アイデンティティ ソース：パッシブ アイデンティティ エージェント

次のトピックでは、passive identity agent を設定および使用する方法について説明します。

passive identity agent アイデンティティソース

passive identity agentのアイデンティティソースは、Microsoft Active Directory（AD）から Secure Firewall Management Center にセッションデータを送信します。必要なものは、レルムとレルムシーケンスについての説明に従ってセットアップされた、サポートされている Microsoft AD だけです。

passive identity agent バージョン 1.0 は IPv4 ユーザーセッションのみを送信しますが、バージョン 1.1 は IPv4 および IPv6 ユーザーセッションを送信します。

（注） このアイデンティティソースを使用するために Cisco Identity Services Engine（ISE）を設定する必要はありません。

Passive identity agent のロール

passive identity agent は、以下のロールをサポートしています。

- スタンドアロン：冗長ペアの一部ではない passive identity agent。スタンドアロンエージェントは、複数の Active Directory（AD）サーバーとドメインコントローラのすべてにソフトウェアがインストールされている場合に、それらからユーザーとグループを読み取ることができます。
- プライマリ：（冗長ペアのプライマリエージェント）Microsoft AD ドメインコントローラ、ディレクトリサーバ、または任意のネットワーククライアントにインストールできます。

  Secure Firewall Management Center とのすべての通信を処理します。ただし、通信が停止した場合はセカンダリエージェントによって処理されます。
- セカンダリ：（冗長ペアのセカンダリ（バックアップ）エージェント）Microsoft AD ドメインコントローラ、ディレクトリサーバー、または任意のネットワーククライアントにインストールできます。

  プライマリエージェントの正常性をモニタリングし、プライマリエージェントが Secure Firewall Management Center との通信を停止した場合に引き継ぎます。

Passive identity agent システム要件

passive identity agent の前提条件は次のとおりです。

- Windows Active Directory サーバーに passive identity agent をインストールする場合は、サーバーで Windows Server 2008 以降を実行する必要があります。
- ドメインに接続されている Windows クライアントにインストールする場合、クライアントは Windows 8 以降を実行している必要があります。
- すべてのシステムのシステムクロックを同期する必要があります。すべてのシステムで同じ NTP サーバーを使用することを強く推奨します。これは、以下を意味します。
  - Secure Firewall Management Center。

    詳細については、「時刻の同期」を参照してください。
  - すべての Windows Active Directory サーバーおよびドメインコントローラ。
  - passive identity agent がインストールされているマシン。
- Secure Firewall Management Center では 7.6 以降を実行する必要があります。
- Secure Firewall Management Center によって管理される Secure Firewall Threat Defense は、7.1 以降を実行する必要があります。
- Secure Firewall Threat Defense デバイスで Snort 3 を有効にする必要があります。

Passive identity agent の制限事項

passive identity agent には次の制限があります。

- 同時に最大 10 のエージェント
- 1 つの passive identity agent アイデンティティソースで最大 50 の AD ディレクトリをモニタリングできます。
- 最大 300,000 の同時ユーザーセッション
- IPv6 アドレスはサポートされていません（passive identity agent1.0）
- IPv6 アドレスはサポートされています（passive identity agent1.1）

passive identity agent の導入

展開オプションについては、passive identity agent の導入 （3 ページ）を参照してください。

（注） passive identity agentの最新バージョンを使用することを推奨します。使用可能なバージョンを確認するには、software.cisco.com にアクセスします。passive identity agentをアップグレードするには、「passive identity agent ソフトウェアをアップグレードする （32 ページ）」を参照してください

passive identity agent の導入

ユーザー認識と制御に使用する Microsoft Active Directory（AD）ドメインの一部である任意のマシンに passive identity agent ソフトウェアをインストールできます。つまり、以下のいずれかにインストールできます。

- Microsoft Active Directory サーバー
- ドメインコントローラ
- ディレクトリサーバーでもドメインコントローラでもないネットワークに接続されているクライアント

特定の passive identity agent は、同じドメイン内の 1 つまたは複数の Active Directory ドメインコントローラをモニタリングできます。

passive identity agent が TLS/SSL プロトコルを使用して Secure Firewall Management Center と通信する必要があるマシン。詳細については、「passive identity agent のインターネットアクセス要件 （37 ページ）」を参照してください。

エージェントのタイプ

Microsoft ADディレクトリサーバー、ドメインコントローラ、またはドメインに接続されている任意のクライアントで、次のタイプのエージェントを設定できます。

- スタンドアロンエージェント：同じドメイン内の1つまたは複数のアクティブディレクトリ ドメインコントローラをモニタリングできる 1 つのエージェント。
- プライマリエージェントとセカンダリエージェントは、同じドメイン内の1つまたは複数の AD ドメインコントローラをモニタリングできます。冗長性を目的として、プライマリエージェントとセカンダリエージェントを異なるマシンにインストールできます。プライマリは Secure Firewall Management Center との通信を担当しますが、通信が失敗した場合はセカンダリエージェントが引き継ぎます。

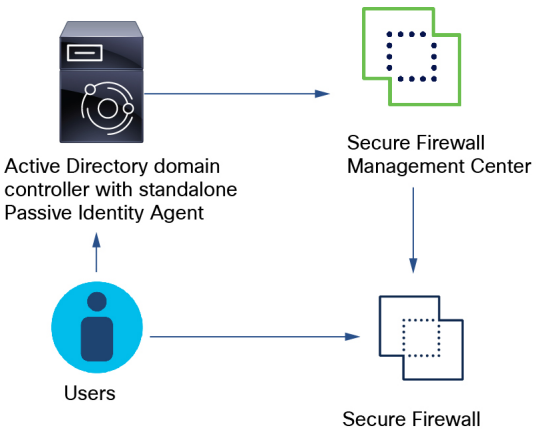
詳細については、次のトピックの 1 つを参照してください。

関連トピック

シンプルな passive identity agent の展開 （4 ページ）
複数のドメイン コントローラの単一 passive identity agent によるモニタリング （5 ページ）
複数の passive identity agent による複数のドメイン コントローラのモニタリング （5 ページ）
Passive identity agent プライマリ/セカンダリ エージェントの展開 （7 ページ）

シンプルな passive identity agent の展開

次の図に、最もシンプルな passive identity agent の展開を示します。

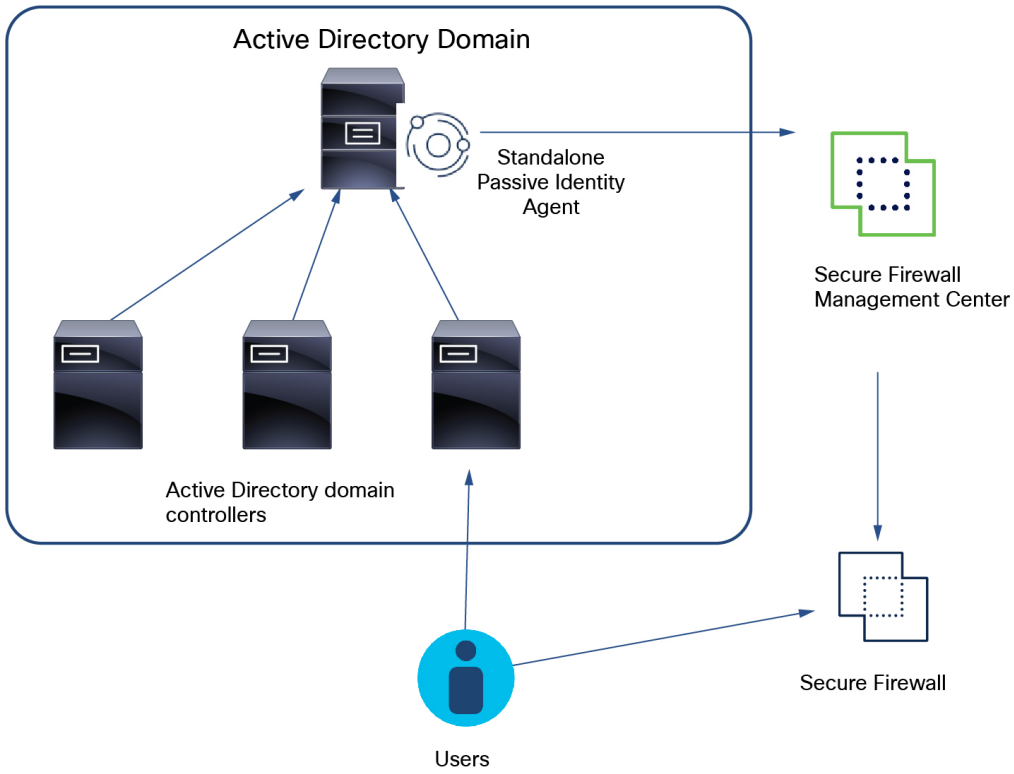


前の例では、スタンドアロンの passive identity agent が AD ドメイン コントローラにインストールされています。ユーザーが AD ドメインにログインおよびログアウトすると、エージェントはユーザー名と IP アドレスの情報を Secure Firewall Management Center に送信します。ユーザーがネットワークにアクセスするときに、Secure Firewall Threat Defense に展開されたアクセス コントロール ポリシーとアイデンティティ ポリシーによって、アクセスを許可するかどうか、およびアクセスを許可する方法が決定されます。

passive identity agent は、AD ドメインコントローラ、ディレクトリサーバー、またはモニタリングするドメインに接続されている任意のクライアントにインストールできます。

