

シスコ共通ポリシー統合ガイド

2025 年 7 月 22 日

ドキュメントの目的と使用方法

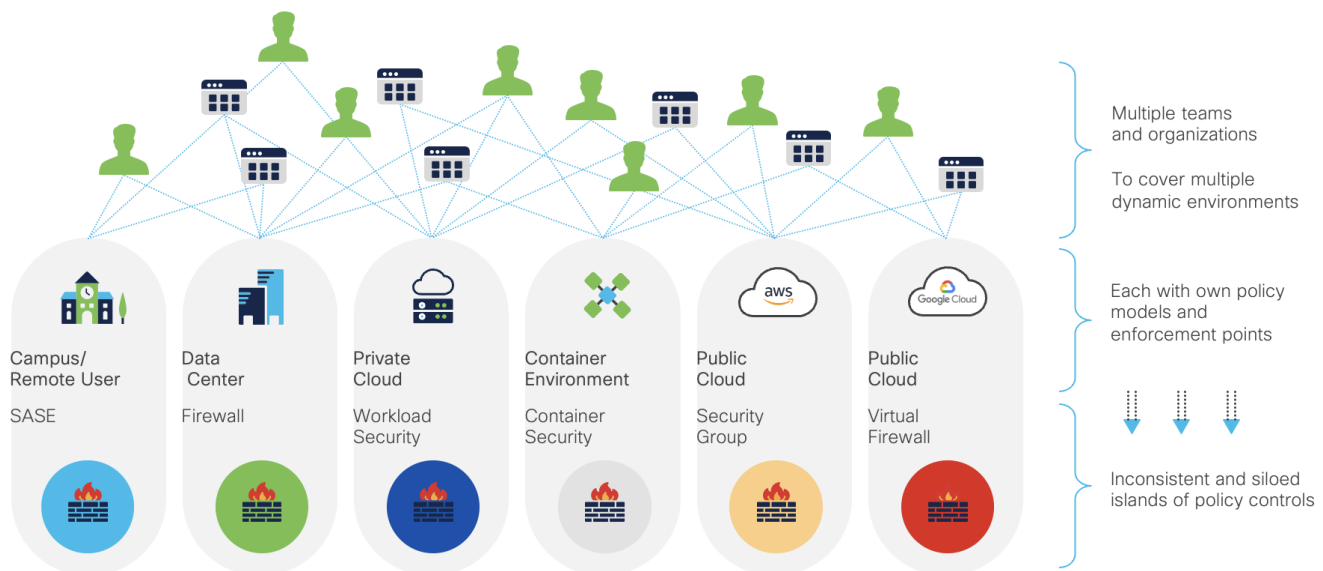
このドキュメントの目的は、シスコシステムズが推奨する一般的な共通ポリシー導入プロファイルの概要を示すことです。SD-Access ネットワークを管理するための **Catalyst Center**、SD-WAN ファブリックを管理するための **SD-WAN Manager**、**Application Centric Infrastructure (ACI)** データセンターを管理するための **Cisco Application Policy Infrastructure Controller (APIC)**、および **Cisco Firepower** プラットフォームを管理するための **Cisco Secure Firewall Management Center** (旧 **Firepower Management Center**) を含む、一般的な展開のガイドラインを提供します。導入エンジニアがサービス要件を理解するのに役立つように、このドキュメントの理論的なセクションと実践的なセクションを組み合わせる必要があります。このドキュメントは、導入エンジニアが導入および設定時にネットワークに関する最適な決定を下すのにも役立ちます。

ターゲット層

この共通ポリシープロファイルのターゲット層は、ネットワークのエンジニアリングと運用を担当する技術スタッフ、および実装チームです。

はじめに

パンデミック以降のハイブリッドワークスペースの大幅な増加により、プライベートデータセンターとパブリッククラウドの両方でホストされているアプリケーションにアクセスするリモートワーカーと社内ワーカーが増加しました。さらに、多くの IoT デバイスが企業ネットワークに接続されているため、ユーザーとデバイスのトラフィック保護の複雑さがさらに増えています。ハイブリッド環境全体に一貫したセキュリティポリシーを適用することは、各ドメインに独自のポリシーモデルと適用ポイントがあるため、複雑となり、不整合となることがよくあります。たとえば、キャンパスおよびリモートユーザー、データセンター、プライベートクラウドおよびパブリッククラウド内のワークロードには、それぞれ異なるポリシー適用ポイントを設定できます。その結果、アクセスポリシーはサイロ化されたものになります。



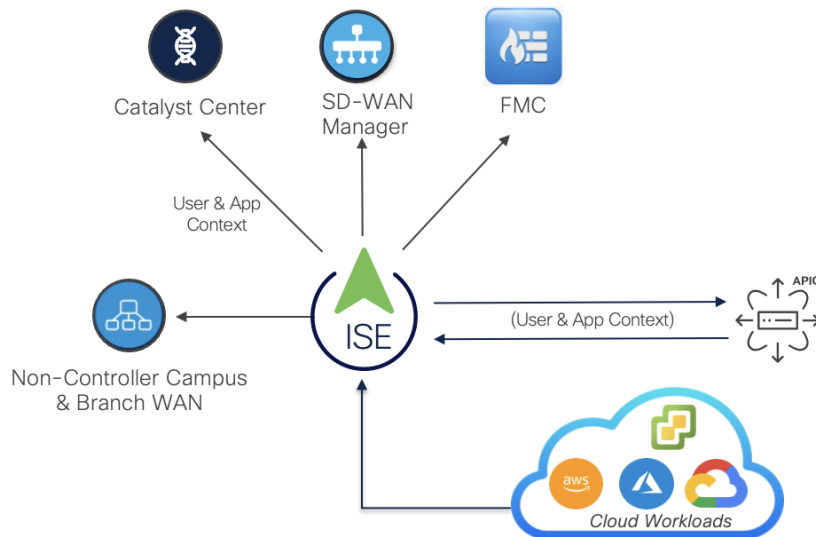
共通ポリシーアーキテクチャは、ユーザー、エンドポイント、およびアプリケーションに関するコンテキスト情報をドメイン間で共有できるようにすることで、この懸念に対処します。これにより、IT セキュリティ管理者は、さまざまな適用ポイントで一貫したアクセスポリシーを作成して適用できます。

このガイドでは、**Cisco Identity Services Engine (ISE)** がハブとして機能し、各ドメインで共有および理解できるコンテキスト情報を正規化する、検証済みの共通ポリシーソリューションについて説明します。このソリューションテストでは、ISE は **Catalyst Center**、**SD-WAN Manager**、**Cisco Secure Firewall Management Center (FMC)** などのさまざまなコントローラとすでに統合されています。次に、ISE は **Application Centric Infrastructure (ACI)** およびクラウドプロバイダーと接続されます。**Cisco ACI** から受信したコンテキスト情報は、ISE 上でセキュリティグループタグ (SGT) として正規化され、ISE エコシステムと共有されます。ACI と共有されるキャンパス SGT は、外部エンドポイントグループ (EPPG) に変換されます。コンシューマとプロバイダーのコントラクトは、ACI のポリシー適用に関する EPPG に適用できます。さらに、ISE は **AWS**、**Azure**、**GCP**、および **vCenter** の展開に接続して、ワークロード情報をダウンロードし、SGT をワークロードに割り当てることができます。このソリューションテストでは、ドメイン間のコンテキスト交換と、さまざまな適用ポイントに適用される一貫したポリシーの適用を検証します。

共通ポリシーの概要

共通ポリシーフレームワークは、ハイブリッド環境で一貫したポリシーを実現します。共有ポリシーで、**Cisco ISE** はハブとして機能し、コンテキスト情報を学習して正規化し、複数のドメインとコンテキストを共有します。**ISE** は、ワークロードコネクタを介して **ACI** と **AWS**、**Azure**、**GCP**、および **vCenter** の展開へのセキュアな接続を形成します。

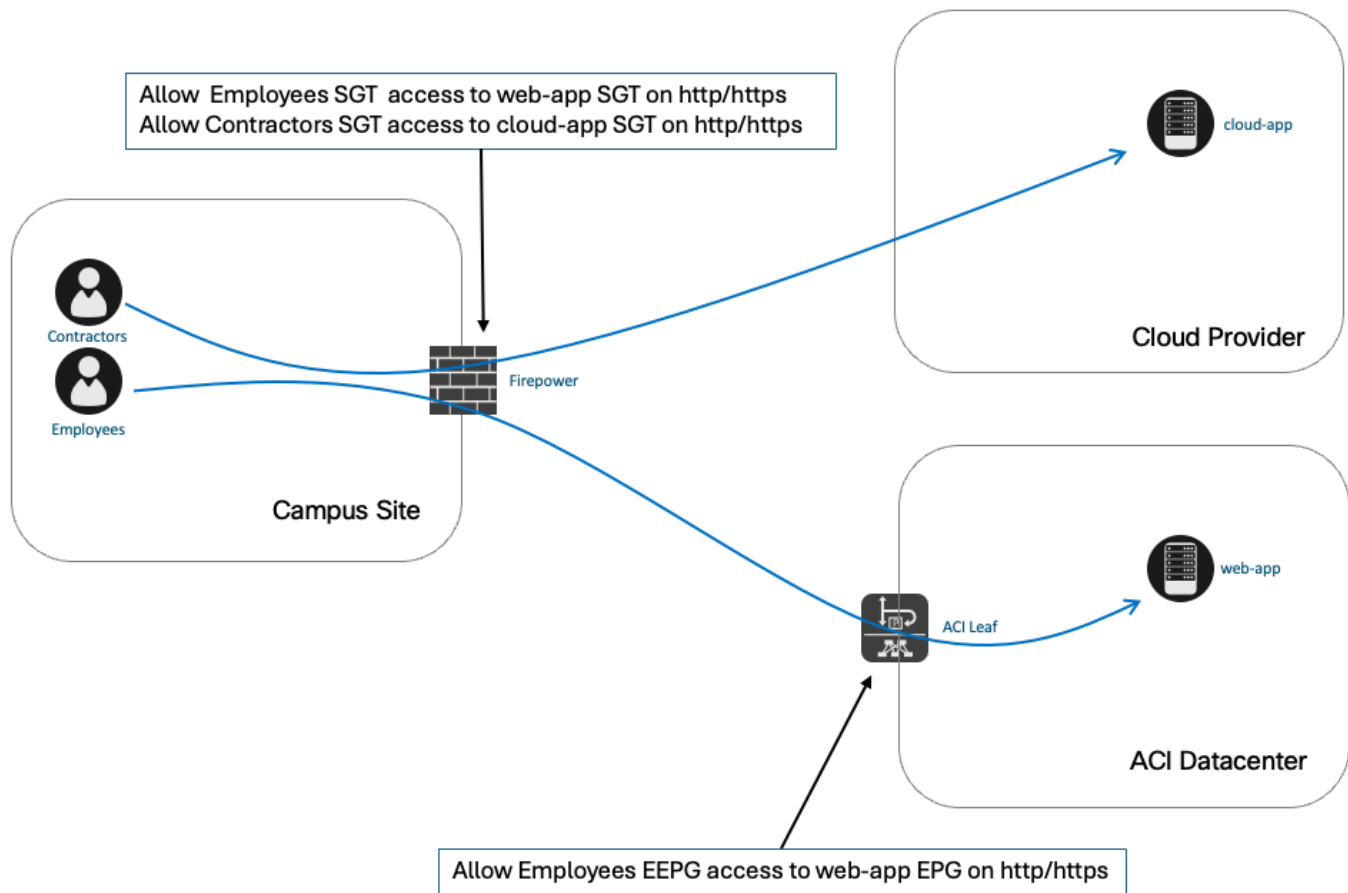
ポリシーは、データセンター、キャンパス、**SD-WAN** エッジ、または **Cisco Firepower** のどこにあるかに関係なく、ネットワークのさまざまな適用ポイントに適用できます。



共通ポリシーアーキテクチャを有効にする **ISE 3.4** パッチ 1 の機能には、次のものが含まれます。

- **ISE ACI** コネクタは、**Cisco APIC** への接続を作成してエンドポイントグループ (EPG) とエンドポイントセキュリティグループ (ESG) を検出し、これらを **SGT** にマッピングします。
- **ISE Cloud Connector** は、**vCenter**、**AWS**、**Azure**、および **GCP** の展開への接続を作成して、アプリケーションワークロード、仮想マシンを学習し、それらを **SGT** にマッピングします。
- **ISE** はその後、コンテキスト (IP から **SGT** へのバインディング) を **pxGrid** の宛先 (**Catalyst Center**、**SD-WAN Manager**、**Cisco FMC**、**APIC**) または **SXP** デバイスに通信して、さまざまなドメインの適用ポイントで一貫したポリシーを適用できるようにします。

この使用例は、ネットワーク内のさまざまな適用ポイントでポリシーを適用できる柔軟性を示しています。



キャンパスサイトのファイアウォールにより、ネットワークに接続する従業員として分類されたユーザーは、データセンター内の **Web** アプリケーション (**Web** アプリケーション **SGT** として分類) にアクセスできます。また、ファイアウォールは、請負業者として分類されたユーザーにのみ、クラウドアプリケーション (ワークロード分類ルールによって「クラウドアプリケーション」**SGT** として分類) にアクセスすることを許可します。

