プロバイダ

ISE-PIC が ID 情報を、サービスをサブスクライブするコンシューマ（サブスクライバ）に提供できるようにするため、最初に ISE-PIC プローブを設定する必要があります。このプローブは ID プロバイダに接続します。

次の表に、ISE-PIC で使用可能なすべてのプロバイダとプローブタイプの詳細を示します。Active Directory の詳細については、プローブおよびプロバイダとしての Active Directoryを参照してください。

定義できるプロバイダ タイプを次に示します。

表 *1:* プロバイダ タイプ

プロバイダ タイプ（プローブ）	説明	送信元システム（プロバイダ）	テクノロジー	収集されるユーザー ID 情報	ドキュメント リンク
Active Directory（AD）	ユーザー情報の取得元である安全性が高く正確で最も一般的なソース。 プローブとして機能する場合、AD は WMI テクノロジーを使用して認証済みユーザー ID を送信します。 また AD 自体が、プローブではなく、その他のプローブがユーザー データを取得するソース システム（プロバイダ）として機能します。	Active Directory ドメイン コントローラ	WMI	• ユーザー名（User name） • IP アドレス • ドメイン	プローブおよびプロバイダとしての Active Directory
エージェント（Agents）	Active Directory ドメイン コントローラまたはメンバー サーバーにインストールされているネイティブ 32 ビット アプリケーション。エージェント プローブは、ユーザー ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。		ドメイン コントローラまたはメンバー サーバーにインストールされているエージェント。	• ユーザー名（User name） • IP アドレス • ドメイン	Active Directory エージェント（4 ページ）
エンドポイント（Endpoint）			WMI	ユーザーが接続しているかどうか	

プロバイダタイプ（プローブ）	説明	送信元システム（プロバイダ）	テクノロジー	収集されるユーザー ID 情報	ドキュメントリンク
	設定されているその他のプローブに加えて、ユーザーが接続しているかどうかを確認するため、常にバックグラウンドで実行されます。				エンドポイント プローブ（41 ページ）
SPAN	ネットワーク トラフィックをリッスンし、Active Directory データに基づいてユーザー ID 情報を抽出するため、ネットワーク スイッチに導入されています。		SPAN（スイッチにインストール）と Kerberos メッセージ	• ユーザー名（User name） • IP アドレス • ドメイン	SPAN （14 ページ）
API プロバイダ	ISE-PIC が提供する RESTful API サービスを使用して、RESTful API クライアントと通信するようにプログラミングされている任意のシステムから、ユーザー ID 情報を収集します。	REST API クライアントと通信するようにプログラミングされている任意のシステム。	RESTful API。JSON 形式でサブスクライバに送信されるユーザー ID。	• ユーザー名（User name） • IP アドレス • ポート範囲（Port range） • ドメイン（Domain）	API プロバイダ （9 ページ）
Syslog	syslog メッセージを解析し、ユーザー ID（MAC アドレスを含む）を取得します。	• 標準 syslog メッセージ プロバイダ • DHCP サーバー	syslog メッセージ	• ユーザー名（User name） • IP アドレス • MAC アドレス • ドメイン	syslog プロバイダ （16 ページ）

（注） pxGrid は、セッショントピックに対して 1 秒あたり 200 イベントを送信して、クライアントのオーバーロードを回避します。パブリッシャが 200 を超えるイベントを送信すると、追加のイベントはキューに入り、次のバッチで送信されます。

pxGrid が長時間にわたって 1 秒あたり 200 を超えるイベントを継続的に受信する場合、バックログイベントを保存するために通常よりも多くのメモリが消費される可能性があり、pxGrid のパフォーマンスに影響を与える場合があります。

Active Directory エージェント

ISE-PICから、ネイティブ 32 ビット アプリケーション、ドメイン コントローラ（DC）エージェントを、（設定に応じて）Active Directory（AD）ドメイン コントローラ（DC）またはメンバー サーバー上の任意の場所にインストールし、AD からユーザー ID 情報を取得して、設定したサブスクライバにこれらの ID を送信します。エージェント プローブは、ユーザー ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。エージェントは個別のドメインまたは AD ドメインにインストールできます。インストールされたエージェントは、1 分ごとに ISE-PIC にステータス更新情報を提供します。

エージェントは ISE-PIC が自動的にインストールおよび設定するか、またはユーザーが手動でインストールすることができます。インストールが完了すると、次のようになります。

- エージェントとその関連ファイルはパス **Program Files/Cisco/Cisco ISE PassiveID Agent** にインストールされています。
- エージェントのロギング レベルを指定する **PICAgent.exe.config** という設定ファイルがインストールされます。この設定ファイル内でロギング レベルを手動で変更できます。
- CiscoISEPICAgent.log ファイルにはすべてのロギング メッセージが保存されます。
- nodes.txt ファイルには、展開内でエージェントが通信できるすべてのノードのリストが含まれています。エージェントはリストの最初のノードと通信します。このノードと通信できない場合、エージェントはリストのノード順序に従ってノードとの通信を試行します。手動でのインストールの場合、このファイルを開き、ノード IP アドレスを入力する必要があります。（手動または自動での）インストールの完了後にこのファイルを変更するには、このファイルを手動で更新する必要があります。ファイルを開き、ノード IP アドレスを必要に応じて追加、変更、または削除します。

- Cisco ISE PassiveID Agent サービスはマシン上で稼働します。このサービスは [Windows サービス（Windows Services）] ダイアログボックスから管理できます。
- ISE-PIC は 74 個のドメインコントローラで検証されています。
- Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。エージェントをインストールできない場合、パッシブ ID サービスには Active Directory プローブを使用します。詳細については、プローブおよびプロバイダとしての Active Directoryを参照してください。

（注） メンバーサーバーで AD エージェントを実行している場合でも、Active Directory にログイン要求をクエリします。

Active Directory エージェントの自動インストールおよび展開

ユーザー ID についてドメイン コントローラをモニターするようにエージェント プロバイダを設定するときには、エージェントがメンバー サーバーまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE-PIC が自動的にインストールするか、またはユーザーが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニターするように設定する必要があります。このプロセスでは、自動インストールを有効にし、ドメイン コントローラをモニターするようにエージェントを設定する方法について説明します。

始める前に

- サーバー側からの関連 DNS サーバーの逆引き参照を設定します。ISE-PIC の DNS サーバー設定要件の詳細については、DNS サーバーを参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/frameworkを参照してください。
- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダとしての Active Directoryを参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザー グループを使用します。AD グループの詳細については、Active Directory ユーザー グループの設定を参照してください。

ステップ 1 **[プロバイダ（Providers）]** > **[エージェント（Agents）]** を選択します。

ステップ 2 新しいエージェントを追加するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 新しいエージェントを作成し、この設定で指定するホストに自動的にインストールするには、[新規エージェントの展開（Deploy New Agent）] を選択します。