複数のドメイン コントローラの単一 passive identity agent によるモニタリング

次の図は、複数の AD ドメインコントローラをモニターするスタンドアロンの passive identity agent を示しています。



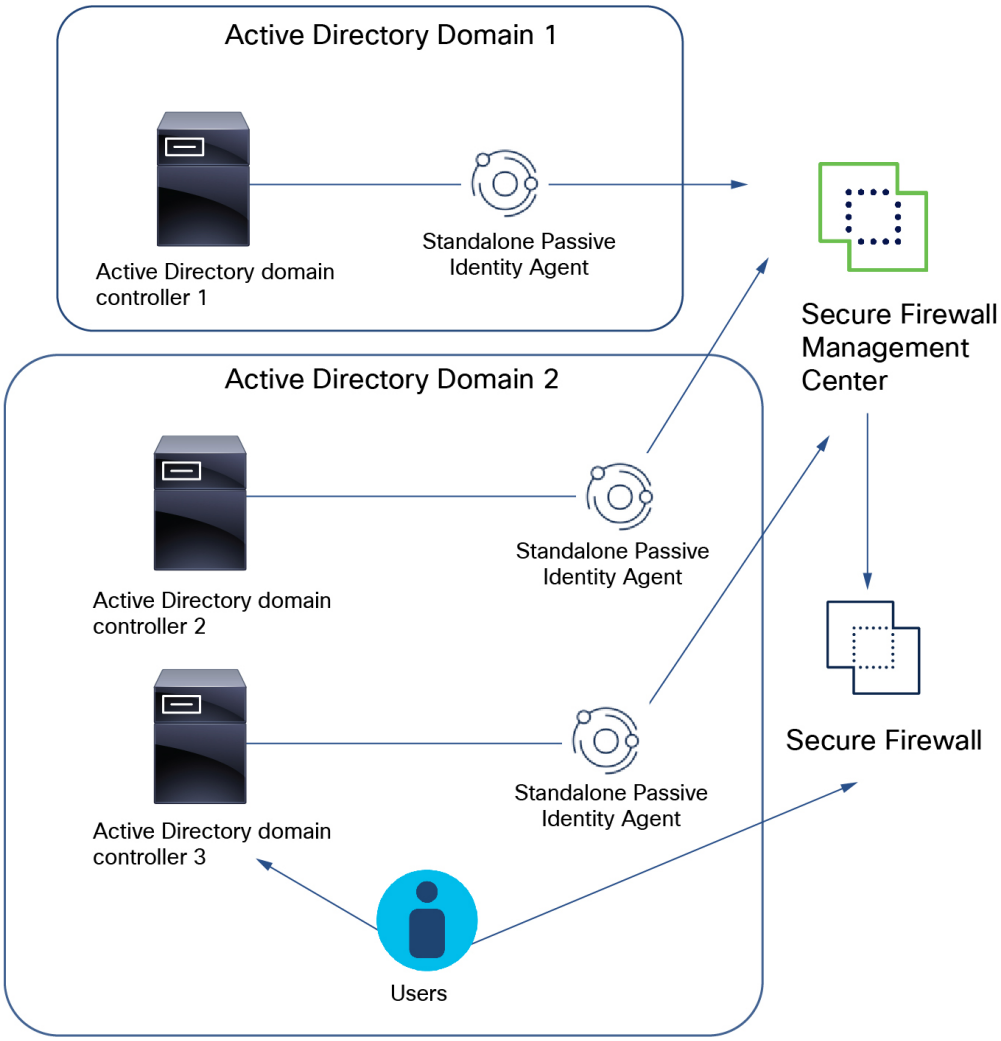
前の図では、スタンドアロンの passive identity agent が、AD ドメイン（またはドメイン コントローラ自体）に接続されたクライアントにインストールされています。ユーザーがいずれかのドメイン コントローラにログインすると、エージェントはユーザーと IP アドレスの情報を Secure Firewall Management Centerに送信します。ユーザーがネットワークにアクセスするときに、Secure Firewall Threat Defense に展開されたアクセス コントロール ポリシーとアイデンティティ ポリシーによって、アクセスを許可するかどうか、およびアクセスを許可する方法が決定されます。

passive identity agent は、AD ドメインコントローラ、ディレクトリサーバー、またはモニタリングするドメインに接続されている任意のクライアントにインストールできます。

複数の passive identity agent による複数のドメイン コントローラのモニタリング

次の図は、複数の AD ドメインコントローラのスタンドアロンモニタリングを示しています。

- AD ドメイン 1 では、AD ドメイン コントローラ 1 に接続されたマシンにインストールされたスタンドアロン passive identity agent が、ユーザーおよび IP アドレスのマッピングデータを Secure Firewall Management Centerに送信します。
- AD ドメイン 2 では、AD ドメインコントローラ 1 および 2 にインストールされているスタンドアロン エージェントが、ユーザーおよび IP アドレスのマッピングデータを Secure Firewall Management Centerに送信します。



passive identity agent は、AD ドメインコントローラ、ディレクトリサーバー、またはモニタリングするドメインに接続されている任意のクライアントにインストールできます。

前の図は、それぞれスタンドアロンとして設定された 3 つの passive identity agentを示しています。手順

1. 2 つの Microsoft AD レルムを作成します（各 AD ドメインに 1 つ）。

   LDAP レルムまたはActive Directory（AD）レルムおよびレルムディレクトリを作成するを参照してください。

2. AD ドメイン 2 では、各ドメインコントローラに 1 つずつ、2 つのディレクトリを作成します。
3. ドメインにログインできるクライアントに Passive Identity Agent ソフトウェアをインストールします。

   passive identity agent 送信元を設定する Secure Firewall Management Center と通信するように、各 passive identity agent を個別に設定します。

   Passive Identity Agent ソフトウェアのインストール （27 ページ）を参照してください。
4. passive identity agent アイデンティティ ソースを作成します。

   「プライマリまたはセカンダリ passive identity agent アイデンティティソースを作成する（15 ページ）」を参照してください。

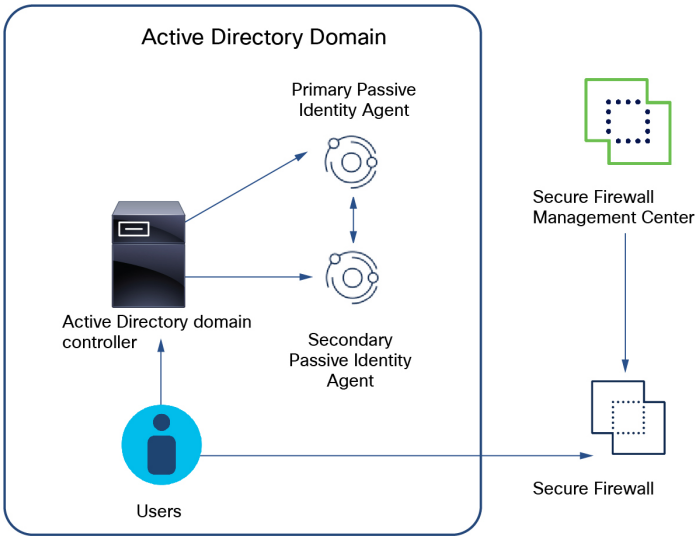
Passive identity agent プライマリ/セカンダリ エージェントの展開

冗長性を提供し、シングルポイント障害を回避するために、このトピックで示されているいずれかの方法でプライマリおよびセカンダリ passive identity agent を設定できます。

passive identity agent は、AD ドメインコントローラ、ディレクトリサーバー、またはモニタリングするドメインに接続されている任意のクライアントにインストールできます。

プライマリ エージェントとセカンダリ エージェントを備えた単一の AD ドメイン コントローラ

次の図は、1 つの AD ドメイン コントローラ上でプライマリおよびセカンダリ passive identity agentを設定する方法を示しています。プライマリ エージェントで障害が発生すると、セカンダリが引き継ぎます。



これを設定するには、次の手順を実行します。

1. ドメインコントローラ用に 1 つのディレクトリを持つ Microsoft AD レルムを作成します。

   LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成するを参照してください。

2. ドメイン コントローラに接続されている任意の 2 台のネットワーク マシンに passive identity agent ソフトウェアをインストールします。

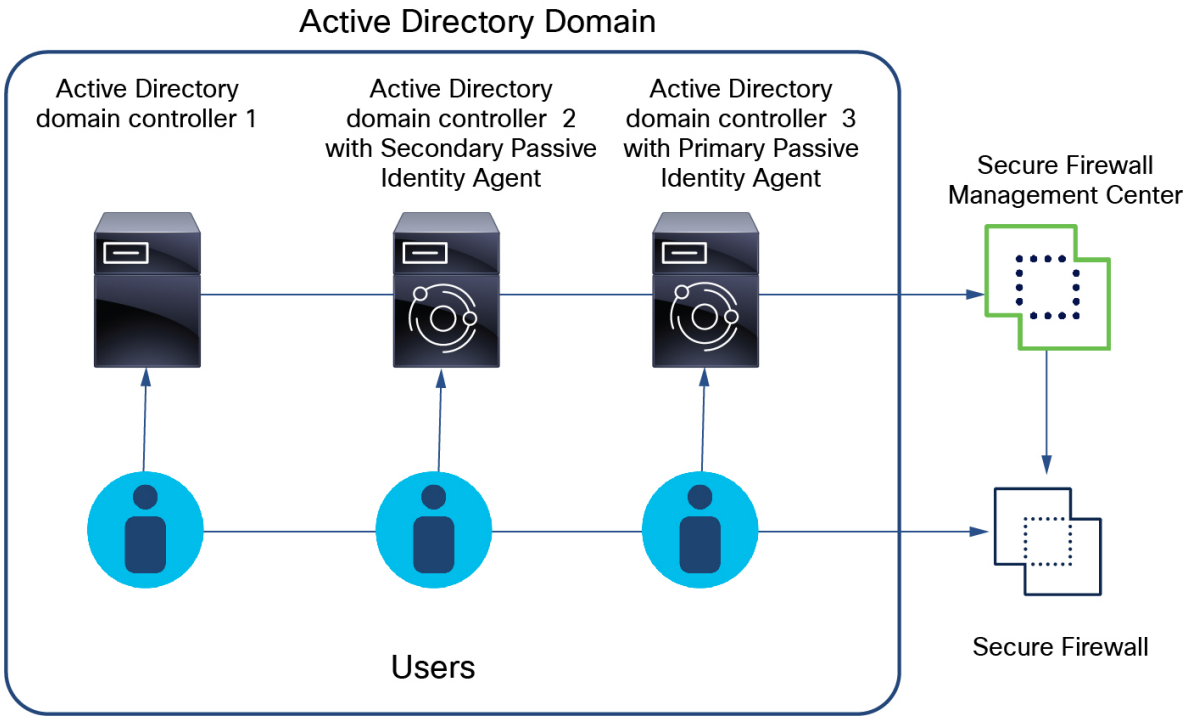
   passive identity agent 送信元を設定する Secure Firewall Management Center と通信するように、各 passive identity agent を個別に設定します。