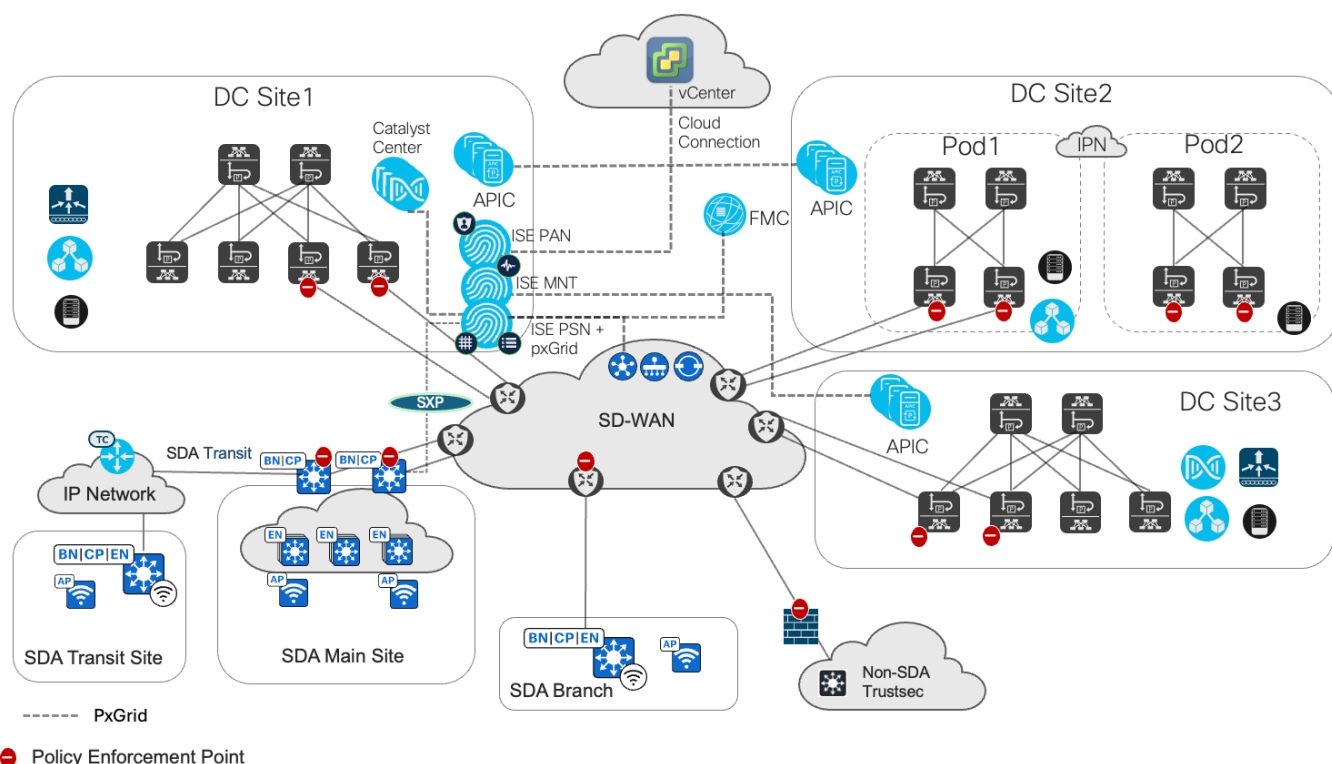
さらに、**APIC** は、ポリシーを **ACI** リーフスイッチに適用して、従業員ユーザー (従業員 **EEPG** として分類) のみに **Web** アプリ **EPG** へのアクセスを許可することができます。

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアで検証されています。

ロール	Model name	ハードウェア プラットフォーム	ソフトウェアのバージョン	ソフトウェアのバージョン
Catalyst Center コントローラ	DN2-HW-APL	Catalyst Center アプライアンス 3 ノードクラスタ	Cisco Catalyst Center 2.3.7.7	Catalyst Center 2.3.7.9
アイデンティティ管理、 RADIUS サーバー	ISE-VM-K9 Cisco SNS-3600 Cisco SNS-3700	仮想アプライアンスおよび Cisco SNS アプライアンス上の Cisco Identity Services Engine	Cisco Identity Services Engine 3.4 パッチ 1	Cisco Identity Services Engine 3.4 パッチ 1
Cisco SD WAN	SD-WAN Manager	Cisco SD-WAN Manager	20.15.1	20.15.1
	C8300 C8500	Cisco Edge サービスルータ	17.9.5f、17.12.4b、 17.15.1a	17.9.5f、17.12.4b、 17.15.1a
シスココアおよび分散 ノード	C9500H C9600	Cisco Catalyst 9500 シリーズ スイッチ Cisco Catalyst 9600 シリーズ スイッチ	17.9.6a、17.12.4、 17.15.1	17.9.6a、17.12.5、 17.15.3
Cisco アクセスノード	C9300-48P C9300-24P	Cisco Catalyst 9300 シリーズ スイッチ	17.9.6a、17.12.4、 17.15.1	17.9.6a、17.12.5、 17.15.3
シスコ ワイヤレス コントローラ	C9800-40-K9	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	17.9.6、17.12.4、 17.15.1	17.9.6、17.12.5、 17.15.3
Cisco アクセス ポイント	9120-AXI 9130-AXI	Cisco Catalyst アクセスポイント	17.9.6、17.12.4、 17.15.1	17.9.6、17.12.5、 17.15.3
Cisco Firepower Threat Defense セ キュリティアプライ アンス	FPR2110	Firepower 2100	7.2.5	7.2.5
Cisco Secure Firewall Management Center	FMCv	Cisco Firewall Management Center Virtual	7.2.5	7.2.5
Cisco APIC コント ローラ	APIC-SERVER- M3	Cisco APIC アプライアンス	6.1.2	6.1.2
Cisco ACI スイッチ	N9K-C93240YC- FX2 N9K-C9332C	Cisco Nexus 9000 ACI モード スイッチ	16.1.2	6.1.2

ソリューショントポロジ



共通ポリシーソリューションの検証に使用されるソリューションのテストベッドは、3つの **ACI** データセンター、**SD-Access** サイト、および **SD-Access** なしの **TrustSec** サイトで構成されます。適用ポイントは、**ACI** ボーダーリーフ、**SD-Access** ファブリックボーダー、**SD-WAN** エッジ、および **Cisco Firepower** デバイスです。

3つの **ACI** データセンターは、個別の **ACI** ファブリックを持ち、サイト間でレイヤ 3 のみの接続を介したマルチファブリック設計を使用します。各 **ACI** ファブリックは一意的な IP サブネットで自律し、レイヤ 3 Out (L3Out) データパスを介して他の **ACI** ファブリックへのレイヤ 3 接続を確立します。

注： L3Out は、マルチポッドファブリックの両方のポッドでボーダーリーフを使用して展開できます。

メインキャンパスサイトとブランチキャンパスサイトは、**Cisco SD-WAN** ファブリックを介して接続されています。データプレーン、コントロールプレーン、およびポリシープレーンの統合は、**SD-Access** ボーダーノードと **Cisco SD-WAN** エッジデバイス間の **eBGP**、**VRF-Lite**、およびインライン **SGT** を使用して実現されます。展開手順は、『[Cisco SD-Access | SD-WAN Independent Domain Pairwise Integration Prescriptive Deployment Guide](#)』に基づいています。

SXP は、各仮想ネットワーク (VN) の **ISE** と **SD-Access** メインサイトボーダーノードの間に設定されます。**SXP** サブスクリプションから学習した **SGT** は、**SD-Access** ファブリックと **SD-WAN** エッジにインラインで伝播され、**SD-Access** および **SD-WAN** ファブリック全体で一貫したポリシープレーンを維持します。

ソリューションの使用例

カテゴリ	使用例
ISE の統合	ISE と ACI の統合
	ACI マルチテナントとマルチ VRF
	ACI ファブリック間でのコンテキスト交換
	ISE と Catalyst Center の統合
	ISE と SD-WAN Manager の統合
	ISE と Cisco Secure Firewall Management Center の統合
ポリシーの実施	ACI リーフスイッチでのポリシーの適用
	SD-Access ボーダーノードでのポリシーの適用
	SD-WAN エッジノードでのポリシーの適用
	Firepower アプライアンスでのポリシーの適用
ネットワークの堅牢性	リンク障害
	ノード障害
Day-N 運用	設定の追加、削除、および変更
IPv6 のシナリオ	IPv6 バインディングのコンテキスト交換

スケール

このソリューションのテストでは、次の表に示すスケールの数値について確認しました。

表 1. ACI ファブリックごとのスケール

パラメータ	スケール
ACI テナント	10
ACI VRF	50
EPG	500
IPv4 + IPv6 の最大組み合わせ数	64,000
エンドポイントの数	32,000
ISE から L3Out への SGT の数 (EEPG として)	500
EEPG ごとのマッピング数	8000

ACI では、ISE からの IP-SGT バインディングの受信上限は 64,000 です。ISE スケール情報については、[「Performance and Scalability Guide for Cisco Identity Services Engine」](#)を参照してください。

- Cisco ISE and Cisco application centric infrastructure scaling
- Cisco ISE workload connector scaling

ソリューションの基調講演

ISE の統合

このセクションでは、ワークロードコネクタを使用した **ACI** およびクラウドプロバイダーへの **ISE** の統合、および他のドメインコントローラ、**Catalyst Center**、**SD-WAN Manager**、**FMC** との **ISE** 統合について説明します。

Cisco ISE と ACI の統合

Cisco ISE と **ACI** の統合は、共通ポリシーアーキテクチャの一部です。この統合を有効にするには、**Cisco ISE** と **Cisco APIC** の間にセキュアな接続を構築します。**ISE** は、ワークロードコンテキストをインポートし、コンテキストを **SGT** に正規化し、コンテキストを他のドメインと共有して、一貫したポリシーを構築します。

Cisco ISE 3.4 パッチ 1 および **ACI リリース 6.1(2)** での **Cisco ISE** と **ACI** の統合では、次の機能がサポートされます。

- 複数の **Cisco ACI** ファブリック（個別またはマルチポッド）
- **Cisco ACI** マルチテナント、マルチ **VRF**、および複数の **L3Out**
- **VRF** 間および共有の **L3Out**
- 異なる **ACI** ファブリック間でのコンテキスト共有
- **ISE** は、**ACI** コントラクトを学習し、管理者が共有 **SGT**（**EEPG**）とともに既存のコントラクトを選択できるようにします。

ISE は、**EPG** と **ESG** を **Cisco ISE** の **SGT** に同期することで、**Cisco ACI** ドメインから **TrustSec** ドメインに着信するパケットをサポートします。**EPG** と **ESG** に関連付けられた **ACI** エンドポイントは、**Cisco ISE** の対応する **IP-SGT** バインドにマッピングされます。

Cisco ACI は、**SGT** を **EEPG** に同期し、受信 **IP-SGT** バインディングに基づいたエンドポイント バインディングを作成することで、**TrustSec** ドメインから **Cisco ACI** ドメインに届くパケットをサポートします。

ISE 前提条件：

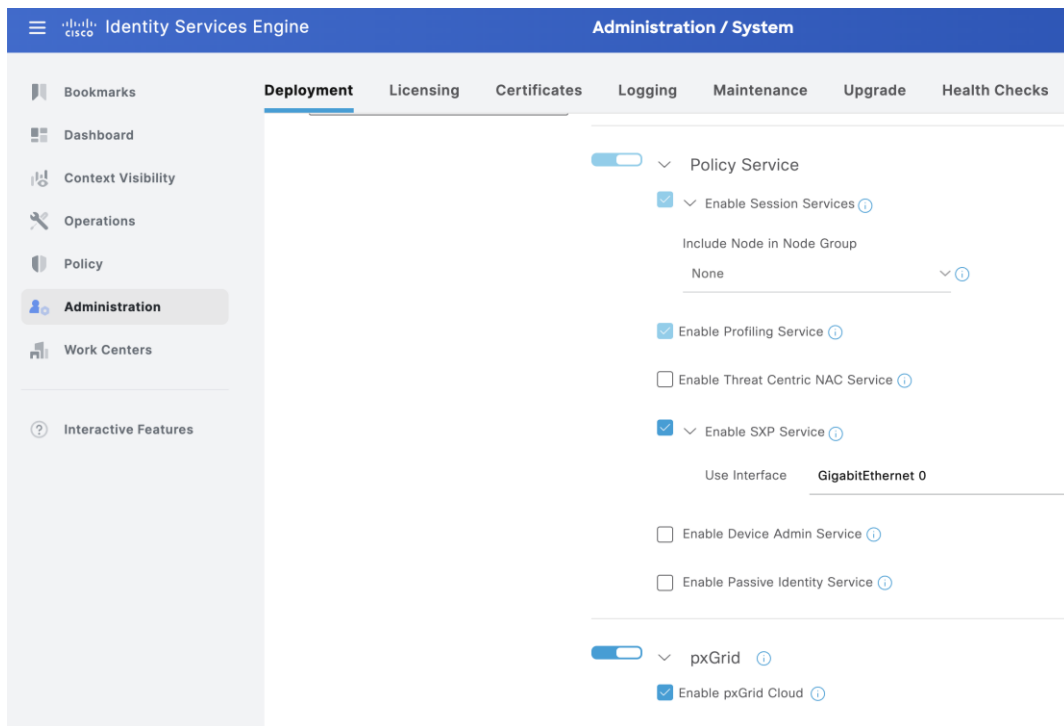
- **pxGrid** および **SXP** サービスが有効になっています。
- **DNS** は、**APIC** ノードのホスト名を解決するように設定されています。
- 従来の **ACI** 統合が存在する場合は削除します。