ステップ 4 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （8 ページ）を参照してください。

ステップ 5 [展開（Deploy）] をクリックします。
設定で指定したドメインに基づいてエージェントが自動的にホストにインストールされ、設定が保存されます。エージェントは [エージェント（Agents）] テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 6 **[プロバイダ（Providers）]** > **[Active Directory]** を選択し、現在選択されているすべての参加ポイントを表示します。

ステップ 7 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 8 前提条件の一部として追加したドメインコントローラを設定するには、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 9 作成したエージェントを使用してモニターするドメインコントローラを選択し、[編集（Edit）] をクリックします。

ステップ 10 [プロトコル（Protocol）] ドロップダウンリストから [エージェント（Agent）] を選択します。

ステップ 11 **作成したエージェントを [エージェント（Agent）]** ドロップダウンリストから選択します。作成したエージェントのユーザー名とパスワードのログイン情報を入力し、**[保存（Save）]** をクリックします。

ユーザー名とパスワードのログイン情報は、ドメインコントローラにエージェントをインストールするために使用されます。最後に、[展開する（Deploy）] をクリックすると、*picagent.exe* が */opt/pbis/bin* から指定した Windows マシンにコピーされます。

Active Directory エージェントの手動インストールおよび展開

ユーザー ID についてドメイン コントローラをモニターするようにエージェント プロバイダを設定するときには、エージェントがメンバー サーバーまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE-PIC が自動的にインストールするか、またはユーザーが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニターするように設定する必要があります。このプロセスでは、エージェントを手動でインストールし、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について説明します。

始める前に

- サーバー側からの関連 DNS サーバーの逆引き参照を設定します。ISE-PIC の DNS サーバー設定要件の詳細については、DNS サーバーを参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。

- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダとしての Active Directoryを参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザー グループを使用します。AD グループの詳細については、Active Directory ユーザー グループの設定を参照してください。

ステップ 1 **[プロバイダ（Providers）]** > **[エージェント（Agents）]** を選択します。

ステップ 2 [エージェントのダウンロード（Download Agent）] をクリックし、手動でインストールするための **`picagent-installer.zip`** ファイルをダウンロードします。
このファイルは Windows の標準ダウンロード フォルダにダウンロードされます。

ステップ 3 ZIP ファイルを指定のホスト マシンに保存してインストールを実行します。

ステップ 4 ISE-PIC GUI で **[プロバイダー（Providers）]** > **[エージェント（Agents）]** をもう一度選択します。

ステップ 5 新しいエージェントを設定するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 6 すでにホストマシンにインストールしているエージェントを設定するには、[既存のエージェントの登録（Register Existing Agent）] を選択します。

ステップ 7 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （8 ページ）を参照してください。

ステップ 8 **[保存（Save）]** をクリックします。
エージェント設定が保存されます。エージェントは[エージェント（Agents）]テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 9 **[プロバイダー（Providers）]** > **[Active Directory]** を選択し、現在設定されているすべての参加ポイントを選択します。

ステップ 10 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 11 前提条件の一部として追加したドメインコントローラを設定するには、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 12 作成したエージェントを使用してモニターするドメインコントローラを選択し、[編集（Edit）]をクリックします。

ステップ 13 [プロトコル（Protocol）] ドロップダウンリストから [エージェント（Agent）] を選択します。

ステップ 14 作成したエージェントを[エージェント（Agent）] ドロップダウンリストから選択します。エージェントに接続するためのユーザー名とパスワードを入力し、[保存（Save）] をクリックします。

ユーザーアカウントには、セキュリティイベントを読み取るために必要な権限が必要です。WMIベースのエージェントのユーザーアカウントには、WMI/DCOM 権限が必要です。

エージェントのアンインストール

自動または手動でインストールされたエージェントは、Windowsから直接（手動で）簡単にアンインストールできます。

ステップ 1 [Windows] ダイアログで [プログラムと機能（Programs and Features）] に移動します。

ステップ 2 インストールされているプログラムのリストで [Cisco ISE PassiveID エージェント（Cisco ISE PassiveID Agent）] を見つけて選択します。

ステップ 3 [アンインストール（Uninstall）] をクリックします。

Active Directory エージェントの設定

ISE-PIC が、さまざまなドメイン コントローラ（DC）からユーザー ID 情報を取得し、その情報を ISE-PIC サブスクライバに配信するために、ネットワーク内の指定されたホストにエージェントを自動的にインストールすることを許可します。

エージェントを作成および管理するには、**[プロバイダー（Providers）]** > **[エージェント（Agents）]** を選択します。Active Directory エージェントの自動インストールおよび展開 （5 ページ）を参照してください。

表 *2*：*[*エージェント（*Agents*）*]* ウィンドウ

フィールド名	説明
Name	設定したエージェント名。
ホスト（Host）	エージェントがインストールされているホストの完全修飾ドメイン名。
モニターリング（Monitoring）	指定されたエージェントがモニターするドメインコントローラのカンマ区切りリストです。

表 *3*：新規エージェント（*Agents New*）

フィールド	説明
新規エージェントの展開（Deploy New Agent）または既存のエージェントの登録（Register Existing Agent）	• 新規エージェントの展開（Deploy New Agent）：指定されたホストに新規エージェントをインストールします。 • 既存のエージェントの登録（Register Existing Agent）：ホストにエージェントを手動でインストールし、ISE-PIC がサービスを有効にできるようにするため、この画面でそのエージェントを設定します。

フィールド	説明
名前（**Name**）	エージェントを容易に把握できる名前を入力します。
説明（**Description**）	エージェントを容易に把握できる説明を入力します。
ホスト FQDN（**Host FQDN**）	エージェントがインストールされているホスト(既存のエージェントの登録の場合）またはインストールされるホスト（自動展開の場合）の完全修飾ドメイン名です。
ユーザー名（**User Name**）	エージェントをインストールするホストにアクセスするためのユーザー名を入力します。ISE-PIC はこれらのクレデンシャルを使用してエージェントを自動的にインストールします。 ユーザーアカウントには、リモートで接続して PIC エージェントをインストールするための権限が必要です。
パスワード	エージェントをインストールするホストにアクセスするためのパスワードを入力します。ISE-PIC はこれらのクレデンシャルを使用してエージェントを自動的にインストールします。

API プロバイダ

Cisco ISE-PIC の API プロバイダ機能では、カスタマイズしたプログラムまたはターミナル サーバー（TS）エージェントから組み込み ISE-PICREST API サービスにユーザー ID 情報をプッシュできます。これにより、ネットワークからプログラミング可能なクライアントをカスタマイズして、任意のネットワーク アクセス制御（NAC）システムから収集されたユーザー ID をこのサービスに送信するようにできます。さらに Cisco ISE-PIC API プロバイダにより、すべてのユーザーの IP アドレスが同一であるが、各ユーザーに固有のポートが割り当てられるネットワーク アプリケーション（Citrix サーバーの TS-Agent など）と対話できます。