   Passive Identity Agent ソフトウェアのインストール （27 ページ）を参照してください。

3. アイデンティティ ソースを作成します。

   プライマリまたはセカンダリ passive identity agent アイデンティティ ソースを作成する （15 ページ）を参照してください。

複数の AD ドメイン コントローラ、プライマリ エージェントとセカンダリ エージェント



前の図は、プライマリ エージェントとセカンダリ エージェントを 3 つの AD ドメイン コントローラをモニターするように設定する方法を示しています。プライマリ エージェントで障害が発生すると、セカンダリ エージェントが引き継ぎます。

これを設定するには、次の手順を実行します。

1. ドメインコントローラ用に 1 つのディレクトリを持つ Microsoft AD レルムを作成します。

   LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成するを参照してください。

2. ドメイン コントローラに接続されている任意のマシンに passive identity agent ソフトウェアをインストールします。

   passive identity agent 送信元を設定する Secure Firewall Management Center と通信するように、各 passive identity agent を個別に設定します。

   Passive Identity Agent ソフトウェアのインストール （27 ページ）を参照してください。

3. アイデンティティ ソースを作成します。

   「プライマリまたはセカンダリ passive identity agent アイデンティティソースを作成する（15 ページ）」を参照してください。

passive identity agent アイデンティティ ソースの作成方法

次に、Secure Firewall Management Center で passive identity agent アイデンティティ ソースを設定し、Microsoft Active Directory（AD）サーバーにエージェント ソフトウェアを展開するために必要なタスクの概要を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	Dynamic Attributes Connector をイネーブルにします。	dynamic attributes connector は、 passive identity agentを使用するための要件です。 dynamic attributes connector の有効化 （11 ページ）を参照してください。
ステップ 2	Microsoft AD ドメインとドメインコントローラのレルムを作成します。	レルムとは、Secure Firewall Management Center とモニタリング対象のサーバー上にあるユーザーアカウントの間の接続です。レルムでは、サーバの接続設定と認証フィルタの設定を指定します。 詳細については、LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成するを参照してください。
ステップ 3	passive identity agent 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 ソースにより Secure Firewall Management Center と passive identity agent の相互通信が可能になります。必要に応じて、スタンドアロン、プライマリ、またはセカンダリ エージェントを作成します。

	コマンドまたはアクション	目的
		詳細については、以下を参照してください。 • passive identity agent ロールについて（18 ページ） • passive identity agent アイデンティティ ソースを作成する （11 ページ）
ステップ 4	Secure Firewall Management Center で passive identity agent ユーザーを作成します。	エージェントとマネージャが相互に通信するのに十分なロールを提供します。passive identity agent ユーザーには、そのロールを使用し、他のロールを使用しないことを推奨します。
ステップ 5	passive identity agent ソフトウェアをインストールします。	エージェントのインストール方法は、展開によって異なります。 passive identity agent は、AD ドメインコントローラ、ディレクトリサーバー、またはモニタリングするドメインに接続されている任意のクライアントにインストールできます。 詳細については、以下を参照してください。 • passive identity agent の導入 （3 ページ） • Passive Identity Agent ソフトウェアのインストール （27 ページ）

次のタスク

LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する。

passive identity agent の設定

次のトピックでは、passive identity agent を設定する方法について説明します。

関連トピック

LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する
passive identity agent アイデンティティ ソースを作成する （11 ページ）
Passive Identity Agent ソフトウェアのインストール （27 ページ）

passive identity agent に対して Secure Firewall Management Center ユーザーを作成する （18 ページ）

dynamic attributes connector の有効化

このタスクでは、Secure Firewall Management Center で dynamic attributes connector を有効にする方法について説明します。dynamic attributes connector は、クラウドネットワーキング製品のオブジェクトを Secure Firewall Management Center アクセス制御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 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 **Integration** > **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 dynamic attributes connector 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。

Microsoft Active Directory レルムの作成

LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する で説明されているように、passive identity agent では、Secure Firewall Management Center に Microsoft Active Directory（AD）レルムおよびディレクトリを作成する必要があります。

passive identity agent アイデンティティソースを作成する

このタスクでは、ユーザー セッション アクティビティを Secure Firewall Management Center に送信する passive identity agent を作成する方法について説明します。

始める前に

次の手順を実行します。

- passive identity agent ロールについて （18 ページ） の説明に従って、 passive identity agent ロールを確認します。
- LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する の説明に従って、Microsoft AD レルムを作成します。

手順

ステップ 1 管理者として Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Other Integrations** > **Identity Sources** をクリックします。

ステップ 3 **[パッシブ アイデンティティ エージェント（Passive Identity Agent）]** をクリックします。

ステップ 4 Dynamic Attributes Connector がまだイネーブルになっていない場合は、イネーブルにするように求められます。

dynamic attributes connector の有効化の詳細については、dynamic attributes connector の有効化（11 ページ）を参照してください。

ステップ 5 [エージェントの作成（Create Agent）] をクリックします。

ステップ 6 [エージェントの設定（Configure Agent）] ダイアログ ボックスに、次の情報を入力します。

項目	説明
名前（Name）	この passive identity agent を識別するための一意の名前を入力します。
説明（Description）	任意で説明を入力します。
[ロール（Role）]	次のいずれかをクリックします。 • **プライマリ**： Secure Firewall Management Centerとの通信を担当するエージェント。 **[スタンドアロン（Standalone）]**を選択した場合には使用できません。 • **セカンダリ**：プライマリ が Secure Firewall Management Centerとの接続を失った場合にプライマリになります。 **[スタンドアロン（Standalone）]**を選択した場合には使用できません。 • **スタンドアロン**：passive identity agent が 1 つしかない場合。 ロールの詳細については、passive identity agent ロールについて （18 ページ）を参照してください。

ステップ 7 次に進みます：

• スタンドアロン passive identity agent アイデンティティ ソースを作成する （13 ページ）

- プライマリまたはセカンダリ passive identity agent アイデンティティ ソースを作成する （15 ページ）

スタンドアロン passive identity agent アイデンティティ ソースを作成する

このタスクでは、スタンドアロン passive identity agent の設定方法について説明します。

始める前に

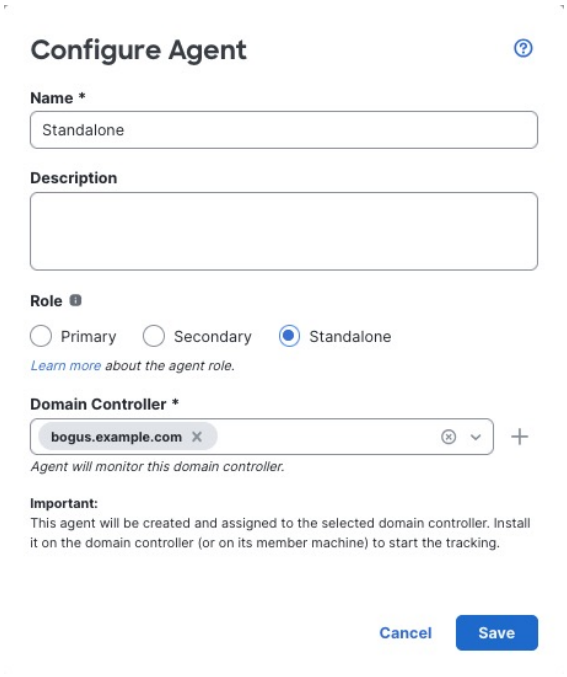
「passive identity agent アイデンティティ ソースを作成する （11 ページ）」で説明されているタスクを完了します。

手順

ステップ 1 [エージェントの設定（Configure Agent）] ダイアログ ボックスに、次の情報を入力します。

項目	説明
[ロール（Role）]	**[スタンドアロン（Standalone）]**をクリックします。
ドメインコントローラ（Domain Controller）	リストから、アイデンティティ管理とユーザー制御に使用する passive identity agent を持つ各ドメイン コントローラの横にあるチェックボックスをオンにします。 （オプション）**Add** (＋) をクリックして新しいものを追加します。

