Cisco Secure Firewall Management Center 向け Cisco Umbrella DNS Connector の設定

最終更新：2025 年 7 月 25 日

Cisco Secure Firewall Management Center 向け Cisco Umbrella DNS Connector の設定

このドキュメントでは、Cisco Secure Firewall Management Center で Cisco Umbrella DNS コネクタを設定する方法について説明します。

Cisco Umbrella Connector のメリット

Management Center の Cisco Umbrella DNS 接続は、DNS クエリを Cisco Umbrella にリダイレクトするのに役立ちます。これにより、Cisco Umbrella で要求を検証し、ドメイン名に基づいて要求を許可するかブロックするかを決定し、要求に DNS ベースのセキュリティポリシーを適用できます。Cisco Umbrella を使用する場合、Cisco Umbrella 接続を設定して DNS クエリを Cisco Umbrella へリダイレクトできます。

Umbrella Connector は、システムの DNS インスペクションの一部です。既存の DNS インスペクション ポリシーマップにより、DNS インスペクションの設定に基づいて要求をブロックするか、または、要求をドロップすることに決定した場合、その要求は Cisco Umbrella へ転送されません。したがって、ローカルの DNS インスペクション ポリシーと Cisco Umbrella のクラウドベースのポリシーの 2 つを保護します。

DNS ルックアップ要求を Cisco Umbrella へリダイレクトすると、Umbrella Connector は EDNS（DNS の拡張機能）レコードを追加します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。クラウドベースのポリシーでこれらの条件を使用することで、FQDN のレピュテーションだけでなくアクセスを制御することができます。また、DNSCrypt を使用して DNS 要求を暗号化し、ユーザー名と内部の IP アドレスのプライバシーを確保することもできます。

制限事項

Management Center は、プロキシ経由の Cisco Umbrella との統合をサポートしていません。

システム要件

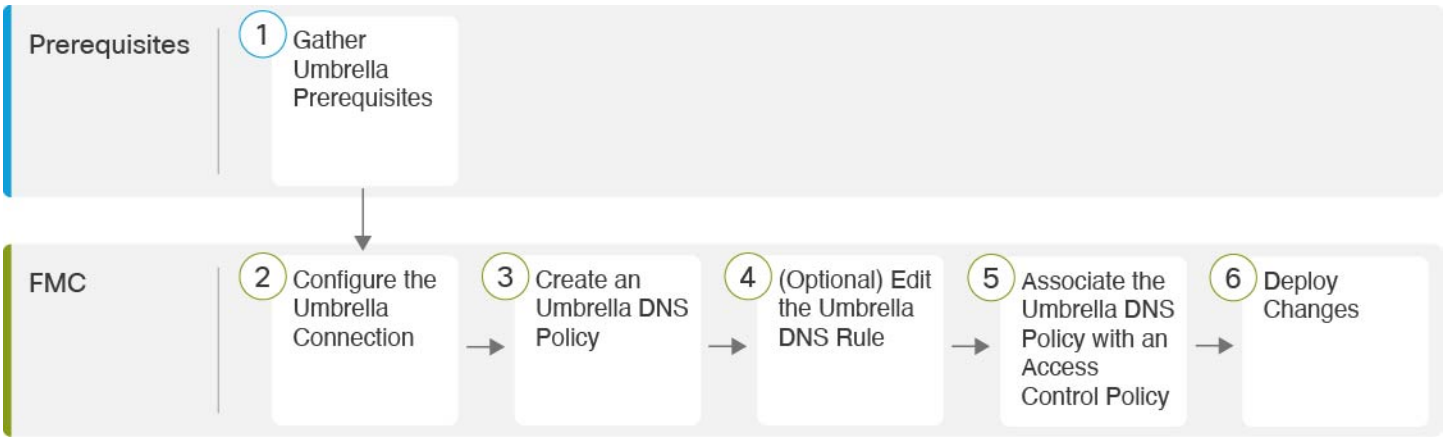
次の表に、この手順でサポートされるプラットフォームを示します。

表 *1*: サポートされる最小プラットフォーム

製品	バージョン
Firepower Threat Defense	6.6.0 以降
Firewall Management Center	7.2 以降

Management Center Umbrella DNS Connector の設定

図 *1*: エンドツーエンドの手順



1	前提条件	Cisco Umbrella の前提条件を収集する （3 ページ）
2	Management Center	Cisco Umbrella 接続を設定する （5 ページ）
3	Management Center	Cisco Umbrella DNS ポリシーを作成する （6 ページ）
4	Management Center	（オプション）Umbrella DNS ルールを設定する （7 ページ）
5	Management Center	Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付ける （9 ページ）
6	Management Center	変更の展開 （9 ページ）

