services Engine] を選択し、ISE への接続をテストします。

## Test Communication with ISE Server

Start Test

Checking connection to ISE PxGrid server...  
Success: Connection to ISE PxGrid server was successful. Retrieved 4 SGTs

Checking connection to ISE REST server...  
Success: Connection to ISE REST server was successful.

Test completed successfully.

### ステップ 4 : ISE 識別プロファイル

[Web Security Manager] > [Identification profiles] を選択して、ISE の新しいプロファイルを追加します。 [Identification and Authentication] には [Transparently identify users with ISE] を使用します。

The screenshot shows the Cisco S000V Web Security Virtual Appliance interface. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The main content area is titled 'Identification Profiles' and contains a table of 'Client / User Identification Profiles'. The table has five columns: Order, Transaction Criteria, Authentication / Identification Decision, End-User Acknowledgement, and Delete. There are two rows: one for an ISE profile and one for a Global Identification Profile.

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	<b>ISE</b> Protocols: HTTP/HTTPS	Identify Users Transparently: Identity Services Engine Guest privileges for users falling transparent user identification	(global profile)	
	<b>Global Identification Profile</b>	Exempt from Authentication / User Identification	Not Available	

### ステップ 5 : SGT タグに基づくポリシーへのアクセス

[Web Security Manager] > [Access Policies] を選択して、新しいポリシーを追加します。メンバーシップには ISE プロファイルが使用されます。

## Access Policy: PolicyForIT

### Policy Settings

Enable Policy

Policy Name:   
(e.g. my IT policy)

Description:

Insert Above Policy:

### Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile

Authorized Users and Groups

- All Authenticated Users
- Selected Groups and Users ?
  - ISE Secure Group Tags:
    - IT
  - Users: No users entered
- Guests (users failing authentication)



[Selected Groups and Users] で、SGT タグ 2 ( IT ) が追加されます。

## Access Policies: Policy "PolicyForIT": Edit Secure Group Tags

### Authorized Secure Group Tags

Use the search function below to add Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option.

1 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete
IT	2	__NONE__	<input type="checkbox"/>

[Delete](#)

### Secure Group Tag Search

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

Search  x

0 Secure Group Tag(s) selected for Add

[Add](#)

Secure Group Tag Name	SGT Number	SGT Description	Select
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Marketing	3	__NONE__	<input type="checkbox"/>
IT	2	__NONE__	<input checked="" type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

このポリシーは、SGT IT に属するユーザに対し、すべてのスポーツ サイトへのアクセスを拒否します。

## Access Policies

Policies							
<a href="#">Add Policy...</a>							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	<b>PolicyForIT</b> Identification Profile: ISE 1 tag (IT)	(global policy)	Block: 2 Monitor: 78	(global policy)	(global policy)	(global policy)	
	<b>Global Policy</b> Identification Profile: All	No blocked items	Monitor: 79	Monitor: 377	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Disabled	