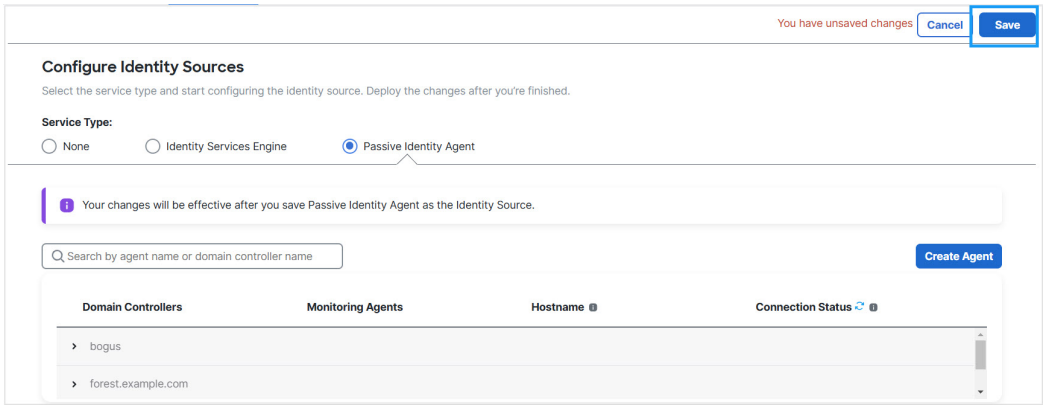
次の図に、スタンドアロン passive identity agent アイデンティティ ソースの例を示します。



ステップ 2 [エージェントの構成（Configure Agent）] ダイアログボックスで、**[保存（Save）]**をクリックします。

ステップ 3 ページの右上隅で、**[保存（Save）]** をクリックします。

次の図は例を示しています。



（注）
passive identity agent は、ユーザーを作成してソフトウェアをインストールするまでアクティブになりません。

次のタスク

- passive identity agent に対して Secure Firewall Management Center ユーザーを作成する （18 ページ）を参照してください
- 「passive identity agent インストールについて （22 ページ）」を参照してください。

プライマリまたはセカンダリ passive identity agent アイデンティティ ソースを作成する

次のタスクは、passive identity agent アイデンティティ ソースを作成する （11 ページ） からの続きです。

始める前に

「passive identity agent アイデンティティ ソースを作成する （11 ページ）」で説明されているタスクを完了します。

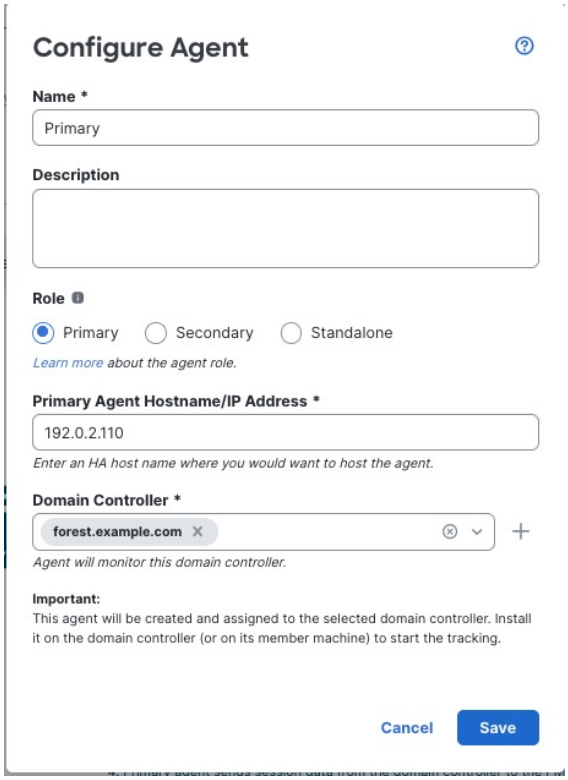
手順

ステップ 1 [エージェントの設定（Configure Agent）] ダイアログ ボックスに、次の情報を入力します。

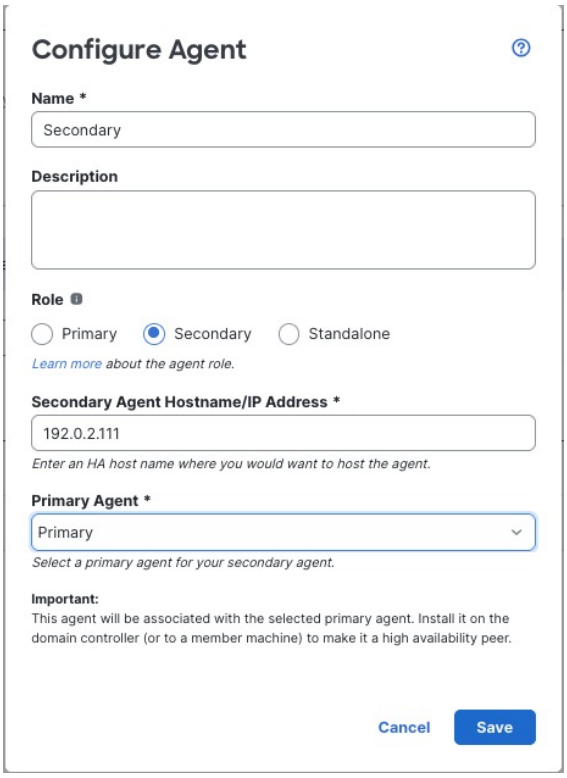
項目	説明
[ロール（Role）]	次のいずれかをクリックします。 • **プライマリ**： Secure Firewall Management Centerとの通信を担当するエージェント。 • **セカンダリ**：プライマリ が Secure Firewall Management Centerとの接続を失った場合にプライマリになります。 ロールの詳細については、passive identity agent ロールについて （18 ページ）を参照してください。
プライマリエージェントのホスト名/IPアドレス	（プライマリ エージェントのみ）。プライマリ passive identity agentがインストールされているサーバーの完全修飾ドメイン名または IP アドレスを入力します。 passive identity agent バージョン 1.0 は、IPv4 アドレスと完全修飾ドメイン名のみをサポートしています。バージョン 1.1 は、IPv4、IPv6、および完全修飾ドメイン名をサポートしています。

項目	説明
セカンダリエージェントのホスト名/IPアドレス	（セカンダリ エージェントのみ）。セカンダリ passive identity agent がインストールされているサーバーの完全修飾ホスト名または IP アドレスを入力します。 passive identity agent バージョン 1.0 は、IPv4 アドレスと完全修飾ドメイン名のみをサポートしています。バージョン 1.1 は、IPv4、IPv6、および完全修飾ドメイン名をサポートしています。
プライマリエージェント	（セカンダリ エージェントのみ）。リストから、プライマリ passive identity agent の名前をクリックします。
ドメインコントローラ（Domain Controller）	（プライマリ エージェントのみ）。リストから、アイデンティティ管理とユーザー制御に使用する passive identity agent を持つ各ドメイン コントローラの横にあるチェックボックスをオンにします。

次の図に、プライマリ エージェントの例を示します。



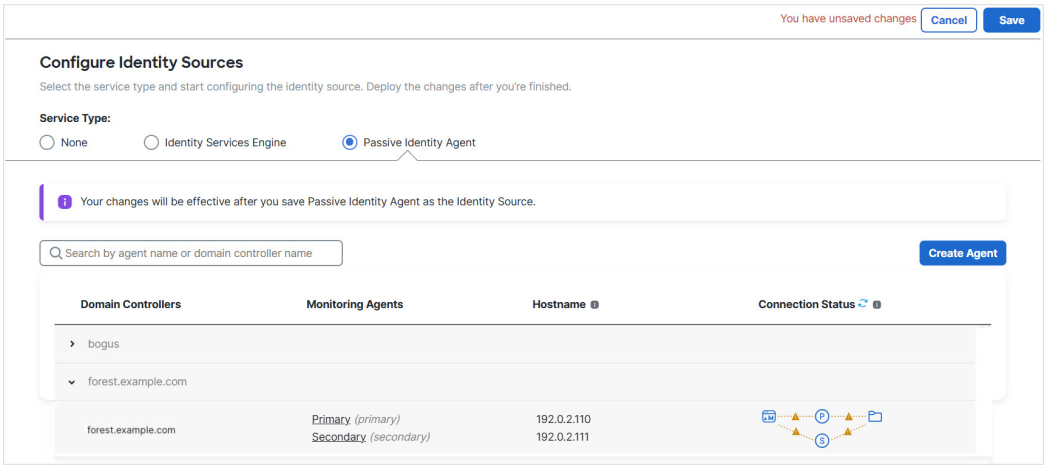
次の図はセカンダリ エージェントの例を示しています。



ステップ 2 [エージェントの構成（Configure Agent）] ダイアログボックスで、**[保存（Save）]**をクリックします。

ステップ 3 ページの右上隅で、**[保存（Save）]** をクリックします。

次の図は例を示しています。



（注）

passive identity agent は、ユーザーを作成してソフトウェアをインストールするまでアクティブになりません。

次のタスク

- passive identity agent に対して Secure Firewall Management Center ユーザーを作成する （18 ページ）を参照してください
- 「passive identity agent インストールについて （22 ページ）」を参照してください。

passive identity agent ロールについて

passive identity agent には、次のロールがあります。

- スタンドアロン：冗長ペアの一部ではない passive identity agent。スタンドアロンエージェントは、複数の Active Directory（AD）サーバーとドメインコントローラのすべてにソフトウェアがインストールされている場合に、それらからユーザーとグループを読み取ることができます。
- プライマリ：（冗長ペアのプライマリエージェント）Microsoft AD ドメインコントローラ、ディレクトリサーバ、または任意のネットワーククライアントにインストールできます。

  Secure Firewall Management Center とのすべての通信を処理します。ただし、通信が停止した場合はセカンダリエージェントによって処理されます。
- セカンダリ：（冗長ペアのセカンダリ（バックアップ）エージェント）Microsoft AD ドメインコントローラ、ディレクトリサーバー、または任意のネットワーククライアントにインストールできます。

  プライマリエージェントの正常性をモニタリングし、プライマリエージェントが Secure Firewall Management Center との通信を停止した場合に引き継ぎます。