Cisco Umbrella の前提条件を収集する

始める前に

- https://umbrella.cisco.com で Cisco Umbrella のアカウントを確立し、http://login.umbrella.com で Umbrella にログインします。
- Cisco Umbrella アカウントは、DNS ポリシーを使用して設定する必要があります。
- Management Center に DigiCert 中間証明書をインストールします（[デバイス（Device）] > [証明書（Certificates）]）。コピーして貼り付ける証明書は次のとおりです。


```
-----BEGIN CERTIFICATE-----
MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
SaZMkE4f97Q=
-----END CERTIFICATE-----
```


  Management Center に証明書を追加する場合は、[CAのみ（CA Only）] チェックボックスをオンにします。

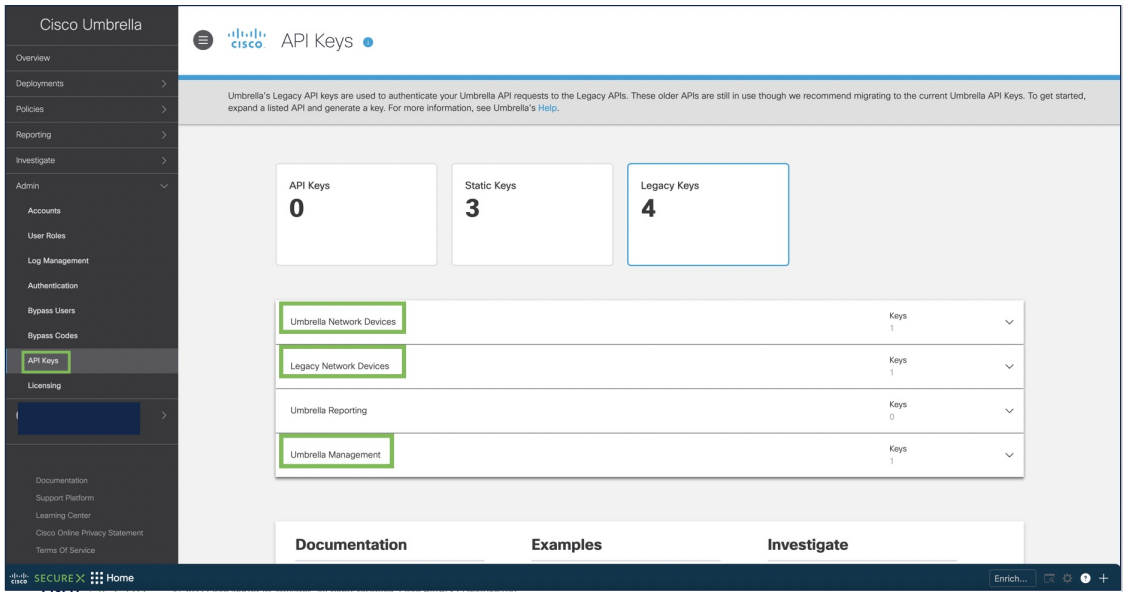
- Cisco Umbrella から次のデータを取得します。
  - 組織 ID
  - ネットワークデバイスキー
  - ネットワーク デバイス シークレット
  - レガシー ネットワーク デバイス トークン
- Management Center がインターネットに接続していることを確認します。
- Management Center で、輸出規制機能オプションのある基本ライセンスが有効になっていることを確認します。
- api.opendns.com を解決するように DNS サーバーが設定されていることを確認します。

- Management Center がポリシー構成の management.api.umbrella.com を解決できることを確認します。
- api.opendns.com への Threat Defense ルートを設定します。

手順

ステップ 1 Umbrella ダッシュボードで、**[管理（Admin）]>[APIキー（API Keys）]>[レガシーキー（Legacy Keys）]** を選択します。

図 *2*：統合のための *Umbrella* キー



ステップ 2 次の URL から [組織ID（Organization ID）] を取得します：

```
dashboard.umbrella.com/o/[Organization ID]/#/admin/apikeys
```

