



## ダイナミック ファイアウォール ソリューション ガイド

最終更新：2026年5月11日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



# 第 1 章

## ダイナミック ファイアウォール について

以下のトピックでは、ダイナミック ファイアウォールに関する一般情報を提供します。

- [ダイナミック ファイアウォール について \(1 ページ\)](#)

## ダイナミック ファイアウォール について

これまで、Cisco Secure Firewall Management Center は、Microsoft Active Directory、パッシブ ID エージェント、Cisco Identity Services Engine (Cisco ISE) などの設定されたアイデンティティソースからのみユーザーに関する情報を収集していました。この情報には通常、ユーザー名、グループ、IP アドレスが含まれていました。

ダイナミック ファイアウォール を使用すると、アイデンティティソースが提供する情報に Cisco アイデンティティ インテリジェンスからのユーザーリスクスコアを追加できるため、常に最新のユーザーポスチャとリスクに基づいてポリシーを設定することが可能です。ユーザーアイデンティティとインテリジェンスを組み合わせ、その情報をレポートおよびアクセスコントロール ポリシーで使用できるようにします。

ダイナミック ファイアウォール を使用するには、次の条件を満たしている必要があります。

- アイデンティティ インテリジェンス テナントがあること。  
『[Duo Identity Security with Cisco Identity Intelligence](#)』を参照してください。
- 動的属性コネクタの有効化
- アイデンティティソースをセットアップしていること。
  - Cisco Identity Services Engine (Cisco ISE)
  - pxGrid クラウド  
pxGrid クラウドは同じフィールドでアイデンティティとポスチャを組み合わせます。  
詳細については、「[What is pxGrid?](#)」を参照してください。

認証情報に加えて、Cisco ISE と pxGrid クラウドは次の情報を提供できます。

- SGT Exchange Protocol over TCP (SXP) バインディングおよびディレクトリセッション情報（必要に応じて）。詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』を参照してください。
- ポスチャおよびモバイルデバイス管理のコンプライアンス。詳細については、『[Compliance](#)』を参照してください。
- アイデンティティレルムをセットアップしていること。
  - [LDAP](#) レルムまたは [Active Directory](#) レルムおよびレルムディレクトリの作成
  - [パッシブ認証用の Azure AD \(SAML\)](#) レルムの作成

アイデンティティソースは、認証情報（ログイン、ログアウト）とポスチャを提供します。アイデンティティソースは、必要に応じて SXP バインディングおよびセッションディレクトリ情報も提供できます。

アイデンティティレルムは、ユーザー、グループ、および IP アドレス情報を提供します。



## 第 2 章

# ダイナミック ファイアウォールの設定

- [ダイナミック ファイアウォールの設定方法 \(3 ページ\)](#)
- [ダイナミック属性フィルタの作成 \(17 ページ\)](#)

## ダイナミック ファイアウォールの設定方法

このトピックは、「[ダイナミック ファイアウォールについて \(1 ページ\)](#)」で説明されているダイナミック ファイアウォールを設定するための概念とオプションを理解するのに役立ちます。

### process\_summary

ダイナミック ファイアウォールは、Cisco Secure Firewall Management Center にユーザー信頼情報を提供する Cisco Identity Intelligence と (Cisco ISE などの) アイデンティティソースを統合します。

1. ユーザー信頼情報を収集するように Cisco Identity Intelligence を設定します。
2. サポートされている Cisco Secure Firewall Management Center アイデンティティソースを設定します。
3. サポートされているアイデンティティレルムを設定します。
4. 動的属性コネクタをイネーブルにします。
5. ダイナミック ファイアウォールを設定します。

### process\_workflow

次に、ダイナミック ファイアウォールを設定する方法の概要を示します。

1. 所有者ロールを持つ Duo ユーザーとして、Cisco アイデンティティ インテリジェンス テナントをプロビジョニングします。

[Cisco Identity Intelligence テナントのプロビジョニング](#)で説明されているように、Duo Advantage からテナントをプロビジョニングできます。