同じドメインの一部である複数の AD ドメインコントローラをモニターできます。

passive identity agent に対して Secure Firewall Management Center ユーザーを作成する

このタスクでは passive identity agentと通信するための十分な権限を持つ Secure Firewall Management Center ユーザーを作成する方法について説明します。このユーザーは、他のタスクを実行する権限が制限されています。ユーザーは、 passive identity agentとの通信がイネーブルになっていることのみが期待されています。

（注） passive identity agent ユーザーには **Passive Identity User** ロールのみを使用します。特に、passive identity agent に対して **Administrator** ロールを使用しないでください。 **Administrator** は、passive identity agent が Secure Firewall Management Centerと通信するため、定期的にログオフされます。

始める前に

「passive identity agent アイデンティティソースを作成する （11 ページ）」で説明されているタスクを完了します。

（注） Passive Identity Agent ユーザーで外部認証を使用することはできません。

手順

ステップ 1 管理者として Secure Firewall Management Center にログインします。

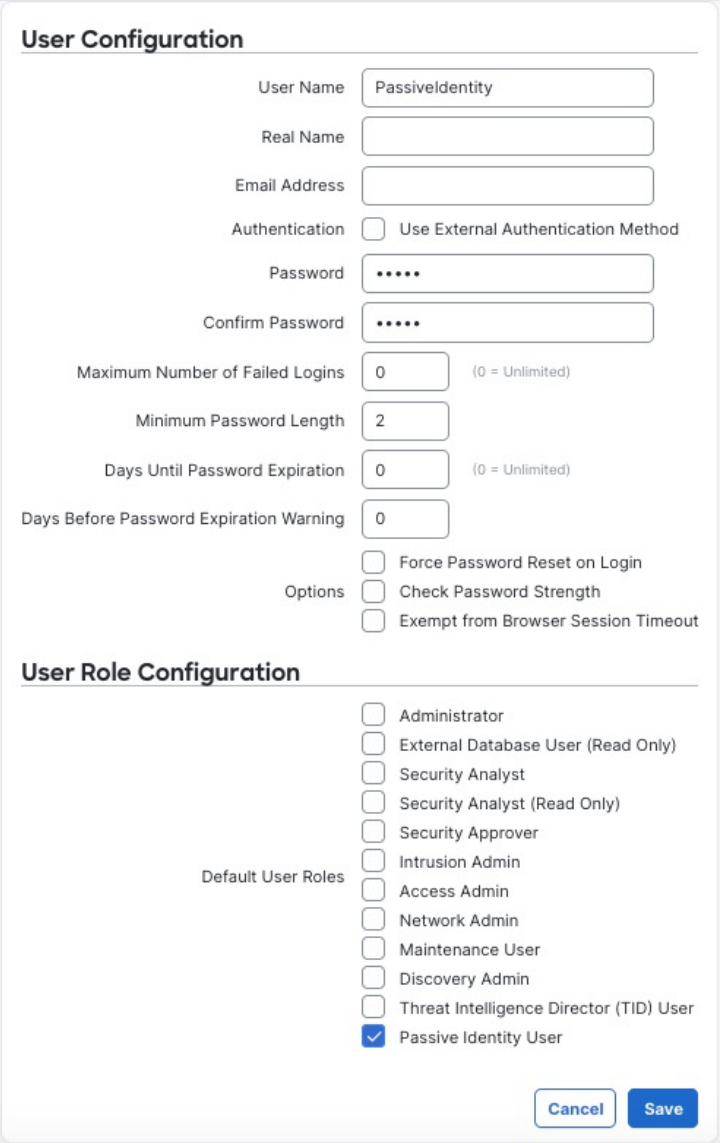
ステップ 2 **System** (⚙) > **Users** > **Users** をクリックします。

ステップ 3 [ユーザの作成（Create User）] をクリックします。

ステップ 4 *Cisco Secure Firewall Management Center* アドミニストレーション ガイドの内部ユーザーの追加または編集の説明に従ってユーザーを作成します。

ステップ 5 **[パッシブ アイデンティティのユーザー（Passive Identity User）]** ロールを選択します。

次の図は例を示しています。



（注）
エージェントが適切に機能しなくなるため、passive identity agent ユーザーには **Passive Identity User** 以外のロールを選択しないでください。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

passive identity agent インストールについて （22 ページ）。

passive identity agent のトラブルシューティング

このトピックでは、Windows AD ドメインコントローラまたはディレクトリサーバー上の passive identity agent ソフトウェアのトラブルシューティング方法について説明します。

（オプション）ログ レベルを設定します。

デフォルトでは、passive identity agent は INFO レベルでログに書き込みます。オプションでログレベルを変更するには、テキストエディタで **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config** を開き、ファイルを保存して、Cisco Passive Identity Agent サービスを再起動します。

ロギング サービスの名前は変更しないでください

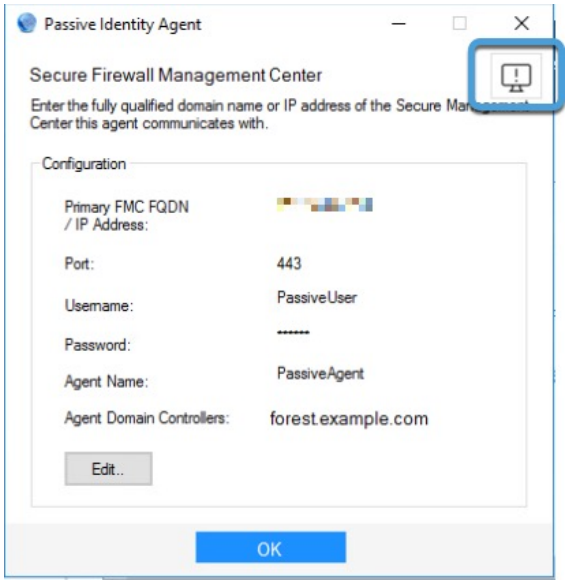
C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config の名前は変更しないでください。変更した場合、passive identity agent はログ ファイルの生成を停止します。**.exe.config** ファイルの拡張子を削除または変更しないでください。

トラブルシューティング ファイルの生成

トラブルシューティング ファイルを含む .zip を生成するには：

1. Microsoft Active Directory ドメイン コントローラにログインします。
2. ソフトウェア passive identity agent を起動します。
3. ウィンドウの右上隅の [トラブルシューティング（Troubleshooting）] ボタンをクリックします。

   次の図は例を示しています。



確認メッセージが表示されます。

トラブルシューティングログは、システムの [ダウンロード（Download）] フォルダに保存されます。ファイル名は **TroubleshootLogs**で始まります。

ログ ファイルを手動で表示する

Passive identity agent ログファイルは、エージェントのインストールディレクトリである **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**にプレーン テキスト形式で保存されます。

これらのファイルを表示するには、メモ帳または別のテキストエディタを使用します。ログファイルは、サイズが 10MB に達するとローテーションされます。

Microsoft Active Directory イベントビューアを使用する

Secure Firewall Management Center にユーザー セッションが表示されない場合は、Microsoft Active Directory サーバーのイベント ビューアで次の Kerberos 関連イベントを調べることができます。

- 4770
- 4768

監査ポリシーの一般的な情報については、learn.microsoft.com の Audit Policy Recommendations を参照してください。

Windows グループ ポリシー オブジェクトの設定の詳細については、learn.microsoft.com の Group Policy Objects を参照してください。

passive identity agent インストールについて

以下のトピックでは、passive identity agentをインストールするために必要な前提条件とタスクについて説明します。

（注） passive identity agentの最新バージョンを使用することを推奨します。使用可能なバージョンを確認するには、software.cisco.com にアクセスします。passive identity agentをアップグレードするには、「passive identity agent ソフトウェアをアップグレードする （32 ページ）」を参照してください

passive identity agent をインストールするための前提条件

passive identity agent ソフトウェアをインストールする前に次のタスクをすべて完了させる必要があります。

Passive identity agent システム要件

Passive identity agent システム要件

passive identity agent の前提条件は次のとおりです。

- Windows Active Directory サーバーに passive identity agent をインストールする場合は、サーバーで Windows Server 2008 以降を実行する必要があります。
- ドメインに接続されている Windows クライアントにインストールする場合、クライアントは Windows 8 以降を実行している必要があります。
- すべてのシステムのシステムクロックを同期する必要があります。すべてのシステムで同じ NTP サーバーを使用することを強く推奨します。これは、以下を意味します。
  - Secure Firewall Management Center。

    詳細については、「時刻の同期」を参照してください。
  - すべての Windows Active Directory サーバーおよびドメインコントローラ。
  - passive identity agent がインストールされているマシン。
- Secure Firewall Management Center では 7.6 以降を実行する必要があります。
- Secure Firewall Management Center によって管理される Secure Firewall Threat Defense は、7.1 以降を実行する必要があります。
- Secure Firewall Threat Defense デバイスで Snort 3 を有効にする必要があります。

Windows イベントビューアを有効にして ケルベロス認証試行をログに記録する

次のタスクでは、Windows Group Policy Object（GPO）セキュリティ設定を構成して、Windows イベントビューアを有効にし、ケルベロス認証試行の成功と失敗をログに記録する方法を説明します。passive identity agent は、イベントビューアからのユーザーセッションを読み取るため、この設定は、passive identity agent を正常に機能させるために必要です。

詳細については、learn.microsoft.com の「システム監査ポリシーの推奨事項」を参照してください。

手順

ステップ 1 ドメイン管理者として、アクティブ ディレクトリ サーバにログインします。

ステップ 2 管理者として DOS コマンドプロンプトを開きます。

ステップ 3 `gpmc.msc` と入力して、グループ ポリシー管理エディタを起動します。

ステップ 4 必要に応じて、新しい GPO を作成します。すでに存在する場合は編集します。

GPO の作成の詳細については、learn.microsoft.com の Create a Group Policy Object などのリソースを参照してください。

