



Cisco Umbrella

Cisco Umbrella で定義されている FQDN ポリシーをユーザー接続に適用できるようにするために、DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。次のトピックでは、デバイスを Cisco Umbrella と統合するように Umbrella Connector を設定する方法について説明します。

- [Cisco Umbrella Connector について](#) (1 ページ)
- [Cisco Umbrella Connector のライセンス要件](#) (3 ページ)
- [Cisco Umbrella のガイドラインと制限事項](#) (3 ページ)
- [Cisco Umbrella Connector の設定](#) (5 ページ)
- [Umbrella Connector のモニタリング](#) (11 ページ)
- [Cisco Umbrella Connector の履歴](#) (15 ページ)

Cisco Umbrella Connector について

Cisco Umbrella を使用する場合、Cisco Umbrella Connector を設定して DNS クエリを Cisco Umbrella へリダイレクトできます。これにより、Cisco Umbrella で未許可もしくは疑義のあるドメイン名に対する要求を特定し、DNS ベースのセキュリティポリシーを適用できます。

Umbrella Connector は、システムの DNS インспекションの一部です。既存の DNS インспекション ポリシーマップにより、DNS インспек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спек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、DNSECrypt 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。

Cisco Umbrella エンタープライズセキュリティ ポリシー

クラウドベースの Cisco Umbrella エンタープライズセキュリティ ポリシーでは、DNS ルックアップ要求の完全修飾ドメイン名 (FQDN) のレピュテーションに基づいてアクセスを制御することができます。エンタープライズセキュリティ ポリシーによって、次のいずれかのアクションを強制できます。

- 許可：FQDN に対するブロックルールがなく、悪意のないサイトに属していると Cisco Umbrella が判断した場合は、サイトの実際の IP アドレスが返されます。これは、DNS ルックアップの通常の動作です。
- プロキシ：FQDN に対するブロックルールはないが、疑わしいサイトに属していると Cisco Umbrella が判断した場合は、Umbrella インテリジェントプロキシの IP アドレスが DNS 応答で返されます。次に、プロキシで HTTP 接続を検査し、URL フィルタリングを適用します。インテリジェントプロキシが Cisco Umbrella ダッシュボード ([**Security Setting**] > [**Enable Intelligent Proxy**]) で有効になっていることを確認する必要があります。
- ブロック：FQDN が明示的にブロックされている場合、または悪意のあるサイトに属していると Cisco Umbrella が判断した場合は、ブロックされた接続の Umbrella クラウドランディング ページの IP アドレスが DNS 応答で返されます。

Cisco Umbrella の登録

Umbrella Connector をデバイスに設定するとき、クラウドで Cisco Umbrella に登録します。登録プロセスでは、次のいずれかを特定する単一のデバイス ID が割り当てられます。

- シングル コンテキスト モードのスタンドアロンデバイス。
- シングル コンテキスト モードのハイ アベイラビリティ ペア。
- シングル コンテキスト モードのクラスタ。
- マルチコンテキスト スタンドアロン デバイスのセキュリティ コンテキスト。
- ハイ アベイラビリティ ペアのセキュリティ コンテキスト。
- クラスタのセキュリティ コンテキスト。

登録が完了すると、Cisco Umbrella ダッシュボードにデバイスの詳細が表示されます。次に、デバイスに関連付けられているポリシーを変更できます。登録中は、設定で指定するポリシーが使用されるか、デフォルトのポリシーが割り当てられます。複数のデバイスに同じ Umbrella ポリシーを割り当てることができます。ポリシーを指定する場合、受信するデバイス ID はポリシーを指定しなかった場合に取得する ID とは異なります。

レガシー API トークンから API/秘密鍵への切り替え

Cisco Umbrella は、ASA 9.23(1) 以降、API 登録メカニズムを API トークンから API キーと秘密キーに変更しました。レガシートークンを使用している場合は、次の手順を実行してレガシー

API から API/秘密キー API に切り替えることができます。詳細な手順については、関連する手順を参照してください。

手順

- ステップ 1 新しい API の証明書をインポートします。ISRG ルート X1 自己署名証明書をインストールする必要があります。
- ステップ 2 Cisco Umbrella を無効にします。
- ステップ 3 既存のトークン登録を削除します。
- ステップ 4 新しい API と秘密鍵を設定します。
- ステップ 5 Cisco Umbrella を再度有効にします。