たとえば、Active Directory（AD）サーバーに対して認証されたユーザーの ID マッピングを提供する Citrix サーバーで稼働するエージェントは、新しいユーザーがログインまたはログオフするたびに、ユーザー セッションを追加または削除する REST 要求を ISE-PIC に送信できます。ISE-PIC は、クライアントから送信されたユーザー ID 情報（IP アドレス、割り当てられたポートなど）を取得し、事前に設定されているサブスクライバ（Cisco Firepower Management Center（FMC）など）に送信します。

ISE-PIC REST API フレームワークは、HTTPS プロトコルを介した REST サービスを実装し（クライアント証明書の検証は不要）、ユーザー ID 情報が JSON（JavaScript Object Notation）形式で送信されます。JSON の詳細については、http://www.json.org/ を参照してください。

ISE-PIC REST API サービスは、1 つのシステムに同時にログインしている複数のユーザーを区別するため、ユーザーIDを解析し、その情報をポート範囲にマッピングします。ポートがユーザーに割り当てられるたびに、API がメッセージを ISE-PIC に送信します。

REST API プロバイダのフロー

カスタマイズしたクライアントを ISE-PIC のプロバイダとして宣言し、そのカスタマイズした特定のプログラム（クライアント）が RESTful 要求を送信できるようにして、ISE-PIC からカスタマイズしたクライアントへのブリッジを設定している場合、ISE-PIC REST サービスは次のように機能します。

1. Cisco ISE-PIC はクライアント認証のために認証トークンを必要とします。通信開始時と、ISE-PIC から以前のトークンの期限が切れたことが通知されるたびに、クライアント マシンのカスタマイズしたプログラムから認証トークンを求める要求が送信されます。この要求への応答としてトークンが返されます。これによりクライアントと ISE-PIC サービス間の継続的な通信が可能になります。
2. ユーザーがネットワークにログインすると、クライアントはユーザー ID 情報を取得し、API Add コマンドを使用してこの情報を ISE-PIC REST サービスに送信します。
3. Cisco ISE-PIC はユーザー ID 情報を受信してマッピングします。
4. Cisco ISE-PIC はマッピングされたユーザー ID 情報をサブスクライバに送信します。
5. 必要な場合は常に、カスタマイズされたマシンはユーザー情報削除要求を送信できます。このためには、Remove API コールを送信し、Add コールの送信時に応答として受信したユーザー ID を含めます。

ISE-PIC での REST API プロバイダの操作

ISE-PIC で REST サービスをアクティブにするには、次の手順に従います。

1. クライアント側を設定します。詳細については、クライアント ユーザー マニュアルを参照してください。
2. DNS サーバーを適切に設定していることを確認します。これには、ISE-PIC からのクライアント マシンの逆引きの設定も含まれます。ISE-PIC の DNS サーバー設定要件の詳細については、DNS サーバーを参照してください。
3. パッシブ ID サービス の ISE-PIC REST サービスへのブリッジの設定 （11 ページ）を参照してください。

（注） TS-Agent と連携するように API プロバイダを設定するには、ISE-PIC からそのエージェントへのブリッジの作成時に TS-Agent 情報を追加します。その後、TS-Agent のマニュアルで API コールの送信について確認してください。

4. 認証トークンを生成し、追加要求と削除要求を API サービスに送信します。

パッシブ ID サービス の ISE-PIC REST サービスへのブリッジの設定

ISE-PIC REST API サービスが特定のクライアントから情報を受信できるようにするには、まず Cisco ISE-PIC でその特定のクライアントを定義する必要があります。異なる IP アドレスを使用して複数の REST API クライアントを定義できます。

始める前に

- DNS サーバーを適切に設定していることを確認します。これには、Cisco ISE-PIC からのクライアントマシンの逆引きの設定も含まれます。Cisco ISE-PIC の DNS サーバー設定要件の詳細については、DNS サーバーを参照してください。

ステップ 1 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[プロバイダ（Providers）] > [API プロバイダ（API Providers）]** を選択して、現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定します。
[API プロバイダ（API Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しいクライアントを追加するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、API プロバイダの設定 （12 ページ）を参照してください。

ステップ 4 [送信（Submit）] をクリックします。
クライアント設定が保存され、更新された [API プロバイダ（API Providers）] テーブルが画面に表示されます。これで、クライアントは ISE-PIC REST サービスにポストを送信できるようになりました。

次のタスク

認証トークンとユーザー ID を ISE-PIC REST サービスに送信するように、カスタマイズしたクライアントをセットアップします。ISE-PIC REST サービスへの API コールの送信 （11 ページ） を参照してください。

ISE-PIC REST サービスへの API コールの送信

始める前に

パッシブ ID サービス の ISE-PIC REST サービスへのブリッジの設定 （11 ページ）

ステップ 1 Cisco ISE URL をブラウザのアドレス バーに入力します（たとえば *https://<ise hostname or ip address>/admin/*）。

ステップ 2 [API プロバイダ（API Providers）] ウィンドウで指定および設定したユーザー名とパスワードを入力します。詳細については、パッシブ ID サービス の ISE-PIC REST サービスへのブリッジの設定 （11 ページ）を参照してください。

ステップ 3 Enter キーを押します。

ステップ 4 ターゲットノードの [URL アドレス（URL Address）] フィールドに API コールを入力します。

ステップ 5 [送信（Send）] をクリックして API コールを発行します。

次のタスク

さまざまな API コールとそのスキーマおよび結果の詳細については、API コール （13 ページ）を参照してください。

API プロバイダの設定

ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[プロバイダ（Providers）]** > **[API プロバイダ（Providers）]** を選択して、パッシブ ID サービス の新しい REST API クライアントを設定します。

（注） 次のようにリクエスト コールを使用して完全な API 定義とオブジェクト スキーマを取得できます。

- 完全な API の指定（wadl）：https://YOUR_ISE:9094/application.wadl
- API モデルとオブジェクト スキーマ：https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 *4: API* プロバイダの設定

フィールド	説明
名前	このクライアントを他のクライアントから容易に区別できる一意の名前を入力します。
説明（Description）	このクライアントのわかりやすい説明を入力します。
ステータス（Status）	設定完了後すぐにクライアントが REST サービスとやりとりできるようにするには、[有効（Enabled）] を選択します。
ホスト/IP（Host/ IP）	クライアント ホスト マシンの IP アドレスを入力します。DNS サーバーを適切に設定していることを確認します。これには、ISE-PIC からのクライアント マシンの逆引きの設定も含まれます。
ユーザー名（User name）	REST サービスへの送信時に使用する一意のユーザー名を作成します。

フィールド	説明
パスワード（Password）	REST サービスへの送信時に使用する一意のパスワードを作成します。

API コール

Cisco ISE-PIC で パッシブ ID サービスのユーザー ID イベントを管理するには、次の API コールを使用します。

目的：認証トークンの生成

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/fmi_platform/v1/identityauth/generatetoken