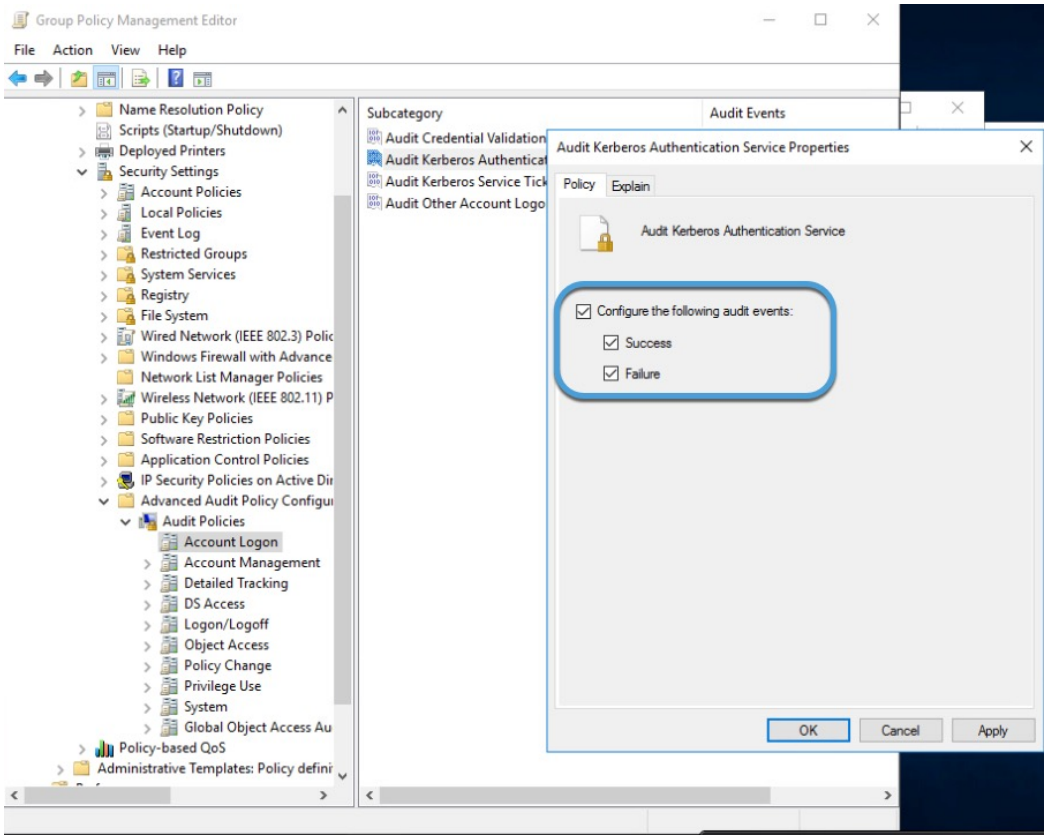
ステップ 5 GPO で、**[コンピュータの構成（Computer Configuration）]** > **[ポリシー（Policies）]** > **[Windows の設定（Windows Settings）]** > **[セキュリティの設定（Security Settings）]** > **[監査ポリシーの詳細な構成（Advanced Audit Policy Configuration）]** > **[監査ポリシー（Audit Policies）]**を展開します。

ステップ 6 **[アカウントへのログオン（Account Logon）]** をクリックします。

ステップ 7 右側のペインで、**[Kerberos認証サービスの監査（Audit Kerberos Authentication Service）]** をダブルクリックします。

ステップ 8 表示されるダイアログボックスで、システムが成功と失敗をログに記録できるように、すべてのチェックボックスをオンにします。

次の図は例を示しています。



ステップ 9 画面に表示される指示に従って変更を保存します。

ステップ 10 （オプション）GPO をただちに更新するには、DOS コマンド プロンプト ウィンドウに **`gpupdate /force`** と入力します。

次のタスク

「Active Directory（AD）ユーザーをグループに追加する （25 ページ）」を参照してください。

Active Directory（AD）ユーザーをグループに追加する

この手順を実行して、Active Directory（AD）およびpassive identity agent サービスユーザーにActive Directory（AD）に対する十分な権限を付与します。

正常に機能させるには、passive identity agent をドメインに接続し、Windows イベントログを読み取る必要があります。このトピックでは、適切な権限を次に付与する方法について説明します。

- passive identity agent サービスユーザー。
- Active Directory（AD）ユーザー（つまり、Secure Firewall Management Center の Active Directory（AD）レルム内の **ディレクトリユーザー名**ユーザー）。

Before you begin

ユーザーをグループに追加する方法と Windows サービスを設定して具体的なユーザーとして実行する方法を熟知している Microsoft Server 管理者である必要があります。

手順

ステップ 1 passive identity agent が実行されているシステムに管理者としてログインします。

次のいずれかにログインできます。

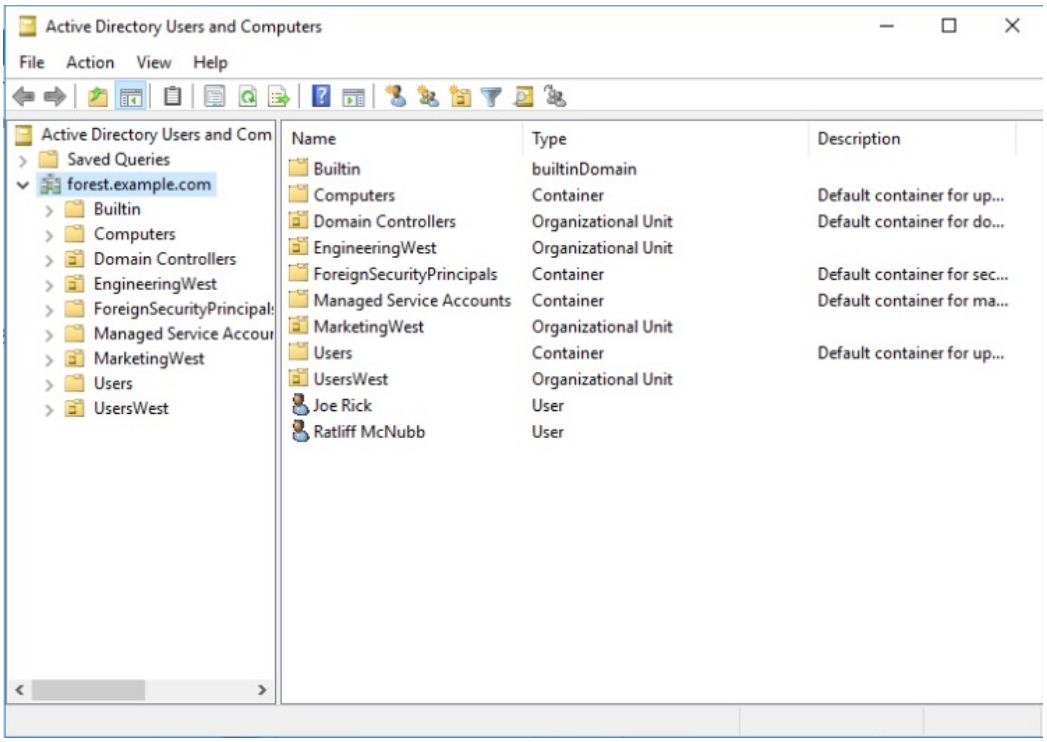
- ドメインコントローラ。
- Active Directory サーバ。

ステップ 2 Server Manager を起動します。

ステップ 3 **[ツール（Tools）]** > **[Active Directory（AD）ユーザーとコンピューター（Active Directory Users and Computers）]**クリックします。

ステップ 4 [Active Directory（AD）ユーザーとコンピューター（Active Directory Users and Computers）] で、ディレクトリユーザーが定義されているフォレストを展開します。

次の図は例を示しています。

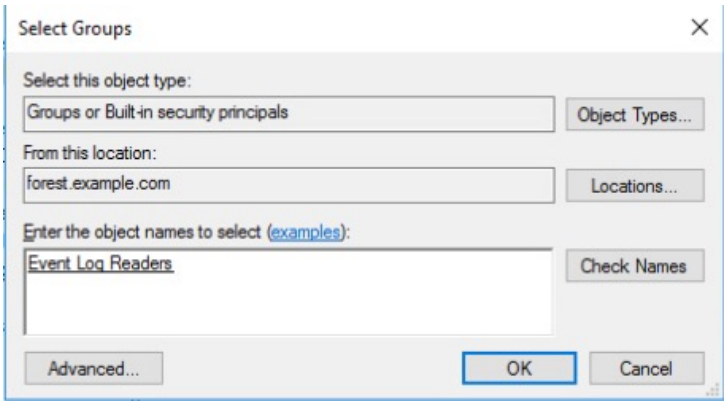


ステップ 5 組織単位またはグループを展開すると、ディレクトリユーザーが表示されます。（**[新規（New）] > [ユーザー（User）]**を選択すると、新規ユーザーを作成できます）。

ステップ 6 ディレクトリユーザーを右クリックし、**[グループに追加（Add to a group）]** をクリックします。

ステップ 7 [グループを選択（Select Groups）] ダイアログボックスで、**`Event Log Readers`** と入力し、**[名前を確認（Check Names）]** をクリックします。