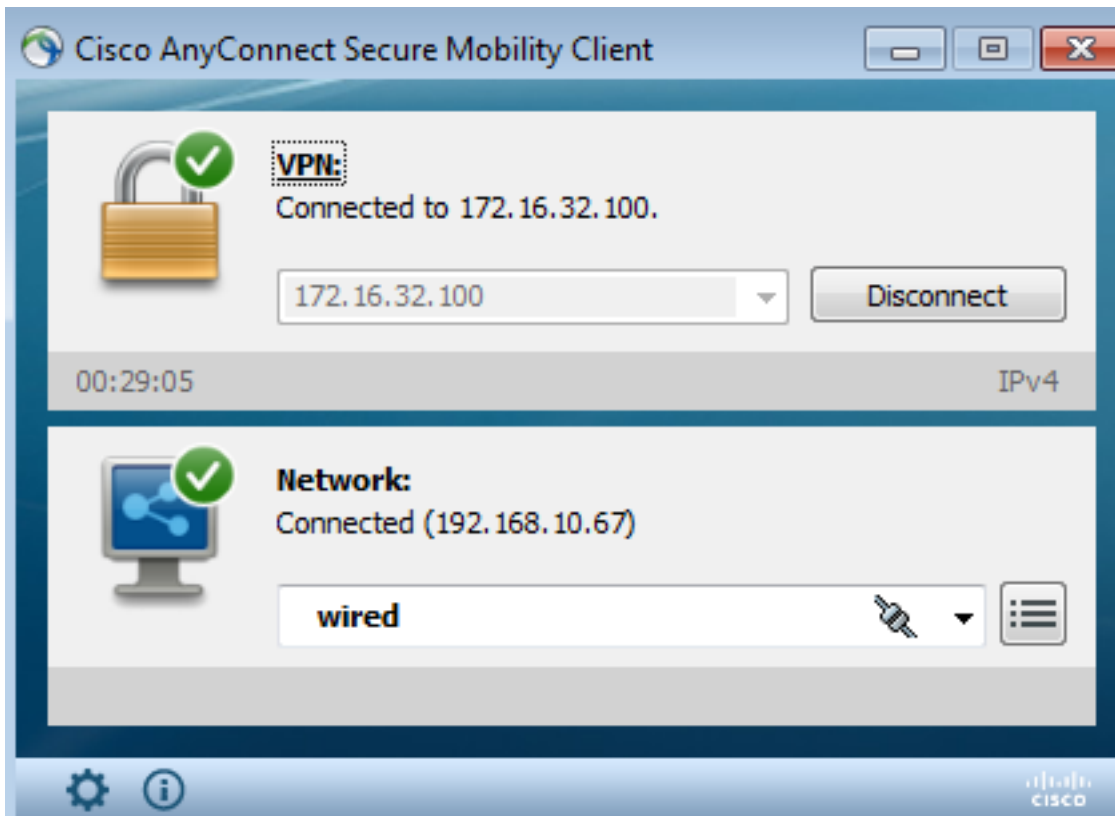
[Edit Policy Order...](#)

## 確認

このセクションでは、設定が正常に機能していることを確認します。

## ステップ 1 : VPN セッション

VPN ユーザが ASA-VPN への VPN セッションを開始します。



ASA-VPN は認証に ISE を使用します。ISE がセッションを作成し、SGT タグ 2 ( IT ) を割り当てます。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes "Home", "Operations", "Policy", "Guest Access", and "Administration". Below that, there are tabs for "Authentications", "Reports", "Adaptive Network Control", and "Troubleshoot". The main content area shows "Show Live Authentications" with a refresh button. Below that is a table with the following columns: "Initiated", "Updated", "Session Status", "CoA Action", "Endpoint ID", "Identity", "IP Address", and "Security Group". The table contains one row of data: "2015-05-06 19:17:50...", "2015-05-06 19:17:55...", "Started", a dropdown menu, "192.168.10.67", "cisco", "172.16.32.50", and "IT".

認証に成功すると、ASA-VPN が ( cisco-av-pair の Radius Access-Accept で返される ) SGT タグ 2 を使用して VPN セッションを作成します。

```
asa-vpn# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      : cisco                Index      : 2
Assigned IP   : 172.16.32.50          Public IP  : 192.168.10.67
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 12979961             Bytes Rx   : 1866781
```

```
Group Policy : POLICY Tunnel Group : SSLVPN
Login Time : 21:13:26 UTC Tue May 5 2015
Duration : 6h:08m:03s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : ac1020640000200055493276
Security Grp : 2:IT
```

ASA-VPN と ASA-FW 間のリンクは TrustSec に対応していないため、ASA-VPN からそのトラフィックのタグなしフレームが送信されます ( この場合 CMD/TrustSec フィールドがインジェクトされたイーサネット フレームを GRE によりカプセル化することができません )。

## ステップ 2 : WSA により取得されるセッション情報

この段階で、WSA は IP アドレス、ユーザ名、および SGT 間のマッピングを ( pxGrid プロトコルを使用して ) 受信しているはずですが。

```
wsa.example.com> isedata

Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
[ ]> CACHE

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[ ]> SHOW

IP                Name                SGT#
172.16.32.50      cisco                2

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[ ]> █
```

