デバイス管理のインフラストラクチャの準備

ここでは、次の内容について説明します。

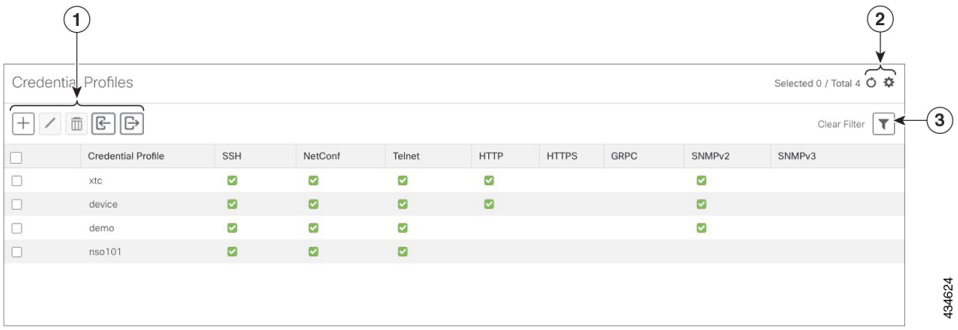
クレデンシャルプロファイルの管理

クレデンシャルプロファイルは、SNMP、Telnet、SSH、HTTP、およびその他のネットワークプロトコルのクレデンシャルの集まりです。1 つのクレデンシャルプロファイルに複数のプロトコルとクレデンシャルを設定できます。

クレデンシャルプロファイルを使用すると、デバイス設定の変更とモニタリングを自動化したり、プロバイダと通信したりできます。デバイスを追加またはインポートする場合、またはプロバイダーを作成する場合は、クレデンシャルプロファイルを指定します。

[クレデンシャルプロファイル（Credential Profiles）] ウィンドウから、新しいクレデンシャルプロファイルを作成したり、既存のプロファイルの設定を更新したり、プロファイルを削除したりできます。このウィンドウを開くには、メインメニューから **[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択します。

図 *1 : [*クレデンシャルプロファイル（***Credentials Profile***）*]* ウィンドウ



項目	説明
1	をクリックして、クレデンシャルプロファイルを追加します。「クレデンシャルプロファイルの作成 （3 ページ）」を参照してください。
	をクリックして、選択したクレデンシャルプロファイルの設定を編集します。「クレデンシャルプロファイルの編集 （8 ページ）」を参照してください。
	をクリックして、選択したクレデンシャルプロファイルを削除します。「クレデンシャルプロファイルの削除 （9 ページ）」を参照してください。
	クリックして、CSV ファイルから新しいクレデンシャルプロファイルをインポートします。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。「クレデンシャルプロファイルのインポート （5 ページ）」を参照してください。
	をクリックして、クレデンシャルプロファイルを CSV ファイルにエクスポートします。クレデンシャルプロファイルのエクスポート （9 ページ）を参照してください。
2	をクリックして、[クレデンシャルプロファイル（Credential Profiles）] ウィンドウを更新します。
	をクリックして、[クレデンシャルプロファイル（Credential Profiles）] ウィンドウに表示する列をクリックして選択します。

項目	説明
3	をクリックして、[クレデンシャルプロファイル（Credential Profiles）] ウィンドウの 1 つ以上の列にフィルタ条件を設定します。
	設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。

クレデンシャルプロファイルの作成

新しいクレデンシャルプロファイルを作成するには、次の手順を実行します。次に、プロファイルを使用し、新しいデバイスまたはプロバイダを追加するときにクレデンシャルを一貫して適用できます。必要な数のプロトコルと対応するクレデンシャルをプロファイルに追加できます。

追加するクレデンシャルプロファイルが多数ある場合は、CSV ファイルに情報を入れてファイルをインポートするほうが効率的です。「クレデンシャルプロファイルのインポート（5 ページ）」を参照してください。

SNMP クレデンシャルを含んでいるデバイスクレデンシャルプロファイルを作成する場合は、デバイスで実際に有効になっている SNMP のバージョンのクレデンシャルと、そのバージョンのみを含めることをお勧めします。たとえば、デバイス設定で SNMPv3 が有効になっていない場合は、そのデバイスのクレデンシャルプロファイルに SNMPv3 クレデンシャルを含めないでください。

インポートおよびエクスポートの機能と CSV ファイルを使用してクレデンシャルプロファイルを一括して作成する場合は、次の点に注意してください。

- CSV ファイルにエクスポートされたすべてのクレデンシャルプロファイルの各パスワードまたはコミュニティ文字列のエントリのすべての文字がアスタリスク（クレデンシャルプロファイルのエクスポート （9 ページ））に置き換えられます。
- CSV ファイルのパスワードとコミュニティ文字列が空白の場合は、クレデンシャルプロファイルをインポートできません（「クレデンシャルプロファイルのインポート（5 ページ）」を参照）。

ネットワークセキュリティを維持するために、インポートする CSV ファイルでは、実際のパスワードとコミュニティ文字列の代わりにアスタリスクを使用することをお勧めします。インポート後、「クレデンシャルプロファイルの編集 （8 ページ）」の手順に従ってアスタリスクを実際のパスワードとコミュニティ文字列に置き換えます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 2 をクリックします。

ステップ 3 [プロファイル名（Profile Name）] フィールドに、内容がわかるプロファイル名を入力します。名前には、最大 128 文字の英数字と、ドット（.）、アンダースコア（「_」）、またはハイフン（「-」）を含めることができます。その他の特殊文字は使用できません。

クレデンシャルプロファイルが多くなる場合は、[クレデンシャルプロファイル（Credential Profiles）] パネルに情報が表示されるため、可能な限り識別しやすい名前と説明にします。

ステップ 4 [接続タイプ（Connectivity Type）] ドロップダウンからプロトコルを選択します。

ステップ 5 次の表に示されているクレデンシャルフィールドに値を入力します。表示される必須フィールドとオプションフィールドは、選択した接続タイプによって異なります。入力する値は、デバイスに設定されている値と一致している必要があります。

接続タイプ（Connectivity Type）	フィールド
SSH	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。[イネーブルパスワード（Enable Password）] はオプションです。
SNMPv2	必須の SNMPv2 の [読み取りコミュニティ（Read Community）] 文字列を入力します。[書き込みコミュニティ（Write Community）] はオプションです。
NETCONF	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
TELNET （注） このプロトコルを使用する場合、いくつかのセキュリティ上の制限があります。	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。[イネーブルパスワード（Enable Password）] はオプションです。
HTTP	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
HTTPS	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
GRPC	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
gNMI	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
TL1	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。

接続タイプ（Connectivity Type）	フィールド
SNMPv3	必須の [セキュリティレベル（Security Level）] を選択し、[ユーザー名（User Name）] に入力します。 AUTH_NO_PRIV または AUTH_PRIV の [セキュリティレベル（Security Level）] に NO_AUTH_NO_PRIV を選択した場合、残りのフィールドはオプションです。 [セキュリティレベル（Security Level）] に AUTH_NO_PRIV を選択した場合は、[認証タイプ（Auth Type）] を選択し、[認証パスワード（Auth Password）] を入力する必要があります。 [セキュリティレベル（Security Level）] に AUTH_PRIV を選択した場合は、[認証タイプ（Auth Type）] と [プライバシータイプ（Priv Type）] を選択し、[認証パスワード（Auth Password）] と [プライバシーパスワード（Priv Password）] を入力する必要があります。 次の SNMPv3 プライバシータイプのみがサポートされています。 • CFB_AES_128 • CBC_DES_56 次のプライバシータイプはサポートされていません。 • AES192 • AES256 • 3DES

ステップ 6 （オプション）このクレデンシャルプロファイルに追加する他のすべてのプロトコルと対応するクレデンシャルに対して、必要に応じて、[+ もう 1 つ追加する（+ Add Another）] をクリックし、上記の手順を繰り返します。

ステップ 7 [保存（Save）] をクリックします。

クレデンシャルプロファイルのインポート

複数のクレデンシャルプロファイルを指定する CSV ファイルを作成し、Cisco Crosswork アプリケーションにインポートするには、次の手順を実行します。

CSVファイルからクレデンシャルプロファイルをインポートすると、まだデータベースに存在しないプロファイルが追加されます。すでに存在するクレデンシャルプロファイルはインポートできません。

以前にエクスポートし、変更したクレデンシャルプロファイル CSV ファイルを再インポートする場合は、エクスポートしたクレデンシャルプロファイルの CSV ファイル内のすべてのパスワードとコミュニティ文字列がアスタリスクに置き換えられることに注意してください。エ

クスポートしたクレデンシャルプロファイルの CSV ファイルのパスワードが空白で設定されている場合は再インポートできません。セキュリティを維持するために、CSV ファイルの実際のパスワードとコミュニティ文字列の代わりにアスタリスクを使用することをお勧めします。インポート後、「クレデンシャルプロファイルの編集 （8 ページ）」の手順に従ってアスタリスクを実際のパスワードとコミュニティ文字列に置き換えます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 2 をクリックして、ダイアログボックスを開きます。

ステップ 3 インポートするクレデンシャルプロファイルのCSVファイルをまだ作成していない場合は、次の手順を実行します。

a) [「Credential template（*.csv）」サンプルファイルのダウンロード（Download sample 'Credential template (*.csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルディスクに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加し始めます（クレデンシャルファイルごとに 1 行）。

同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。それらのエントリ間に2つのセミコロンをスペースなしで使用することで、フィールドを空白のままにすることを示します。複数のエントリをセミコロンで区切る場合は、各フィールドに値を入力する順序が重要であることに注意してください。たとえば、[接続タイプ（Connectivity Type）] フィールドに **SSH;NETCONF;TELNET** と入力し、[ユーザー名（User Name）] フィールドに **UserTom;UserDick;UserHarry;** と入力する場合、エントリの順序によって 2 つのフィールド間のマッピングが決定されます。

- SSH：UserTom
- NETCONF：UserDick
- TELNET：UserHarry

次の点にも注意してください。

- デバイスで現在入力されている SNMP コミュニティ文字列情報を正確に入力してください。
- ユーザー ID に関連付けられたパスワードとコミュニティ文字列情報は、作成した CSV ファイルにプレーンテキストで保存されます。これがセキュリティに与える影響に注意し、適切な保護対策を適用してください。

フィールド	エントリ	必須またはオプション
クレデンシャルプロファイル（Credential Profile）	クレデンシャルプロファイルの名前。 例：。	必須
接続タイプ（Connectivity Type）	有効な値：**SSH**、**SNMPv2**、**NETCONF**、**TELNET** 、**HTTP**、**HTTPS**、**GRPC**、または **SNMPv3**	