  要求には BasicAuth 認証ヘッダーが含まれている必要があります。ISE-PIC GUI から以前に作成した API プロバイダのログイン情報を入力します。詳細については、API プロバイダの設定 （12 ページ）を参照してください。

- **応答ヘッダー**

  このヘッダーには X-auth-access-token が含まれています。これは、追加の REST 要求を送信するときに使用するトークンです。

- **応答本文**

  HTTP 204 No Content

目的：ユーザーの追加

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity

  POST 要求のヘッダーに X-auth-access-token を追加します（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）。

- **応答ヘッダー**

  201 Created

- **応答本文**

  {

  "user": "<ユーザー名>",

  "srcPatRange": {

  "userPatStart": <ユーザー PAT 開始値>,

"userPatEnd": <ユーザー PAT 終了値>,

"patRangeStart": <PAT 範囲開始値>

},

"srcIpAddress": "<src IP アドレス>",

"agentInfo": "<エージェント名>",

"timestamp": "<ISO_8601 形式、例：“YYYY-MM-DDTHH:MM:SSZ" >",

"domain": "<ドメイン>"

}

- **注記**
  - 上記の JSON で 1 つの IP ユーザー バインディングを作成するには srcPatRange を削除します。
  - 応答本文には「ID」（作成されたユーザーセッションバインディングの固有識別子）が含まれています。削除するユーザーを指定する DELETE 要求を送信するときに、この ID を使用してください。
  - この応答には、新たに作成されたユーザー セッション バインディングの URL であるセルフ リンクも含まれています。

目的：ユーザーの削除

- **要求**

  DELETE

  https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity/<id>

  <id> に、Add 応答で受信した ID を入力します。

  DELETE 要求のヘッダーに X-auth-access-token を追加します（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）。

- **応答ヘッダー**

  200 OK

- **応答本文**

  応答本文には、削除されたユーザーセッションバインディングの詳細が含まれています。

SPAN

SPANです。このとき、Active Directory が Cisco ISE-PIC と直接連携するように設定する必要はありません。SPAN はネットワーク トラフィックをスニフィングし、特に Kerberos メッセージを調べ、Active Directory により保存されているユーザー ID 情報を抽出し、その情報を ISE-PIC

に送信します。ISE-PIC は次にその情報を解析し、最終的にはユーザー名、IP アドレス、およびドメイン名を、ISE-PIC からすでに設定しているサブスクライバに送信します。

SPAN がネットワークをリッスンし、Active Directory ユーザー情報を抽出できるようにするには、ISE-PIC と Active Directory の両方がネットワーク上の同一スイッチに接続している必要があります。これにより、SPAN は Active Directory からすべてのユーザー ID データをコピーおよびミラーリングできます。

SPAN により、ユーザー情報は次のように取得されます。

1. ユーザーエンドポイントがネットワークにログインします。
2. ログイン データとユーザー データは Kerberos メッセージに保存されます。
3. ユーザーがログインし、ユーザーデータがスイッチを通過すると、SPAN がネットワークデータをミラーリングします。
4. Cisco ISE-PIC は、ユーザー情報を取得するためネットワークをリッスンし、ミラーリングされたデータをスイッチから取得します。
5. Cisco ISE-PIC はユーザー情報を解析し、パッシブ ID マッピングを更新します。
6. Cisco ISE-PIC は解析後のユーザー情報をサブスクライバに送信します。

SPAN の使用

始める前に

ISE-PIC がネットワーク スイッチから SPAN トラフィックを受信できるようにするには、最初にそのスイッチをリッスンするノードとノードインターフェイスを定義する必要があります。インストールされている複数の ISE-PIC ノードをリッスンするには、SPAN を設定します。ネットワークをリッスンするように設定できるインターフェイスは、ノードごとに 1 つのみです。また、リッスンするために使用するインターフェイスは SPAN 専用である必要があります。

また、次の操作を行う必要があります。

- ネットワークで Active Directory が設定されていることを確認します。
- スイッチが ISE-PIC と通信できることを確認するために、Active Directory に接続しているネットワーク上のスイッチで CLI を実行します。
- AD からネットワークをミラーリングするようにスイッチを設定します。
- SPAN 専用の ISE-PIC ネットワーク インターフェイス カード（NIC）を設定します。この NIC は SPAN トラフィック専用で使用されます。
- SPAN 専用の NIC が、コマンドライン インターフェイスからアクティブにされていることを確認します。
- Kerberos トラフィックのみを SPAN ポートに送信する VACL を作成します。

ステップ 1 **[プロバイダ（Providers）]** > **[SPAN]** を選択して SPAN を設定します。

ステップ 2 （注） GigabitEthernet0 ネットワーク インターフェイス カード（NIC）は使用可能なままにし、SPAN の設定には使用可能な別の NIC を選択することを推奨します。GigabitEthernet0 は、システム管理の目的で使用されます。

わかりやすい説明を入力し（オプション）、[有効（Enabled）] ステータスを選択し、ネットワーク スイッチのリッスンに使用する関連 NIC とノードを選択します。詳細については、SPAN 設定 （16 ページ）を参照してください。

ステップ 3 **[保存（Save）]** をクリックします。
SPAN 設定が保存され、ISE-PIC がネットワーク トラフィックをアクティブにリッスンします。

SPAN 設定

SPAN をクライアント ネットワークにインストールすることで、展開した各ノードから、ISE-PIC がユーザー ID を受信することを簡単に設定できます。

表 *5 : SPAN* 設定

フィールド	説明
説明（Description）	現在有効なノードとインターフェイスがわかる固有の説明を入力します。
ステータス（Status）	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
インターフェイス NIC（Interface NIC）	ISE-PIC にインストールされているノードの 1 つまたは両方を選択してから、選択したノードごとに、ネットワークをリッスンして情報を得るノードインターフェイスを選択します。 （注） GigabitEthernet0 NIC を引き続き使用可能にし、SPAN の設定には他の使用可能な NIC を選択することを推奨します。GigabitEthernet0 は、システム管理の目的で使用されます。

syslog プロバイダ

ISE-PIC は syslog メッセージを配信する任意のクライアント（ID データプロバイダ）からの syslog メッセージを解析し、MAC アドレスなどのユーザー ID 情報を送信します。syslog メッ

セージには、通常の syslog メッセージ（InfoBlox、Blue Coat、BlueCat、Lucent などのプロバイダからのメッセージ）と DHCP syslog メッセージがあります。このマッピングされたユーザー ID データがサブスクライバに配信されます。

ユーザー ID データを受信する syslog クライアントを指定できます（syslog クライアントの設定 （18 ページ）を参照）。プロバイダの設定時に、接続方法（TCP または UDP）および解析に使用する syslog テンプレートを指定する必要があります。