## ステップ 3 : WSA へのトラフィック リダイレクション

VPN ユーザが sport.pl への接続を開始し、これが ASA-FW によりインターセプトされます。

```
asa-fw# show wccp

Global WCCP information:
  Router information:
    Router Identifier: 172.16.33.110
    Protocol Version: 2.0

  Service Identifier: 90
```

```
Number of Cache Engines:          1
Number of routers:                1
Total Packets Redirected:      562
Redirect access-list:             wccp-redirect
Total Connections Denied Redirect: 0
Total Packets Unassigned:         0
Group access-list:                wccp-routers
Total Messages Denied to Group:   0
Total Authentication failures:    0
Total Bypassed Packets Received:  0
```

```
asa-fw# show access-list wccp-redirect
```

```
access-list wccp-redirect; 3 elements; name hash: 0x9bab8633
access-list wccp-redirect line 1 extended deny tcp any host 172.16.32.204 (hitcnt=0)
0xfd875b28
access-list wccp-redirect line 2 extended permit tcp any any eq www (hitcnt=562)
0x028ab2b9
access-list wccp-redirect line 3 extended permit tcp any any eq https (hitcnt=0)
0xe202a11e
```

また、GRE で WSA へトンネリングされます ( WCCP ルータ ID が、設定されている最も大きい IP アドレスであることに注意してください )。

```
asa-fw# show capture
```

```
capture CAP type raw-data interface inside [Capturing - 70065 bytes]
match gre any any
```

```
asa-fw# show capture CAP
```

```
525 packets captured
```

```
1: 03:21:45.035657      172.16.33.110 > 172.16.32.204: ip-proto-47, length 60
2: 03:21:45.038709      172.16.33.110 > 172.16.32.204: ip-proto-47, length 48
3: 03:21:45.039960      172.16.33.110 > 172.16.32.204: ip-proto-47, length 640
```

WSA は TCP ハンドシェイクを続行し、GET 要求を処理します。結果として、PolicyForIT という名前のポリシーに一致し、トラフィックがブロックされます。

Notification: Policy: Destination - Windows Internet Explorer

http://sport.pl/

File Edit View Favorites Tools Help

★ Favorites Notification: Policy: Destination

### This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site ( http://sport.pl/ ) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Wed, 06 May 2015 17:50:15 GMT  
 Username: cisco  
 Source IP: 172.16.32.50  
 URL: GET http://sport.pl/  
 Category: LocalSportSites  
 Reason: BLOCK-DEST  
 Notification: BLOCK\_DEST

これは、WSA Report により確認されます。

**Cisco S000V**  
Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

### Web Tracking

**Search**

**Proxy Services** L4 Traffic Monitor SOCKS Proxy

Available: 06 May 2015 11:22 to 06 May 2015 18:02 (GMT +00:00)

Time Range: Hour

User/Client IPv4 or IPv6: cisco (e.g. jdoe, DOMAIN/jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type: Blocked

Advanced Current Criteria: Policy: PolicyForIT.

Clear Search

Generated: 06 May 2015 18:03 (GMT) Printable Download

**Results**

Displaying 1 - 3 of 3 items.

Time (GMT +00:00)	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
06 May 2015 18:02:22	http://sport.pl (2)	(2)	Block - URL Cat	0B	cisco 172.16.32.50
06 May 2015 17:50:15	http://sport.pl (2)	(2)	Block - URL Cat	0B	cisco 172.16.32.50
06 May 2015 17:48:36	http://sport.pl (2)	(2)	Block - URL Cat	0B	cisco 172.16.32.50

Displaying 1 - 3 of 3 items.



ISE がユーザ名を表示していることに注意してください。

## トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

### 誤った証明書

WSA が正しく初期化されていない場合 (証明書)、ISE 接続で障害が発生しているかどうかを確認するためのテストを行います。

#### Test Communication with ISE Server

Start Test

Validating ISE Portal certificate ...

Success: Certificate validation successful

Checking connection to ISE PxGrid server...