フィールド	エントリ	必須またはオプション
ユーザー名（User Name）	例：	[接続タイプ（Connectivity Type）] が **SSH**、**NETCONF**、**TELNET**、**HTTP**、**HTTPS**、**SNMPv3**、または **GRPC** の場合は必須です。
パスワード（Password）	前述の [ユーザー名（User Name）] のパスワード。	[接続タイプ（Connectivity Type）] が **SSH**、**NETCONF**、**TELNET**、**HTTP**、**HTTPS**、または **GRPC** の場合は必須です。
イネーブルパスワード（Enable Password）	イネーブルパスワードを使用します。有効な値は、**ENABLE**、**DISABLE**です。	
イネーブルパスワード値（Enable Password Value）	使用するイネーブルパスワードを指定します。	
SNMPV2 読み取りコミュニティ（SNMPV2 Read Community）	例：**readprivate**	[接続タイプ（Connectivity Type）] が **SNMPv2** の場合は必須です。
SNMPV2 書き込みコミュニティ（SNMPV2 Write Community）	例：**writeprivate**	
SNMPV3 ユーザー名（SNMPV3 User Name）	例：**DemoUser**	[接続タイプ（Connectivity Type）] が **SNMPv3** の場合は必須です。
SNMPV3 セキュリティレベル（SNMPV3 Security Level）	有効な値は、**noAuthNoPriv**、**AuthNoPriv**、または **AuthPriv** です。	[接続タイプ（Connectivity Type）] が **SNMPv3** の場合は必須です。
SNMPV3 認証タイプ（SNMPV3 Auth Type）	有効な値は **HMAC_MD5** または **HMAC_SHA** です。	[接続タイプ（Connectivity Type）] が **SNMPv3** で、[SNMPV3 セキュリティレベル（SnmpV3 Security Level）] が **AuthNoPriv** または **AuthPriv** の場合は必須です。
SNMPV3 認証パスワード（SNMPV3 Auth Password）	この認可タイプのパスワード。	[接続タイプ（Connectivity Type）] が **SNMPv3** で、[SNMPV3 セキュリティレベル（SnmpV3 Security Level）] が **AuthNoPriv** または **AuthPriv** の場合は必須です。

フィールド	エントリ	必須またはオプション
SNMPV3 プライバシータイプ（SNMPV3 Priv Type）	有効な値は **CFB_AES_128** または **CBC_DES_56** です。 AES192、AES256、3DES については、 SNMPv3 プライバシータイプはサポートされていません。	[接続タイプ（Connectivity Type）] が **SNMPv3** で、[SNMPV3 セキュリティレベル（SnmpV3 Security Level）] が **AuthPriv** の場合は必須です。
SNMPV3 プライバシーパスワード（SNMPV3 Priv Password）	この権限タイプのパスワード。	[接続タイプ（Connectivity Type）] が **SNMPv3** で、[SNMPV3 セキュリティレベル（SnmpV3 Security Level）] が **AuthPriv** の場合は必須です。

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

ステップ 4 [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

インポートしたクレデンシャルプロファイルが [クレデンシャルプロファイル（Credential Profiles）] ウィンドウに表示されます。

クレデンシャルプロファイルの編集

クレデンシャルプロファイルは、複数のデバイスで（大規模なネットワーク内の何百台ものデバイスでも）共有できます。次の手順を実行し、クレデンシャルプロファイルの設定を変更します。

クレデンシャルプロファイルを編集する前に、変更するプロファイルの CSV バックアップをエクスポートすることをお勧めします（「クレデンシャルプロファイルのエクスポート （9 ページ）」を参照）。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[クレデンシャル（Credential）]** を選択します。

ステップ 2 [クレデンシャルプロファイル（Credential Profiles）] ウィンドウの左側から、更新するプロファイルを選択し、  をクリックします。
選択したクレデンシャルの [プロファイルの編集（Edit Profile）] ウィンドウが表示されます。

ステップ 3 必要な変更を加えて、[保存（Save）] をクリックします。

クレデンシャルプロファイルのエクスポート

クレデンシャルプロファイルをエクスポートすると、選択したすべてのプロファイルが CSV ファイルに保存されます。これは、クレデンシャルプロファイルのバックアップコピーをすばやく作成する方法です。また、必要に応じて CSV ファイルを編集して再インポートし、新しいプロファイルを追加したり、クレデンシャルプロファイルのデータを変更したりすることもできます。

エクスポートしたクレデンシャルプロファイルの CSV ファイルに、実際のパスワードやコミュニティ文字列は含まれていません。エクスポートした CSV ファイルでは、クレデンシャルプロファイルのパスワードとコミュニティ文字列のエントリのすべての文字がアスタリスクに置き換えられます。エクスポートした CSV ファイルを変更してから再インポートする場合は、実際のパスワードとコミュニティ文字列の代わりにアスタリスクを使用することをお勧めします。インポート後、「クレデンシャルプロファイルの編集 （8 ページ）」の手順に従って、アスタリスクを実際のパスワードとコミュニティ文字列に置き換えます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 2 （オプション）[クレデンシャルプロファイル（Credential Profiles）] ウィンドウで、必要に応じてクレデンシャルプロファイルのリストをフィルタ処理します。

ステップ 3 エクスポートするプロファイルのチェックボックスをオンにします。エクスポートするすべてのプロファイルを選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 4 をクリックします。ブラウザによっては、CSV ファイルを保存するときに使用するパスとファイル名を選択するか、またはすぐに開くよう求められます。

クレデンシャルプロファイルの削除

クレデンシャルプロファイルを削除するには、次の手順を実行します。

（注） 1 つ以上のデバイスまたはプロバイダに関連付けられているクレデンシャルプロファイルは削除できません。

ステップ 1 削除するクレデンシャルプロファイルを含むバックアップ CSV ファイルをエクスポートします（「クレデンシャルプロファイルのエクスポート （9 ページ）」を参照）。

ステップ 2 削除するクレデンシャルプロファイルを使用しているデバイスまたはプロバイダーがあるかどうかを確認します。これは、[デバイス（Devices）] ウィンドウ（**[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択）と [プロバイダ（Provider）] ウィンドウ（**[管理（Administration）] > [プロバイダアクセス管理（Manage Provider Access）]**）の両方で使用可能な [クレデンシャルプロファイル（Credential Profile）] 列でフィルタリングすることで実行できます。

ステップ 3 デバイスまたはプロバイダを別のクレデンシャルプロファイルに再割り当てします（このタスクのヘルプについては、「複数のデバイスのクレデンシャルプロファイルの変更 （10 ページ）」と「プロバイダの編集 （40 ページ）」を参照してください）。

ステップ 4 すべてのデバイスとプロバイダのクレデンシャルプロファイルを再割り当てした後、メインメニューから、**[デバイス管理（Device Management）]** > **[クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 5 [クレデンシャルプロファイル（Credential Profiles）] ウィンドウで、削除するプロファイルを選択し、🗑をクリックします。

複数のデバイスのクレデンシャルプロファイルの変更

多数のネットワークデバイスのクレデンシャルプロファイルを変更する場合は、デバイスCSVファイルを編集して変更するほうが効率的です。基本的な方法は次のとおりです。

1. クレデンシャルプロファイルを変更するデバイスが含まれている CSV ファイルをエクスポートします（「CSV ファイルへのデバイス情報のエクスポート」を参照）。
2. CSVファイルを編集し、各デバイスのクレデンシャルプロファイルを変更します（このクレデンシャルプロファイルはすでに存在している必要があります）。編集したファイルを保存します。

変更するクレデンシャルプロファイルがすでに存在していることを確認する必要があります。そのクレデンシャルプロファイルをまだ作成していない場合、CSV のインポートは失敗します。これらのデバイスに関連付けるクレデンシャルプロファイルには、オンボーディング時にこれらのデバイスに設定されたすべてのプロトコルの認証クレデンシャルも必要です。デバイスに設定された特定のプロトコルのクレデンシャルがクレデンシャルプロファイルに存在していないか、または正しくない場合、CSVインポートは成功しますが、これらのデバイスの到達可能性チェックは失敗します。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[デバイス（Devices）]** を選択します。

ステップ 2 クレデンシャルプロファイルを変更するデバイスを選択します。選択できるオプションは、次のとおりです。

- ⎘をクリックしてすべてのデバイスを含めます。
- [検索（Search）] フィールドにテキストを入力するか、または特定の列をフィルタ処理して、デバイスリストをフィルタ処理します。次に、⎘をクリックし、フィルタ処理したデバイスのリストのみを含めます。
- 変更するデバイスレコードの横にあるチェックボックスをオンにします。次に、⎘をクリックし、オンにしたデバイスのみを含めます。

ステップ 3 任意のツールを使用して、新しい CSV ファイルを編集し、保存します。各デバイスの [クレデンシャルプロファイル（Credential Profile）] フィールドに正しいクレデンシャルプロファイル名を入力してください。

ステップ 4 をクリックします。

ステップ 5 [インポート（Import）] ダイアログボックスで [参照（Browse）] をクリックし、新しい CSV ファイルを参照して [インポート（Import）] をクリックします。

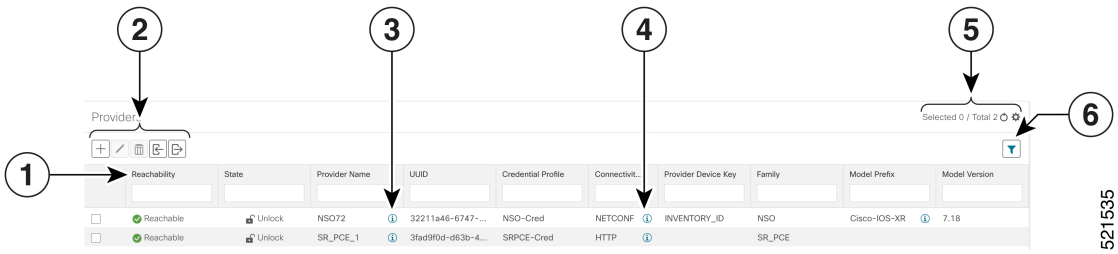
プロバイダの管理

Cisco Crosswork アプリケーションは、外部プロバイダと通信します。Cisco Crosswork はプロバイダ接続の詳細を保存し、その情報をアプリケーションで使用できるようにします。詳細については、「はじめる前に」を参照してください。

[プロバイダ（Providers）] ウィンドウから、新しいプロバイダの追加、既存のプロバイダ設定の更新、および特定のプロバイダの削除を行うことができます。このウィンドウを開くには、**[管理（Administration）] > [プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

（注） 一連の更新を実行する間にアプリケーションが応答するまで待機します。たとえば、プロバイダーの追加、削除、または再読み込みの間にしばらく待機します。これらのアクションの実行が速すぎると、トポロジサービスがこれらの変更を受信しない可能性があります。ただし、トポロジが同期していない場合は、トポロジサービスを再起動します。

図 *2 : [プロバイダ（Providers）] ウィンドウ*



項目	説明
1	この列のプロバイダの横に表示されるアイコンは、プロバイダの [到達可能性（Reachability）] を示します。デバイスの状態（Device State）を参照してください。

項目	説明
2	をクリックして、プロバイダを追加します。「プロバイダの追加について （14 ページ）」を参照してください。
	をクリックして、選択したプロバイダの設定を編集します。「プロバイダの編集 （40 ページ）」を参照してください。
	をクリックして、選択したプロバイダを削除します。「プロバイダの削除 （41 ページ）」を参照してください。
	をクリックして、CSV ファイルから新しいプロバイダをインポートするか、または既存のプロバイダを更新します。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。「プロバイダのインポート （38 ページ）」を参照してください。
	をクリックして、プロバイダを CSV ファイルにエクスポートします。「プロバイダのエクスポート （42 ページ）」を参照してください。
3	[プロバイダ名（Provider Name）] 列のプロバイダの横にある をクリックして、プロバイダのスタートアップ セッション キー/値のペアの詳細が表示された [対象のプロパティ（Properties for）] ポップアップウィンドウを開きます。
4	[接続タイプ（Connectivity Type）] 列のプロバイダの横にある をクリックして、プロバイダのプロトコル、IP、およびその他の接続情報が表示された [接続の詳細（Connectivity Details）] ポップアップウィンドウを開きます。
5	をクリックして、[プロバイダ（Providers）] ウィンドウを更新します。
	をクリックして、[プロバイダ（Providers）] ウィンドウに表示する列を選択します（参照）。
6	をクリックして、[プロバイダ（Providers）] ウィンドウの 1 つ以上の列にフィルタ条件を設定します。
	設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。