URL に表示されている番号をコピーして、[Management Center Umbrella接続の詳細（management center Umbrella Connection Details）] ページの [組織ID（Organization ID）] フィールドに貼り付けます。

ステップ 3 [Umbrellaネットワークデバイス（Umbrella Network Devices）] をクリックします。

a) [キー（Key）] と [シークレット（Secret）] が使用できない、または不明な場合は、[更新（Refresh）] をクリックしてキーとシークレットのペアを生成します。

b) キーをコピーして、[Management Center Umbrella接続の詳細（Management Center Umbrella Connection Details）] ページの [ネットワークデバイスキー（Network Device Key）] フィールドに貼り付けます。

c) シークレットをコピーして、[Management Center Umbrella接続の詳細（Management Center Umbrella Connection Details）] ページの [ネットワークデバイスシークレット（Network Device Secret）] に貼り付けます。

ステップ 4 [レガシー ネットワーク デバイス（Legacy Network Devices）] をクリックします

a) [キー（Key）]が使用できない、または不明な場合は、[更新（Refresh）] をクリックしてキーを生成します。

b) キーをコピーして、[Management Center Umbrella接続の詳細（Management Center Umbrella Connection Details）] ページの [レガシーネットワークデバイストークン（Legacy Network Device Token）] フィールドに貼り付けます。

Cisco Umbrella 接続を設定する

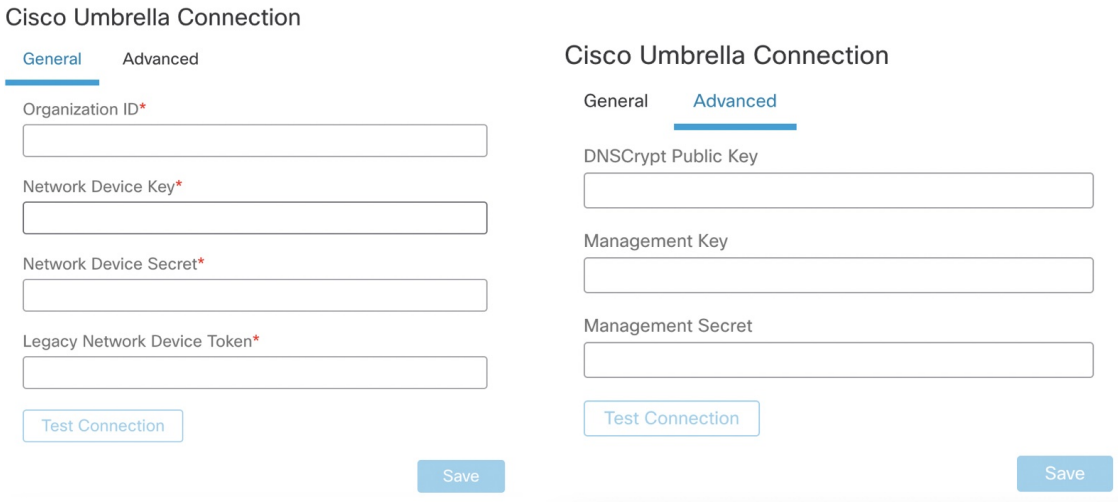
手順

ステップ 1 Management Center で、**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[クラウドサービス（Cloud Services）]** > **[Cisco Umbrella接続（Cisco Umbrella Connection）]**を選択します。

ステップ 2 次の詳細を取得し、[一般（General）] 設定に追加します。

- [組織ID（Organization ID）]：Cisco Umbrella で組織を識別する一意の番号。すべての Umbrella 組織は、Umbrella の個別のインスタンスであり、独自のダッシュボードを持ちます。組織は名前と組織 ID によって識別されます。
- [ネットワークデバイスキー（Network Device Key）]：Cisco Umbrella から Umbrella ポリシーを取得するためのキー。
- [ネットワークデバイスシークレット（Network Device Secret）]：Cisco Umbrella から Umbrella ポリシーを取得するためのシークレット。
- [レガシーネットワークデバイストークン（Legacy Network Device Token）]：Cisco Umbrella レガシー ネットワーク デバイス API トークンは、Cisco Umbrella ダッシュボードを通じて発行されます。Cisco Umbrella では、ネットワークデバイスを登録するために API トークンが必要です。