ACI 前提条件：

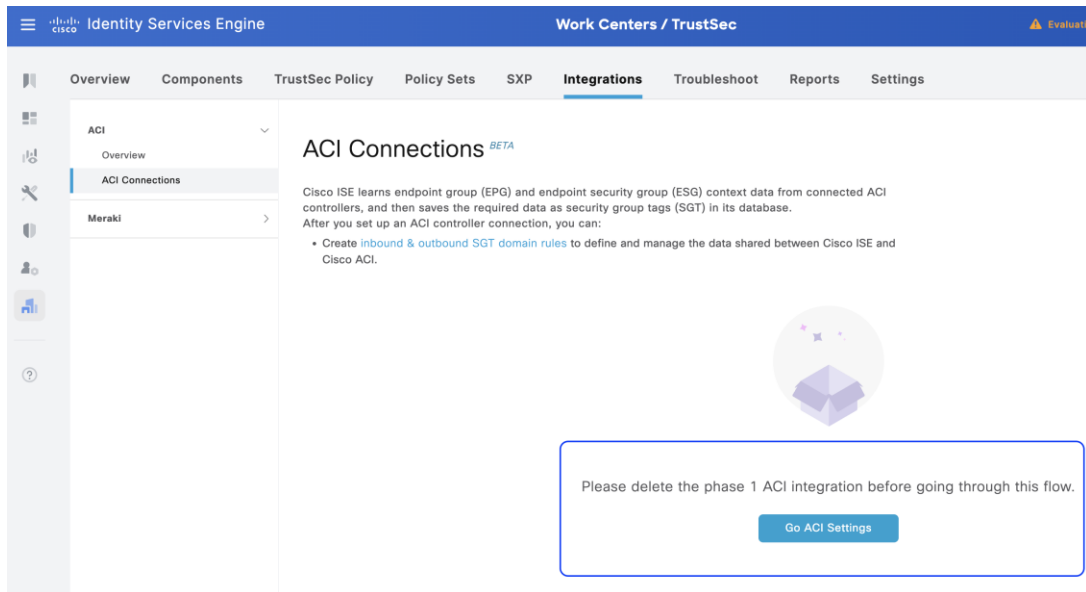
- テナント、**VRF**、アプリケーション **EPG** または **ESG**、**L3Out**、およびコントラクトは、すでに **APIC** で設定されています。
- **DNS** は、**ISE pxGrid** ホスト名を解決するように設定されています。

手順 1. **Cisco ISE** と **ACI** を統合するには：

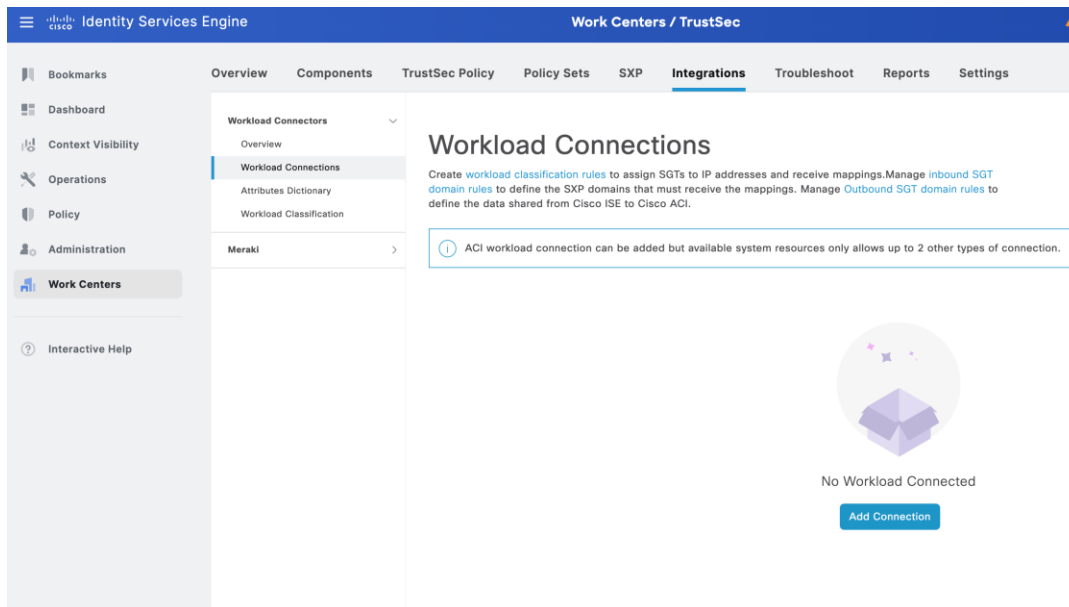
ステップ 1. **[Administration] > [Deployment] > [Deployment Node]** で、**[Enable SXP Service]** と **[Enable pxGrid Cloud]** を選択します。



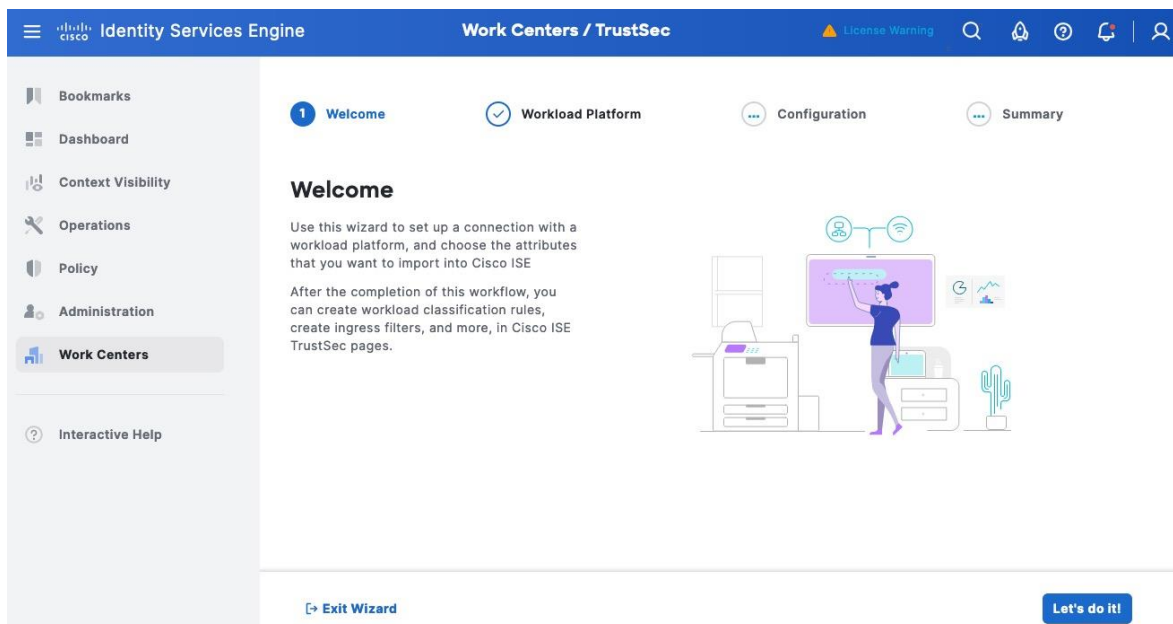
ステップ 2. 従来の ACI 統合が存在する場合は削除します。



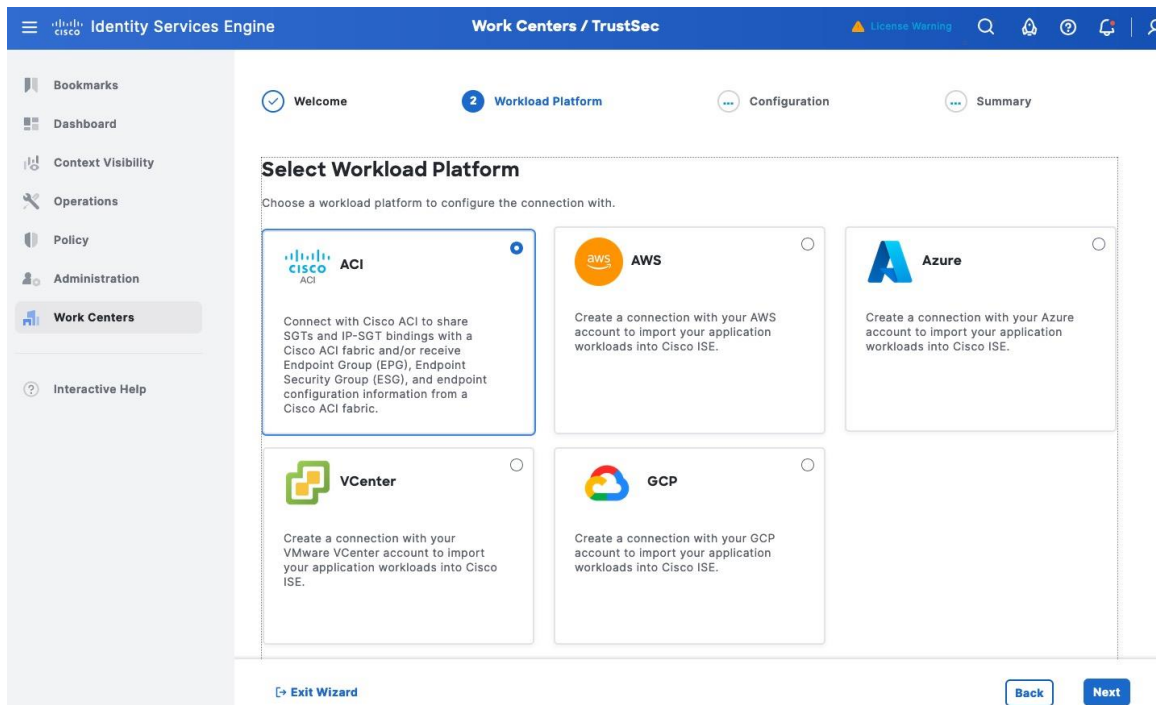
ステップ 3. [Work Centers] > [Workload Connections] で、[Add Connection] をクリックします。



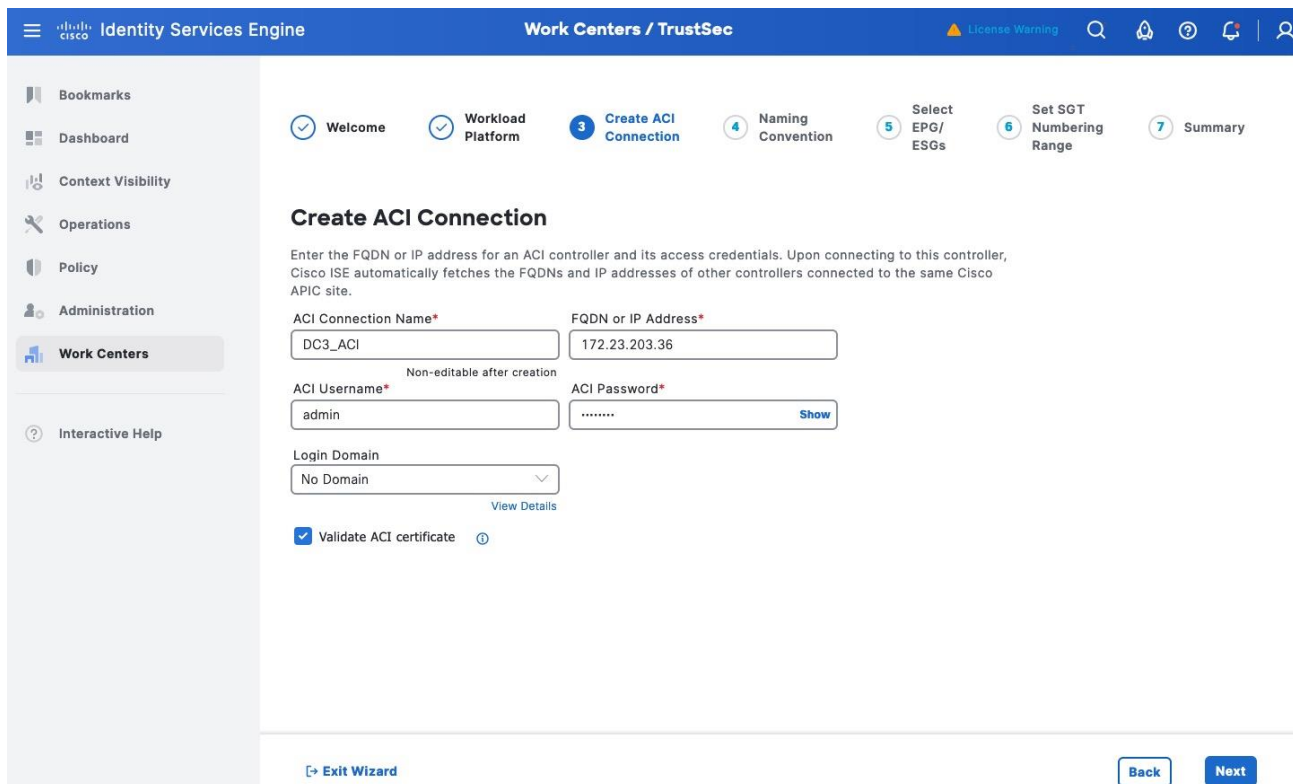
ステップ 4. [Welcome] ウィンドウの [Add Connection] で、[Let's do it] をクリックします。