（注） 設定されている接続タイプが TCP であり、メッセージヘッダーに問題があるためにホスト名を解析できない場合、ISE-PIC はパケットで受信した IP アドレスを、ISE-PIC で設定されている syslog メッセージのプロバイダリストにあるすべてのプロバイダの IP アドレスと照合しようとします。このリストを表示するには、**[プロバイダ（Providers）]** > **[syslog プロバイダ（Syslog Providers）]** を選択します。メッセージヘッダーを確認し、必要に応じて、解析が正常に実行されるようにカスタマイズすることをお勧めします。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （25 ページ） を参照してください。

syslog プローブが受信した syslog メッセージを ISE-PIC パーサーに送信します。パーサーはユーザー ID 情報をマッピングし、その情報を ISE-PIC に公開します。次に ISE-PIC が、解析およびマッピングされたユーザー ID 情報をISE-PIC サブスクライバに配信します。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE-PIC は、ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているいずれのユーザーとも一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

ISE-PIC からの syslog メッセージを解析してユーザー ID を取得するには、次の手順を実行します。

- ユーザー ID データの送信元 syslog クライアントを設定します。syslog クライアントの設定 （18 ページ）を参照してください。
- 1 つのメッセージヘッダーをカスタマイズします。syslog ヘッダーのカスタマイズ （25 ページ）を参照してください。
- テンプレートを作成してメッセージ本文をカスタマイズします。syslog メッセージ本文のカスタマイズ （23 ページ）を参照してください。
- 解析に使用するメッセージテンプレートとして syslog クライアントを設定する場合には、ISE-PIC で事前に定義されているメッセージテンプレートを使用します。あるいは、これらの事前に定義されたテンプレートに基づいてヘッダーまたは本文のテンプレートをカスタマイズします。Syslog 事前定義メッセージテンプレートの使用 （29 ページ） を参照してください。

syslog クライアントの設定

Cisco ISE-PIC が特定のクライアントからの syslog メッセージをリッスンできるようにするには、最初に Cisco ISE-PIC でそのクライアントを定義する必要があります。異なる IP アドレスを使用して複数のプロバイダを定義できます。

ステップ 1 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[プロバイダ（Providers）]** > **[syslog プロバイダ（syslog Providers）]** を選択して、現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定します。
[syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを設定するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドを入力し（詳細についてはSyslog の設定（18 ページ）を参照）、必要に応じてメッセージテンプレートを作成します（詳細についてはsyslog メッセージ本文のカスタマイズ （23 ページ）を参照）。

ステップ 4 **[送信（Submit）]** をクリックします。

Syslog の設定

特定のクライアントからの syslog メッセージを介してユーザー ID（MAC アドレスを含む）を受信するように Cisco ISE-PIC を設定します。異なる IP アドレスを使用して複数のプロバイダを定義できます。

表 6 : syslog プロバイダ

フィールド名	説明
Name	設定したこのクライアントを容易に区別できる一意の名前を入力します。
説明（Description）	この syslog プロバイダのわかりやすい説明。
ステータス（Status）	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
Host	ホスト マシンの FQDN を入力します。

フィールド名	説明
接続タイプ（Connection Type）	ISE-PIC が syslog メッセージをリッスンするチャネルを指定するため、UDP または TCP を入力します。 （注） TCP が設定されている接続タイプである場合で、メッセージヘッダーとホスト名が解析できない問題がある場合は、Cisco ISE は syslog メッセージに設定されているプロバイダのリストにあるいずれかのプロバイダの IP アドレス宛のパケットで受信した IP アドレスと照合しようとします。 このリストを表示するには、**[プロバイダ（Providers）]** > **[syslog プロバイダ（Syslog Providers）]** を選択します。メッセージヘッダーを確認し、必要に応じて、解析が正常に実行されるようにカスタマイズすることをお勧めします。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （25 ページ） を参照してください。

フィールド名	説明
テンプレート（**Template**）	

フィールド名	説明
	テンプレートにより正確な本文メッセージ構造が指定されます。これにより、パーサーは syslog メッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。 たとえば、テンプレートでは正確なユーザー名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザー名を検出できます。 このフィールドでは、syslog メッセージを認識して正しく解析するために使用される（syslog メッセージの本文の）テンプレートを指定します。 事前定義のドロップダウンリストから選択するか、または [新規（New）] をクリックして独自のカスタム テンプレートを作成します。新しいテンプレートの作成の詳細については、syslog メッセージ本文のカスタマイズ （23 ページ）を参照してください。ほとんどの事前定義テンプレートでは正規表現が使用されています。カスタム テンプレートでも正規表現を使用する必要があります。 （注） 編集または削除できるのはカスタム テンプレートだけであり、ドロップダウンの事前定義システム テンプレートは変更できません。 現在 ISE-PIC に含まれている事前定義 DHCP プロバイダ テンプレートを次に示します。 • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP （注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより Cisco ISE は ユーザー ID 情報を正しく解析して配

フィールド名	説明
	信するために、最初にローカルセッションディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合しようとします。 DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。 Cisco ISE には次の事前定義の標準 syslog プロバイダテンプレートがあります。 • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN テンプレートについては、Syslog 事前定義メッセージテンプレートの使用（29 ページ） を参照してください。
デフォルト ドメイン（**Default Domain**）	syslog メッセージで特定のユーザーに対してドメインが指定されていない場合、このデフォルト ドメインが自動的にそのユーザーに割り当てられます。これにより、すべてのユーザーにドメインが割り当てられます。 デフォルト ドメインまたはメッセージから解析されたドメインにユーザー名が付加され、username@domain となります。したがって、ユーザーとユーザーグループに関する詳細情報を取得するためには、ドメインを含めます。

syslog メッセージ構造のカスタマイズ（テンプレート）

テンプレートは正確なメッセージ構造を指定します。これにより、パーサーはsyslogメッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。たとえば、テンプレートでは正確なユーザー名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザー名を検出できます。テンプレートにより、新規マッピングメッセージとマッピング削除メッセージの両方に対応する構造が決定します。

Cisco ISE-PIC では、ISE-PIC パーサーが使用する 1 つのメッセージ ヘッダーと複数の本文構造をカスタマイズできます。

ISE-PIC パーサーが、メッセージがユーザー ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザーの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

メッセージテンプレートをカスタマイズするときに、事前定義オプションで使用されている正規表現とメッセージ構造を調べ、ISE-PIC の事前定義メッセージ テンプレートに基づいてカスタマイズを行うかどうかを決定できます。事前定義テンプレートの正規表現、メッセージ構造、例などの詳細については、Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照してください。

次の内容をカスタマイズできます。

- 1 つのメッセージ ヘッダー：syslog ヘッダーのカスタマイズ （25 ページ）
- 複数のメッセージ本文：syslog メッセージ本文のカスタマイズ （23 ページ）。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより Cisco ISE は ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合しようとします。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

DHCPメッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCPメッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義のDHCPテンプレートを使用してください。

syslog メッセージ本文のカスタマイズ

Cisco ISE-PIC では、ISE-PIC パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます（メッセージ本文のカスタマイズ）。テンプレートには、ユーザー名、IPアドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE はユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog クライアント設定画面から、syslog メッセージ本文テンプレートを作成および編集します。