プロバイダファミリについて

Cisco Crossworkは、さまざまなタイプまたはファミリのプロバイダをサポートしています。各プロバイダファミリは独自の組み合わせで特別なサービスを提供し、それぞれに固有の要件とオプションがあります。

次の表に、現在サポートされているプロバイダファミリを示します。

表 *1*:サポートされているプロバイダファミリ

プロバイダファミリ	説明
NSO	ネットワークデバイスの設定に使用する Cisco Network Services Orchestrator のインスタンス（Cisco NSO）。「Cisco NSO プロバイダの追加 （17 ページ）」を参照してください。
SR-PCE	Cisco Crossworkアプリケーションがネットワークと通信し、そのネットワークのセグメントルーティング情報を取得するのに必要な設定情報が含まれている Cisco セグメント ルーティング パス計算要素（Cisco SR-PCE） のインスタンス。「Cisco SR-PCE プロバイダの追加 （20 ページ）」を参照してください。
WAE	Cisco WAN Automation Engine（Cisco WAE）のインスタンスは、ネットワークの変化を評価するために使用する「What-If」分析を提供します。「Cisco WAE プロバイダの追加 （33 ページ）」を参照してください。
Syslog ストレージ	KPI と プレイブック によってデバイスから取得した syslog とその他のデータを保存するストレージサーバ（リモートまたはCisco Crossworkアプリケーション VM 自体）のインスタンス。「Syslog ストレージプロバイダの追加 （34 ページ）」を参照してください。
アラート	KPIモニタリング時に収集されたアラートの転送先となるプロバイダのインスタンス（Cisco Crosswork Situation Manager など）。アラートプロバイダの追加 （36 ページ）を参照してください
プロキシ	プロキシプロバイダーのインスタンス。プロキシプロバイダーを追加 （37 ページ）を参照してください

プロバイダの依存関係

この項では、各 Cisco Crosswork アプリケーションと Cisco Crosswork Network Controller に必要なプロバイダ設定について説明します。

Cisco Crosswork Network Controller は、Cisco Crosswork Active Topology と Cisco Crosswork Optimization Engine を組み合わせた統合ソリューションです。また、オプションで Crosswork Network Controller と Crosswork Change Automation、Crosswork Health Insights、Crosswork Zero Touch Provisioning を統合することもできます。

表 *2:* プロバイダ依存性マトリックス

Cisco Crosswork 製品	**Cisco NSO プロバイダ**	**Cisco SR-PCE プロバイダ**	**Cisco WAE プロバイダ**	**Syslog ストレージプロバイダ**	**アラートプロバイダー**
Crosswork Network Controller	必須 必要なプロトコルは HTTPS です プロバイダプロパティキーの **forward** は *true* に設定する必要があります。	必須 必要なプロトコルは HTTP です。	オプション	オプション	オプション
Crosswork 最適化エンジン	オプション	必須 必要なプロトコルは HTTP です。	オプション	オプション	オプション
Crosswork Change Automation Crosswork Health Insights	必須 必要なプロトコルは HTTPS です。 プロバイダプロパティキーの **forward** は *true* に設定する必要があります。	オプション	オプション	オプション	オプション
Crosswork ゼロタッチプロビジョニング	オプション	オプション	オプション	オプション	オプション

プロバイダの追加について

Cisco Crosswork は、さまざまな機能を実行するためにさまざまなプロバイダに依存しています。たとえば、Cisco Network Services Orchestrator はセグメント ルーティング ポリシーとデバイス情報を提供します。新しいプロバイダに依存する機能が将来追加される可能性があり、単一のプロバイダの複数のインスタンスと通信する必要がある場合があります。各プロバイダのサービスにアクセスするには、プロバイダを Cisco Crosswork アプリケーションのシステム設定に追加する必要があります。

プロバイダを追加するには、次の 2 つの方法があります。

1. **UI によるプロバイダの追加**：この方法については、「UI を使用したプロバイダの追加（15ページ）」を参照してください。この方法は最も時間がかかりますが、多数のプロバイダインスタンスを必要としない展開がほとんどであるため、多くの場合に使用されています。
2. **プロバイダ CSV ファイルからのプロバイダのインポート**：この方法については、「プロバイダのインポート（38ページ）」を参照してください。CSV ファイルのインポートは、一度に追加または更新するプロバイダインスタンスの数が多い場合に便利です。

どちらの方法でも、次が必要です。

- Cisco Crosswork アプリケーションがプロバイダにアクセスできるように、対応するクレデンシャルプロファイルを事前に作成します。ヘルプについては、「クレデンシャルプロファイルの作成 （3 ページ）」を参照してください。
- プロバイダーとの接続に必要なプロトコル、IPアドレス、ポート番号、およびその他の情報を把握します。
- セッションの起動時にプロバイダが必要とする可能性がある特別なプロパティを把握しておきます。

UI を使用したプロバイダの追加

新しい外部プロバイダーを追加するには、次の手順を使用します。その後で、プロバイダをデバイスにマッピングできます。

ステップ 1 メインメニューから、**[管理（Administration）]>[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 次の表に示すように、プロバイダーの値を入力します。

ステップ 4 すべての必須フィールドに入力が完了したら、[保存（Save）] をクリックして新しいプロバイダを追加します。

ステップ 5 （オプション）プロバイダをさらに追加するには、この手順を繰り返します。

表 *3 : [プロバイダの追加（Add Provider）]* フィールド（ =必須*）**

フィールド	説明
*** プロバイダ名（Provider Name）**	Cisco Crosswork アプリケーションで参照のために使用するプロバイダの名前。例：**`Linux_Server`**。名前には、最大 128 文字の英数字と、ドット（.）、アンダースコア（「_」）、またはハイフン（「-」）を含めることができます。その他の特殊文字は使用できません。

フィールド	説明
* クレデンシャルプロファイル（Credential Profile）	Cisco Crosswork アプリケーションがプロバイダへの接続に使用するクレデンシャルプロファイルの名前を選択します。
* ファミリ（Family）	プロバイダーファミリを選択します。選択肢は、**NSO**、**WAE**、**SR-PCE**、**ALERT**、および **SYSLOG_STORAGE** です。
接続タイプ（Connection Type）	
* プロトコル（Protocol）	Cisco Crosswork アプリケーションがプロバイダへの接続に使用する主要プロトコルを選択します。オプションには、**HTTP**、**HTTPS**、**SSH**、**SNMP**、**NETCONF**、**TELNET** などがあります。 このプロバイダの接続プロトコルをさらに追加するには、最初の行の最後にある⊕をクリックします。入力したプロトコルを削除するには、その行の横にある⊗をクリックします。 同じプロトコルを複数セットなど、必要な数の接続の詳細のセットを入力できます。
* IP アドレス/サブネットマスク（IP Address/Subnet Mask）	プロバイダのサーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
* ポート（Port）	プロバイダのサーバーへの接続に使用するポート番号を入力します。これは、設定するプロトコルに対応するポートです。たとえば、プロバイダサーバーとの通信に使用するプロトコルが SSH の場合、ポート番号は通常 22 です。
タイムアウト（Timeout）	接続がタイムアウトするまで待機する時間を入力します（秒単位）。デフォルトは 30 秒です。
モデルのプレフィックス情報（Model Prefix Info）	
* モデル（Model）	Cisco NSO プロバイダを追加する場合にのみ必須：Cisco NSO で使用されている NED CLI に一致するモデルプレフィックスを選択します。有効な値は次のとおりです。 **Cisco-IOS-XR** **Cisco-NX-OS** **Cisco-IOS-XE** テレメトリでは、**Cisco-IOS-XR** のみがサポートされています。 この Cisco NSO プロバイダのモデルプレフィックス情報をさらに追加するには、[モデルプレフィックス情報（Model Prefix Info）] セクションの任意の行の末尾にある⊕をクリックします。入力したモデルプレフィックスを削除するには、その行の横にある⊗をクリックします。
* バージョン（Version）	Cisco NSO プロバイダを追加する場合にのみ必須：NSO サーバーで使用する Cisco NSO NED ドライバのバージョンを入力します。
プロバイダのプロパティ（Provider Properties）	

フィールド	説明
プロパティキー（**Property Key**）	設定する特別なプロバイダプロパティのキーの名前を入力します。 プロバイダプロパティは、Cisco Crosswork アプリケーションがプロバイダと連携する方法を制御します。すべてのプロバイダーが必要とするわけではなく、プロパティの数とタイプはプロバイダーファミリによって異なります。これらのプロパティについては、このガイドの特定のプロバイダの追加に関するトピックを参照してください。ただし、Cisco Crosswork アプリケーションはプロバイダのプロパティを検証しないことに注意してください。入力したプロパティがプロバイダに対して有効であることを確認します。 （注） 2 ネットワーク インターフェイス設定では、Cisco Crosswork アプリケーションはデフォルトで管理ネットワーク インターフェイス（**eth0**）を使用してプロバイダと通信します。この動作は、[プロパティキー（Proverty Key）] と [プロパティ値（Proverty Value）] をそれぞれ **outgoing-interface** と **eth1** として追加することで変更できます。この操作はほとんどの場合、管理インターフェイスが管理ネットワークではなく、データネットワークに存在することがあるため、SR-PCE プロバイダの作成時に必要になります。
プロパティ値（**Proverty Value**）	プロパティキーに割り当てる値を入力します。 このプロバイダの特別なプロパティをさらに追加するには、[プロバイダのプロパティ（Provider Properties）] セクションのキー/値ペアの末尾にある ⊕ をクリックします。入力したキー/値のペアを削除するには、そのペアの横に表示される ⊗ をクリックします。

Cisco NSO プロバイダの追加

Cisco Network Services Orchestrator（Cisco NSO）プロバイダは次の機能を提供します。

- Cisco Crosswork アプリケーションへのネットワークサービスとデバイス設定サービス。
- デバイス管理サービスと設定メンテナンスサービス。

（注） Crosswork は、Cisco NSO Layered Service Architecture（LSA）展開をサポートしています。LSA 展開は、すべてのサービスを含む顧客向けサービス（CFS）NSO として機能する複数の NSO プロバイダーと、デバイスを含むリソース向けサービス（RFS）から構成されます。Crosswork は、NSO プロバイダーを CFS または RFS として自動的に識別します。許可される CFS は 1 つだけです。[マネージャ プロバイダー アクセス（Manager Provider Access）] ページの [タイプ（Type）] 列は、NSO プロバイダーを CFS として識別します。