2. Cisco アイデンティティ インテリジェンス で、API 統合を作成し、その情報を使用してダイナミック ファイアウォール をセットアップします。

シスコでは、Cisco アイデンティティ インテリジェンス を使用してネットワーク内のユーザーおよびデバイスリスク情報を特定しています。

Cisco アイデンティティ インテリジェンス の詳細については、[ハウツーガイド](#)を参照してください。

このタスクの詳細については、「[アイデンティティ インテリジェンス の必要な情報の取得 \(6 ページ\)](#)」を参照してください。

3. (Microsoft Azure AD レルムのみ) アイデンティティ インテリジェンス で、Microsoft Entra ID 統合を作成します。

詳細については、『[Microsoft Entra ID \(Azure AD\) Data Integration](#)』を参照してください。

4. アイデンティティソースを作成します (アイデンティティソースがすでにある場合は、次のステップに進みます)。

これは、次のいずれかの方法で実行できます。

- [\[ダイナミックファイアウォールの設定 \(Configure Dynamic Firewall\)\]](#) ダイアログボックスに、アイデンティティソースの設定を開始するための [\[設定 \(Configure\)\]](#) リンクが表示されます。
- [\[システム \(System\)\]](#) (⚙️) > [\[統合 \(Integration\)\]](#) > [\[アイデンティティソース \(Identity Sources\)\]](#) をクリックします。

アイデンティティソースの詳細については、以下を参照してください。

- [Cisco Identity Services Engine \(Cisco ISE\) のアイデンティティソースの設定方法](#)
- [pxGrid クラウドアイデンティティ ソースの設定方法 \(ISE 3.3 以前\)](#)
- [pxGrid クラウドアイデンティティ ソースの設定方法 \(ISE 3.4 以降\)](#)

5. アイデンティティレルムを作成します。

次のレルムをサポートしています。

- [LDAP レルム](#)または [Active Directory レルム](#)および[レルムディレクトリの作成](#)  
Microsoft AD のみがサポートされています。LDAP レルムはサポートされていません。
- [パッシブ認証用の Azure AD \(SAML\) レルムの作成](#)

6. 動的属性コネクタ をイネーブルにします。

動的属性コネクタ は、ダイナミック ファイアウォール を使用するために必要です。これにより、アイデンティティソースをアイデンティティ インテリジェンス と統合して、ユーザーアクティビティに関する洞察を強化できます。

「[ダイナミック属性コネクタの有効化](#)」を参照してください。

7. ダイナミック ファイアウォール インスタンスを作成します（ダイナミック ファイアウォール インスタンスがすでにある場合は、次のステップに進みます）。  
**[統合 (Integration) ] > [ダイナミック属性コネクタ (Dynamic Attributes Connector) ]**の順にクリックし、**[ダイナミックファイアウォールの設定 (Configure Dynamic Firewall) ]** をクリックします。  
[ダイナミック ファイアウォール インスタンスを作成します。 \(8 ページ\)](#) を参照してください。
8. アイデンティティソースを Cisco アイデンティティ インテリジェンスに関連付けます。  
[アイデンティティ インテリジェンス とアイデンティティソースとの関連付け \(9 ページ\)](#) を参照してください。
9. システム定義フィルタを表示します。  
ダイナミック属性フィルタは以下を区別するために作成します。
  - 信頼できないデバイス
  - 信頼できるデバイス
  - 信頼できないユーザー
  - 疑わしいユーザー  
「[ダイナミック属性フィルタの作成 \(17 ページ\)](#)」で説明されているように、これらのダイナミック属性フィルタを編集または置換できます。
10. システム定義のアクセス制御ルールを表示します。  
次のルールを使用して、Dynamic Firewall Policy という（または同様の）名前のアクセスコントロール ポリシーを作成します。
  - 任意の送信元ネットワークから任意の宛先ネットワークへの信頼できないユーザーをブロックします。
  - 任意の送信元ネットワークから任意の宛先ネットワークへの疑わしいユーザーを監視します。
  - 任意の送信元ネットワークから任意の宛先ネットワークへの信頼できないデバイスをブロックします。  
「[システム作成のアクセスコントロール ポリシーの表示と編集 \(16 ページ\)](#)」で説明されているように、アクセスコントロールポリシーとアクセス制御ルールを編集または削除します。