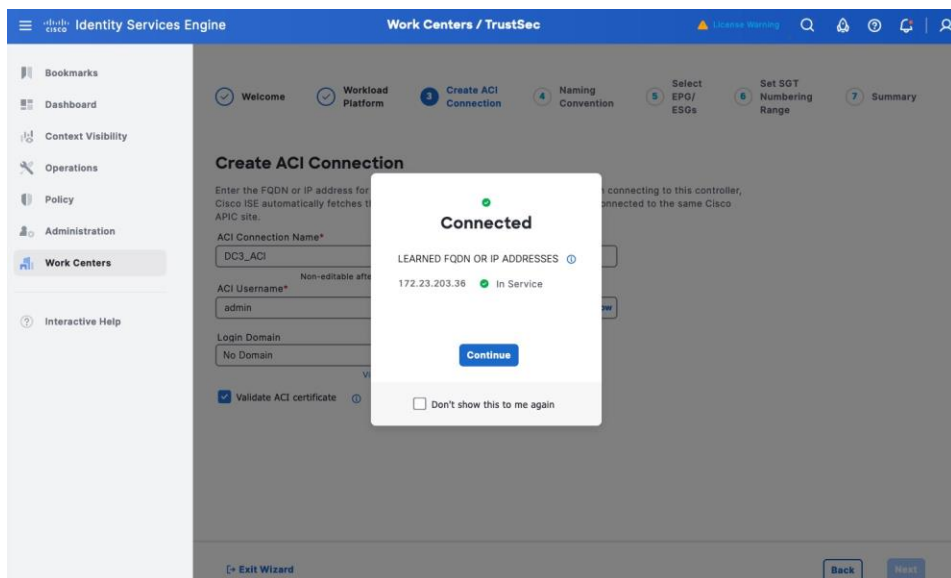
ステップ 5. ワークロードプラットフォームとして [Cisco ACI] を選択します。



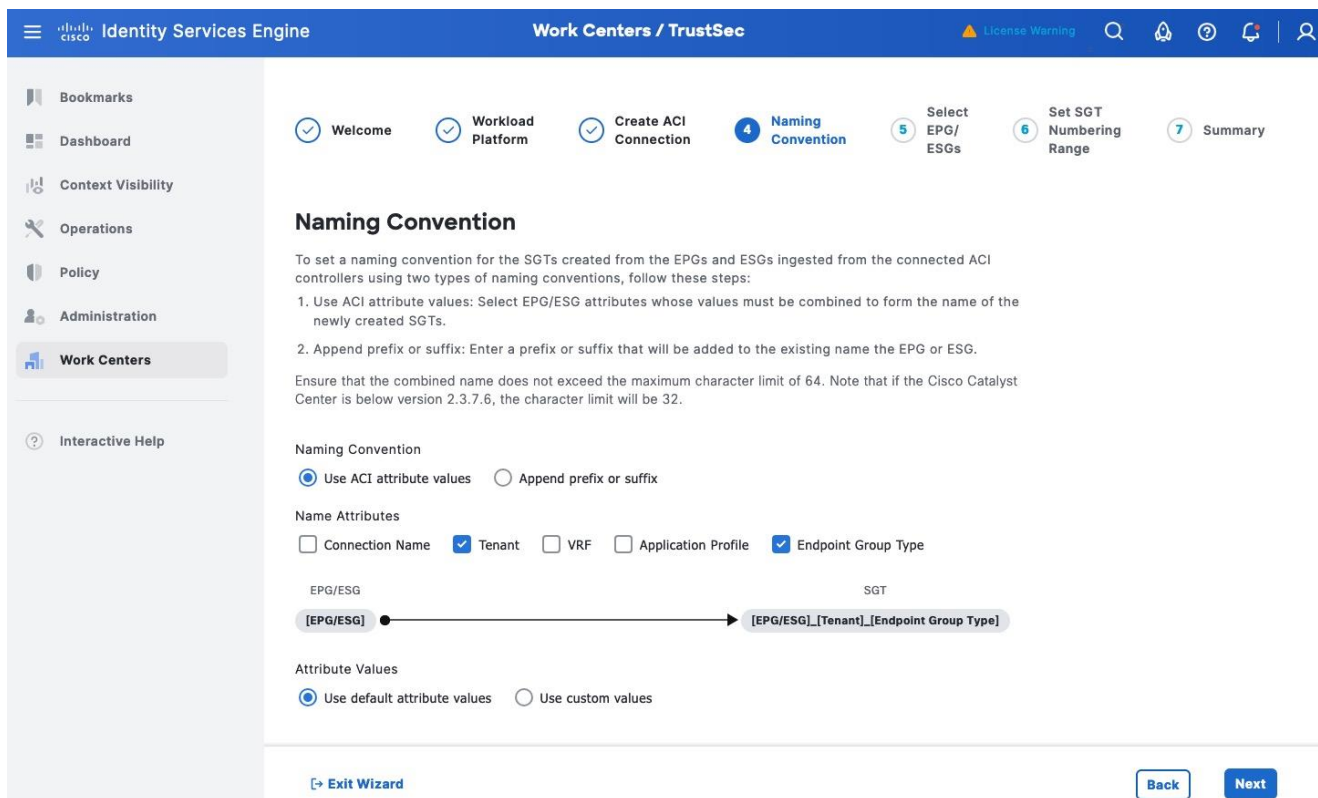
ステップ 6. ACI 接続を設定します。



- ACI 証明書の検証が必要な場合は、[Validate ACI certificate] チェックボックスをオンにします。ACI 証明書を ISE の証明書信頼ストアに追加する必要があります。
- 接続が成功すると、[Connected] ステータスが表示されます。[Continue] をクリックします。



ステップ 7. SGT の命名規則を選択します。属性は、**Connection Name**、**Tenant**、**VRF**、**Application Profile**、および **Endpoint Group Type** に基づいている場合があります。



ステップ 8. EPG と ESG を選択します。

Identity Services Engine Work Centers / TrustSec

License Warning

Welcome Workload Platform Create ACI Connection Naming Convention **Select EPG/ESGs** Set SGT Numbering Range Summary

Select EPG/ESGs

Choose the EPGs and ESGs to be fetched into Cisco ISE and converted to SGTs. You cannot choose the select all option if the number of listed EPG/ESGs is greater than the numbering range configured. Note that a number from the configured range is allotted only to newly created SGTs. If an SGT name populated from this connection already exists in the Cisco ISE database, the SGT isn't assigned a new number.

Q VRF1

2 Selected

	EPG/ESG name	Generated SGT Name	Tenant	VRF	Application Profile	Endpoint Group Type
☒	DC3-APP	DC3_APP_TENANT_1_EPG	TENANT-1	VRF1	DC3_VRF1_APP_PROF	EPG
☐	DC3-T2-APP	DC3_T2_APP_TENANT_2_EPG	TENANT-2	VRF1-T2	DC3-VRF1_APP_PROF_T2	EPG
☐	DC3-T2-WEB	DC3_T2_WEB_TENANT_2_EPG	TENANT-2	VRF1-T2	DC3-VRF1_APP_PROF_T2	EPG
☒	DC3-WEB	DC3_WEB_TENANT_1_EPG	TENANT-1	VRF1	DC3_VRF1_APP_PROF	EPG

26 Record(s) Show Records: 10 1 - 10 1 2 3

Exit Wizard Back Next

注： 管理者は、ACI 接続から EPG/ESG および対応する IP バインディングを選択できます。EGP/ESG が選択されていない場合、接続は作成時に一時停止状態のままになります。

ステップ 9. (オプション) [SGT Numbering Ranges] を予約します。

Identity Services Engine Work Centers / TrustSec

License Warning

Welcome Workload Platform Create ACI Connection Naming Convention Select EPG/ESGs **Set SGT Numbering Range** Summary

Set SGT Numbering Range

Enable this option to manually configure a numbering range for the new SGTs that will be created from the EPGs and ESGs ingested from the ACI connector. When setting a numbering range, account for existing and anticipated EPGs and ESGs.

☒ Set SGT Numbering Range for EPG/ESGs (Optional)

Available Range 19-49, 90-99, 756-2499, 2509-3099, 3300-3999, 4043-4043, 4225-4227, 4251-4309, 4351-5000, 5007-5999, 16000-65534

SGT Numbering Range
3300-3399

Specify ranges from 2-65535, eg. 2-1000

2 new SGTs must be created for the chosen EPGs and ESGs. The current SGT numbering range allows for 100 new SGTs.

OCCUPIED RANGES

Others 0-18, 50-89, 100-255, 256-755, 2500-2508, 4000-4042, 4044-4224, 4228-4250, 4310-4350, 5001-5006, 6000-15999, 65535-65535

DC1_ACI 3100-3199

DC2_ACI 3200-3299

Exit Wizard Back Next

注： デフォルトでは、選択されたすべての SGT に使用可能な SGT タグが自動的に割り当てられます。このオプションは、ACI データセンターから学習した EPG/ESG に特定の SGT を割り当てて、番号範囲でそれらを識別するのに役立ちます。たとえば、3100 番台の SGT は DC1、3200 番台の SGT は DC2 となります。

ステップ 10. [Summary] ウィンドウを確認し、[Create] をクリックして接続を確立します。

Identity Services Engine

Work Centers / TrustSec

License Warning

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Summary

Review the Cisco ISE - ACI Connector configurations defined through this workflow. Click Edit for the section in which you want to change any configurations.

Create ACI Connection

Edit

ACI Connection NameDC3_ACI

FQDN/IP Address172.23.203.36

ACI Usernameadmin

Learned FQDN or IP Addresses172.23.203.36

Login Domain

ACI Password*****

Naming Convention

Edit

Naming ConventionNAME

Name AttributesTenant,Endpoint Group Type

EPG/ESG

SGT

[EPG/ESG]

Attribute ValuesDEFAULT

[EPG/ESG].[Tenant].[Endpoint Group Type]

Select EPG/ESGs

Edit

Search Table

EPG/ESG name	Generated SGT Name	Tenant	VRF	Application Profile	Endpoint Group Type
DC3-APP	DC3_APP_TENANT_1_EPG	TENANT-1	VRF1	DC3_VRF1_APP_PROF	EPG
DC3-WEB	DC3_WEB_TENANT_1_EPG	TENANT-1	VRF1	DC3_VRF1_APP_PROF	EPG

2 Record(s)

Show Records: 10

1 - 2

1

Set SGT Numbering Range

Edit

SGT Numbering Range3300-3399

Exit Wizard

Back

Create

ステップ 11. ACI での ISE 統合を確認します。ACI 接続が APIC の [Integrations] > [ISE Integrations] で確立されていることを確認します。

APIC

admin

SystemTenantsFabricVirtual NetworkingAdminOperationsIntegrations

ISE Integrations | Integration Groups

This object was created by the ISE orchestrator. It is recommended to only modify this object using the ISE orchestrator.

ISE Integrations

DC3_AC1

Inter Domain Policy

SummaryConnection DetailsEndpointsConfigurationHistory

Properties

Name: DC3_AC1

Description:

Admin State: publish-and-listen

Connection Mode: coband

Connection Type: pxGrid connection

Username: aci-qjxn65r8

Servers:

IP Address

Domain Name

172.23.203.85

ISE-PSN1.cdp.com

172.23.203.86

ISE-PSN2.cdp.com

Topics:

Topic Name

Role

/topic/com.cisco.aci.binding/DC3_AC1

Publisher

/topic/com.cisco.ise.sxp.binding

Subscriber

インバウンド SGT ドメインルールとアウトバウンド SGT ドメインルールの定義

インバウンド SGT ドメインルール

インバウンド SGT ドメインルールは、管理者が着信 SGT バインディングを特定の SGT ドメインにマップするために使用されます。インバウンド SGT ドメインルールが定義されていない場合、バインディングはデフォルト SGT ドメインに送信されます。デフォルト SGT ドメインは自動的に有効になり、無効にすることはできません。

Identity Services Engine

Work Centers / TrustSec

Evaluation Mode 88 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

OverviewComponentsTrustSec PolicyPolicy SetsSXPIntegrationsTroubleshootReportsSettings

SXP Devices

SGT Domains

Inbound & Outbound SGT Domain Rules

SGT Bindings

Inbound & Outbound SGT Domain Rules

Create inbound and outbound SGT domain rules to define and manage the data shared between Cisco ISE and Cisco ACL.

Inbound SGT Domain Rules

Outbound SGT Domain Rules

Search table

The default rule will be applied to bindings that do not match any customized rule.

+ Add Inbound Rule

As of: Jun 6, 2024 8:10 PM

Inbound Rule Name

Status

Destinations

SGT Bindings

Actions

Default-inbound-rule

default

0

...