（注） Cisco NSO 機能パックのサンプルは、Cisco Crosswork Network Controller の VPN サービスプロビジョニング機能の出発点として提供されます。これらのサンプルは、一部の限定されたネットワーク設定では「そのまま」使用できますが、Cisco Crosswork Network Controller の拡張可能な設計を示すことを意図としています。一般的な質問への回答は Cisco Devnet で確認できます。シスコ カスタマー エクスペリエンスの担当者は、サンプルに関する一般的な質問への回答を提供できます。特定のユースケースに合わせたサンプルのカスタマイズについては、シスコアカウントチームを通じてサポートを提供いたします。

始める前に

必要な作業は次のとおりです。

- Cisco NSO プロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （3 ページ）」を参照）。
- Cisco NSO プロバイダに割り当てる名前を確認します。
- トポロジで使用する Cisco NSO NED デバイスモデルとドライババージョンを確認します。

（注） `version` コマンドを使用して Cisco NSO のバージョンを検索できます。次に例を示します。

```
admin@ncs# show ncs-state version
ncs-state version 5.7.6
```

- Cisco NSO サーバーの IP アドレスとホスト名を確認します。NSO が HA で設定されている場合、IP アドレスは管理 VIP アドレスになります。
- Cisco NSO デバイスの設定を確認します。詳細については、「Cisco NSO デバイスの設定例」を参照してください。
- Cisco NSO LSA 展開を有効にするには、階層化されたサービスアーキテクチャ（LSA）を有効にする の手順に従ってください。

UI から Cisco NSO プロバイダを追加するには、次の手順を実行します。すべてのプロバイダの詳細を含む CSV ファイルを作成して Crosswork にインポートすることで、複数のプロバイダを同時にインポートできることに注意してください（「プロバイダのインポート （38 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋をクリックします。

ステップ 3 Cisco NSO プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：プロバイダの名前を入力します。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したCisco NSOのクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[NSO] を選択します。
- [接続タイプ（Connection Type(s)）] の [プロトコル（Protocol）] で、Cisco Crossworkアプリケーションがプロバイダへの接続に使用するプロトコルを選択します。 通常は **HTTPS** が優先されます。詳細については、「プロバイダの依存関係 （13 ページ）」を参照してください。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：Cisco NSO サーバーの IP アドレスサブネットマスクを入力します。
- [ポート（Port）]：HTTPS の場合、HTTPS を使用して NSO にアクセスするには、etc/ncs/ncs.conf で NSO VM の設定と一致するポートを入力します。NSO ではデフォルトポートとして 8888 を使用します。
- [モデル（Model）]：ドロップダウンリストからモデル（[Cisco-IOS-XR]、[Cisco-NX-OS]、または [Cisco-IOS-XE]）を選択し、関連付けられている NED ドライババージョンを入力します。トポロジで使用するデバイスのタイプごとにモデルを追加します。複数ある場合は、サポートされている別のモデルを追加します。
- [バージョン（Version）]：NSO のデバイスモデルにインストールされている NED ソフトウェアバージョンを入力します。

b) オプション値：

- [タイムアウト（Timeout）]：Cisco NSO サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 [プロバイダプロパティ（Provider Properties）] で、[プロパティキー（Property Key）] に **forward**、[プロパティ値（Property Value）] に **true** と入力します。このプロパティは、Cisco Crossworkネットワークコントローラ ソリューションを使用して UI 内でプロビジョニング操作をできるようにし、Crosswork API ゲートウェイを介して NSO へのノースバウンドインターフェイスを有効にする場合に必要です。

（注） Cisco Crossworkには、NSO アプリケーションを Crosswork UI から相互起動するオプションがあります（この機能は、読み取り専用権限を持つユーザーロールでは使用できません）。相互起動機能を有効にするには、次のいずれかの設定で Cisco NSO をプロバイダとして追加します。

- **Property Key nso_crosslaunch_url** では、[プロパティーキー（Property Key）] フィールドに有効な URL が入力されています。
- プロトコルは **HTTP** か **HTTPS** で、プロバイダは到達可能です。

上記の設定のいずれかが存在する場合、相互起動アイコン（  ）が [プロバイダ名（Provider Name）]列に表示されます。または、ウィンドウの右上隅にある起動アイコンを使用して、NSO アプリケーションを相互起動することができます。

ステップ 5 すべての必須フィールドに入力したら、[保存（Save）] をクリックしてプロバイダとして Cisco NSO を追加します。

ステップ 6 [プロバイダー（Providers）] ウィンドウで、作成した NSO プロバイダーを選択し、**[アクション（Actions）]> [ポリシーの詳細の編集（Edit Policy Details）]** をクリックします。

選択した NSO プロバイダーの [ポリシーの詳細の編集（Edit Policy Details）] ウィンドウが表示されます。

ステップ 7 環境の要件に合わせて構成フィールドを編集します。[保存（Save）] をクリックして変更を保存します。

Cisco SR-PCE プロバイダの追加

Cisco セグメント ルーティング パス計算要素（Cisco SR-PCE）プロバイダは、デバイス検出、管理、設定メンテナンス、およびルート計算サービスを Cisco Crosswork アプリケーションに提供します。SR ポリシー、レイヤ 3 リンク、およびデバイスを学習および検出するには、少なくとも 1 つの SR-PCE プロバイダが必要です。2 番目の SR-PCE をバックアップとして設定するオプションがあります。 が複数のドメインの管理をサポートしていないため、両方の SR-PCE デバイスを同じネットワークに接続する必要があります。

（注） 管理ドメインの SDN コントローラとして SR-PCE への Cisco Crosswork アプリケーションアクセスを有効にするには、SR-PCE をプロバイダとして追加する必要があります。

Cisco SR-PCE の 1 つ以上のインスタンスを（UI を介して）プロバイダとしての追加するには、次の手順を実行します。

始める前に

必要な作業は次のとおりです。

- SR-PCE として機能するようにデバイスを設定します。特定のデバイスプラットフォームの SR 設定ドキュメントを参照して、SR を有効にし（IS-IS または OSPF プロトコルの場合）、SR-PCE を設定します（例：*Cisco NCS 540* シリーズ ルータのセグメントルーティング設定ガイド）。
- Cisco SR-PCE プロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （3 ページ）」を参照）。これは、基本的な HTTP テキスト認証クレデンシャルである必要があります（現在、MD5 認証はサポートされていません）。追加する Cisco SR-PCE サーバーが認証を必要としない場合でも、プロバイダのクレデンシャルプロファイルを指定する必要がありますが、HTTP プロトコルを使用しない任意のプロファイルを指定できます。
- Cisco SR-PCE プロバイダに割り当てる名前を確認します。通常、これは Cisco SR-PCE サーバーの DNS ホスト名です。
- Cisco SR-PCE サーバーの IP アドレスを確認します。

- Cisco SR-PCE と Cisco Crosswork アプリケーションサーバー間の通信に使用するインターフェイスを確認します。
- Cisco SR-PCE が検出するデバイスを自動でオンボーディングするかどうか、また、その場合は新しいデバイスの追加時にその管理ステータスを [オフ（off）]、[管理対象（managed）]、または[管理対象外（unmanaged）] にするかどうかを決定します。
- Cisco SR-PCE プロバイダが検出する自動オンボーディングデバイスを予定し、それらをデータベースに追加するときに管理対象の状態に設定する場合は、次の手順を実行します。
  - 新しい管理対象デバイスとの通信用に既存のクレデンシャルプロファイルを割り当てます。
  - クレデンシャルプロファイルは、SNMP プロトコルを使用して設定する必要があります。
- 高可用性を実現するには、一意の名前と IP アドレスを使用し、設定が一致する 2 つの個別の Cisco SR-PCE プロバイダを設定します

ステップ 1 メインメニューから、**[管理（Administration）]**>**[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 SR-PCE プロバイダのフィールドに次の値を入力します。

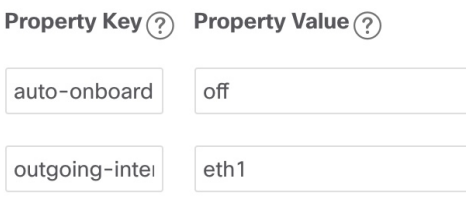
a) 必須フィールド：

- [プロバイダ名（Provider Name）]：SR-PCE プロバイダの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成した Cisco SR-PCE のクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[SR_PCE] を選択します。他のすべてのオプションは無視する必要があります。
- [プロトコル（Protocol）]：[HTTP] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号として **8080** を入力します。
- [プロバイダプロパティ（Provider Properties）]：最初のフィールドセットに、次のキー/値ペアのいずれかを入力します。

プロパティキー	値
auto-onboard	**off** （注） すべてのネットワークデバイスを手動で（UI または CSV インポート経由で）入力する場合は、このオプションを使用します。 デバイスが検出されると、デバイスデータは Cisco SR-PCE データベースに記録されますが、Cisco Crosswork インベントリ管理データベースには登録されません。
auto-onboard	**unmanaged** このオプションを有効にすると、Cisco Crosswork が検出するすべてのデバイスが Cisco Crosswork インベントリ管理データベースに登録され、設定済みの状態が **unmanaged** に設定されます。これらのデバイスの SNMP ポーリングが無効になり、管理 IP 情報は含められません。これらのデバイスを後で **managed** の状態にするには、UI を使用してデバイスを編集するか、CSV にエクスポートして変更を加え、更新した CSV をインポートする必要があります。インポート前にデバイス CSV ファイルに追加することによって、クレデンシャルプロファイルを割り当てることもできます（クレデンシャルプロファイルはすでに存在している必要があります）。
auto-onboard	**managed** このオプションは、IPv4 展開でのみ使用できます。このオプションを有効にすると、Cisco SR-PCE が検出するすべてのデバイスが Cisco Crosswork インベントリ管理データベースに登録され、設定済みの状態が **managed** に設定されます。これらのデバイスに対して SNMP ポーリングが有効になり、Cisco SR-PCE は管理 IP アドレス（ルータ ID）も報告します。デバイスは、SR-PCE プロバイダ設定のデバイスプロファイルキーに関連付けられたクレデンシャルプロファイルを使用して追加されます。 （注） IPv6 展開でこのオプションを有効にしても、デバイスはインベントリに [管理対象外（unmanaged）] として登録されます。

プロパティキー	値
device-profile	すべての新しいデバイスの SNMP クレデンシャルが含まれているクレデンシャルプロファイルの名前。 （注） このフィールドは、**auto-onboard** が **managed** または **unmanaged** に設定されている場合にのみ必要です。
outgoing-interface	**eth1** （注） 2 つの NIC 設定を使用する場合に、データ ネットワーク インターフェイスを介して Cisco Crosswork アプリケーションが SR-PCE にアクセスできるようにする場合にのみ、これを設定する必要があります。
topology	**off** または **on**。 これはオプションのプロパティです。指定しない場合、デフォルト値は **on** です。 値を **off** に指定している場合は、SR-PCE プロバイダが L3 トポロジにアクセスできないことを意味します。
pce	**off** または **on**。 これはオプションのプロパティです。指定しない場合、デフォルト値は **on** です。 値を **off** に指定している場合は、SR-PCE プロバイダが LSP とポリシーにアクセスできないことを意味します。

図 *3:* プロバイダープロパティのキーと値の例



（注） [管理対象（managed）] または [管理対象外（unmanaged）] のオプションが設定されていて、後でデバイスを削除する場合は、次のいずれかを実行する必要があります。