## 動的属性コネクタ の有効化

このタスクでは、Cisco Secure Firewall Management Center で動的属性コネクタ を有効にする方法について説明します。動的属性コネクタは、クラウドネットワーキング製品のオブジェクト

を Cisco Secure Firewall Management Center のアクセス制御 のルールで使用できるようにする統合です。

#### 手順

ステップ1 Cisco Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ2 [統合 (Integration) ] > [ダイナミック属性コネクタ (Dynamic Attributes Connector) ] をクリックします。

ステップ3 [有効 (Enabled) ] にスライドします。

ステップ4 動的属性コネクタ が有効になっている間、メッセージが表示されます。

エラーが発生した場合は、再試行してください。エラーが続く場合には、[Cisco TAC](#)に連絡してください。

## アイデンティティ インテリジェンス の必要な情報の取得

このタスクでは、ダイナミック ファイアウォール でアイデンティティ インテリジェンス をセットアップするために必要なすべての情報を提供する API クライアントの作成方法について説明します。

すでに API クライアントがあり、次のすべての値がわかっている場合は、この手順をスキップして「」に進むことができます。

- **Client ID**
- **API URL**
- **トークン URL**
- **クライアントのシークレット (Client Secret)**

#### 始める前に

ダイナミック ファイアウォール と統合するには、アイデンティティ インテリジェンス で API クライアント統合を作成する必要があります。

API クライアント統合について知っておく必要がある値の中に、クライアントシークレットがあります。これは、API クライアントを作成するときのみ表示されます。このため、最初に API 統合を作成する必要があります。

API クライアント統合の作成の詳細については、「[Public API](#)」を参照してください。

#### 手順

ステップ1 [アイデンティティ インテリジェンス テナント](#) にログインします。

ステップ2  ([統合 (Integrations) ]) をクリックします。

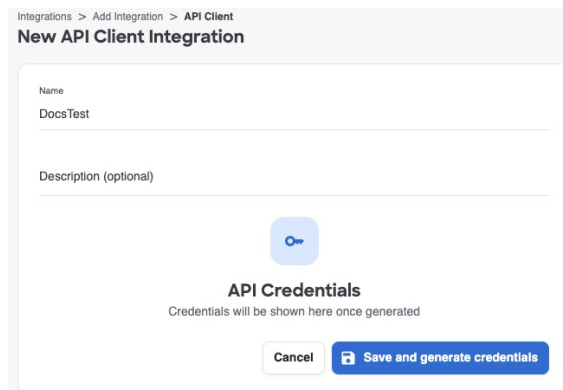
**ステップ 3** [統合の追加 (Add Integration) ] をクリックします。

**ステップ 4** 次のページの [APIクライアント (API Clients) ] で、[APIクライアントの追加 (Add API Client) ] をクリックします。

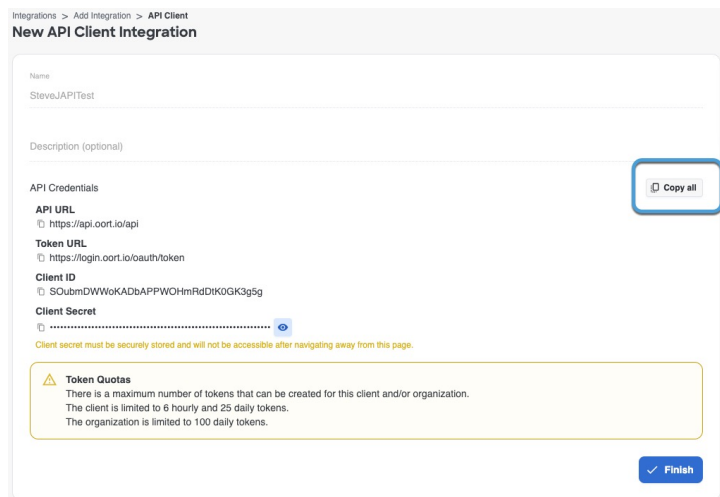
**ステップ 5** [名前 (Name) ] とオプションの [説明 (Description) ] を入力します。