1 Record(s)

Show Records: 101 - 1

Save

アウトバウンド SGT ドメインルール

アウトバウンド SGT ドメインルールは、Cisco ISE から Cisco ACI に共有されるデータを定義します。

手順 2. アウトバウンド SGT ドメインルールを定義するには：

ステップ 1. [Work Centers] > [Inbound & Outbound SGT Domain Rules] > [Outbound SGT Domain Rules] の順に選択し、[+ Add Outbound Rule] をクリックします。

管理者は、アウトバウンド SGT ドメインルールを作成して、ACI 接続への IP バインディングを共有するための条件を定義します。

デフォルトでは、ACI は ISE からコンテキストを学習しません。ACI 接続と共有する SGT を決定するために ISE のアウトバウンドルールを設定します。これは、ACI が ISE からコンテキストを学習するために必要です。

ステップ 2. [Outbound Rule Name] に入力します。

ステップ 3. [Destinations] フィールドで、ACI 接続を選択します。

ステップ 4. このルールを適用する [L3 Outs] を選択します。

Add Outbound Rule

Rule Settings

Outbound Rule Name*

to_DC3

Status

☒ Enabled ☐ Disabled

Destination Configuration

Destinations *

DC3_ACI x

Destinations
DC3_ACI

L3 Outs *

L3-OUT-VRF1 (TENANT-1) x

Rule Configuration

SGT Domain: default x

SGT Name: Contractors x, Developers x, Employees x

SGT Name: DC1_SCALE1_VRF1_DC1_ACI_V... x

+ Add AND/OR Statement + Add Condition

[Rule Settings] で、次の 2 つの条件を定義します。

- デフォルト SGT ドメインからの SGT。
- 請負業者、開発者、従業員、または DC1_SCALE_VRF1_DC1（DC1 ACI を通じて学習）に一致する SGT 名は、この DC3 ACI 接続に伝播されます。

選択した SGT ごとに、ISE は設定を ACI にプッシュして、選択した L3Out に EEPG を作成します。条件が定義されると、コントラクト設定を選択するオプションが使用可能になります。ISE は、ACI の EEPG のルールで定義されているプロバイダーと利用者のコントラクトを接続します。

[Rule Configuration] セクションの下で、管理者は選択した SGT に適用する [Consumed Contract] と [Provided Contract] を選択できます。選択した SGT は、選択した L3Out の下に EEPG として ACI に表示されます。コントラクトは EEPG に適用されます。

Contract Configuration

SGT Name	Connection/ Tenant/ L3out	Consumed Contract ⓘ	Provided Contract ⓘ
Contractors	DC3_ACI/ TENANT-1/ L3-OUT-VRF1	TENANT-1 CONTRACT X ⓧ ↓	↓
Developers	DC3_ACI/ TENANT-1/ L3-OUT-VRF1	TENANT-1 CONTRACT X ⓧ ↓	↓
Employees	DC3_ACI/ TENANT-1/ L3-OUT-VRF1	TENANT-1 CONTRACT X ⓧ ↓	↓
DC1_SCALE1_VRF1_DC1_ACI_VRF1	DC3_ACI/ TENANT-1/ L3-OUT-VRF1	Search ☐ common CONTRACT ↓ ☐ common CONTRACT INTERFACE ↓ ☒ TENANT-1 CONTRACT ↓	↓

4 Record(s)

ステップ 5. [Save] をクリックして、新しいアウトバウンドルールを送信します。

Identity Services Engine

Work Centers / TrustSec

License Warning

🔍 🔔 ⓘ ↺

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Overview

Components

TrustSec Policy

Policy Sets

SXP

Integrations

Troubleshoot

Reports

Settings

SXP Devices

SGT Domains

Inbound & Outbound SGT Domain Rules

SGT Bindings

Inbound & Outbound SGT Domain Rules

Create inbound and outbound SGT domain rules to define and manage the data shared between Cisco ISE and Cisco ACI.

Inbound SGT Domain Rules

Outbound SGT Domain Rules

🔍 Search table

+ Add Outbound Rule ↺

Outbound Rule Name ^	Status	Destinations	Actions
to_DC1_VRF1	🟢	DC1_ACI	...
to_DC1_VRF2	🟢	DC1_ACI	...
to_DC2	🟢	DC2_ACI	...
to_DC3	🟢	DC3_ACI	...

4 Record(s) Show Records: 10 ▾ 1 - 4 < ⓘ >

Save

ISE から vCenter の統合

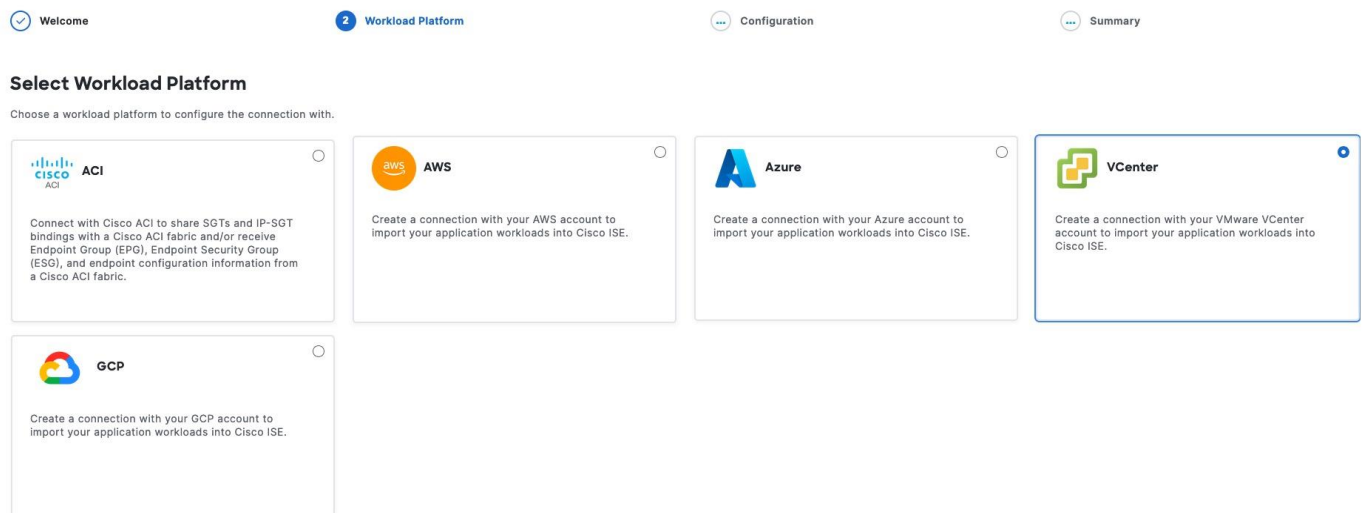
ワークロードコネクタは、ACI への接続の作成に加えて、AWS、Azure、GCP、および vCenter の展開への接続も作成できます。AWS、Azure、および GCP の展開のワークロードコネクタの設定は似ています。

手順 1. ワークロードコネクタを使用して vCenter に接続し、ワークロードを学習するには：

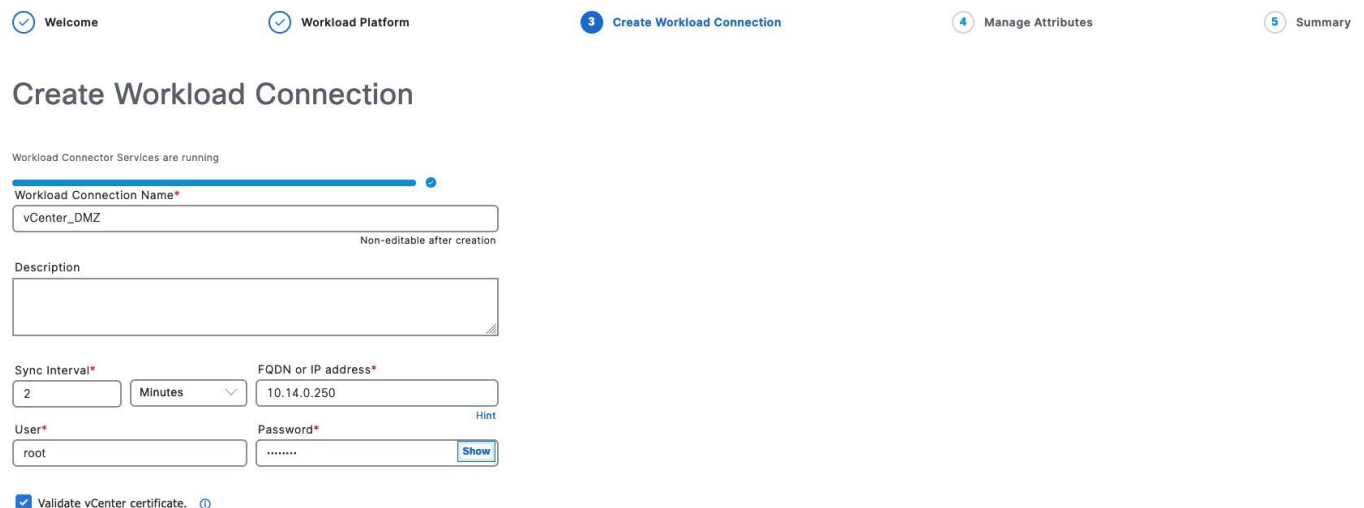
ステップ 1. [Work Centers] > [Integrations] > [Workload Connections] > [+ Add Connection] の順に選択します。

ステップ 2. [Welcome] ウィンドウで、[Let's do it] をクリックします。

ステップ 3. [Workload Platform] で [VCenter] を選択します。



ステップ 4. ワークロード接続のパラメータに入力します。



ステップ 5. [Validate vCenter certificate] を選択した場合は、vCenter 証明書が ISE の信頼できる証明書ストアにアップロードされていることを確認します。

ステップ 6. SGT 内のワークロードを分類する属性を選択します。



✓ Welcome

✓ Workload Platform

✓ Create Workload Connection

4 Manage Attributes

5 Summary

Manage Attributes

All the attributes learned from the workload connection is listed here. For optimum use of search lists and memory, include in the Cisco ISE dictionary only those attributes that you want to use to create classification policies, inbound and outbound SGT domain rules, and in authorization policies. At least one attribute must be added to dictionary to proceed to next step. If you have an existing connection with the same platform, any attributes already added to the Cisco ISE dictionary are automatically enabled in this list as well. You can also edit the attribute name to be displayed in the Cisco ISE dictionary.

☐ Include All in Dictionary

Included in Dictionary	Workload Attribute	Attribute Name in Dictionary	References
☐	vmid	vmid	--
☐	uuid	uuid	--
☐	guest.guestFullName	guest.guestFullName	--
☒	VM-Name	VM-Name	--
☐	host	host	--
☒	Power	Power	--
☐	os	os-type	1
☐	network	network	--

[Exit Wizard](#)

[Back](#) [Next](#)

ステップ 7. [Summary] ウィンドウの情報を確認してから、[Create] をクリックします。

✓ Welcome

✓ Workload Platform

✓ Create Workload Connection

✓ Manage Attributes

5 Summary

Summary

Review the Cisco ISE – Workload Connector configurations defined through this workflow. Click Edit for the section in which you want to change any configurations.

Select Workload Platform [Edit](#)

Workload Platform V-CENTER

Create Workload Platform [Edit](#)

Workload Connection Name	vCenter_DMZ	Description	
Sync Interval	2 Minutes	Host	10.14.0.250
User	root	Password	****
Validate vCenter certificate	Enabled		

Manage Attributes [Edit](#)

Included in Dictionary	Workload Attribute	Attribute Name in Dictionary	References
☐	vmid	vmid	--
☐	uuid	uuid	--
☐	guest.guestFullName	guest.guestFullName	--
☒	VM-Name	VM-Name	--

[Exit Wizard](#)

[Back](#) [Create](#)

ワークロード分類ルール

vCenter 接続が確立したら、[Work Centers] > [Workload Connectors] > [Workload Classification] > [+ Add Classification Rule] から、ワークロード分類ルールを作成して、ワークロードの分類方法を定義します。

Workload Classification

Classification rules allow you to assign primary and secondary SGTs to workloads. The primary SGT is marked as "Security Group" in pxGrid session topic and is used to publish IP-to-SGT mappings via SXP. Secondary SGTs are published on the pxGrid session topic as an ordered array named "Secondary Security Groups".

If multiple classification rules are matched and multiple primary SGTs are assigned, only the first assigned SGT is considered as the primary SGT and the remaining SGTs are taken as secondary SGTs. The order of secondary SGTs depend on the order of classification rule execution. When a second primary SGT is assigned, it will be added to the end of "Secondary Security Groups" and any secondary SGTs in the same rule will then be added. Manage **Inbound SGT domain Rules** to define the SGT domains for these IP mappings.

For a workload from an ACI connection, the primary SGT is always the one derived from its EPG/ESG.

Search table

+ Add Classification Rule

As of: Jan 9, 2025 4:14 PM

図 1. IP アドレスに基づく分類ルールの例

Classification Rule Details

RULE SETTINGS

Rule Name*
IP-150.1.1.0

Status
☒ Enabled ☐ Disabled

AUTHORIZATION CONFIGURATION

Primary SGT*
SGT106

Secondary SGTs (Optional)
SGT107 x

RULE CONFIGURATION ⓘ

AND

Source Equals vcenter1

IP Address IP Equals Value* 150.1.1.0/24

+ Add AND/OR Statement + Add Condition

図 2. オペレーティング システム タイプ (os-type) に基づく分類ルール の例

Classification Rule Details

RULE SETTINGS

Rule Name*
Windows-OS

Status
☒ Enabled ☐ Disabled

AUTHORIZATION CONFIGURATION

Primary SGT *
SGT116

Secondary SGTs (Optional)
SGT126 x

RULE CONFIGURATION ⓘ

AND

Source

Equals

vcenter1

Vcenter - os-type

Equals

Microsoft Windows 10 (64-bit)

+ Add AND/OR Statement

+ Add Condition

Cancel Preview Done

プライマリ SGT は pxGrid セッショントピックで **Security Group** としてマーク付けされ、SXP を介して IP から SGT へのマッピングを公開するために使用されます。セカンダリ SGT は、**Secondary Security Groups** という名前の順序付き配列として pxGrid セッショントピックに含まれています。

手順 1. 分類ルールの結果を表示するには :

ステップ 1. 検索条件で [Preview Rule] ウィンドウを使用します。

Preview Rule

SGT Bindings (7144/25310)



Q Windows-OS



IP Address	Primary SGT	Secondary SGTs (in order)	Matching Rules	Source	Learned From	Learned By
10.1.0.161	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.1	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.10	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.100	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.101	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.102	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.103	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.104	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.105	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.106	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.107	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session
150.1.10.108	SGT116	SGT126	Windows-OS	Vcenter	172.23.203.1	Session

7144 Record(s)

Show Records: 25 1 - 25 1 2 3 4 5 ... 286

Processed 25310 out of 25310 records

Close Preview

ステップ 2. [Save] をクリックして、分類ルールを送信します。

Identity Services Engine Work Centers / TrustSec

License Warning

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Overview Components TrustSec Policy Policy Sets SXP Integrations Troubleshoot Reports Settings

Workload Connectors Overview Workload Connections Attributes Dictionary Workload Classification Meraki

considered as the primary SGT and the remaining SGTs are taken as secondary SGTs. The order of secondary SGTs depend on the order of classification rule execution. When a second primary SGT is assigned, it will be added to the end of "Secondary Security Groups" and any secondary SGTs in the same rule will then be added. Manage **Inbound SGT domain Rules** to define the SGT domains for these IP mappings.