- Cisco Crosswork からデバイスを削除する前に、ネットワークからデバイスを再設定して削除します。これにより、Cisco Crosswork がデバイスを再検出して追加しないようにします。
- auto-onboard を **off** に設定してから、デバイスを Cisco Crosswork から削除します。ただし、これを行うと、Cisco Crosswork はネットワーク内の新しいデバイスを検出または自動オンボーディングできなくなります。

b) オプション値：

- [タイムアウト（Timeout）]：SR-PCE サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックして SR-PCE プロバイダを追加します。

ステップ 5 SR-PCE プロバイダにエラーのない緑色の到達可能性ステータスが表示されていることを確認します。[イベント（Events）] ウィンドウ（**[管理（Administration）] > [イベント（Events）]**）を表示して、プロバイダが正しく設定されているかどうかを確認することもできます。

ステップ 6 SR-PCE プロバイダごとにこのプロセスを繰り返します。

（注） 一度設定した自動オンボーディングオプションを変更することは推奨されません。これらを変更する必要がある場合は、次の手順を実行します。

1. プロバイダを削除し、[イベント（Events）] ウィンドウに削除の確認が表示されるまで待ちます。
2. 更新した自動オンボーディングオプションでプロバイダを再追加します。
3. [イベント（Events）] ウィンドウで、正しい自動オンボーディングオプションを使用してプロバイダが追加されたことを確認します。

次のタスク

- **auto-onboard/off** ペアの場合は、**[デバイス管理（Device Management）] > [ネットワークデバイス（ Network Devices）]** に移動してデバイスを追加します。
- 自動的にデバイスをオンボーディングする選択をした場合は、**[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** に移動してデバイスリストを表示します。地理的な場所の詳細などのノード情報の詳細を追加するには、デバイスリスト（.csv）をエクスポートし、更新してからインポートします。地理的な場所データが欠落している場合は、論理マップを使用してのみデバイストポロジを表示できます。

Cisco SR-PCE の到達可能性の問題

到達可能性の問題は、[イベント（Events）]テーブルで確認でき、到達可能性ステータスは[プロバイダ（Providers）]ウィンドウで確認できます（「プロバイダの詳細の取得（39ページ）」を参照）。SR-PCE がダウンした場合、SR-PCE は通知の更新を送信できないため、トポロジ内のすべてのリンクは既知であった最後の状態で表示されます。SR-PCE が再度到達可能になると、SR-PCE が再接続され、それに応じてトポロジが更新されることを示すメッセージが[イベント（Events）]テーブル（）に表示されます。SR-PCE が長時間ダウンし、同期されておらず、更新が行われていないことに気づいた場合は、次の UI を使用して SR-PCE を削除し、（接続が戻ったら）もう一度追加します。

1. makecall ディレクトリで、次のコマンドを実行します。

   ```
   # process restart pce_server
   ```

2. UI で、**[管理（Administration）]>[プロバイダアクセスの管理（Manage Provider Access）]** に移動し、SR-PCE プロバイダを削除してから、もう一度追加します。

次の手順を実行して、到達可能性をトラブルシューティングすることもできます。

ステップ 1 デバイスのクレデンシャルを確認します。

ステップ 2 プロバイダホストに ping を実行します。

ステップ 3 プロバイダの接続設定で指定されたプロトコルを使用して接続を試行します。SR-PCE プロバイダの場合、通常は HTTP でポート 8080 です。

ステップ 4 ファイアウォール設定とネットワーク設定を確認します。

ステップ 5 接続できるユーザーを制限する可能性のあるアクセスコントロールリストの設定については、Cisco SR-PCE のホストまたは介入デバイスを確認します。

複数の Cisco SR-PCE HA ペア

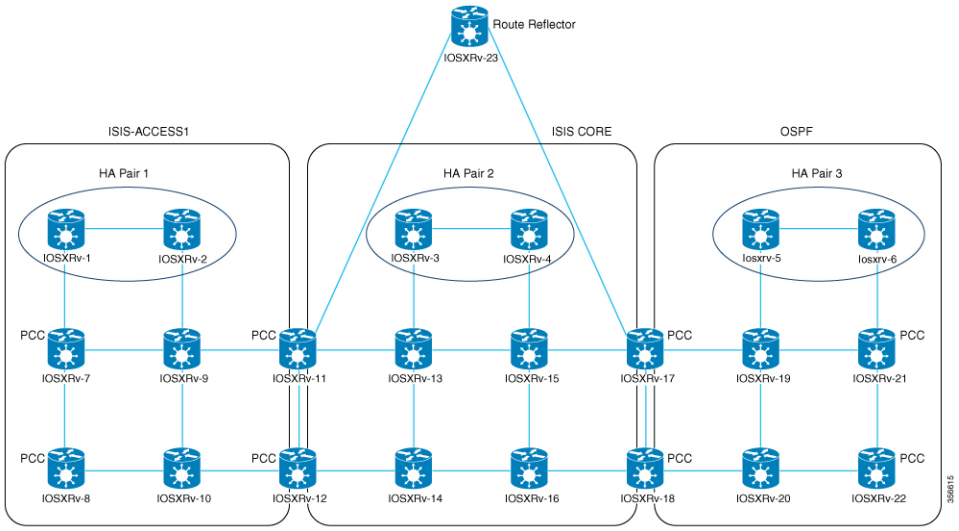
高可用性（HA）を確保するために、最大 8 つの Cisco SR-PCE HA ペア（合計 16 の SR-PCE）を設定できます。Cisco SR-PCE プロバイダの各 HA ペアには、同じネットワークトポロジをサポートしている一致する設定が必要です。HA では、プライマリ SR-PCE が到達不能になった場合に、Cisco Crosswork 最適化エンジンはセカンダリ SR-PCE を使用してネットワークトポロジを検出します。このペアが失敗すると、次の HA ペアが引き継ぎます。ネットワークトポロジは引き続き正しく更新され、[イベント（Events）] テーブル（）で SR-PCE 接続イベントを表示できます。

複数の HA ペア

複数の SR-PCE HA ペアの場合、各 SR-PCE ペアは同じトポロジを認識しますが、パス計算クライアント（PCC）から作成されたトンネルを管理し、それらのみを認識します。次の図に、3 つの SR-PCE HA ペアトポロジの例を示します。次の点に注意してください。

- HA ペア 1：PCE iosxrv-1 と iosxrv-2 は、ヘッドエンドが iosxrv-7 と iosxrv-8 であるトンネルのみをプロビジョニングおよび検出します。iosxrv-9 と iosxrv-10 は PCC ルータではないことに注意してください。
- HA ペア 2：PCE iosxrv-3 と iosxrv-4 は、ヘッドエンドが iosxrv-11、iosxrv-12、iosxrv-17、および iosxrv-18 であるトンネルのみをプロビジョニングおよび検出します。iosxrv-13、iosxrv-14、iosxrv-15、および iosxrv-16 は PCC ルータではないことに注意してください。
- HA ペア 3：PCE iosxrv-5 と iosxrv-6 は、ヘッドエンドが iosxrv-21 と iosxrv-22 であるトンネルについてのみプロビジョニングおよび検出します。iosxrv-19 と iosxrv-20 は PCC ルータではないことに注意してください。

図 *4: HA* ペアが *3* つの場合のトポロジの例



（注） いずれかの SR-PCE がメインネットワークトポロジのサブセットに含まれている場合、その SR-PCE プロバイダは、[プロパティキー（Property Key）] を **topology**、[プロパティ値（Property Value）] を **off** として追加する必要があります。この値が設定されている場合、この SR-PCE はトポロジの学習に使用されません。

HA の設定

HA Cisco SR-PCE プロバイダの各ペアを Cisco Crosswork 最適化エンジン に追加するには、次の設定を行う必要があります。

（注） HA を有効にするには、両方の SR-PCE 間に復元力のある IPv4 接続が必要です。他の SR-PCE の PCE IP アドレスは、常にピアから到達可能である必要があります。

Cisco SR-PCE デバイスのそれぞれで次のコマンドを発行します。

インターフェイスを有効にします。

```
# interface <interface><slot>/<port>
ipv4 address <sync-link-interface-ip-address> <subnet-mask>
no shut
```

HA を有効にします。

```
# pce rest sibling ipv4 <other-node-pce-address>
```

2 つの SR-PCE 間に同期リンクを確立します。

```
# router static
address-family ipv4 unicast
<other-node-pce-ip-address>/<subnet-mask-length> <remote-sync-link-ip-address>
```

（オプション）`# pce segment-routing traffic-eng peer ipv4 <other-node-pce-ip-address>`

他の PCE ノードではなく、PCC ごとに入力する必要があります。

PCC で次のコマンドを発行します。

SR ポリシーの場合：`# segment-routing traffic-eng pcc redundancy pcc-centric`

RSVP-TE トンネルの場合：`# mpls traffic-eng pce stateful-client redundancy pcc-centric`

兄弟 SR-PCE 設定の確認

SR-PCE から `show tcp brief` コマンドを入力して、HA 内の SR-PCE 間の同期が完全であることを確認します。

```
#show tcp brief | include <remote-SR-PCE-router-id>
```

次の情報が正しいことを確認します。

ローカル アドレス	外部アドレス	状態
<local-SR-PCE-router-id>:8080	*<remote-SR-PCE-router-id>*:*<any-port-id>*	ESTAB
<local-SR-PCE-router-id>:*<any-port-id>*	*<remote-SR-PCE-router-id>*:8080	ESTAB

次に例を示します。

```
RP/0/0/CPU0:iosxrv-1#sh tcp brief | i 192.168.0.2:
Mon Jun 22 18:43:09.044 UTC
0x153af340 0x60000000 0 0 192.168.0.1:47230 192.168.0.2:8080 ESTAB
0x153aaa6c 0x60000000 0 0 192.168.0.1:8080 192.168.0.2:16765 ESTAB
```

この例では、192.168.0.2 がリモート SR-PCE IPです。

SR-PCE 委任

SR-TE ポリシーが作成される場所に応じて、次の SR-PCE 委任が行われます。

- SR-PCE で開始：PCE に設定されたポリシー。SR-TE ポリシーの委任は、送信元 SR-PCE に戻されます。

（注）
- ポリシーは、UI を使用して作成された場合でも PCE で開始できますが、その場合は SR-PCE には明示的に設定されません。
- PCE で RSVP-TE トンネルを直接設定することはできません。

- PCC で開始：デバイスに直接設定された SR-TE ポリシーまたは RSVP-TE トンネル。最も低い優先順位で設定された SR-PCE は、委任された SR-PCE です。優先順位が設定されていない場合、最小の PCE IP アドレスを持つ SR-PCE が委任 SR-PCE になります。次の設定例では、**10.0.0.1** に優先順位値 10 が割り当てられており、これが委任 SR-PCE になることを示しています。

```
segment-routing
  traffic-eng
    pcc
      source-address ipv4 10.0.0.2
      pce address ipv4 10.0.0.1
        precedence 10
       !
      pce address ipv4 10.0.0.8
        precedence 20
       !
       report-all
       redundancy pcc-centric
```