**ステップ 6** [保存してログイン情報を生成 (Save and Generate Credentials) ] をクリックします。

次の図は例を示しています。



**ステップ 7** 次の図に示すように、次のページで [すべてコピー (Copy all) ] をクリックします。



**ステップ 8** 後で使用できるようにログイン情報を保存します。

**ステップ 9** [終了 (Finish) ] をクリックします。

## ダイナミック ファイアウォールのアイデンティティソースおよびレルムの作成

ダイナミック ファイアウォール を設定する前に、サポートされているアイデンティティレルムとアイデンティティソースを設定する必要があります。

### アイデンティティレルムの設定

次のアイデンティティレルムがサポートされています。

- [LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成](#)  
Microsoft AD のみがサポートされています。LDAP レルムはサポートされていません。
- [パッシブ認証用の Azure AD \(SAML\) レルムの作成](#)

### アイデンティティソースの設定

次のアイデンティティソースがサポートされています。

- オンプレミスの Cisco ISE : [Cisco Identity Services Engine \(Cisco ISE\) のアイデンティティソースの設定方法](#)
- 単一または複数の Cisco ISE クラスター :
  - [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.3 以前\)](#)
  - [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.4 以降\)](#)

## ダイナミック ファイアウォール インスタンスを作成します。

このタスクでは、アイデンティティソースとアイデンティティ インテリジェンス 間の関連付けであるダイナミック ファイアウォールの新しいインスタンスを作成する方法について説明します。

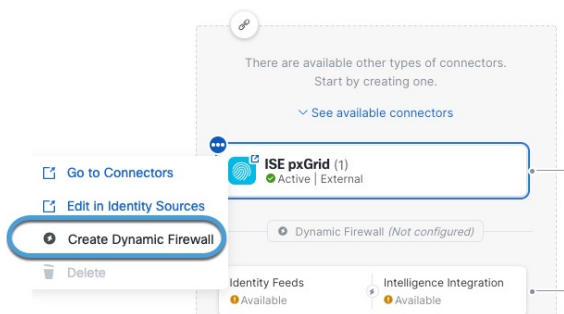
### 始める前に

次のことをすべて行います。

- 「」の説明に従って 動的属性コネクタ を有効にします。
- アイデンティティソースを作成します。
  - オンプレミスの Cisco ISE : [Cisco Identity Services Engine \(Cisco ISE\) のアイデンティティソースの設定方法](#)
  - 単一または複数の Cisco ISE クラスター :
    - [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.3 以前\)](#)
    - [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.4 以降\)](#)

## 手順

- ステップ 1** まだログインしていない場合は、Cisco Secure Firewall Management Center にログインします。
- ステップ 2** [統合 (Integrations)] > [ダイナミック属性コネクタ (Dynamic Attributes Connector)] の順にクリックします。
- ステップ 3** アイデンティティソースの名前の横にある  をクリックし、ダイナミック ファイアウォール を追加します。
- 次の図は例を示しています。



(注)

アイデンティティソースが表示されない場合は、続行する前に作成します。

- [Cisco Identity Services Engine \(Cisco ISE\) のアイデンティティソースの設定方法](#)。
- [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.3 以前\)](#)
- [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.4 以降\)](#)

- ステップ 4** [ダイナミックファイアウォールの作成 (Create Dynamic Firewall)] をクリックします。
- ステップ 5** 「[アイデンティティソースとアイデンティティ インテリジェンスの関連付け](#)」に進みます。