次の図は例を示しています。



ステップ 8 上記のタスクを繰り返して、ユーザーをドメインユーザーグループに追加します。

ステップ 9 [グループを追加（Add Groups）] ダイアログボックスで、**[OK]**をクリックします。

これで、ディレクトリユーザーは適切な権限を持ち、passive identity agent サービスがそのユーザーとして実行されます。

次のタスク

「Passive Identity Agent ソフトウェアのインストール （27 ページ）」を参照してください。

Passive Identity Agent ソフトウェアのインストール

このタスクでは、passive identity agent ソフトウェアをインストールする方法について説明します。シンプルなインストールの場合は、Microsoft Active Directory（AD）ドメインコントローラにインストールできます。その他のオプションについては、を参照してください passive identity agent の導入 （3 ページ）。

（注） passive identity agentの最新バージョンを使用することを推奨します。使用可能なバージョンを確認するには、software.cisco.com にアクセスします。passive identity agentをアップグレードするには、「passive identity agent ソフトウェアをアップグレードする （32 ページ）」を参照してください

始める前に

次のすべてのタスクを完了します。

- Windows イベントビューアを有効にして ケルベロス認証試行をログに記録する （23 ページ）
- Active Directory（AD）ユーザーをグループに追加する （25 ページ）
- Passive Identity Agent サービスにログオンを追加する （30 ページ）

手順

ステップ 1 passive identity agent を software.cisco.com からダウンロードします。

ステップ 2 passive identity agent をインストールするマシンに管理者グループのメンバーとしてログインします。

ステップ 3 **CiscoPassiveIdentityAgentInstaller-1.1.msi** をダブルクリックします。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 passive identity agent のインストール先フォルダを選択し、**[次へ（Next）]**をクリックします。

デフォルトのインストールフォルダは **Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**です。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [インストール（Install）] をクリックします。

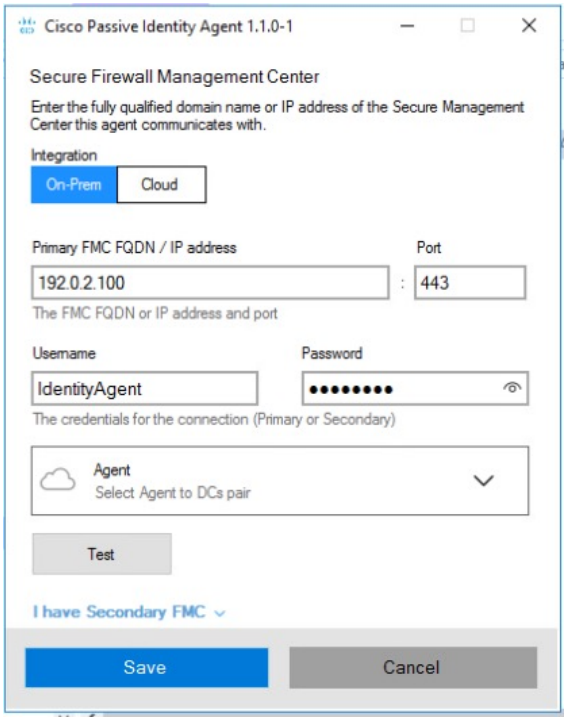
ステップ 8 インストールが完了したら、**[完了（Finish）]** をクリックし、必要に応じてチェックボックスをオンにして passive identity agent を起動します。

ステップ 9 passive identity agent が起動したら、オンプレミスの Secure Firewall Management Center（物理または仮想）でエージェントを使用している場合は**[オンプレミス（On-Prem）]** タブをクリックし、Cloud-Delivered Firewall Management Center でエージェントを使用している場合は **[クラウド（Cloud）]** タブをクリックします。

ステップ 10 [Cisco パッシブ エージェント（Cisco Passive Agent）] ダイアログ ボックスに、次の情報を入力します。

項目	説明
FMC FQDN / IP アドレス	passive identity agent アイデンティティ ソースを作成した Secure Firewall Management Center のアドレスを入力します。 passive identity agent バージョン 1.0 は、IPv4 アドレスと完全修飾ドメイン名のみをサポートしています。バージョン 1.1 は、IPv4、IPv6、および完全修飾ドメイン名をサポートしています。
ポート（Port）	Secure Firewall Management Center リッスン ポートを入力します（デフォルトは 443）。
Username	passive identity agent に対して Secure Firewall Management Center ユーザーを作成する （18 ページ） で作成したユーザーのユーザー名を入力します。
パスワード	ユーザーのパスワードを入力します。
エージェント	リストをクリックして、以前に Secure Firewall Management Centerで作成した passive identity agent のドメイン コントローラを見つけます。

次の図は例を示しています。

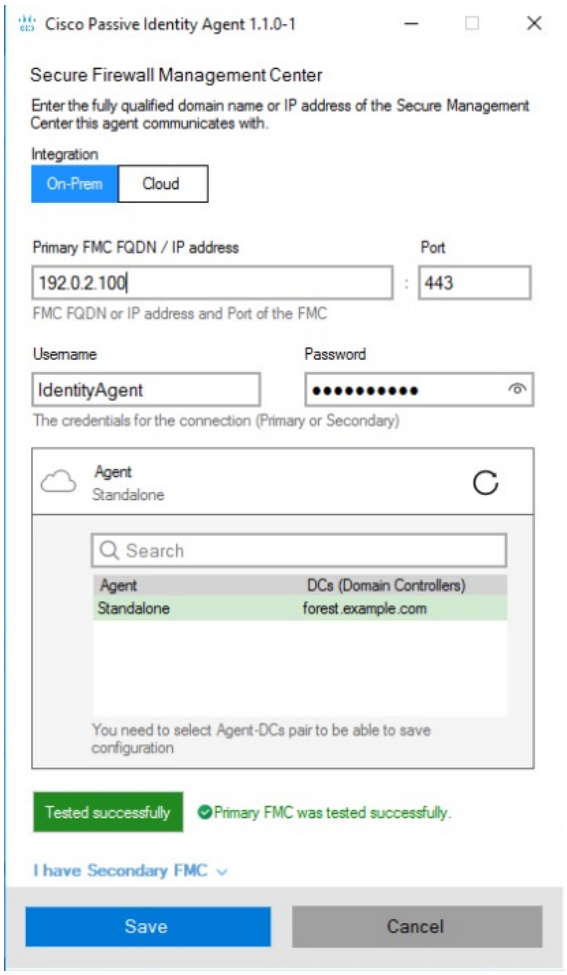


ステップ 11 **[エージェント（Agent）]** リストをクリックします。

ステップ 12 リストから、モニターするドメイン コントローラの名前をクリックします。

ステップ 13 [テスト（Test）] をクリックします。

次の図は例を示しています。



ステップ 14 高可用性ペアがある場合、**[セカンダリ FMC があります（I have Secondary FMC）]** をクリックして、セカンダリの IP アドレスまたは完全修飾ホスト名とそのリッスン ポートを入力します。

ステップ 15 テストが成功した場合は **[保存（Save）]** をクリックします。

次のタスク

「Passive Identity Agent サービスにログオンを追加する （30 ページ）」を参照してください。

Passive Identity Agent サービスにログオンを追加する

次の手順を実行して、Active Directory（AD）ユーザーとして実行できるように passive identity agent サービスを有効にします。（つまり、Secure Firewall Management Center のActive Directory（AD）レルム内の **Directory Username** ユーザー）。

このタスクはオプションですが、ログイン情報を Secure Firewall Management Center に送信するために必要な最小限の権限で passive identity agent サービスを実行できるためお勧めします。

Before you begin

「Active Directory（AD）ユーザーをグループに追加する （25 ページ）」で説明されているタスクを完了します。

ユーザーをグループに追加する方法と Windows サービスを設定して具体的なユーザーとして実行する方法を熟知している Microsoft Server 管理者である必要があります。

手順

ステップ 1 passive identity agent が実行されているシステムに管理者としてログインします。

次のいずれかにログインできます。

- ドメインコントローラ。
- Active Directory サーバ。

ステップ 2 Windows の検索バーに、**`Services`** と入力します。

ステップ 3 [サービス（Services）] ウィンドウで、**[シスコパッシブアイデンティティエージェント（Cisco Passive Identity Agent）]** をダブルクリックします。

ステップ 4 [プロパティ（Properties）] をクリックします。

ステップ 5 **[プロパティ（Properties）]** ダイアログボックスで、[ログオン（Log On）] タブをクリックします。

ステップ 6 **[このアカウント（This account）]** をクリックします。

ステップ 7 **[参照（Browse）]** をクリックして、画面のプロンプトに従い、ディレクトリユーザーを選択します。

ステップ 8 指定されたフィールドにユーザーのパスワードを入力します。

ステップ 9 [適用（Apply）] をクリックします。

次のタスク

- アイデンティティ ポリシーの作成の説明に従って、制御するユーザーおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- 『*Cisco Secure Firewall Management Center Administration Guide*』の「*Using Workflows*」の説明に従ってユーザーアクティビティをモニターします。

passive identity agent ソフトウェアをアンインストールする

このタスクでは、Microsoft AD サーバーからpassive identity agentソフトウェアをアンインストールする方法について説明します。

手順

ステップ 1 passive identity agentがインストールされているマシンに管理者としてログインします。
ステップ 2 [プログラムの追加と削除（Add or Remove Programs）] を検索します。
ステップ 3 [Ciscoパッシブ IDエージェント（Cisco Passive Identity Agent）] をクリックします。
ステップ 4 [アンインストール（Uninstall）] をクリックします。
ステップ 5 アンインストールを確認する必要があります。

passive identity agent ソフトウェアをアップグレードする

passive identity agentの新しいバージョンにアップグレードするには、以前のバージョンをアンインストールしてから、新しいバージョンをインストールする必要があります。