RSVP-TE トンネルの場合：

```
mpls traffic-eng
interface GigabitEthernet0/0/0/0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/2
!
pce
  peer source ipv4 192.168.0.02
  peer ipv4 192.168.0.9
    precedence 10
  !
  peer ipv4 192.168.0.10
    precedence 20
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
  !
!
auto-tunnel pcc
  tunnel-id min 1000 max 5000
```

- Cisco Crosswork SR-PCE で開始：Cisco Crosswork を使用して設定された SR-TE ポリシー。SR-PCE 委任はポリシーごとにランダムです。

（注） Cisco Crosswork 最適化エンジン で変更または削除できるのは、Cisco Crosswork 最適化エンジン によって作成された SR-TE ポリシーまたは RSVP-TE トンネルのみです。

HA の注意事項と制限事項

- すべての PCC が両方の SR-PCE に接続された PCEP であると想定されます。
- SR-PCE が Cisco Crosswork からのみ切断されると、次のようになります。
  - SR-PCE 委任の割り当ては残りますが、切断された SR-PCE は Cisco Crosswork に表示されません。
  - 切断された SR-PCE が委任 PCE の場合、Cisco Crosswork SR-PCE で開始した SR-TE ポリシーを変更することはできません。
- 場合によっては、UI を介して作成した SR-TE ポリシーが Cisco Crosswork Optimization Engineから自動的に削除された場合（意図的であり、予期していた場合）、警告メッセージが表示されません。たとえば、送信元 PCC がリロードされると、UI で作成した SR ポリシーは表示されず、ユーザーには通知されません。
- 1 つの SR-PCE が Cisco Crosswork 最適化エンジン へのアップリンクを除くすべてのリンク（PCC/トポロジデバイスへの）で失敗する極端な場合、Cisco Crosswork 最適化エンジンでトポロジ情報が正確でなくなります。この場合は、接続の問題を修正するか、または [プロバイダ（Provider）]ページから両方の SR-PCE を削除し、到達可能な方をもう一度追加します。

SR-PCE 設定例

次に、HA の場合の複数SR-PCE設定を行うのに役立つ例を示します。適宜変更してください。

冗長 SR-PCE の設定例（Cisco IOS-XR 7.x.x を使用する PCE ）

```
pce
 address ipv4 192.168.0.7
 state-sync ipv4 192.168.0.6
 api
  sibling ipv4 192.168.0.6
```

冗長 SR-PCE の設定例（PCC）

```
segment-routing
 traffic-eng
  pcc
   source-address ipv4 192.0.2.1
   pce address ipv4 192.0.2.6
    precedence 200
   !
   pce address ipv4 192.0.2.7
    precedence 100
   !
```

```
   report-all
   redundancy pcc-centric
```

RSVP-TE の場合の冗長 SR-PCE 設定例（PCC 上）

（注） `Loopback0` は TE ルータ ID を表します。

```
ipv4 unnumbered mpls traffic-eng Loopback0
!
mpls traffic-eng
 pce
  peer source ipv4 209.165.255.1
  peer ipv4 209.165.0.6
   precedence 200
  !
  peer ipv4 209.165.0.7
   precedence 100
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
  !
 !
 auto-tunnel pcc
  tunnel-id min 1000 max 1999
 !
!
```

SR-TM の設定例

```
telemetry model-driven
 destination-group crosswork
  address-family ipv4 198.18.1.219 port 9010
   encoding self-describing-gpb
   protocol tcp
  !
 !
 sensor-group SRTM
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes

 !
 subscription OE
  sensor-group-id SRTM sample-interval 60000
  destination-id crosswork
  source-interface Loopback0
!
traffic-collector
 interface GigabitEthernet0/0/0/3
 !
 statistics
  history-size 10
```

（注） 接続先アドレスは、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） VM のサウスバウンド データ インターフェイス（eth1）アドレスを使用します。

プレフィックスとトンネルのカウンタを取得するには、NSO を介してテレメトリ設定でセンサーパスをプッシュする必要があります。トラフィックコレクタがすべてのトラフィック入力インターフェイスで設定されていることを前提としています。この設定は、オンデマンド帯域幅と帯域幅最適化の機能パックを動作させる要求を満たすために必要です。

テレメトリセンサーパス

```
sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
```

NSO 経由ですべてのヘッドエンドルータに Cisco Crosswork 最適化エンジン がプッシュするテレメトリ設定

```
telemetry model-driven
  destination-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
    vrf default
    address-family ipv4 172. 19.68.206 port 31500
      encoding self-describing-gpb
      protocol top
    !
  !
destination-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  vrf default
  address-family ipv4 172. 19.68.206 port 31500
    encoding self-describing-gpb
    protocol top
  !
!
sensor-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
!
sensor-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
!
subscription CW_43dc8a5ea99529715899b4f5218408a785e40fce
  sensor-group-id CW_43dc8a5ea99529715899b4f5218408a785e40fce sample-interval 300000
  destination-id CW_43dc8a5ea99529715899b4f5218408a785e40fce
!
subscription CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  sensor-group-id CW_4b3c69a200668b%a8dc155caff295645c684a8f8 sample-interval 300000
  destination-id CW_463c69a200668b0a8dc155caff295645c684a8f8
  !
!
```

トラフィックコレクタの設定（トラフィックコレクタ下に追加するすべての入力トラフィックインターフェイス）

```
RP/0/RSP0/CPU0:PE1-ASR9k#sh running-config traffic-collector
Fri May 22 01:14:35.845 PDT
traffic-collector
  interface GigabitEthernet0/0/0/0
  !
```

```
  statistics
    history-size 1
    collection-interval 1
    history-timeout 1
    history-minute-timeout
  !
!
```

すべてのプレフィックスでの **BGP neighbor next-hop-self** の追加（**TM** レートカウンタを表示）。

```
bgp router-id 5.5.5.5
address-family ipv4 unicast
  network 5.5.5.5/32
  redistribute static
!
address-family link-state link-state
!
neighbor 1.1.1.1
  remote-as 65000
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
!
```

トラフィック コレクタ トンネルとプレフィックスカウンタ

```
RP/0/RSP0/CPU0:PE1-ASR9k#show traffic-collector ipv4 counters prefix
Fri May 22 01:13:51.458 PDT
Prefix              Label         Base rate         TM rate        State
                                  (Bytes/sec)       (Bytes/sec)
------------------  ------------  ---------------  --------------  -----------------
1.1.1.1/32          650001         3                0              Active
2.2.2.2/32          650002         3                0              Active
3.3.3.3/32          650003         6                0              Active
4.4.4.4/32          650004         1                0              Active
6.6.6.6/32          650200         6326338          6326234        Active
7.7.7.7/32          650007         62763285         62764006       Active
8.8.8.8/32          650008         31129168         31130488       Active
9.9.9.9/32          650009         1                0              Active
10.10.10.10/32      650010         1                0              Active
RP/0/RSP0/CPU0:PE1-ASR9k#stt
RP/0/RSP0/CPU0:PE1-ASR9k#show traffic-collector ipv4 counters tunnel
Fri May 22 01:13:52.169 PDT
RP/0/RSP0/CPU0:PE1-ASR9k#]
```

パス計算クライアント（PCC）サポート

PCC は、SR-PCE への RSVP-TE トンネルと SR ポリシーの両方の委任とレポートをサポートできます。両方を同じ PCC でサポートするには、SR-PCE との 2 つの個別の PCEP 接続を確立する必要があります。各 PCEP 接続には、PCC の個別の送信元 IP アドレス（ループバック）が必要です。

次に、RSVP-TE の場合の PCEP 接続の Cisco IOS-XR 設定例を示します。192.168.0.2 は、SR-PCE に委任され、報告される RSVP-TE トンネルの PCEP セッション送信元 IP です。これは、ルータ上のループバックアドレスです。PCEP セッション用に 2 つの SR-PCE が設定されます。1 つ目は優先順位による RSVP-TE トンネルの委任に優先されます。自動トンネル PCC は、Cisco Crosswork 最適化エンジン で作成されたような PCE によって開始された RSVP-TE トンネルへの割り当てに使用されるトンネル ID の範囲で設定されます。

```
mpls traffic-eng
interface GigabitEthernet0/0/0/2
admin-weight 1
!
interface GigabitEthernet0/0/0/3
admin-weight 1
  pce
    peer source ipv4 192.168.0.2
    peer ipv4 192.168.0.1
      precedence 10
     !
    peer ipv4 192.168.0.8
      precedence 11
     !
    stateful-client
      instantiation
      report
     !
   !
   auto-tunnel pcc
    tunnel-id min 10 max 1000
   !
!
ipv4 unnumbered mpls traffic-eng Loopback0

rsvp
interface GigabitEthernet0/0/0/2
bandwidth 1000000
!
interface GigabitEthernet0/0/0/3
bandwidth 1000000
!
!
```

Cisco WAE プロバイダの追加

Cisco WAN Automation Engine（Cisco WAE）プロバイダは、Cisco Crosswork アプリケーションにトラフィックとトポロジ分析を提供します。基盤となるソフトウェアは Cisco WAE Planning であり、トラフィック、トポロジ、および機器の状態の広範囲に及ぶビューを提供します。障害の影響の「What-If」分析を実行する予測モデルを利用します。

UI を使用しての 1 つ以上の Cisco WAE のインスタンスをプロバイダとして追加するには、次の手順を実行します。CSV ファイルを使用してプロバイダを追加することもできます（「プロバイダのインポート （38 ページ）」を参照）。

始める前に

必要な作業は次のとおりです。

- Cisco WAE プロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （3 ページ）」を参照）。これは基本的な HTTP/HTTPS テキスト認証クレデンシャルである必要があります（現在、MD5 認証はサポートされていません）。追加する Cisco WAE サーバーが認証を必要としない場合でも、プロバイダのクレデンシャルプロファイルを指定する必要がありますが、HTTP/HTTPS プロトコルを使用しないプロファイルを指定できます。

- プロバイダーに割り当てる名前を確認します。通常、これは Cisco WAE サーバーの DNS ホスト名です。
- Cisco WAE サーバーの IP アドレスとポートを確認します。接続プロトコルは HTTP または HTTPS になります。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 [+] をクリックします。

ステップ 3 プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：Cisco WAE プロバイダの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[WAE] を選択します。
- [プロトコル（Protocol）]：使用しているクレデンシャルプロファイルに従って、それぞれに [HTTP] または [HTTPS] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号を入力します（通常、HTTP の場合は **8080**、HTTPS の場合は **8843**）。

b) オプション値：

- [タイムアウト（Timeout）]：サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックしてプロバイダを追加します。

Syslog ストレージプロバイダの追加

ストレージプロバイダーは、プレイブックの実行中に収集されたデータのストレージを提供します。

UI を使用して 1 つ以上のストレージプロバイダを追加するには、次の手順を実行します。CSV ファイルを使用してプロバイダを追加することもできます（「プロバイダのインポート （38 ページ）」を参照）。

始める前に

必要な作業は次のとおりです。

- ストレージプロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （3 ページ）」を参照）。これは SSH クレデンシャルである必要があります。
- ストレージプロバイダーに割り当てる名前を確認します。通常、これはサーバーの DNS ホスト名です。
- ストレージプロバイダのサーバーの IPv4 アドレスとポートを確認します。接続プロトコルは SSH になります。
- ストレージプロバイダのサーバーの接続先ディレクトリを確認します。[プロバイダプロパティ（Provider Properties）] フィールドを使用してこれを指定する必要があります。