## アイデンティティ インテリジェンス とアイデンティティソースとの関連付け

このタスクでは、ユーザーとデバイスの信頼評価を Cisco Secure Firewall Management Center に提供する アイデンティティ インテリジェンス にアイデンティティソースを関連付ける方法について説明します。

詳細については、『[User Trust Level](#)』を参照してください。

### 始める前に

手順を開始する前に、次の点を確認してください。

- 「[ダイナミック ファイアウォールについて \(1 ページ\)](#)」に記載されている、アイデンティティレルム、アイデンティティソース、およびアイデンティティ インテリジェンスが連携する仕組みを理解している。
- 「[ダイナミック ファイアウォール インスタンスを作成します。 \(8 ページ\)](#)」で説明されているタスクを完了している。

## 手順

**ステップ 1** [ダイナミック ファイアウォール インスタンスの作成](#)から開始します。

**ステップ 2** 次のページの左列で、アイデンティティソースをクリックします。右列で[Cisco Identity Intelligence] チェックボックスをオンにして、ユーザーとデバイスのリスクを含むユーザーインテリジェンスを追加します。

次の図は例を示しています。

The screenshot shows the 'Dynamic Firewall' configuration interface. It is divided into two main columns: 'User identity feeds' and 'Intelligence integration'. In the 'User identity feeds' column, the 'ISE pxGrid On-Prem' option is selected. In the 'Intelligence integration' column, the 'Cisco Identity Intelligence' option is checked. A 'Next' button is visible at the bottom right of the configuration area.

**Dynamic Firewall** [?] [X]

**1 Associate an identity source with an identity intelligence integration**

In the left column, click the name of an identity source from which to retrieve authentication information.

In the right column, select the check box to associate the identity source with intelligence integration.

**User identity feeds**

- ISE pxGrid Cloud  
Enable ISE pxGrid Cloud in [Identity Sources](#) to use it in the dynamic firewall.
- ISE pxGrid On-Prem  
Use ISE pxGrid On-Prem as a source of user identity to set up dynamic firewall.
- Passive Identity Agent  
Identity is not yet supported in dynamic firewall.
- Captive Portal  
Identity is not yet supported in dynamic firewall.

**Intelligence integration**

- Cisco Identity Intelligence  
Associate user and device risk assessment from Cisco Identity Intelligence with the selected identity source. If you want you can go to [Cisco Identity Intelligence Dashboard](#)

Enriched by

**Next**

**2 View system-defined filters**

**3 View system-defined access control policy rules**

**ステップ 3** [Next] をクリックします。

**ステップ 4** [アイデンティティ インテリジェンス の設定 \(11 ページ\)](#) に進みます。

## アイデンティティ インテリジェンス の設定

このタスクでは、ユーザーとデバイスのリスクレーティングを Cisco Secure Firewall Management Center に提供する アイデンティティ インテリジェンス にアイデンティティソースを関連付ける方法について説明します。

### 始める前に

「[アイデンティティ インテリジェンス とアイデンティティソースとの関連付け \(9 ページ\)](#)」で説明されているタスクを完了します。

### 手順

- ステップ 1 「[アイデンティティ インテリジェンス とアイデンティティソースとの関連付け \(9 ページ\)](#)」で説明されているタスクを完了します。
- ステップ 2 [Cisco Identity Intelligence] チェックボックスをオンにした場合は、「[アイデンティティ インテリジェンス の必要な情報の取得 \(6 ページ\)](#)」の説明に従って、アイデンティティ インテリジェンス について見つけた情報を入力します。

次の図は例を示しています。

The screenshot shows the 'Dynamic Firewall' configuration interface. It is divided into two main sections: '1 Associate an identity source with an identity intelligence integration' and '2 Configure CII connector'. The 'Configure CII connector' section contains several input fields: 'Name' (filled with 'CII'), 'CII API URL\*' (filled with 'https://.../lo/api'), 'Token URL\*' (filled with 'https://.../token'), 'Client ID\*' (filled with a long alphanumeric string), and 'Client Secret\*' (filled with a long alphanumeric string). There is also a 'Pull interval (hours)' field set to '24'. At the bottom, there is an 'EXCLUSION LIST' section with a toggle switch that is currently turned off. Below the toggle, it says 'No exclusions for this connector.' At the very bottom of the form are three buttons: 'Test', 'Back', and 'Next'.