Order of assignment maintained

Secondary SGTs All Matched Rules

Order of assignment maintained

SGT binding Stored in ISE

For a workload from an ACI connection, the primary SGT is always the one derived from its EPG/ESG.

Search table

+ Add Classification Rule As of: Jan 9, 2025 4:14 PM

#	Rule Name	Status	Primary SGT	Secondary SGTs	SGT Bindings	Actions
0	IP-150.1.4.0	✓	SGT106	SGT107	103	
1	IP-150.1.3.0	✓	SGT106	SGT107	103	
2	IP-150.1.2.0	✓	SGT106	SGT107	103	
3	IP-150.1.1.0	✓	SGT106	SGT107	103	
4	Windows-OS	✓	SGT116	SGT126	7144	
5	Default-classifi...	✗	Unknown		0	

6 Record(s) 1 - 6

Save

vCenter ワークロードが SGT にマッピングされた後、ACI リーフ、SD-Access ボーダーノード、SD-WAN エッジノード、Cisco Firepower デバイスなどのさまざまな適用ポイントで、これらのワークロードにポリシーを適用できます。

ISE と Cisco Catalyst Center の統合

このソリューションテストでは、『[Catalyst Center and Cisco ISE Integration](#)』で説明されているように、ISE が Cisco Catalyst Center と統合されます。

Catalyst Center は、ポリシー管理ポイントとして設定されます。TrustSec ポリシーの設定は、Catalyst Center から行います。ISE 内のセキュリティグループ、アクセス契約、およびポリシーは読み取り専用です。

Catalyst Center

Overview / Configurations

Policy Settings Analytics Settings

Policy Settings

Administration Mode View migration log Last migration: Jan 9, 2025 4:29 PM

Manage Group-Based Access Control in

☒ Catalyst Center, policy UI in Cisco Identity Services Engine will be read-only

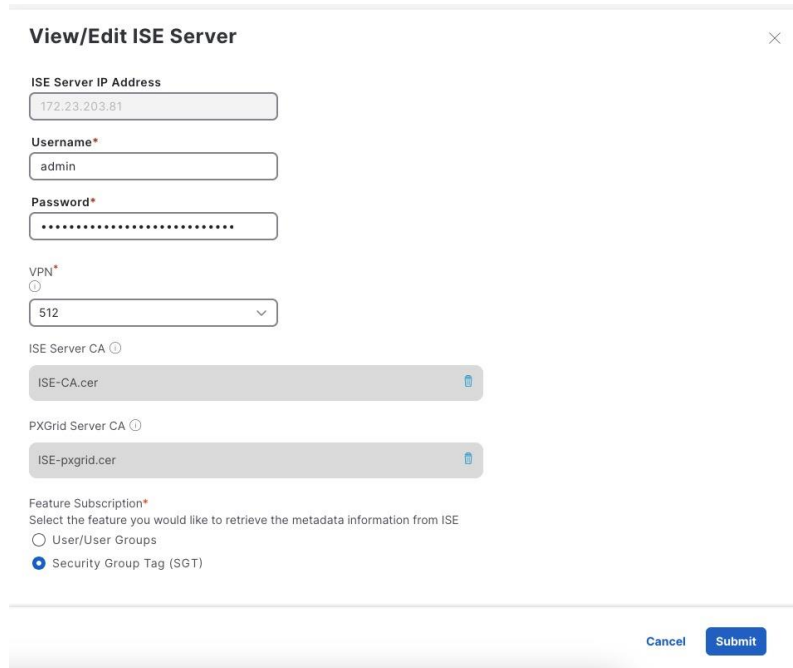
For emergent cases, such as Catalyst Center not responding, you can override the read-only mode in Cisco Identity Services Engine Security Group settings so that you can make policy changes directly in Cisco Identity Services Engine. Be cautious that this will cause both sides out of sync. A full re-sync might be necessary after recovery. [Re-sync policy data](#)

☐ Cisco Identity Services Engine, Group-Based Access Control UI in Catalyst Center will be inactive

Cisco SD-WAN Manager との ISE 統合

Cisco ISE との SGT 統合のための Cisco Catalyst SD-WAN アイデンティティベースのファイアウォールポリシー拡張は、Cisco SD-WAN リリース 20.10.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a 以降でサポートされています。

Cisco SD-WAN Manager との ISE 統合は、[Administration] > [Integration Management] > [Identity Services Engine] の順に選択して、Cisco SD-WAN Manager UI から開始します。手順については、「[Configure PxGrid in Cisco ISE for Connectivity to Cisco SD-WAN Controller](#)」を参照してください。



SD-WAN コントローラで ISE pxGrid の統合を確認します。

```
sdwan-controller# show idmgr pxgrid-status
idmgr pxgrid-status default
-----
Identity Manager Tenant - default
-----
State                               Connection and subscriptions successful
Current event                       EVT-None
Previous event                      SXP websocket create eveent
Session base URL
Session pubsub base URL
Session topic
UserGroups topic
Session Websocket status            ws-disconnected
SXP base URL                       https://ISE-MNT1.cdp.com:8910/pxgrid/ise/sxp
SXP pubsub base URL                 wss://ISE-PSN1.cdp.com:8910/pxgrid/ise/pubsub
SXP topic                           /topic/com.cisco.ise.sxp.binding
SXP Websocket status                ws-connected
Last notification sent               Connection successful
Timestamp of recent session
```

統合が有効になったら、SD-WAN 管理者は Cisco Catalyst SD-WAN アイデンティティベースのファイアウォールポリシーを設定できます。SGT は、ポリシー設定のために SD-WAN Manager (旧 vManage) に送

信されます。IP-SGT マッピングが SD-WAN コントローラ（旧 vSmart）に送信されます。設定された SGT ドメインインバウンドルールに基づいて、ISE は、ACI から学習した IP-SGT バインディングを SGT ドメイン名と一致する特定の SD-WAN VPN に送信します。

FMC との ISE 統合

pxGrid 2.0 を使用した ISE との FMC 統合は、リリース 6.7 以降でサポートされています。統合は、FMC UI から開始されます。

手順 1. FMC との ISE 統合を設定するには：

ステップ 1. [Integration] > [Identity Sources] > [Identity Services Engine] で、FMC との ISE 統合を設定します。

The screenshot shows the FMC configuration interface for Identity Services Engine. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Integration' tab is active, and the 'Identity Sources' sub-tab is selected. The configuration form includes the following fields:

- Service Type:** Radio buttons for 'None' and 'Identity Services Engine' (selected).
- Primary Host Name/IP Address*:** Text box containing '172.23.203.85'.
- Secondary Host Name/IP Address:** Text box containing '172.23.203.86'.
- pxGrid Client Certificate*:** Dropdown menu showing 'pxGrid_FMC'.
- MNT Server CA*:** Dropdown menu showing 'ISE_rootCA'.
- pxGrid Server CA*:** Dropdown menu showing 'ISE_rootCA'.
- ISE Network Filter:** Text box containing 'ex. 10.89.31.0/24'.
- Subscribe To:** Checkboxes for 'Session Directory Topic' and 'SXP Topic' (both checked).
- Test:** A button to test the configuration.

ステップ 2. [Test] をクリックして、ISE への pxGrid 接続が成功することを確認します。

The screenshot shows a 'Status' dialog box with the following information:

- ISE connection status:** Information icon.
- Primary host:** Success
- Secondary host:** Success
- Additional Logs:** A scrollable list of log messages:
 - Primary host:
 - [INFO]: PXGrid v2 is enabled
 - [INFO]: pxgrid 2.0: account activate succeeded
 - [INFO]: Successful connection to ISE-MNT2.cdp.com:8910
- OK:** A button to close the dialog.

ISE を FMC と統合するための詳細な手順については、「[Configure and Troubleshoot ISE 3.2 with FMC 7.2.4 Integration](#)」を参照してください。

ISE は、ACI ファブリック内の選択された EPG と ESG にサブスクライブし、これらはトラフィック適用のために FMC に送信されます。

ポリシー適用ポイント

ACI リーフポリシー適用

ISE は dot1x または MAC 認証バイパス (MAB) を介して、キャンパスネットワークに接続するユーザーまたはデバイスの IP-SGT バインディングを学習します。このコンテキストは、ACI リーフでのポリシー適用を有効にするために、アウトバウンド SGT ドメインルールを介して ACI データセンターに伝播されます。

ポリシー制御の適用方向は、ACI VRF ポリシーの設定で [Ingress] (デフォルト) または [Egress] のいずれかに設定できます。

The screenshot shows the 'VRF - VRF1' configuration page in the FMC GUI. The 'Policy' tab is selected. The 'Properties' section on the left includes fields for Name (VRF1), Alias, Description (optional), Annotations (+ Click to add a new annotation), Global Alias, Routing Domain ID (0), and Segment (2785280). The 'Policy Control Enforcement Preference' is set to 'Enforced'. The 'Policy Control Enforcement Direction' is set to 'Egress'. The 'BD Enforcement Status' is unchecked. The 'Preferred Group' is set to 'Enabled'. The 'BGP Timers' dropdown is set to 'select a value'. The 'BGP Context Per Address Family' section shows a table with columns 'BGP Address Family Type' and 'BGP Address Family Context'. Below this, a message states 'No items have been found. Select Actions to create a new item.' The 'BGP Route Target Profiles' section shows a table with columns 'Address Family' and 'Route Targets'.

この手順例では、従業員 SGT ユーザーが TCP ポート 22、80、443 の ACI データセンターの背後にある Web サーバーにアクセスできるようにするコントラクトを適用します。Web サーバーは WEB EPG に属します。

手順 1. コントラクトを適用するには :

ステップ 1. [Outbound Rule Details] の [Contract Configuration] セクションで、[Employees] SGT の [Consumed Contract] ドロップダウンリストで、[ALLOW_WEB_SSH] コントラクトを選択します。

この場合、[ALLOW_WEB_SSH] の [Consumed Contract] が [Employees] SGT に適用されます。

Outbound Rule Details

AND

OR

SGT Name

Equals

Contractors x Developers x
Employees x Production_Servers x
Production_Users x BYOD x

SGT Name

Equals

DC2_SCALE1_VRF1_DC2_ACI_V... x

SGT Name

Equals

SGT5001 x SGT5002 x
SGT5005 x

+ Add AND/OR Statement

+ Add Condition

+ Add AND/OR Statement

+ Add Condition

Contract Configuration

SGT Name	Connection/ Tenant/ L3out	Consumed Contract	Provided Contract
Contractors	DC1_ACI/ prod/ L3-OUT-VRF1	prod CONTRACT · Allow_All_Prod x	
Developers	DC1_ACI/ prod/ L3-OUT-VRF1	prod CONTRACT · Allow_All_Prod x	
Employees	DC1_ACI/ prod/ L3-OUT-VRF1	prod CONTRACT · ALLOW_WEB_SSH x	

ステップ 2. 消費されるコントラクトが対応する EEPG に適用されることを ACI で確認します。

注： この例では、データセンターデバイスがキャンパスデバイスにアクセスする必要がないため、[Consumed Contract] 設定のみが SGT に適用されます。ただし、データセンターデバイスがキャンパスデバイスにアクセスする必要がある場合は、指定されたコントラクトを設定する必要があります。

APIC

System Tenants Fabric Virtual Networking Admin Operations Integrations

ALL TENANTS Add Tenant Tenant Search: prod staging mgmt infra

This object was created by the ISE orchestrator. It is recommended to only modify this object using the ISE orchestrator.

prod

Application Profiles
Networks
VLAN Stretch
Bridge Domains
VRFs
L2Outs
L3Outs
L3-OUT-VRF1
Logical Node Profiles
External EPGs
BYOD-ISE_BYOD
Contractors:ISE_Contractors
DC2_SCALE1_VRF1_DC2_ACI_VRF1_T1ISE_DC2_SCALE1_VRF1_DC2_ACI_VRF1_T1
Developers:ISE_Developers
Employees:ISE_Employees