**Failure: Connection to ISE PxGrid server timed out**

**Test interrupted: Fatal error occurred, see details above.**

### ISE pxgrid-cm.log レポート

```
[2015-05-06T16:26:51Z] [INFO ] [cm-1.jabber-172-16-31-202]
[TCPSocketStream::_doSSLHandshake] [] Failure performing SSL handshake: 1
```

障害の原因は、Wireshark で確認できます。

Source	Destination	Protocol	Info
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=66429032 TSecr=21743402
172.16.32.204	172.16.31.202	XMPP/XML	STREAM > xgrid.cisco.com
172.16.31.202	172.16.32.204	TCP	xmpp-client > 34491 [ACK] Seq=1 Ack=121 Win=14592 Len=0 TSval=21743403 TSecr=66429032
172.16.31.202	172.16.32.204	XMPP/XML	STREAM < xgrid.cisco.com
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=121 Ack=179 Win=131584 Len=0 TSval=66429032 TSecr=21743403
172.16.31.202	172.16.32.204	XMPP/XML	FEATLRES
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=121 Ack=362 Win=131584 Len=0 TSval=66429032 TSecr=21743403
172.16.32.204	172.16.31.202	XMPP/XML	STARTTLS
172.16.31.202	172.16.32.204	XMPP/XML	PROCEED
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=172 Ack=412 Win=131712 Len=0 TSval=66429072 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TCP	[TCP segment of a reassembled PDU]
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=290 Ack=1860 Win=130904 Len=0 TSval=66429082 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=290 Ack=3260 Win=130968 Len=0 TSval=66429082 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done, Ignored Unknown Record
172.16.31.202	172.16.32.204	TLSv1	Ignored Unknown Record
172.16.32.204	172.16.31.202	TLSv1	Client Hello, Alert (Level: Fatal, Description: Unknown CA), Alert (Level: Fatal, Description: Unknown CA)

> Frame 21: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)  
 > Ethernet II, Src: Vmware\_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware\_58:cb:ad (00:0c:29:58:cb:ad)  
 > Internet Protocol Version 4, Src: 172.16.32.204 (172.16.32.204), Dst: 172.16.31.202 (172.16.31.202)  
 > Transmission Control Protocol, Src Port: 34491 (34491), Dst Port: xmpp-client (5222), Seq: 297, Ack: 3310, Len: 14  
 > [3 Reassembled TCP Segments (139 bytes): #13(118), #18(7), #21(14)]

Secure Sockets Layer  
 > TLSv1 Record Layer: Handshake Protocol: Client Hello  
 > TLSv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)  
 > TLSv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)  
 > TLSv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)

( pxGrid により使用される ) Extensible Messaging and Presence Protocol ( XMPP ) 交換を保護するために使用される SSL セッションで、サーバが提示する不明な証明書チェーンが原因で、クライアントから SSL エラーが報告されます。

## 正しいシナリオ

正しいシナリオについては、ISE pxgrid-controller.log に次のように記録されています。

```
2015-05-06 18:40:09,153 INFO [Thread-7][] cisco.pxgrid.controller.sasl.SaslWatcher
-:~::~:- Handling authentication for user name wsa.example.com-test_client
また、正しい機能を備えたサブスクリバとして WSA が ISE GUI に示されます。
```

Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-ise14		Capabilities(2 Pub, 1 Sub)	Online	Administrator	<a href="#">View</a>
ise-mn1-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator	<a href="#">View</a>
Ironport.example.com-pxgr...	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	<a href="#">View</a>

**Capability Detail** 1 - 2 of 2 Show 25

Capability Name	Capability Version	Messaging Role	Message Filter
SessionDirectory	1.0	Sub	
TrustSecMetaData	1.0	Sub	

wsa.example.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	<a href="#">View</a>
-----------------------------	----------------------------	----------------------------	---------	---------	----------------------

## 関連情報

- [ASA バージョン 9.2.1 VPN ポスチャおよび ISE の設定例](#)
- [WSA 8.7 ユーザ ガイド](#)
- [ASA および Catalyst 3750X シリーズ スイッチ TrustSec の設定例およびトラブルシューティング ガイド](#)
- [Cisco TrustSec スイッチ コンフィギュレーション ガイド Cisco TrustSec について](#)
- [セキュリティ アプライアンスのユーザ承認用の外部サーバの設定](#)
- [Cisco ASA シリーズ VPN CLI 構成ガイド 9.1](#)
- 『[Cisco Identity Services Engine User Guide, Release 1.2 \( Cisco Identity Services Engine ユーザ ガイド リリース 1.2 \)](#)』
- [テクニカル サポートとドキュメント – Cisco Systems](#)