次の情報を参照してください。

- passive identity agent ソフトウェアをアンインストールする （32 ページ）
- passive identity agent インストールについて （22 ページ）

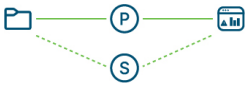
passive identity agent のモニター

passive identity agent は、プライマリ セカンダリとして構成されている場合に、Secure Firewall Management Centerやその他のエージェントと通信できるかどうかを示します。**Integration** > **Other Integrations** > **Identity Sources**でステータスを表示できます。

導入

スタンドアロンの passive identity agent は、次のように表されます。

プライマリ-セカンダリペアは次のように表されます。



次の表に、インジケータの意味を示します。

オブジェクト	意味
	Secure Firewall Management Center
	スタンドアロン Passive Identity Agent
	Active Directory ドメイン コントローラ
	プライマリ エージェント
	セカンダリ エージェント

ステータス インジケータと色

passive identity agent は、線（Secure Firewall Management Center との通信がアクティブまたはスタンバイのどちらであるかを示す）および色（通信が成功かどうかを示す）を使用して、ステータスを示します。

次の表に、線と色の意味を示します。

オブジェクト	意味
実線	Secure Firewall Management Center との通信を担当するエージェント。
破線	プライマリ/セカンダリ設定のみ。バックアップ エージェントとして機能しているエージェント。アクティブ（実線）エージェント間の通信障害が発生した場合、このエージェントは Secure Firewall Management Centerと通信します。
青 	エージェント通信は正常です。
オレンジ 	エージェントは、Secure Firewall Management Centerと正常に通信していません。新しく作成されたエージェント ラインはオレンジで、設定が完了するまでオレンジのままです。

オブジェクト	意味
赤 	通信が失敗しました。問題を解決するには、次の手順を実行します。 • エージェントと Secure Firewall Management Center間のネットワーク接続を確認します。 • システム（Microsoft AD サーバー、ドメインコントローラ、および Secure Firewall Management Center）の設定が完了していることを確認します。 詳細については、「passive identity agent アイデンティティ ソースの作成方法 （9 ページ）」を参照してください。

passive identity agent の管理

次のトピックでは、Secure Firewall Management Center で以前に設定した passive identity agent を編集または削除する方法について説明します。

関連トピック

passive identity agentの編集 （34 ページ）
スタンドアロン passive identity agent の削除 （35 ページ）
プライマリおよびセカンダリ passive identity agent の削除 （35 ページ）
passive identity agent ソフトウェアをアンインストールする （32 ページ）

passive identity agentの編集

このタスクでは Secure Firewall Management Center で以前に設定した passive identity agent を編集する方法について説明します。

手順

ステップ 1 管理者として Secure Firewall Management Center にログインします。
ステップ 2 **Integration** > **Other Integrations** > **Identity Sources** をクリックします。
ステップ 3 **[パッシブ アイデンティティ エージェント（Passive Identity Agent）]** をクリックします。
ステップ 4 編集するエージェントの横にある **Edit** (✎) をクリックします。
ステップ 5 必要な変更を加えます。

ステップ 6 **[保存（Save）]** をクリックします。

スタンドアロン passive identity agent の削除

このタスクでは、スタンドアロンの passive identity agent を削除する方法について説明します。

手順

ステップ 1 管理者として Secure Firewall Management Center にログインします。
ステップ 2 **Integration** > **Other Integrations** > **Identity Sources** をクリックします。
ステップ 3 **[パッシブ アイデンティティ エージェント（Passive Identity Agent）]** をクリックします。
ステップ 4 削除するエージェントの横にある **Edit** (✎) をクリックします。
ステップ 5 **[削除（Delete）]** をクリックします。
ステップ 6 処理の確認が求められます。

プライマリおよびセカンダリ passive identity agent の削除

このタスクでは、プライマリおよびセカンダリ passive identity agent を削除する方法について説明します。プライマリ エージェントを削除する前に、セカンダリ エージェントを削除する必要があります。

手順

ステップ 1 管理者として Secure Firewall Management Center にログインします。
ステップ 2 **Integration** > **Other Integrations** > **Identity Sources** をクリックします。
ステップ 3 **[パッシブ アイデンティティ エージェント（Passive Identity Agent）]** をクリックします。
ステップ 4 削除するセカンダリ エージェントの横にある **Edit** (✎) をクリックします。
ステップ 5 **[削除（Delete）]** をクリックします。
ステップ 6 処理の確認が求められます。
ステップ 7 プライマリ エージェントを削除する場合は、まずすべてのセカンダリ エージェントを削除してください。

passive identity agent のトラブルシューティング

このトピックでは、Windows AD ドメインコントローラまたはディレクトリサーバー上の passive identity agent ソフトウェアのトラブルシューティング方法について説明します。

（オプション）ログ レベルを設定します。

デフォルトでは、passive identity agent は INFO レベルでログに書き込みます。オプションでログレベルを変更するには、テキストエディタで **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config** を開き、ファイルを保存して、Cisco Passive Identity Agent サービスを再起動します。

ロギング サービスの名前は変更しないでください

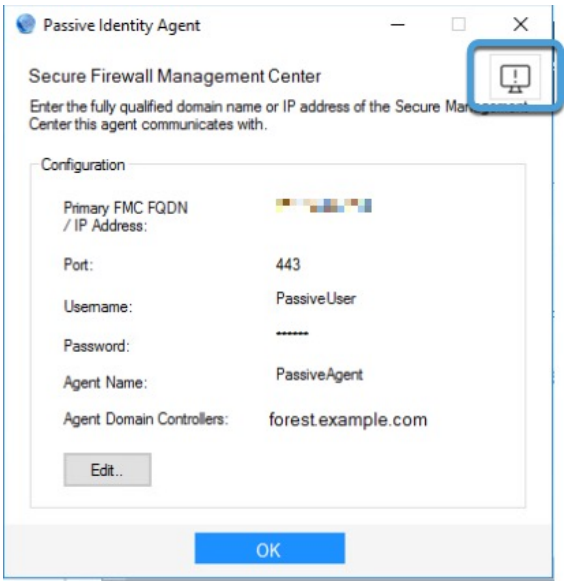
C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config の名前は変更しないでください。変更した場合、passive identity agent はログ ファイルの生成を停止します。**.exe.config** ファイルの拡張子を削除または変更しないでください。

トラブルシューティング ファイルの生成

トラブルシューティング ファイルを含む .zip を生成するには：

1. Microsoft Active Directory ドメイン コントローラにログインします。
2. ソフトウェア passive identity agent を起動します。
3. ウィンドウの右上隅の [トラブルシューティング（Troubleshooting）] ボタンをクリックします。

   次の図は例を示しています。



確認メッセージが表示されます。

トラブルシューティングログは、システムの [ダウンロード（Download）] フォルダに保存されます。ファイル名は **TroubleshootLogs**で始まります。

ログ ファイルを手動で表示する

Passive identity agent ログファイルは、エージェントのインストールディレクトリである **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**にプレーン テキスト形式で保存されます。

これらのファイルを表示するには、メモ帳または別のテキストエディタを使用します。ログファイルは、サイズが 10MB に達するとローテーションされます。

Microsoft Active Directory イベントビューアを使用する

Secure Firewall Management Center にユーザー セッションが表示されない場合は、Microsoft Active Directory サーバーのイベント ビューアで次の Kerberos 関連イベントを調べることができます。

- 4770
- 4768

監査ポリシーの一般的な情報については、learn.microsoft.com の Audit Policy Recommendations を参照してください。

Windows グループ ポリシー オブジェクトの設定の詳細については、learn.microsoft.com の Group Policy Objects を参照してください。

passive identity agent のセキュリティ要件

システムを保護するには、保護された内部ネットワークに passive identity agent をインストールしてください。passive identity agentは、使用可能なサービスとポートのうち必要なもののみを持つように設定されていますが、攻撃が到達できないように確保する必要があります。

passive identity agent と Secure Firewall Management Center が同じネットワーク上に存在している場合は、Secure Firewall Management Center を passive identity agent と同じ保護された内部ネットワークに接続することができます。

アプライアンスの展開方法に関係なく、システム間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でアプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

passive identity agent のインターネットアクセス要件

デフォルトでは、passive identity agent は、ポート 443/tcp（HTTPS）で HTTPS を使用してインターネット経由で Firepower システムと通信するように構成されています。passive identity agent

がインターネットに直接アクセスしないようにするために、プロキシサーバーを構成できます。

次の情報は、passive identity agent が相互通信、Secure Firewall Management Center との通信、および Microsoft Active Directory との通信に使用するポートを示しています。

表 *1 : Passive Identity Agent* のポート要件

ポート	理由
443	Secure Firewall Management Center と通信します。
135	MSRPC プロトコルを使用して Microsoft Active Directory と通信します。
9095	UDP プロトコルを使用して相互に通信します。

passive identity agent の履歴

表 *2 : passive identity agent* の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
パッシブ ID エージェント	7.6	7.1	This feature is introduced. Passive identity agent version 1.1 is compatible with 7.6.0 and later and adds the following: • You can use either FQDN, IPv4, or IPv6 to connect from the Passive Identity Agent to the Secure Firewall Management Center or Security Cloud Control. • Sends both IPv4 and IPv6 user sessions from Microsoft Active Directory (AD) to the Firewall Management Center. • You can zip troubleshooting logs. • When you start the passive identity agent software, a list of prerequisites is displayed. The passive identity agent identity source sends session data from Microsoft Active Directory (AD) to the Firewall Management Center. Passive identity agent software is supported on: • Microsoft AD server (Windows Server 2008 or later) • Microsoft AD domain controller (Windows Server 2008 or later) • Any client connected to the domain you want to monitor (Windows 8 or later)

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。