External EPG - Employees:ISE_Employees

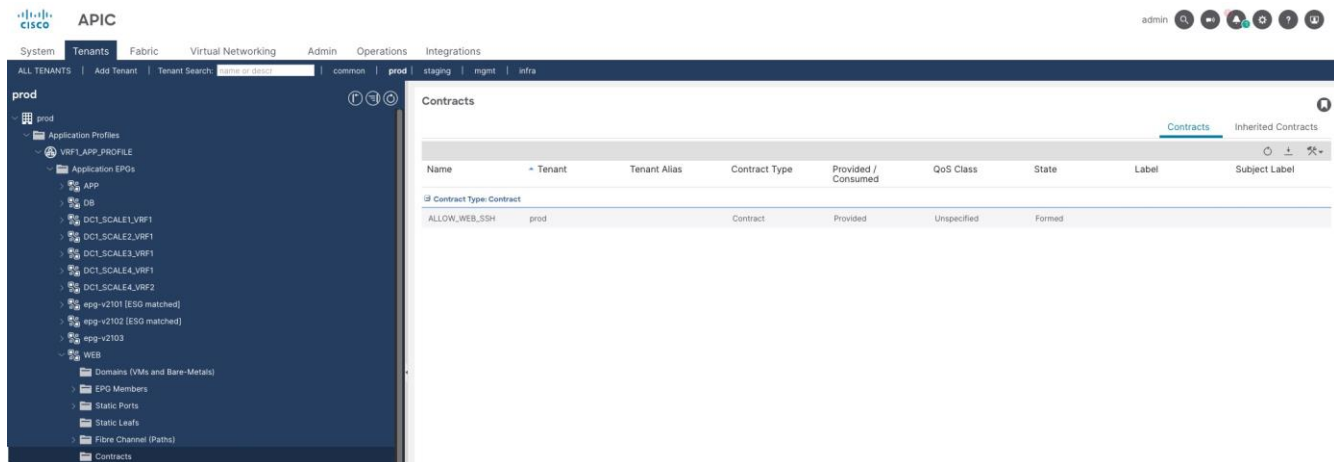
Summary Policy Operational Health Faults History

General Contracts Inherited Contracts Subject Labels EPG Labels

Healthy

Name	Tenant	Tenant Alias	Contract Type	Provided / Consumed	QoS Class	State	Label	Subject Label
Contract Type: Contract								
ALLOW_WEB_SSH	prod		Contract	Consumed	Unspecified	Formed		

ステップ 3. Web サーバーが属する WEB EPG に適用される、対応する指定されたコントラクトがあることを確認します。



SD-Access ボーダーノードでのポリシー適用

SD-Access キャンパスから SD-Access ボーダーノード上の ACI データセンターへのアウトバウンド フィルタリングには、SXP サービスで有効になっている ISE ポリシーサービスノード (PSN) と SD-Access ボーダーノード間の SXP 接続が必要です。ACI から送信された IP-SGT バインディングは、ISE によって学習され、SD-Access ボーダーノードに伝播されます。このコンテキストにより、SD-Access ボーダーノードは、キャンパスから ACI データセンターに向かうトラフィックをフィルタリングできます。

注： ISE は SXP を介して SD-Access ボーダーノードから IP-SGT バインディングを学習する必要がないため、SD-Access ボーダーノードは SXP のリスナーとして設定されます。代わりに、ISE は、Dot1x を介してキャンパス IP-SGT バインディングと、RADIUS を介して SD-Access エッジノードからの MAB 認証を学習します。

手順 1. ISE PSN と SD-Access ボーダーノード間の SXP 接続を作成するには：

ステップ 1. ISE で、[ISE SXP] > [SXP Devices] > [Add] で、SD-Access ボーダーノードを SXP デバイスとして設定します。

Identity Services Engine Work Centers / TrustSec

Bookmarks Overview Components TrustSec Policy Policy Sets **SXP** Integrations Troubleshoot Reports Settings

SXP Devices > SXP Connection

Upload from a CSV file

Add Single Device

Input fields marked with an asterisk (*) are required.

Name
S5-FB1-VN1

IP Address*
51.51.51.1

Peer Role*
LISTENER

Connected PSNs*
ISE-PSN1

SGT Domains*
default

Status*
Enabled

Password Type*
CUSTOM

ステップ 2. SD-Access ボードードに SXP 設定を適用します。

図 3. SD-Access ボードードに適用される SXP 設定の例

!Create a new loopback interface in VRF to be used as the source of the SXP connection to ISE-PSN1 and ISE-PSN2, which are enabled with SXP service

```
interface Loopback 51
 vrf forwarding VN1
 ip address 51.51.51.1 255.255.255.255
```

!Define SXP connection to ISE-PSN1 per VRF

```
cts sxp enable
cts sxp default password 7 060506324F41
cts sxp connection peer 111.30.0.85 source 51.51.51.1 password default mode local
listener hold-time 0 0 vrf VN1
```

!Define SXP connection to ISE-PSN2 per VRF

```
cts sxp connection peer 111.30.0.86 source 51.51.51.1 password default mode local
listener hold-time 0 0 vrf VN1
```

!Enable cts enforcement on SVIs towards fusion router

```
cts role-based enforcement
cts role-based enforcement vlan-list 2003,2005
```

ステップ 3. Catalyst Center ポリシーを設定して、従業員から ACI で学習した SGT である WEB_prod_EPG へのトラフィックを拒否するようにします。

Catalyst Center

Policy / Group-Based Access Control

Overview

Policies

Security Groups

Access Contracts

Migration is complete. Catalyst Center will be the policy administration point, and screens of Security Groups, Access Contracts and Policies in Cisco Identity Services Engine will be Group-Based Access Control Configurations

Policies (1)

Enter full screen

Filter

Deploy

Refresh

Permit

Deny

Custom

Default

Source

Destination

Employees

WEB

WEB

WEB

Employees > Deny IP > WEB_prod_EPG

WEB_prod_EPG > Default Policy > Employees

ステップ 4. SD-Access ボーダーノードでのトラフィック適用を確認します。

図 4. SD-Access ボーダーノードでのトラフィック適用検証の例

```

S5-FB1#show cts role-based permissions
IPv4 Role-based permissions default:
    Permit IP-00
IPv4 Role-based permissions from group 4:Employees to group 3103:WEB_prod_EPG:
    Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

S5-FB1#show cts role-based counters
Role-based IPv4 counters
From      To      SW-Denied  HW-Denied  SW-Permitt  HW-Permitt  SW-Monitor  HW-Monitor
*         *         0           0          987         353681      0           0
4         3103    0           5           0           0           0           0
S5-FB1#

S5-FB1#show cts role-based sgt-map vrf VN1 all | i 111.1.1.101
111.1.1.101          3103      SXP

```

SD-WAN エッジでのポリシー適用

SD-WAN エッジでのトラフィック適用を有効にするには、インバウンド SGT ドメインルールを設定して、特定の SD-WAN VPN 番号にコンテキストを送信します。SGT ドメイン名は SD-WAN VPN 番号と一致します。たとえば、宛先 SGT ドメイン「1」のインバウンドルールは、SD-WAN VPN「1」に SGT コンテキストを送信します。

手順 1. インバウンド SGT ドメインルールを設定するには：

Add Inbound Rule

Rule Settings

Inbound Rule Name*

DC1_ACI_to_1

Status



Enabled



Disabled

Destination Configuration

Destinations *

1 X



Rule Configuration ⓘ

AND ▼

Source

Equals

DC1_ACI

EPG

Equals

DB

+ Add AND/OR Statement

+ Add Condition

Cancel

Preview

Add

ステップ 1. SD-WAN エッジの VPN 1 でバインディングが受信されることを確認します。

```
S3-CE1#show cts role-based sgt-map vrf 1 summary

-IPv4-

IP-SGT Active Bindings Summary
=====
Total number of OMP      bindings = 500
Total number of active   bindings = 500

-IPv6-

IP-SGT Active Bindings Summary
=====
Total number of OMP      bindings = 500
Total number of active   bindings = 500

S3-CE1#show cts role-based sgt-map vrf 1 all | inc 111.11.0.31
111.11.0.31              3101      OMP
```

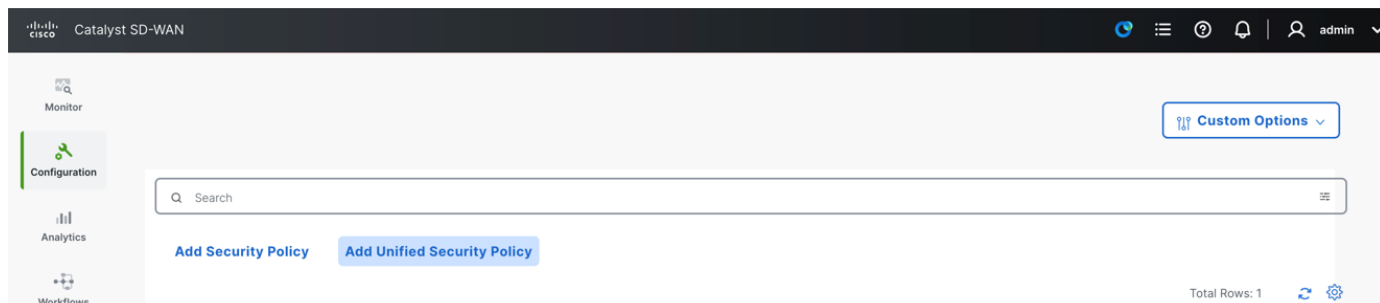
ステップ 2. SD-WAN コントローラで受信したバインディングを確認します。

```
sdwan-controller# show idmgr omp ip-sgt-bindings | inc 111.11.0.31
111.11.0.31/32  1      3101  omp-updated
```

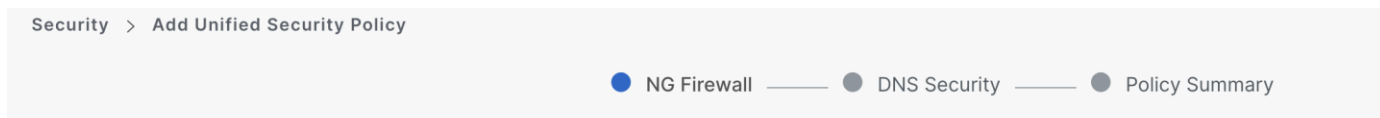
SD-WAN エッジでのポリシー適用

手順 1. SD-WAN セキュリティポリシーを作成するには：

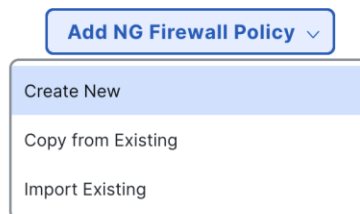
ステップ 1. [Configuration] > [Security] > [Add Unified Security Policy] の順に選択します。



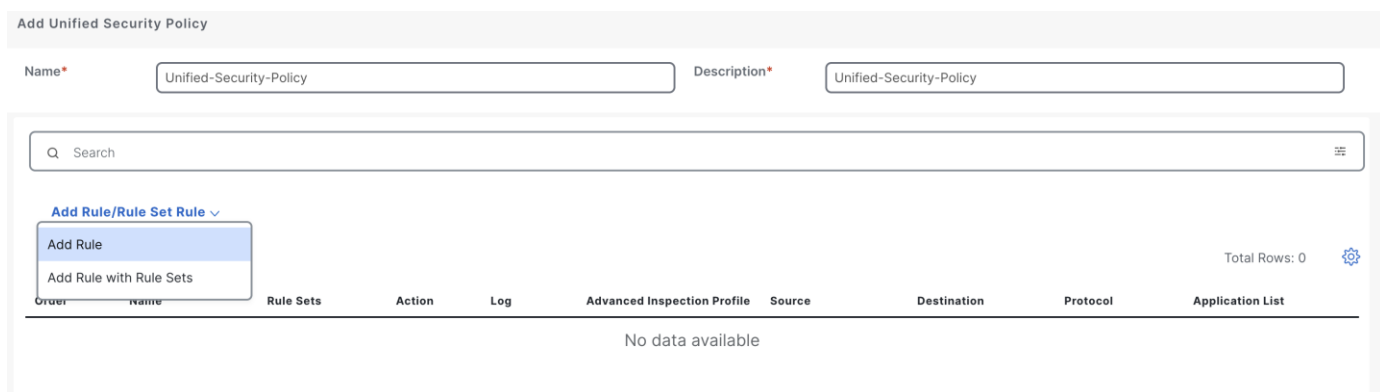
ステップ 2. [Add NG Firewall Policy] をクリックし、[Create New] を選択します。



Create 5-tuple and Application behavior and add the VPN zones.