図 *3 : Cisco Umbrella* 接続パラメータ



ステップ 3 [詳細設定（Advanced）] から次のオプションを設定できます。

- [DNSCrypt公開キー（DNSCrypt Public Key）] : DNSCrypt は、エンドポイントと DNS サーバー間の DNS クエリを認証および暗号化します。DNScrypt を有効にするには、証明書の検証に DNScrypt の公開キーを設定できます。このキーは、32 バイトの 16 進数値で、B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79 に事前設定されています。これは、Umbrella エニーキャストサーバーの公開キーです。
- [管理キー（Management Key）] : VPN ポリシーのために Umbrella クラウドからデータセンターの詳細を取得するためのキー。
- [管理シークレット（Management Secret）] : VPN のために Umbrella クラウドからデータセンターを取得するために使用されるシークレット。

ステップ 4 [接続のテスト（Test Connection）] をクリックします。Cisco Umbrella Cloud が Management Center から到達可能かどうかをテストします。必要な組織 ID とネットワークデバイスの詳細を指定すると、Cisco Umbrella 接続が作成されます。

ステップ 5 情報を追加したら、[保存（Save）] をクリックして接続の詳細を保存します。

Cisco Umbrella DNS ポリシーを作成する

手順

ステップ 1 Management Center で**[ポリシー（Policies）] > [DNS]**を選択します。既存のすべての DNS ポリシーが表示されます。

ステップ 2 **[DNSポリシーの追加（Add DNS Policy）] > [Umbrella DNSポリシー（Umbrella DNS Policy）]** をクリックします。

ステップ 3 ポリシーの名前と説明を入力してから、[保存（Save）] をクリックします。

（オプション）Umbrella DNS ルールを設定する

この手順で説明されている設定を変更する必要がある場合は、Cisco Umbrella DNS ルールを編集します。

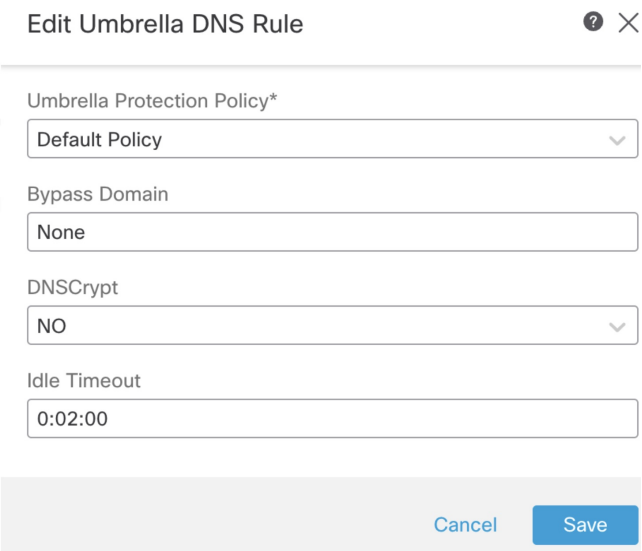
手順

ステップ 1 [ポリシー（Policies）] > [DNS] を選択します。 >

ステップ 2 構成する DNS ポリシーの [編集（Edit）]（✎） アイコンをクリックします。

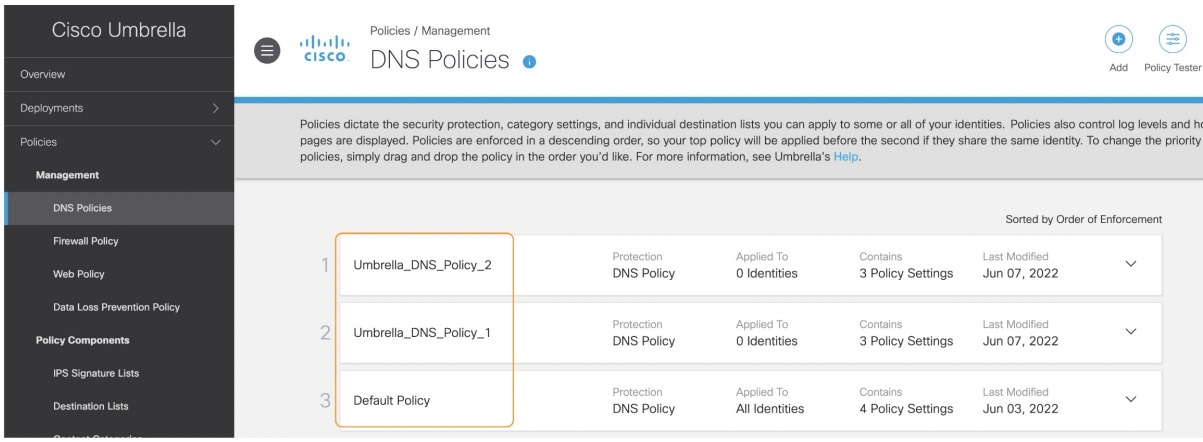
ステップ 3 正しいルールに移動し、[編集（Edit）]（✎） アイコンを再度クリックしてルールを編集します。