- ステップ 3 (オプション) アイデンティティ インテリジェンス に対し、特定のユーザーセットを信頼できるとみなす場合は、[除外リスト (Exclusion List)] を [有効なスライダ (Slider enabled)] () にスライドします。

**username@domain.com** 形式で1行に1つのユーザー名を入力します。このリストのユーザーは、アイデンティティ インテリジェンス によって信頼できるとみなされます。

- ステップ 4 [テスト (Test)] をクリックします。

テストが成功した場合にのみ、次の手順に進みます。

エラーが表示された場合は、アイデンティティインテリジェンスのすべての値を確認して再試行します。

ステップ5 [Next] をクリックします。

ステップ6 [システム定義フィルタの表示 \(12 ページ\)](#) に進みます。

---

## システム定義フィルタの表示

このタスクでは、ユーザーとデバイスのリスクレーティングを Cisco Secure Firewall Management Center に提供する Cisco アイデンティティインテリジェンスにアイデンティティソースを関連付ける方法について説明します。

始める前に

「[アイデンティティインテリジェンスの設定](#)」を参照してください。

手順

---



ステップ1 次の図に示すように、システムにはシステム定義のダイナミック属性フィルタのセットが表示されます。

**Dynamic Firewall** ? ×


- 1 Associate an identity source with an identity intelligence integration
- 2 Configure CII connector
- 3 View system-defined filters
- 4 View system-defined access control policy rules

We're creating the following system-defined filters for you. Click [help](#) for more information.

4 dynamic attributes filters

Name	Query
Untrusted_Device	(PostureStatus eq 'NonCompliant') OR ((MdmRegistered eq 'true') AND (MdmCo... 
Trusted_Device	(PostureStatus eq 'Compliant') OR ((MdmRegistered eq 'true') AND (MdmCo... 
Untrusted_User	TrustScore eq 'UNTRUSTED'
Questionable_User	TrustScore eq 'QUESTIONABLE'

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

**ステップ 2** システムが作成したフィルタを表示します。任意の行の  をクリックしてフィルタを展開すると、フィルタを表示して詳細を確認できます。

**ステップ 3** [Next] をクリックします。

**ステップ 4** [システム定義のアクセス制御ルールの表示 \(13 ページ\)](#) に進みます。

## システム定義のアクセス制御ルールの表示

このタスクでは、ダイナミック ファイアウォールによって作成されたアクセス制御ルールについて説明します。

始める前に

[システム定義フィルタの表示 \(12 ページ\)](#) を参照してください。

## 手順

**ステップ 1** システムで作成されたアクセス制御ルールを表示します。

次の図は例を示しています。

The screenshot shows a window titled "Dynamic Firewall" with a progress indicator on the left. The progress indicator has four steps: 1. Associate an identity source with an identity intelligence integration, 2. Configure CLI connector, 3. View system-defined filters, and 4. View system-defined access control policy rules. Step 4 is currently selected. Below the progress indicator is a table of rules:

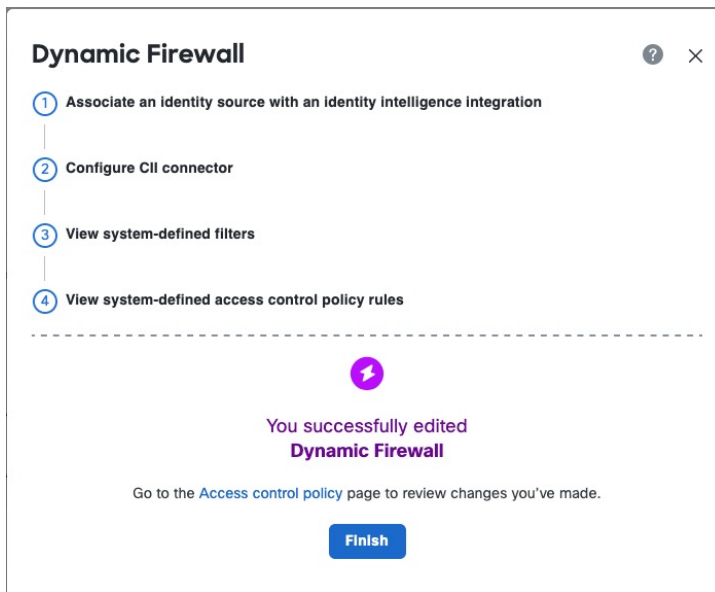
Rule Name	Action	Dynamic Attributes
Block_Untrusted_User	Block	SRC: Untrusted_User, DST: ANY
Inspect_Questionable_User	Monitor	SRC: Questionable_User, DST: ANY
Block_Untrusted_Device	Block	SRC: Untrusted_Device, DST: ANY

At the bottom of the window are three buttons: "Skip", "Back", and "Next".

**ステップ 2** 次のオプションのいずれかを選択します。

- これらのアクセス制御ルールの作成をスキップするには、[スキップ (Skip)] をクリックします。独自の設定はいつでも作成できます。
- [次へ (Next)] をクリックし、前の図に示すルールを使用して **Dynamic Firewall Policy** という名前のアクセスコントロールポリシーを作成します。
- システムが作成したフィルタに戻るには、[戻る (Back)] をクリックします。

**ステップ 3** アクセス制御ルールの作成が成功した場合、[次へ (Next)] をクリックすると次のページが表示されます。




## ユーザー除外リストの編集

(オプション) アイデンティティインテリジェンスに対し、特定のユーザーを信頼できるユーザーとして扱うように指示できます。

### 始める前に

「[ダイナミック ファイアウォール インスタンスを作成します。\(8 ページ\)](#)」の説明に従って [ダイナミック ファイアウォール](#) を設定します。

### 手順

- ステップ 1** まだ Cisco Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ 2** [統合 (Integration)] > [ダイナミック属性コネクタ (Dynamic Attributes Connector)] をクリックします。
- ステップ 3** アイデンティティソースの名前の横にある  をクリックします。
- ステップ 4** [CII除外リストの編集 (Edit CII Exclusion List)] をクリックします。

次のダイアログボックスが表示されます。

**Edit CII Exclusion List**

**EXCLUSION LIST**

Enter each user name on a separate line

Enter one or more users to exclude from filters. These users will not be treated as untrusted users.  
User names are case-sensitive.

Cancel OK

**ステップ 5** 指定のフィールドに、username@domain.com の形式で 1 行に 1 つのユーザー名を入力して Enter を押し、別のユーザー名を入力します。

各ユーザー名はアイデンティティ インテリジェンス によって信頼できるとみなされます。

## システム作成のアクセス コントロール ポリシーの表示と編集

このトピックでは、システムで作成されたアクセス制御ルールとアクセス コントロール ポリシーを編集する方法について説明します。最初は、ポリシーはデバイスに関連付けられていませんが、それを使用する場合は、デバイスの追加、ルールの変更、ルールの順序変更、またはルールの削除を行えます。

### 始める前に

「[システム定義のアクセス制御ルールの表示 \(13 ページ\)](#)」で説明されている操作を完了させます。

### 手順

**ステップ 1** まだ Cisco Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ2 [ポリシー (Policies)] > [アクセス制御 (Access Control)] 見出し > [アクセス制御 (Access Control)] をクリックします。

ステップ3 [Dynamic Firewall Policy] (または同様の名前) という名前のポリシーの横にある [編集 (Edit)] (🔗) をクリックします。