ステップ 1 メインメニューから、**[管理（Administration）]**>**[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：ストレージプロバイダの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したストレージ クレデンシャル プロファイルを選択します。
- [ファミリ（Family）]：[SYSLOG_STORAGE] を選択します。
- [プロトコル（Protocol）]：Cisco Crosswork アプリケーションがプロバイダへの接続に使用するプロトコルとして [SSH] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号を入力します（SSH の場合は通常、**22**）。
- [プロバイダプロパティ（Provider Properties）]：次のキー/値のペアを次のフィールドに入力します。

プロパティキー	プロパティ値
DestinationDirectory	収集されたデータがサーバーに保存される絶対パス。例：**/root/cw-syslogs**

b) オプション値：

- [Timeout（タイムアウト）]：ストレージサーバーへの接続がタイムアウトするまでの待機時間（秒単位）。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックして syslog ストレージプロバイダを追加します。

アラートプロバイダの追加

アラートプロバイダは、KPIモニタリング中に収集されたアラートを転送する接続先です（Cisco Crosswork Situation Manager など）。アラートプロバイダーは、着信アラートパッケージを受信および処理できる必要があります。

UI を使用してアラートプロバイダを追加するには、次の手順を実行します。CSV ファイルをインポートしてアラートプロバイダを追加することもできます（「プロバイダのインポート（38 ページ）」を参照）。

現在、サポートされるアラートプロバイダは 1 つだけです。

始める前に

必要な作業は次のとおりです。

- アラートプロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （3 ページ）」を参照）。これは、基本的な HTTP テキスト認証クレデンシャルである必要があります（現在、MD5 認証はサポートされていません）。プロバイダが認証を必要としない場合でも、プロバイダのクレデンシャルプロファイルを指定する必要がありますが、HTTPプロトコルを使用しない任意のプロファイルを指定できます。
- アラートプロバイダーに割り当てる名前を確認します。通常、これはサーバーの DNS ホスト名です。
- アラートサーバーの IPv4 アドレスとポートを確認します。接続プロトコルは HTTP になります。
- アラート サーバー エンドポイントの URL を確認します。[プロパティ値（Property Value）] フィールドを使用してこれを指定する必要があります。

ステップ 1 メインメニューから、**[管理（Administration）] > [プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：アラートプロバイダの名前。

- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したアラートプロバイダのクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[アラート（ALERT）] を選択します。
- [プロトコル（Protocol）]：HTTP が事前に選択されています。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：アラートサーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号を入力します（通常、HTTP の場合は 80）。
- [プロバイダのプロパティ（Provider Properties）]：**alertEndpointUrl** プロパティキー名が事前に入力されています。[プロパティ値（Property Value）] フィールドに、アラート サーバー エンドポイントのみを入力します。たとえば、エンドポイントへの完全なパスが **http://aws.amazon.com:80/myendpoint/bar1/** の場合、**/myendpoint/bar1/** のみを入力します。

b) オプション値：

- [タイムアウト（Timeout）]：アラートサーバーへの接続がタイムアウトするまで待機する時間（秒単位）。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）]をクリックしてアラートプロバイダを追加します。

プロキシプロバイダーを追加

UI を使用しての 1 つ以上のプロキシのインスタンスをプロバイダーとして追加するには、次の手順を実行します。CSV ファイルを使用してプロバイダを追加することもできます（「プロバイダのインポート （38 ページ）」を参照）。

始める前に

必要な作業は次のとおりです。

- Proxy プロバイダーのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （3 ページ）」を参照）。これは、基本的な HTTPS テキスト認証資格情報である必要があります。
- プロバイダーに割り当てる名前を確認します。これは通常、プロキシサーバーの DNS ホスト名です。
- プロキシサーバーの IP アドレスとポートを確認します。接続プロトコルは HTTPS になります。

ステップ 1 メインメニューから、**[管理（Admin）]** > **[プロバイダー（Providers）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダー名（Provider Name）]：プロバイダーの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：**プロキシ**を選択します。
- [プロトコル（Protocol）]：[HTTPS] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号を入力します（HTTPS の場合、**30603**）。

b) オプション値：

- [タイムアウト（Timeout）]：サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックしてプロバイダを追加します。

プロバイダのインポート

プロバイダを指定する CSV ファイルを作成して Cisco Crosswork アプリケーションにインポートするには、次の手順を実行します。

CSV ファイルからプロバイダをインポートすると、まだデータベースにないプロバイダが追加され、インポートしたプロバイダと同じ名前のプロバイダが更新されます。このため、インポートする前に、現在のすべてのプロバイダのバックアップコピーをエクスポートすることをお勧めします（「プロバイダのエクスポート （42 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 をクリックして、[CSV ファイルのインポート（Import CSV File）] ダイアログボックスを開きます。

ステップ 3 インポートするプロバイダ CSV ファイルをまだ作成していない場合は、次の手順を実行します。

a) [「Provider template（*.csv）」サンプルファイルのダウンロード（Download sample 'Provider template (*.csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルストレージリソースに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加します（プロバイダごとに 1 行）。

同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。それらのエントリ間に 2 つのセミコロンをスペースなしで使用することで、フィールドを空白のままにすることを示します。

エントリをセミコロンで区切る場合は、値を入力する順序が重要です。たとえば、**connectivity_type** フィールドに **SSH;SNMP;NETCONF;TELNET** と入力し、**connectivity_port** フィールドに **22;161;830;23** と入力した場合、エントリの順序によって 2 つのフィールド間のマッピングが決定されます。

- SSH：ポート 22
- SNMP：ポート 161
- NETCONF：ポート 830
- Telnet：ポート 23

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

ステップ 4 [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

インポートしたプロバイダ情報が [プロバイダ（Providers）] ウィンドウに表示されます。

ステップ 6 インポート中に報告されたエラーを解決し、プロバイダの詳細を確認して接続を確定します。

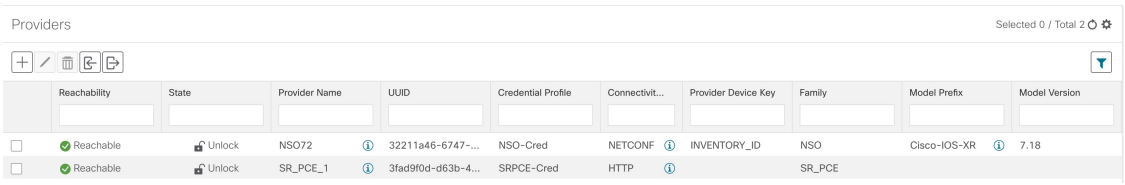
プロバイダの詳細の取得

[プロバイダ（Providers）] ウィンドウを使用して、プロバイダの詳細を取得してそれらの到達可能性を確認します。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

Cisco Crossworkアプリケーションで設定された各プロバイダの [プロバイダ（Providers）] ウィンドウには、次の図に示すように、プロバイダの名前、汎用一意識別子（UUID）、関連するクレデンシャルプロファイルなどの情報が表示されます。

図 5 : [プロバイダ（*Providers*）] ウィンドウ



ステップ 2 [到達可能性（Reachability）] 列のアイコンは、リストされている接続プロトコルを介してプロバイダに到達できるかどうかを示します。詳細については、「デバイスの状態（Device State）」を参照してください。

Cisco Crosswork アプリケーションは、プロバイダが追加または変更された直後にプロバイダの到達可能性を確認します。これらのイベント以外は、Cisco Crosswork Change Automation and Health Insights は 5 分ごとに到達可能性を確認し、Crosswork 最適化エンジン は約 10 秒ごとに SR-PCE の到達可能性を確認します。

ステップ 3 次のように、プロバイダの詳細情報をさらに取得します。

a) [プロバイダ名（Provider Name）] 列で、ⓘ をクリックして、プロバイダ固有のキー/値のプロパティを表示します。

b) [接続タイプ（Connectivity Type）] 列で、ⓘ をクリックして、プロバイダ固有のプロトコル、IP 形式、IP アドレス、ポート、タイムアウト情報など、プロバイダの詳細な接続情報を表示します。

c) [モデルプレフィックス（Model Prefix）] 列で、ⓘ をクリックして、Cisco Network Services Orchestrator（Cisco NSO）プロバイダの設定済み NED モデルプレフィックスでサポートされる NED バージョンを表示します。

d) 完了したら、✕ をクリックして詳細ウィンドウを閉じます。

Cisco SR-PCE の到達可能性の問題が発生している場合は、「Cisco SR-PCE の到達可能性の問題 （25 ページ）」を参照してください。HTTP とポート 8080 が設定されていることを確認します。

一般的なプロバイダーの到達可能性の問題については、次のようにトラブルシューティングできます。

1. プロバイダホストに ping を実行します。
2. プロバイダの接続設定で指定されたプロトコルを使用して接続を試行します。。

   次の CLI コマンドを使用して、このチェックを実行できます。

   ```
   curl -v -H "X-Subscribe: stream" "http://<ip-address>:8080/
   bwod/subscribe/json?keepalive-30&priority=5"
   ```

3. ファイアウォール設定とネットワーク設定を確認します。
4. 接続できるユーザーを制限する可能性のあるアクセスコントロールリストの設定については、プロバイダのホストまたは介入デバイスを確認します。

プロバイダの編集

プロバイダ設定を編集する場合は、大規模ネットワーク内に数千台のデバイスがあっても、多数のデバイスにプロバイダがマッピングされる可能性があることに注意してください。

（注）

- プロバイダーの設定を変更する前に、変更の影響を十分に理解しておく必要があります。変更の潜在的なリスクがわからない場合は、シスコサービスにお問い合わせください。
- SR-PCE プロバイダを変更する前に「Cisco SR-PCE プロバイダの追加 （20 ページ）」を参照してください。SR-PCE プロバイダを編集する場合は、追加の手順を実行する必要があります。

。

プロバイダを編集する前に、変更するプロバイダの CSV バックアップをエクスポートすることをお勧めします（「プロバイダのエクスポート （42 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 [プロバイダ（Providers）] ウィンドウで、更新するプロバイダを選択して をクリックします。

ステップ 3 必要な変更を加えて、[保存（Save）] をクリックします。

ステップ 4 エラーを解決し、プロバイダーの到達可能性を確認します。

プロバイダの削除

プロバイダを削除するには、次の手順を実行します。

1 つ以上のデバイスまたはクレデンシャルプロファイルに関連付けられているプロバイダを削除しようとすると、アラートが表示されます。

ステップ 1 削除するプロバイダが含まれているバックアップCSVファイルをエクスポートします（「プロバイダのエクスポート （42 ページ）」を参照）。

ステップ 2 （オプション）デバイスがプロバイダにマッピングされているかどうかを確認し、削除する前にプロバイダを変更します。

a) メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

b) [ネットワークデバイス（Network Devices）] ウィンドウで、[検索（Search）] フィールドに廃止されたプロバイダ名を入力します。

c) 廃止されたプロバイダにマッピングされているデバイスのチェックボックスをオンにし、をクリックします。

d) [プロバイダ（Provider）] ドロップダウンリストから別のプロバイダを選択します。

e) [保存（Save）] をクリックします。

ステップ 3 次のようにプロバイダーを削除します。

a) メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

b) [プロバイダ（Providers）] ウィンドウで、削除するプロバイダを選択して をクリックします。

c) 確認のダイアログボックスで [削除（Delete）] をクリックします。

プロバイダのエクスポート

プロバイダデータを CSV ファイルにすばやくエクスポートできます。これは、プロバイダー情報のバックアップコピーを保持するための便利な方法です。

（注） CSV ファイルを編集してから再インポートして、既存のプロバイダを更新することはできません。

ステップ 1 メインメニューから、**[管理（Administration）] > [プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 （オプション）[プロバイダ（Providers）] ウィンドウで、必要に応じてプロバイダリストをフィルタ処理します。