（注） 各自でカスタマイズしたテンプレートだけを編集できます。システムに用意されている事前定義テンプレートは変更できません。

ステップ 1 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[プロバイダ（Providers）] > [syslog プロバイダ（syslog Providers）]** を選択して、現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定します。
[syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを追加するには [追加（Add）] をクリックし、すでに設定されているクライアントを更新するには [編集（Edit）] をクリックします。syslog クライアントの設定と更新については、syslog クライアントの設定 （18 ページ） を参照してください。

ステップ 3 [syslog プロバイダ（Syslog Providers）] ウィンドウで、[新規（New）] をクリックして新しいメッセージテンプレートを作成します。既存のテンプレートを編集するには、ドロップダウンリストからテンプレートを選択して [編集（Edit）] をクリックします。

ステップ 4 必須フィールドをすべて指定します。

値を正しく入力する方法の詳細については、syslog カスタマイズ テンプレートの設定と例 （26 ページ） を参照してください。

ステップ 5 [テスト（Test）] をクリックして、入力した文字列に基づいてメッセージが正しく解析されていることを確認します。

ステップ 6 [保存（Save）] をクリックします。

syslog ヘッダーのカスタマイズ

syslog ヘッダーには、メッセージの送信元のホスト名も含まれています。syslog メッセージが Cisco ISE-PIC メッセージパーサーで認識されない場合は、ホスト名の後に続く区切り文字を設定し、Cisco ISE-PIC がホスト名を認識してメッセージを正しく解析できるようにすることで、メッセージヘッダーをカスタマイズする必要がある場合があります。この画面のフィールドの詳細については、syslog カスタマイズ テンプレートの設定と例 （26 ページ）を参照してください。カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダー タイプにこの設定が追加されます。

（注） 1 つのヘッダーだけをカスタマイズできます。ヘッダーをカスタマイズした後、[カスタムヘッダー（Custom Header）] をクリックしてテンプレートを作成すると、最新の設定のみが保存されます。

ステップ 1 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[プロバイダ（Providers）] > [syslog プロバイダ（syslog Providers）]** を選択して、現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定します。
[syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 [カスタム ヘッダー（Custom Header）] をクリックして [syslog カスタム ヘッダー（Syslog Custom Header）] 画面を開きます。

ステップ 3 [サンプル syslog を貼り付ける（Paste sample syslog）] に、syslog メッセージのヘッダー形式の例を入力します。たとえば、メッセージの 1 つからヘッダー **`<181>Oct 10 15:14:08 Cisco.com`** をコピーして貼り付けます。

ステップ 4 [区切り文字（Separator）] フィールドで、単語をスペースとタブのいずれで区切るかを指定します。

ステップ 5 [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドで、ヘッダーのどの位置がホスト名であるかを指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

[ホスト名（Hostname）] フィールドに、最初の 3 つのフィールドに示される詳細情報に基づいてホスト名が表示されます。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。

<181>Oct 10 15:14:08 Cisco.com

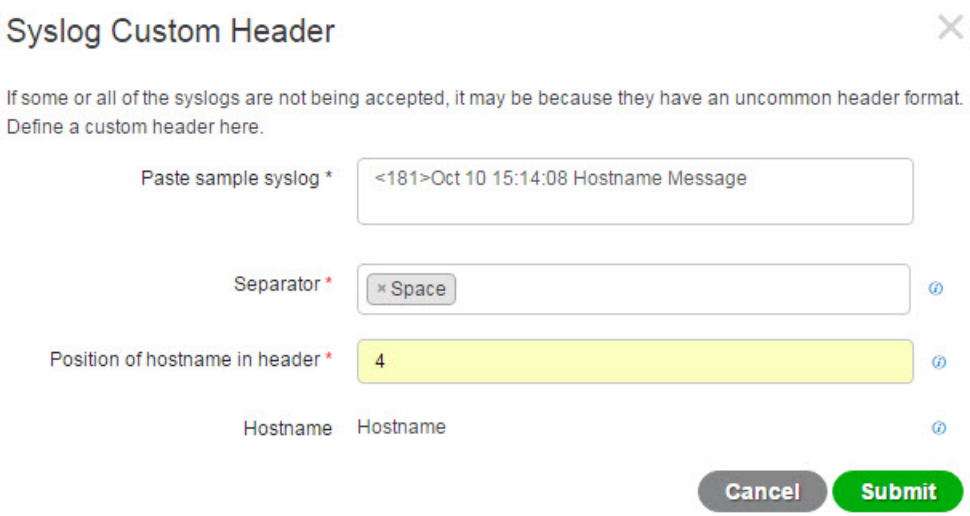
区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。

[ホスト名（Hostname）] には自動的に Cisco.com と表示されます。これは、[syslog の例を貼り付ける（Paste sample syslog）] フィールドに貼り付けたヘッダー フレーズの 4 番目の単語です。

ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

この例を次のスクリーン キャプチャに示します。

図 *1 : syslog* ヘッダーのカスタマイズ



ステップ 6 [送信（Submit）] をクリックします。
カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダータイプにこの設定が追加されます。

syslog カスタマイズ テンプレートの設定と例

Cisco ISE-PIC では、ISE-PIC パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます。カスタマイズされたテンプレートは、新規マッピング メッセージとマッピング削除メッセージの両方に対応する構造を決定します。ISE-PIC パーサーが、メッセージがユーザー ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザーの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されます。カスタマイズテンプレートでも正規表現を使用してください。

syslog ヘッダーの各部分

ホスト名の後に続く区切り文字を設定することで、syslog プローブが認識する単一ヘッダーをカスタマイズできます。

次の表に、カスタムsyslogヘッダーに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 9 : カスタマイズ テンプレートの正規表現（29 ページ）を参照してください。

表 *7 : syslog* カスタム ヘッダー

フィールド	説明
syslog の例を貼り付ける（Paste sample syslog）	syslog メッセージにヘッダー形式の例を入力します。たとえば、次のヘッダーをコピーして貼り付けます。 `<181>Oct 10 15:14:08 Hostname Message`
区切り文字（Separator）	単語をスペースまたはタブのいずれで区切るかを指定します。
ヘッダーのホスト名の位置（Position of hostname in header）	ヘッダーでのホスト名の位置を指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。
ホストネーム	最初の 3 つのフィールドに示される詳細情報に基づいて、ホスト名を表示します。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。 <181>Oct 10 15:14:08 Hostname Message 区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。 [ホスト名（Hostname）] には Hostname が自動的に表示されます。 ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

メッセージ本文の syslog テンプレートの各部分と説明

次の表に、カスタマイズ syslog メッセージ テンプレートに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 9 : カスタマイズ テンプレートの正規表現 （29 ページ）を参照してください。