次の図に、サンプルのアクセス コントロール ポリシーを示します。

	Name	Action	Source			Destination		
			Zones	Networks	Dynamic Attributes	Zones	Networks	Ports
Mandatory 3 rules (1 - 3)								
<input type="checkbox"/>	1	Inspect_Questionable...	Monitor	Any	Any	Questionable_User	Any	Any
<input type="checkbox"/>	2	Block_Untrusted_Device	Block	Any	Any	Untrusted_Device	Any	Any
<input type="checkbox"/>	3	Block_Untrusted_User	Block	Any	Any	Untrusted_User	Any	Any
Default (No rules)								

このアクセスコントロールポリシーでは、疑わしいユーザーを監視するルールセットのみがログに記録されることに注意してください。ロギング設定を調整するには、「[アクセスコントロールポリシーのロギング設定](#)」を参照してください。

ステップ4 次のいずれかを実行します。

- デバイスでアクセス コントロール ポリシーをターゲットにする：[アクセス コントロール ポリシーへのデバイスの割り当て](#)。
- ポリシーを編集する（ロギングの追加など）：[アクセス コントロール ポリシーの管理](#)。
- アクセス制御ルールを編集する：[アクセス制御ルールの管理](#)。
- 詳細ポリシーオプションを設定する：[アクセス コントロール ポリシーの詳細設定](#)。
- このアクセスコントロールポリシーに他のポリシーを関連付ける：[アクセス制御への他のポリシーの関連付け](#)。

## ダイナミック属性フィルタの作成

を使用して定義する動的属性フィルタは、アクセス コントロール ポリシーで使用できるダイナミックオブジェクトとして Cisco Secure Firewall Management Center で公開されます。たとえば、財務部門の AWS サーバーへのアクセスを、Microsoft Active Directory で定義された財務グループのメンバーのみに制限できます。

## 手順

ステップ1 Cisco Secure Firewall Management Center にログインします。

ステップ2 [統合 (Integration)] > [ダイナミック属性コネクタ (Dynamic Attributes Connector)] > [コネクタ (Connectors)] をクリックします。

ステップ3 次のいずれかを実行します。

- 新しいフィルタの追加：追加 (+) をクリックします。
- フィルタの編集または削除：その他 (⋮) をクリックしてから、行の末尾にある [編集 (Edit)] または [削除 (Delete)] をクリックします。

ステップ4 次の情報を入力します。

項目	説明
[名前 (Name)]	アクセス コントロール ポリシーおよび Cisco Secure Firewall Management Center オブジェクトマネージャ ([外部属性 (External Attributes)] > [ダイナミックオブジェクト (Dynamic Object)]) で動的フィルタを (ダイナミックオブジェクトとして) 識別するための一意の名前。
コネクタ (Connector)	リストから、使用するコネクタの名前をクリックします。
クエリ (Query)	[追加 (Add)] (+) をクリックします。

ステップ5 クエリを追加するには、次の情報を入力します。

項目	説明
キー (Key)	リストからキーをクリックします。キーはコネクタから取得されます。
操作 (Operation)	次のいずれかをクリックします。 <ul style="list-style-type: none"> <li>• キーを値に正確に一致させるには、[等しい (Equals)]。</li> <li>• 値のいずれかの部分が一一致する場合に、キーを値に一致させるには、[含む (Contains)]。</li> </ul>
値 (Value)	[任意 (Any)] または [すべて (All)] をクリックし、リストから1つ以上の値をクリックします。[別

項目	説明
	の値を追加 (Add another value) ] をクリックして、クエリに値を追加します。

**ステップ 6** [プレビューを表示 (Show Preview) ] をクリックして、クエリによって返されたネットワークまたは IP アドレスのリストを表示します。

**ステップ 7** 完了したら、[保存 (Save) ] をクリックします。

**ステップ 8** (オプション) Cisco Secure Firewall Management Center のダイナミックオブジェクトを確認します。

- a) 最低限でもネットワーク管理者ロールを持つユーザーとして Cisco Secure Firewall Management Center にログインします。
- b) [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] > [外部属性 (External Attributes) ] > [ダイナミックオブジェクト (Dynamic Objects) ] をクリックします。  
作成した動的属性クエリは、ダイナミックオブジェクトとして表示されます。



## 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。