ステップ 3 エクスポートするプロバイダーのチェックボックスをオンにします。エクスポートするすべてのプロバイダーを選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 4 をクリックします。ブラウザによっては、CSV ファイルを保存するときに使用するパスとファイル名を選択するか、またはすぐに開くよう求められます。

タグの管理

[タグ管理（Tag Management）] ウィンドウを使用して、ネットワーク内のデバイスへの割り当てに使用できるタグを管理します。タグは、デバイスの物理的な場所や管理者の電子メール ID などの情報を提供し、デバイスをグループ化するために使用されます。

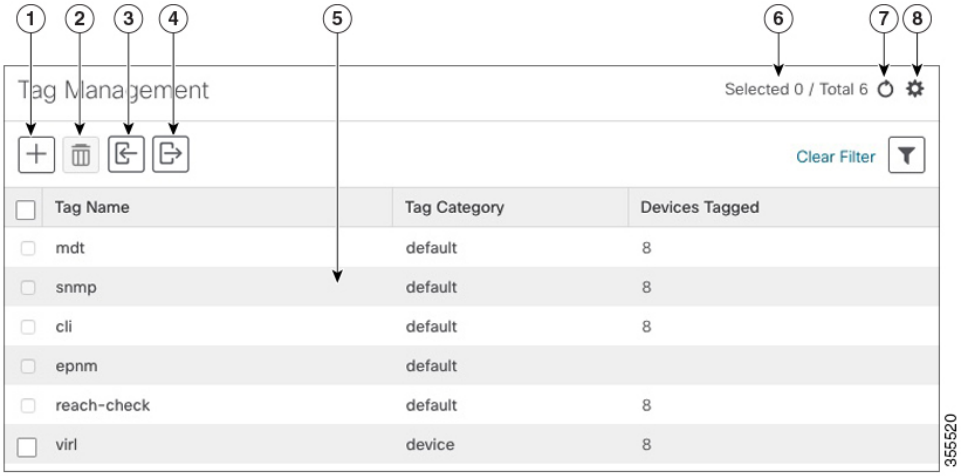
このウィンドウを開くには、**[管理（Administration）] > [タグ（Tags）]** を選択します。

（注） Cisco Crosswork アプリケーションは、タグのデフォルトセットを自動的に作成し、管理するすべてのデバイスに割り当てます。

- cli
- mdt
- reach-check
- snmp
- clock-drift-check

これらのデフォルトタグの選択、編集、削除、または手動によるデバイスとの関連付けは行えません。

図 *6 : [タグ管理（Tag Management）]* ウィンドウ



項目	説明
1	新しいデバイスタグを作成するには、＋をクリックします。タグの作成（44 ページ）を参照してください。
2	現在選択されているデバイスタグを削除するには、🗑をクリックします。「タグの削除 （47 ページ）」を参照してください。
3	CSV ファイルで定義されたデバイスタグを Cisco Crosswork アプリケーションにインポートするには、をクリックします。「タグのインポート（45 ページ）」を参照してください。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。
4	現在設定されているタグとその属性がリストされた CSV ファイルをエクスポートするには、をクリックをクリックします。このファイルを更新して Cisco Crosswork アプリケーションにインポートし直すと、複数のタグをすばやく追加または編集できます。「タグのエクスポート （47 ページ）」を参照してください。
5	Cisco Crosswork アプリケーションで現在使用可能なタグとその属性を表示します。
6	テーブルで現在選択されているタグの数を示します。
7	[タグ管理（Tag Management）] ウィンドウを更新するには、 をクリックします。

項目	説明
8	をクリックし、[タグ管理（Tag Management）] ウィンドウに表示する列を選択します。
	をクリックし、[タグ管理（Tag Management）] ウィンドウの 1 つ以上の列にフィルタ条件を設定します。
	設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。

タグの作成

必要な数のタグとタグカテゴリを作成できます。タグが多数ある場合は、各タグを個別に作成するよりも、CSV ファイルにリストしてファイルをインポートするほうが簡単です。「タグのインポート （45 ページ）」を参照してください。

（注）
- タグとタグカテゴリ名は大文字と小文字を区別せず、最大 128 文字の英数字と、ドット（.）、アンダースコア（「_」）、またはハイフン（「-」）を使用できます。その他の特殊文字は使用できません。
- 作成できるタグの最大数は 100 です。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[タグ（Tags）]** を選択します。[タグ管理（Tag Management）] ウィンドウが開きます。

ステップ 2 をクリックします。[新しいタグの作成（Create New Tags）] ペインが開きます。

ステップ 3 [カテゴリ（Category）] 領域で、次の手順を実行します。

- 新しいタグを既存のカテゴリに関連付けるには、ドロップダウンリストからカテゴリを選択します。
- 新しいタグを新しいカテゴリに関連付けるには、[新しいカテゴリ（New Category）] リンクをクリックし、新しいカテゴリの名前をテキストフィールドに入力し、[保存（Save）] をクリックします。

この手順の後に作成したすべての新しいタグが、選択または作成したカテゴリに割り当てられます。

ステップ 4 [タグ（Tags）] 領域で、作成する新しいタグの名前の入力を開始します。各タグを入力した後、**Return** を押します。

重複するタグを入力しないようにするには、[タグの表示（Show Tags）] リンクをクリックします。[新しいタグの作成（Create New Tags）] ウィンドウには、現在選択されているカテゴリにすでに存在するタグのみが表示されます。

ステップ 5 新しいタグの入力が終了したら、[保存（Save）] をクリックします。

次のタスク

デバイスにタグを追加します。デバイスタグの適用または削除 （46 ページ） を参照してください。

タグのインポート

次の手順を実行して、デバイスに適用するタグがリストされている CSV ファイルを作成し、Cisco Crosswork アプリケーションにインポートします。これは、多数の新しいタグとタグカテゴリをすばやく作成する最も簡単な方法です。

CSV ファイルをインポートすると、データベースにまだ存在していないタグが追加されます。インポートされたタグと同じ名前のタグは上書きされます。このため、インポートする前に、すべての現在のタグのバックアップコピーをエクスポートすることをお勧めします（「タグのエクスポート （47 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Admin）] > [タグ（Tags）]** を選択します。

ステップ 2 をクリックして、[CSV ファイルのインポート（Import CSV File）] ダイアログボックスを開きます。

ステップ 3 インポートする CSV ファイルをまだ作成していない場合は、次の手順を実行します。

a) [「Tags template （*.csv）」サンプルファイルのダウンロード（Download sample 'Tags template (*.csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルストレージリソースに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加します（タグごとに 1 行）。行内の各フィールドを区切るには、カンマを使用します。同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。

フィールド	説明	必須またはオプション
タグ名（Tag Name）	タグの名前を入力します。例：**SanFrancisco** または **Spine/Leaf**。	必須
タグカテゴリ（Tag Category）	タグカテゴリを入力します。例：**City** または **Network Role**。	必須

（注） [タグ名（Tag Name）] フィールドと [タグカテゴリ（Tag Category）] フィールドでは大文字と小文字が区別されず、最大 128 文字の英数字と、ドット（.）、アンダースコア（「_」）、またはハイフン（「-」）を使用できます。その他の特殊文字は使用できません。

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

ステップ 4 [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

インポートしたタグとタグカテゴリが [タグ管理（Tag Management）] ウィンドウに表示されます。

次のタスク

デバイスにタグを追加します。デバイスタグの適用または削除 （46 ページ） を参照してください。

デバイスタグの適用または削除

タグとそのカテゴリは、デバイスをグループ化するための主要なツールです。一連のデバイスを同じタグでタグ付けすると、それらはグループの一部と見なされ、より簡単に管理できます。

デバイスまたはデバイスグループにタグを適用するためには、タグがすでに存在している必要があります（参照：）。

効率性を高めるため、Cisco Crosswork は、タグ付けされたグループ内のすべてのデバイスのインベントリデータ（トポロジを含む）をインベントリ収集ジョブの単一セットとして自動的に更新します。ただし、タググループのメンバーシップは他の機能では静的であることに注意してください。

1 台のデバイスに最大 15 個のタグを適用できます。

デバイスまたはデバイスのセットにタグを適用するには、次の手順を実行します。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択します。[ネットワークデバイス（Network Devices）] タブが表示され、デバイスのリストが示されます。

ステップ 2 （オプション）リストが長い場合は、  をクリックして 1 つ以上のフィルタを設定し、タグ付けするデバイスだけにリストを絞り込みます。

ステップ 3 タグ付けするデバイスの横にあるチェックボックスをオンにします。複数のデバイスを選択した場合、変更内容は選択したすべてのデバイスに適用されます。

ステップ 4 ツールバーで  をクリックします。[タグの変更（Modify Tags）] ウィンドウが開き、選択したデバイスに現在適用されているタグが表示されます。

ステップ 5 [オートコンプリートするアイテムの入力（Type to autocomplete item）] をクリックして既存のタグのリストを表示するか、または目的のタグの名前を入力を開始します。

ステップ 6 リスト内の個々のタグをクリックして、デバイスに適用されているタグのリストにそれらを追加します。適用されたタグを削除するには、そのタグの横に表示される [X] アイコンをクリックします。

タグの削除

デバイスタグを削除するには、次の手順を実行します。

（注） タグがデバイスにマッピングされている場合、タグは削除できません。

ステップ 1 削除する予定のタグを含むバックアップCSVファイルをエクスポートします（「タグのエクスポート（47 ページ）」を参照）。

ステップ 2 メインメニューから、**[管理（Administration）]** > **[タグ（Tags）]** を選択します。[タグ管理（Tag Management）] ウィンドウが表示されます。

ステップ 3 削除するタグの横にあるチェックボックスをオンにします。

ステップ 4 ツールバーで をクリックします。

ステップ 5 確認ダイアログボックスに、削除しようとしているタグを現在使用しているデバイスの数が表示されます。[削除（Delete）] をクリックして削除を確認します。

タグのエクスポート

タグとタグカテゴリを CSV ファイルにすばやくエクスポートできます。これにより、タグのバックアップコピーを保持できます。必要に応じてCSVファイルを編集して再インポートし、既存のタグを上書きすることもできます。場合によっては、デバイスとタグを再度関連付ける必要があります。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[タグ（Tags）]** を選択します。

ステップ 2 （オプション）[タグ管理（Tag Management）] ウィンドウで、必要に応じてタグリストをフィルタ処理します。

ステップ 3 エクスポートするタグのチェックボックスをオンにします。エクスポートするすべてのタグを選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 4 をクリックします。ブラウザによっては、CSVファイルを保存するときに使用するパスとファイル名を選択するか、またはすぐに開くよう求められます。

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。