表 *8 : syslog* テンプレート

パート	フィールド	説明
	名前	このテンプレートの目的がわかる一意の名前。
マッピング操作	新規マッピング	新しいユーザーを追加するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、F5 VPN にログインした新しいユーザーを示すには、このフィールドに「logged on from」と入力します。
	削除されたマッピング	ユーザーを削除するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、削除する必要がある ASA VPN のユーザーを示すには、このフィールドに「session disconnect」と入力します。
ユーザーデータ	IPアドレス	キャプチャする IP アドレスを示す正規表現。 たとえば Bluecat メッセージの場合、この IP アドレス範囲内のユーザーの ID をキャプチャするには、次のように入力します。 (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	ユーザー名	キャプチャするユーザー名形式を示す正規表現。
	ドメイン	キャプチャするドメインを示す正規表現。
	MACアドレス	キャプチャする MAC アドレスの形式を示す正規表現。

正規表現の例

メッセージを解析するため、正規表現を使用します。ここでは、IPアドレス、ユーザー名、およびマッピング追加メッセージを解析する正規表現の例を示します。

たとえば、正規表現を使用して次のメッセージを解析します。

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

次の表に、正規表現の定義を示します。

表 *9:* カスタマイズ テンプレートの正規表現

パート	正規表現
IP アドレス	Address <([^\s]+)>|address ([^\s]+)
ユーザー名 （User name）	User <([^\s]+)>| Username = ([^\s]+)
マッピング追加メッセージ（Add mapping message）	(%ASA-4-722051|%ASA-6-713228)

Syslog 事前定義メッセージテンプレートの使用

syslog メッセージには、ヘッダーとメッセージ本文を含む標準構造があります。

ここでは、メッセージの送信元に基づいてサポートされているヘッダーの内容の詳細や、サポートされている本文の構造など、Cisco ISE-PIC が提供する事前定義テンプレートについて説明します。

また、システムで事前に定義されていないソース用に、カスタマイズした本文コンテンツを使用した独自のテンプレートも作成できます。ここでは、カスタムテンプレートでサポートされる構造について説明します。メッセージの解析時には、システムで事前定義されているヘッダーに加えて、使用する 1 つのカスタマイズヘッダーを設定できます。また、メッセージ本文には、複数のカスタマイズテンプレートを設定できます。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （25 ページ） を参照してください。本文のカスタマイズの詳細については、syslog メッセージ本文のカスタマイズ （23 ページ） を参照してください。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されており、カスタマイズテンプレートでも正規表現を使用する必要があります。

メッセージ ヘッダー

パーサーで認識されるヘッダータイプには、すべてのクライアントマシンのすべてのメッセージタイプ（新規および削除）について認識される 2 つのタイプがあります。これらのヘッダーは次のとおりです。

- <171>Host message
- <171>Oct 10 15:14:08 Host message

受信されたヘッダーはホスト名を検出するため解析されます。ホスト名は、IPアドレス、ホスト名、または完全 FQDN のいずれかです。

ヘッダーもカスタマイズできます。ヘッダーをカスタマイズするには、syslog ヘッダーのカスタマイズ （25 ページ）を参照してください。

syslog ASA VPN 事前定義テンプレート

ASA VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

本文メッセージ	解析例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	

本文メッセージ	解析例
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] （注） このメッセージタイプから解析されるIPアドレスは、メッセージに示されているようにプライベートIPアドレスです。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] （注） このメッセージタイプから解析されたIPアドレスはIPv4アドレスです。

マッピング削除本文メッセージ

ここではパーサーでASA VPNのためにサポートされている マッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,10.1.1.1]

本文メッセージ
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.

本文メッセージ
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

syslog Bluecat 事前定義テンプレート

Bluecat でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

ここでは、Bluecat syslog で新規マッピングとしてサポートされるメッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

本文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

マッピング削除メッセージ

Bluecat のマッピング削除メッセージはありません。

syslog F5 VPN 事前定義テンプレート

F5 VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな F5 VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[user=UserA,ip=172.16.0.12]

本文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

マッピング削除メッセージ

現在、F5 VPN でサポートされている削除メッセージはありません。

syslog Infoblox 事前定義テンプレート

Infoblox でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

本文メッセージ
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

マッピング削除メッセージ

受信された本文が解析され、次のようにユーザーの詳細が判明します。

- MAC アドレスが含まれている場合：

  [00:0c:29:a2:18:34,10.0.10.100]

- MAC アドレスが含まれていない場合：

  [10.0.10.100]

本文メッセージ
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

syslog Linux DHCPd3 事前定義テンプレート

Linux DHCPd3 でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング メッセージ

次の表では、パーサーが認識するさまざまな Linux DHCPd3 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

マッピング削除本文メッセージ

ここではパーサーで Linux DHCPd3 のためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[00:0c:29:a2:18:34 ,10.0.10.100]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

syslog MS DHCP 事前定義テンプレート

MS DHCP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな MS DHCP 本文メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

マッピング削除本文メッセージ

ここではパーサーで MS DHCP のためにサポートされているマッピング削除メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,0

syslog SafeConnect NAC 事前定義テンプレート

SafeConnect NAC でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな SafeConnect NAC 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

本文メッセージ
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

マッピング削除メッセージ

現在、Safe Connect でサポートされている削除メッセージはありません。

syslog Aerohive 事前定義テンプレート

Aerohive でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Aerohive 本文メッセージについて説明します。

本文で解析される詳細には、ユーザー名と IP アドレスがあります。解析に使用される正規表現の例を次に示します。

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,10.5.50.52]

本文メッセージ
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

マッピング削除メッセージ

現在、Aerohive からのマッピング削除メッセージはサポートされていません。

syslog Blue Coat 事前定義テンプレート：Main Proxy、Proxy SG、Squid Web Proxy

Blue Coat の次のメッセージ タイプがサポートされています。

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

BlueCoat メッセージでサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Blue Coat 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,192.168.10.24]

本文メッセージ（この例は、**BlueCoat** プロキシ **SG** メッセージからの引用です）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

次の表では、新規マッピングメッセージに使用されるクライアント別の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4}))\s** ユーザー名（User name） **\s\-\s([a-zA-Z0-9_]+)\s\-\s**
BlueCoat Proxy SG	新規マッピング **(\-\sPROXIED){1}** IP **\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4}))\s[a-zA-Z0-9_]+\s** ユーザー名（User name） **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid Web Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4}))\sTCP** ユーザー名（User name） **\s([a-zA-Z0-9\._]+)\s\-\/**