ステップ 3. 統合されたセキュリティポリシーについて [Name] と [Description] に入力し、[Add Rule] をクリックします。



ステップ 4. ファイアウォールルールについて [Name] に入力します。[Action] で [Inspect] を選択し、[+ Destination] をクリックします。

Edit Firewall Rule

×

Order Name Type

Action ☒ Log [①](#) Advanced Inspection Profile

Source / Destination

+ Source	+ Destination	+ Protocol	+ Application List
Any	Any	Any	Any

ステップ 5. [Type] で [Identity] を選択します。[Identity List] で [New Identity List] をクリックします。

Edit Firewall Rule

×

Order Name Type

Action ☒ Log [①](#) Advanced Inspection Profile

Source / Destination

+ Source	Object Group Select an object group
Any	Type Identity Identity List Select an identity list Search New Identity List

ステップ 6. [Identity List Name] と [Description] に入力し、[Security Group Tag] を選択して [Save] をクリックします。

Identity List

×

Identity List Name

DC1-DB

Description

DC1-DB

Select Security Group Tag (SGT)

DB_prod_EPG - 3101 ×

DB

☒ DB_prod_EPG - 3101

ステップ 7. 新しいアイデンティティリストを作成すると、[Destination] セクションの [Identity List] で選択できるようになります。ステップ 6 で作成したアイデンティティリストを選択し、[Save] をクリックします。

Destination

Object Group

Select an object group

Type

Identity

Identity List

DC1-DB ×

+

Cancel

Save

ステップ 8. ウィンドウの下部にある [Save Unified Security Policy] をクリックします。

Edit Unified Security Policy

Name*

Unified-Security-Policy

Description*

Unified-Security-Policy

Q Search

Add Rule/Rule Set Rule ▾

Default Action

Drop ▾

Total Rows: 0



Order	Name	Rule Sets	Action	Log	Advanced Inspection Profile	Source	Destination	Protocol	Application List
1	Inspect S3 Traffic to	N/A	Inspect	☒	N/A	Any	DC1-DB	Any	Any

ステップ 9. 統合セキュリティポリシーが作成されたら、[Add Zone Pair] をクリックします。

Security > Add Unified Security Policy

● NG Firewall

● DNS Security

● Policy Summary

Q Search

Add NG Firewall Policy (Add a NG Firewall configuration)

Total Rows: 1

Name	Type	Description	Reference Count	Zone Pairs	Updated By	Last Updated
Unified-Security-Policy	zoneBasedFW	Unified-Security-Policy	0	Add Zone Pair	admin	07 Mar 2025 12:27:24 PM P

ステップ 10. [Apply Zone-Pairs] で、[Source Zone] と [Destination Zone] に関連するサービス VPN を選択します。この例では、VPN1 が選択されています。[Save] をクリックします。

Apply Zone-Pair(s)

Target Zone-Pair

Source Zone VPN1 → Destination Zone VPN1

Save Cancel

ステップ 11. ウィンドウの下部にある [Next] をクリックして続行します。[DNS Security] セクション（表示されていません）で、ウィンドウの下部にある [Next] を再度クリックして続行します。

Security > Add Unified Security Policy

● NG Firewall

● DNS Security

● Policy Summary

Q Search

Add NG Firewall Policy (Add a NG Firewall configuration)

Total Rows: 1

Name	Type	Description	Reference Count	Zone Pairs	Updated By	Last Updated
Unified-Security-Policy	zoneBasedFW	Unified-Security-Policy	0	1	admin	07 Mar 2025 12:27:24 PM P

ステップ 12. [Policy Summary] で、[Security Policy Name] と [Security Policy Description] に入力してから、[Save Policy] をクリックします。

Security > Add Security Policy

● NG Firewall — ● DNS Security — ● Policy Summary

Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name

Security Policy Description

ステップ 13. [Configuration] > [Templates] で、デバイスに添付されている既存のデバイステンプレートを選択します。[Additional Templates] セクションで、[Security Policy] をクリックし、以前に作成した [Test-Security-Policy] という [Security Policy] を選択します。

Cisco Catalyst SD-WAN

Monitor

Configuration

Analytics

Workflows

Tools

Reports

Maintenance

Administration

Explore

Additional Templates

AppQoE	Choose...
Global Template *	Factory_Default_Global_CISC... ⓘ
Cisco Banner	Choose...
Cisco SNMP	Choose...
ThousandEyes Agent	Choose...
TrustSec	Choose...
CLI Add-On Template	configure-register
Policy	Choose...
Probes	Choose...
Tenant	Choose...
Security Policy	Test-Security-Policy

Firewall Threat Defense (FTD) ポリシー適用

FMC が ISE と統合されると、SGT および関連する IP-SGT バインドを取得できるようになります。アクセスポリシールールには、[Dynamic Attributes] タブで送信元属性と宛先属性として選択できる使用可能な SGT が表示されます。

Editing Rule - Inside-to-Outside

Name: Inside-to-Outside ☒ Enabled [Move](#)

Action: Allow Time Range: None +

Zones Networks VLAN Tags **Users** Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Available Attributes Security Group Tag

APP_prod_EPG
Auditors
BYOD
Contractors
DB_prod_EPG
DC1_SCALE1_VRF1_prod_EPG
Developers
Development_Servers

Selected Source Attributes (3)
Security Group Tags
Contractors
Developers
Employees

Selected Destination Attributes (1)
Security Group Tags
DB_prod_EPG

[Add to Source](#) [Add to Destination](#)

[Add](#)

Cancel Save

ファイアウォールポリシーは、キャンパスの SGT（請負業者、開発者、および従業員）から、ACI から学習した SGT である DB_prod_EPG へのトラフィックを許可します。

Firewall Management Center Policies / Access Control / Policy Editor Overview Analysis Policies Devices Objects Integration Deploy

Test-FTD1-Policy Try New UI Layout [Analyze Hit Counts](#) [Save](#) [Cancel](#)

Enter Description

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Custom-Prefilter Inheritance Settings Policy Assignments (1) SSL Policy: None Identity Policy: None

[Filter by Device](#) ☐ Show Rule Conflicts [Add Category](#) [Add Rule](#)

#	Name	Sou... Zon...	Dest Zon...	Sou... Net...	Dest Net...	VLAN Tags	Users	App...	Sou... Ports	Dest Ports	URLs	Source Dynamic Attribut...	Destination Dynamic Attributes	Action	
Mandatory - Test-FTD1-Policy (1-1)															
1	Inside-to-Out	INSIDE	OUTSID	Any	Any	Any	Any	Any	Any	Any	Any	Contractors Developers Employees	DB_prod_EPG	Allow	
Default - Test-FTD1-Policy (-)															

There are no rules in this section. [Add Rule](#) or [Add Category](#)

SGT に基づくアクセスルールポリシーの適用は、packet-tracer コマンドを使用して、または [Analysis] > [Connection Events] > [Table View of Connection Events] ウィンドウで確認できます。

図 5. packet-tracer コマンドを使用した検証の例

```
> packet-tracer input FB1-VN1-INSIDE1 tcp 25.1.10.5 1024 111.11.0.31 443

---Truncated---

Phase: 13
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 202428 ns
Config:
```


Network 0, Inspection 0, Detection 0, Rule ID 268435456
Additional Information:
Starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, src sgt: 4, src sgt type:
sxp, dst sgt: 3101, dst sgt type: sxp, user 9999997, no url or host, no xff
Matched rule ids 268435456 - Allow

図 6. [Connection Events] テーブルを使用した検証の例

Firewall Management Center
Analysis / Connections / Events

OverviewAnalysisPoliciesDevicesObjectsIntegration

Bookmark This Page | Reporting | Dash

Connection Events [\(switch workflow\)](#)

No Search Constraints [\(Edit Search\)](#)

Connections with Application DetailsTable View of Connection Events

Jump to...

	Action x	Initiator IP x	Responder IP x	Ingress Security x Zone	Egress Security x Zone	Source Port / ICMP Type x	Destination Port / ICMP Code x	DNS Query x	Intrusion Events x	Access Control Policy x	Access Control Rule x	Source SGT x	Destination SGT x
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	8 (Echo Request) / icmp	0 (No Code) / icmp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	8 (Echo Request) / icmp	0 (No Code) / icmp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	1024 / tcp	443 (https) / tcp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	1024 / tcp	443 (https) / tcp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	1024 / tcp	443 (https) / tcp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	1024 / tcp	443 (https) / tcp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	8 (Echo Request) / icmp	0 (No Code) / icmp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	8 (Echo Request) / icmp	0 (No Code) / icmp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	1024 / tcp	443 (https) / tcp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG
▼	☐ Allow	25.1.10.5	111.11.0.31	INSIDE	OUTSIDE	1024 / tcp	443 (https) / tcp			Test-FTD1-Policy	Inside-to-Outside	Employees	DB_prod_EPG

< > Page 1 of 1 > | Displaying rows 1-10 of 10 rows

ワークロードレポート

ワークロードレポートは、Cisco ACI コントローラとオンプレミス vCenter コントローラから受信したワークロードに関する情報を提供し、IP-SGT バインディングがどのように分類されるかを示します。レポートは、ドメインに存在する IP と、それらがどのように分類されているかを確認するのに役立ちます。記録目的でエクスポートすることもできます。

図 7. ACI レポートの例

Application Profile	EPG / ESG	SGT Name	SGT Binding	Inbound SGT Domain Rules	SGT Domains
VRF1_APP_PROFILE	DB	DB_prod_EPG	111.11.1.26	Default Filter,DC1_ACI_to_1	1,default
VRF1_APP_PROFILE	DB	DB_prod_EPG	111.11.1.0	Default Filter,DC1_ACI_to_1	1,default
VRF1_APP_PROFILE	DB	DB_prod_EPG	111.11.0.17	Default Filter,DC1_ACI_to_1	1,default
VRF1_APP_PROFILE	DB	DB_prod_EPG	111.11.0.142	Default Filter,DC1_ACI_to_1	1,default
VRF1_APP_PROFILE	DB	DB_prod_EPG	111.11.1.196	Default Filter,DC1_ACI_to_1	1,default
VRF1_APP_PROFILE	DB	DB_prod_EPG	111.11.1.143	Default Filter,DC1_ACI_to_1	1,default
VRF1_APP_PROFILE	DB	DB_prod_EPG	111.11.0.124	Default Filter,DC1_ACI_to_1	1,default
VRF1_APP_PROFILE	DB	DB_prod_EPG	111.11.0.223	Default Filter,DC1_ACI_to_1	1,default

トラブルシューティング

ここでは、トラブルシューティングの基本的な手順について説明します。

手順 1. キャンパスからデータセンターへの通信をトラブルシューティングするには：

ステップ 1. キャンパスユーザーとデバイスに正しい SGT が割り当てられていることを確認します。

S5-FE1#**show authentication sessions interface gigabitEthernet 1/0/1 details**

```

Interface: GigabitEthernet1/0/1
  IIF-ID: 0x1B62F583
  MAC Address: 0050.56a4.d8c0
  IPv6 Address: fe80::4f:5b8c:c44:58ed
                2001:db8:51:1::403
                2001:db8:51:1::402
  IPv4 Address: 35.1.1.252
    User-Name: employee-user
    Device-type: VMWare-Device
    Device-name: VMWARE, INC.
      VRF: VN1
      Status: Authorized
      Domain: DATA
    Oper host mode: multi-auth
    Oper control dir: both
    Session timeout: N/A
  Acct update timeout: 172800s (local), Remaining: 85286s
  Common Session ID: 0100011900026AA971A16340
  Acct Session ID: 0x0001967b
    Handle: 0x0b00057c
  Current Policy: PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
  
```

Local Policies:

Server Policies:

Vlan Group: Vlan: 1023

SGT Value: 4

ステップ 2. ISE のキャンパスホストとデータ センター エンドポイントに IP-SGT バインドが存在することを確認します。

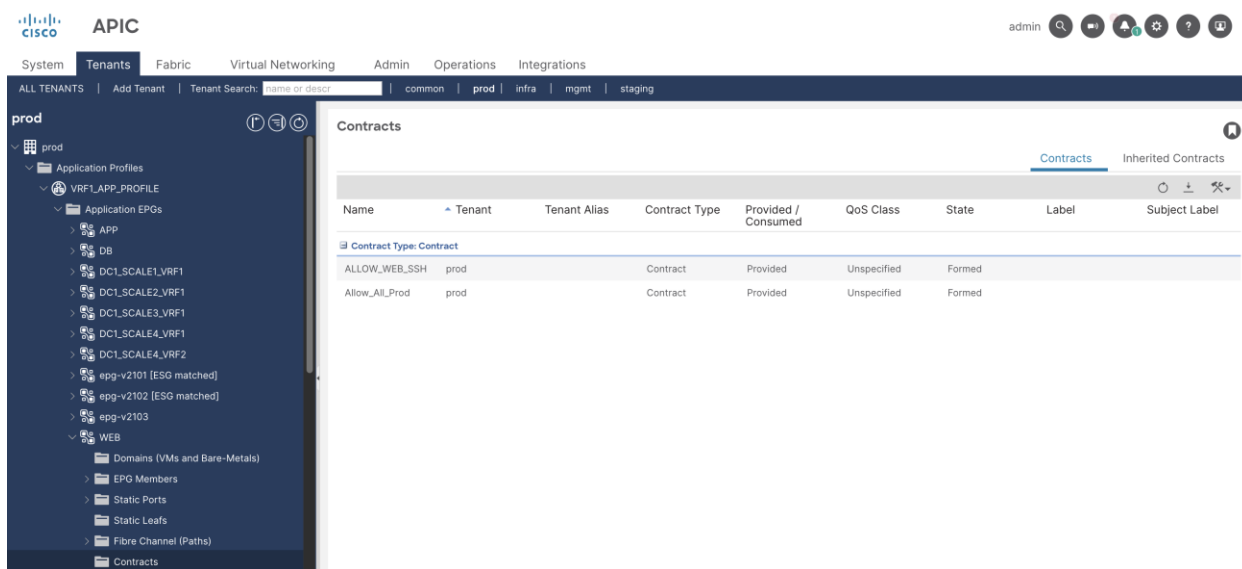
Rows/Page 1 < 1 / 1 > Go 1 Total Rows

IP Address	Primary SGT	VN	Learned From	Learned By	SGT Domain	PSNs Involved	Inbound SGT Domain
35.1.1.252/32	Employees (4/0004)	DEFAULT_VN	111.30.0.86,25.1.0.1	Session	default	ISE-PSN2	

Rows/Page 1 < 1 / 1 > Go 1 Total Rows

IP Address	Primary SGT	VN	Learned From	Learned By	SGT Domain	PSNs Involved	Inbound SGT Domain
111.1.1.101/32	WEB_prod_EPG (3103/0C1F)	DEFAULT_VN	111.30.0.85,172.23.203.121	Session	default		

ステップ 3. IP バインドが ACI EEPG SGT バインドに存在することを確認します。



テクニカルリファレンス

- [Cisco Identity Services Engine のパフォーマンスと拡張性ガイド](#)
- [Catalyst Center と Cisco ISE の統合](#)
- [Configure PxGrid in Cisco ISE for Connectivity to Cisco SD-WAN Controller](#)
- [Configure and Troubleshoot ISE 3.2 with FMC 7.2.4 Integration](#)
- [Cisco SD-Access | SD-WAN Independent Domain Pairwise Integration Prescriptive Deployment Guide](#)

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム (オランダ)

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト (www.cisco.com/jp/go/offices) をご覧ください。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。