図 *4 : Umbrella DNS* ルールの編集



a) **Umbrella 保護ポリシー（Umbrella Protection Policy）** ：Umbrella ダッシュボードで定義されている DNS ポリシーから DNS ポリシーを選択します。

図 *5 : Umbrella の DNS* ポリシー



b) **バイパスドメイン（Bypass Domain）**：どのドメインが Cisco Umbrella をバイパスして DNS サーバーに直接アクセスするかを指定します。

複数のドメインを指定する場合は、カンマ区切りのリストで入力します。たとえば、Umbrella DNS がフィルタリングまたは評価すべきではないローカルドメインのリストを設定できます。

c) **DNSCrypt**：ドロップダウンリストから [はい（Yes）] または [いいえ（No）] を選択します。このオプションは、DNS リクエストを暗号化し、UDP ポート 443 で Umbrella クラウドに転送します。新しいルールが作成されるとき、[DNSCrypt] のデフォルト設定は [はい（YES）] です。

このオプションを有効にする場合は、[Cisco Umbrella接続（Cisco Umbrella Connection）] 設定の [詳細設定（Advanced）] セクションで、[DNSCrypt公開キー（DNSCrypt Public Key）] を指定していることを確認してください。

d) **アイドルタイムアウト（Idle Timeout）**：Umbrella から Management Center 切断されるまでの、Umbrella クラウドからの応答を待機する時間間隔を指定します。新しいルールが作成されるとき、[アイドルタイムアウト（Idle Timeout）] のデフォルト設定は 00:02:00 です

[アイドルタイムアウト（Idle Timeout）] の形式は（hh:mm:ss）です。

Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付ける

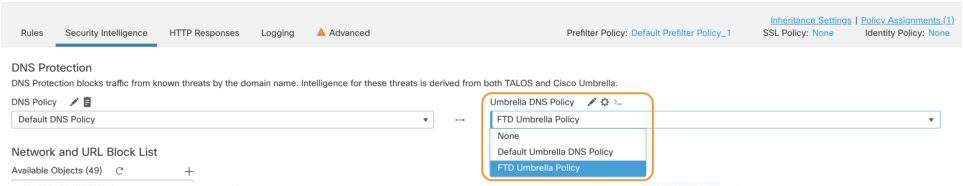
手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**に移動し、編集するアクセスポリシーを選択します。

ステップ 2 [セキュリティインテリジェンス（Security Intelligence）] を選択します。

ステップ 3 [Umbrella DNSポリシー（Umbrella DNS Policy）] で、Cisco Umbrella DNS ポリシーに使用するポリシーを選択します。

図 *6 : Umbrella DNS* ポリシーの割り当て



ステップ 4 [保存（Save）] を選択し、変更をすべて保存します。

変更の展開

手順

ステップ 1 Management Center メニューバーで、[展開（Deploy）] をクリックし、[展開（Deployment）] を選択します。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

- [検索（Search）] : [検索（Search）] ボックスのデバイス名、タイプ、ドメイン、グループ、またはステータスを検索します。
- [展開（Expand）] : 展開するデバイス固有の設定変更を表示するには、**展開矢印**（ › ）をクリックします。

  デバイスのチェックボックスを選択すると、デバイスの下に表示されているデバイスのすべての変更がプッシュされ、展開されます。ただし、[ポリシーの選択（Policy selection）]（ ）を使用すると、展開する個々のポリシーまたは設定を選択できるとともに、残りの変更は展開することなく保留できます。

必要に応じて、表示アイコン（[ポリシーの表示または非表示（Show or Hide Policy）]（））を使用して、関連付けられている未変更のポリシーを選択的に表示したり、非表示にしたりできます。