マッピング削除メッセージ

Blue Coat クライアントではマッピング削除メッセージがサポートされていますが、現在利用できる例はありません。

次の表では、マッピング削除メッセージに使用されるクライアント別の既知の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	現在利用できる例はありません。
BlueCoat Squid Web Proxy	**(TCP_MISS|TCP_NC_MISS){1}**

syslog ISE および ACS 事前定義テンプレート

パーサーは ISE または ACS クライアントをリッスンするときに、次のメッセージ タイプを受信します。

- 認証成功：ユーザーが ISE または ACS により認証されると、認証が成功したことを通知し、ユーザーの詳細情報を記述した認証成功メッセージが発行されます。このメッセージが解析され、このメッセージのユーザーの詳細とセッション ID が保存されます。
- アカウンティング開始およびアカウンティング更新メッセージ（新規マッピング）：アカウンティング開始メッセージまたはアカウンティング更新メッセージは、認証成功メッセージから保存されたユーザーの詳細とセッション ID を使用して解析され、ユーザーがマッピングされます。
- アカウンティング終了（マッピング削除）：システムからユーザーマッピングが削除されます。

ISE および ACS でサポートされる syslog メッセージの形式とタイプについて説明します。

認証成功メッセージ

認証成功メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **解析例**

  ユーザー名とセッション ID だけが解析されます。

  [UserA,5]

アカウンティング開始/更新（新規マッピング）メッセージ

新規マッピング メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザー名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

マッピング削除メッセージ

マッピング削除では次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザー名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

syslog Lucent QIP 事前定義テンプレート

Lucent QIP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （29 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまなLucent QIP本文メッセージについて説明します。

これらのメッセージの正規表現構造を次に示します。

DHCP_GrantLease|:DHCP_RenewLease

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[00:0C:29:91:2E:5D,10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

マッピング削除本文メッセージ

これらのメッセージの正規表現構造を次に示します。

Delete Lease:|DHCP Auto Release:

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

パッシブ ID サービスのフィルタリング

特定のユーザーを名前やIPアドレスに基づいてフィルタリングできます。たとえばITサービスの管理者が、そのエンドポイントの標準ユーザーを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して[ライブセッション（Live Sessions）]に表示されないようにし、そのエンドポイントの標準ユーザーだけが表示されるようにできます。[ライブ セッション（Live Session）] には、マッピング フィルタでフィルタリングされていないパッシブ ID サービス コンポーネントが表示されます。フィルタは必要なだけ追加できます。「OR」論理演算子をフィルタの間に適用します。両方のフィールドを 1 つのフィルタで指定する場合は、「AND」論理演算子をこれらのフィールドの間に適用します。

ステップ 1 **[プロバイダ（Providers）] > [マッピング フィルタ（Mapping Filters）]** を選択します。

ステップ 2 [追加（Add）] をクリックし、フィルタするユーザーのユーザー名や IP アドレスを入力して、[送信（Submit）] をクリックします。

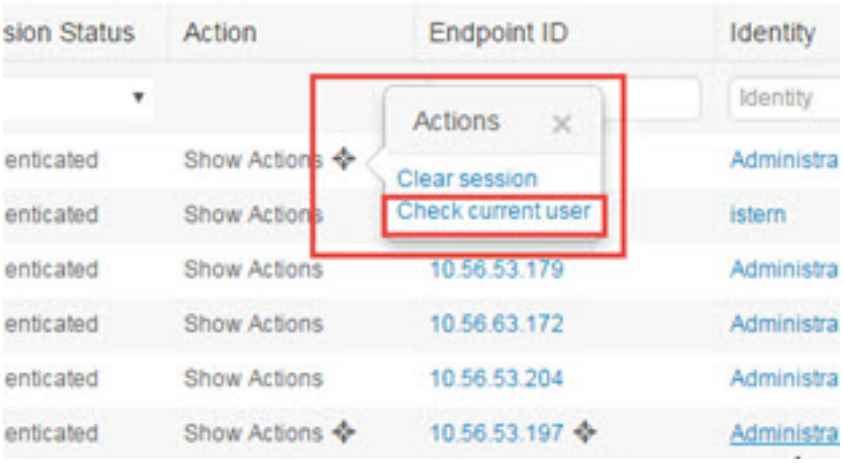
エンドポイント プローブ

設定可能なカスタム プロバイダの他に、インストール完了後にデフォルトで ISE-PICエンドポイント プローブが有効になります。エンドポイント プローブは、特定の各ユーザーがまだシステムにログインしているかどうかを定期的にチェックします。

（注） エンドポイントがバックグラウンドで実行されることを確認するには、まず最初の Active Directory 参加ポイントを設定し、[クレデンシャルの保存（Store Credentials）] を選択していることを確認します。エンドポイントプローブの設定の詳細については、エンドポイントプローブの使用 （42 ページ）を参照してください。

エンドポイントのステータスを手動で確認するには、**[アクション（Actions）]** 列から **[ライブセッション（Live Sessions）]** に移動し、**[アクションを表示（Show Actions）]** をクリックし、次の図に示すように **[現在のユーザーを確認（Check current user）]** を選択します。

図 *2*：現在のユーザーの確認



エンドポイント ユーザーのステータスと手動でのチェックの実行の詳細については、ライブセッションを参照してください。

エンドポイントプローブはユーザーが接続していることを認識します。特定のエンドポイントのセッションが最後に更新された時点から 4 時間経過している場合には、ユーザーがまだログインしているかどうかを確認し、次のデータを収集します。

- MAC アドレス
- オペレーティング システムのバージョン

このチェックに基づいてプローブは次の操作を実行します。

- ユーザーがまだログインしている場合、プローブは Cisco ISE-PIC を [アクティブユーザー（Active User）] ステータスで更新します。
- ユーザーがログアウトしている場合、セッション状態は [終了（Terminated）] に更新され、15 分経過後にユーザーはセッション ディレクトリから削除されます。
- ユーザーと通信できない場合、たとえばファイアウォールによって通信が防止されているか、エンドポイントがシャットダウンしている場合などには、ステータスが [到達不可能（Unreachable）] として更新され、サブスクライバ ポリシーによってユーザー セッションの処理方法が決定します。エンドポイントは引き続きセッション ディレクトリに残ります。

エンドポイント プローブの使用

始める前に

ISE-PIC がインストールされている場合、エンドポイント プローブがデフォルトで有効になっています。プローブを有効または無効にするには、次のように設定していることを確認してください。

- エンドポイントはポート 445 とのネットワーク接続が必要です。
- ISE-PIC で、最初の Active Directory 参加ポイントを設定します。参加ポイントの詳細については、プローブおよびプロバイダとしての Active Directoryを参照してください。

（注） エンドポイントがバックグラウンドで実行するようにするため、最初に 1 番目の Active Directory 参加ポイントを設定する必要があります。これにより、Active Directory プローブが完全に設定されていない場合でもエンドポイント プローブを実行できるようになります。

ステップ 1 **[プロバイダ（Providers）] > [エンドポイントプローブ（Endpoint Probes）]** を選択します。

ステップ 2 [有効（Enabled）] または [無効（Disabled）] を選択します。
画面は変更されません。ただし、選択内容に基づいてプローブが有効化または無効化されます。有効化された場合、プローブはバックグラウンドで稼働しており、データを収集しています。

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。