ステップ 3 （任意）[概算見積（Estimate）] をクリックして展開期間の大まかな見積を取得します。

ステップ 4 [展開（Deploy）] をクリックします。

ステップ 5 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証メッセージ（Validation Messages）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、警告またはエラーの前にある矢印アイコンをクリックします。

次の選択肢があります。

- [展開（Deploy）] : 警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）] : 展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

展開の検証

手順

ステップ 1 展開が完了したら、Management Center で展開を検証します。

ステップ 2 **[展開（Deploy）]**を選択し、[展開履歴（Deployment History）] アイコンを選択します。

ステップ 3 Umbrella Connector に関連付けられているジョブを選択します。

ステップ 4 [トランスクリプトの詳細（Transcript Details）]（） アイコンをクリックします。

次のコマンド ライン インターフェイスのトランスクリプトが生成されます。

例：

```
FMC >> strong-encryption-disable
FMC >> umbrella-global
FMC >> token umbrella_token
10.0.0.0 >> [info] : Please make sure all the Umbrella Connector prerequisites are
satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
FMC >> local-domain-bypass “test.com"
FMC >> timeout edns hh:mm:ss
FMC >> exit
FMC >> policy-map type inspect dns preset_dns_map
FMC >> parameters
```

```
FMC >> umbrella tag "Default Policy"
FMC >> dnscrypt
```

導入に関する問題のトラブルシューティング

- レガシー ネットワーク デバイス トークンは構成されていません （11 ページ）
- 輸出管理機能は有効化されていません （11 ページ）

レガシー ネットワーク デバイス トークンは構成されていません

エラー：レガシー ネットワーク デバイス トークンが空のため、Cisco Umbrella グローバルを設定できません。

- **考えられる原因** Cisco Umbrella 接続の詳細は、[統合（Integration）] タブに追加されませんでした。[統合（Integration）] タブ内の詳細を構成するには Cisco Umbrella 接続を設定する（5 ページ） を使用します。
- **考えられる原因** Management Center はインターネットに接続していません。インターネット接続がないと、Management Center は Umbrella クラウドに接続できません。
- **考えられる原因** Umbrella 接続の詳細が追加されましたが、情報が正しくありません。Cisco Umbrella 接続を設定する （5 ページ） を使用して適切な情報を入力し、接続をテストして、Umbrella が接続されていることを確認します。

輸出管理機能は有効化されていません

オプションのライセンスを有効化（登録）または無効化（リリース）できます。ライセンスによって制御される機能を使用するには、ライセンスを有効にする必要があります。

オプションのターム ライセンスの対象となる機能を使用しなくなった場合、ライセンスを無効化できます。ライセンスを無効にすると、Cisco Smart Software Manager アカウントでライセンスがリリースされるため、別のデバイスにそのライセンスを適用できるようになります。

評価モードで動作させる場合は、これらのライセンスの評価バージョンを有効にすることもできます。評価モードでは、デバイスを登録するまでライセンスは Cisco Smart Software Manager に登録されません。ただし、評価モードでは RA VPN ライセンスまたはキャリアライセンスを有効化できません。

始める前に

ライセンスを無効にする前に、そのライセンスが使用中でないことを確認します。ライセンスを必要とするポリシーは書き換えるか削除します。

高可用性の設定で動作する装置の場合は、アクティブな装置でのみライセンスを有効化または無効化します。スタンバイ装置が必要なライセンスを要求（または解放）すると、次の設定の展開時にスタンバイ装置に変更内容が反映されます。ライセンスを有効にする際は、Cisco Smart

Software Manager アカウントで十分な数のライセンスが使用可能であることを確認する必要があります。これを確認しないと、一方の装置が準拠、もう一方の装置が非準拠になる可能性があります。

手順

ステップ 1 メニューでデバイスの名前をクリックし、スマートライセンスサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 必要に応じて、それぞれのオプション ライセンスの [有効化/無効化（Enable/Disable）] コントロールをクリックします。

- [有効化（Enable）]：Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化（Disable）]：Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。

ステップ 3 RA VPN ライセンスを有効にしている場合、アカウントで使用可能なライセンス タイプを選択します。

次の任意のライセンス（[Plus]、[Apex]、[VPNのみ（VPN Only）]）を使用できます。両方のライセンスがあり、どちらも使用する場合は [PlusおよびApex（Plus and Apex）] を選択できます。

© 2025 Cisco Systems, Inc. All rights reserved.

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。