Cisco Umbrella Connector のライセンス要件

Cisco Umbrella Connector を使用するには、3DES ライセンスが必要です。スマートライセンスを使用している場合は、アカウントで輸出規制による機能限定をイネーブルにする必要があります。

Cisco Umbrella ポータルには、別のライセンス要件があります。

Cisco Umbrella のガイドラインと制限事項

コンテキスト モード

- マルチコンテキスト モードでは、コンテキストごとに Umbrella Connector を設定します。各コンテキストが異なるデバイス ID を持ち、Cisco Umbrella Connector ダッシュボードに別のデバイスとして表示されます。デバイス名は、コンテキストで設定されたホスト名にハードウェア モデルおよびコンテキスト名を追加した形式で作成されます。たとえば、CiscoASA-ASA5515-Context1 となります。

フェールオーバー

- ハイアベイラビリティ ペアのアクティブユニットでは、ペアを単一ユニットとして Cisco Umbrella に登録します。両方のピアで、それぞれのシリアル番号から形成された同じデバイス ID が使用されます (*primary-serial-number_secondary-serial-number*)。マルチ コンテキスト モードでは、セキュリティ コンテキストの各ペアが単一ユニットと見なされます。ハイアベイラビリティを設定する必要があります。ユニットでは、スタンバイ デバイスが現在障害発生状態であったとしても、Cisco Umbrella をイネーブルにする前にハイアベイラビリティ グループを正常に作成する必要があります。これを作成しないと、登録に失敗します。

クラスタ

- クラスタ制御ユニットでは、クラスタを単一ユニットとして Cisco Umbrella に登録します。すべてのピアで同じデバイス ID を使用します。マルチ コンテキスト モードでは、クラスタ内のセキュリティ コンテキストがすべてのピアで単一ユニットと見なされます。

その他のガイドライン

- Cisco Umbrella へのリダイレクションは、通過トラフィックの DNS 要求に対してのみ実行されます。システム自体で開始する DNS 要求が Cisco Umbrella にリダイレクトされることはありません。たとえば、FQDN ベースのアクセス制御ルールが Umbrella のポリシーをベースに解決されたり、他のコマンドまたは構成設定で使用される任意の FQDN となったことはありません。
- Cisco Umbrella Connector は、通過トラフィックの任意の DNS 要求で動作します。ただし、ブロックおよびプロキシアクションは DNS レスポンスが HTTP/HTTPS 接続で使用される場合にのみ有効です（返される IP アドレスが Web サイト用であるため）。非 HTTP/HTTPS 接続のブロックまたはプロキシされたアドレスは、失敗するか誤った方法で完了します。たとえば、ブロックされた FQDN の ping を実行すると、Cisco Umbrella クラウドのブロックページをホストするサーバーに対して ping を実行します。



(注) Cisco Umbrella を試行して、非 HTTP/HTTPS になる可能性がある FQDN をインテリジェントに特定します。プロキシされたドメイン名の FQDN では、インテリジェントプロキシに IP アドレスを返しませんが、

- システムでは、Cisco Umbrella へのみ DNS/UDP トラフィックを送信します。DNS/TCP インスペクションをイネーブルにすると、システムは、Cisco Umbrella に DNS/TCP 要求を送信しません。ただし、DNS/TCP 要求によって Umbrella バイパス カウンタが増えることはありません。
- Umbrella インスペクションで DNSCrypt をイネーブルにすると、システムは暗号化されたセッションに UDP/443 を使用します。DNSCrypt が正しく機能するためには、Cisco Umbrella の DNS インスペクションを適用するクラス マップに UDP/53 とともに UDP/443 を含める必要があります。UDP/443 と UDP/53 はいずれも DNS のデフォルトのインスペクション クラスに含まれていますが、カスタムクラスを作成する場合は、一致するクラスに両方のポートが含まれる ACL を定義する必要があります。
- DNSCrypt は、証明書の更新ハンドシェイクに対してのみ、IPv4 を使用します。ただし、DNSCrypt では、IPv4 と IPv6 の両方のトラフィックを暗号化します。
- api.umbrella.com と api.opendns.com（登録では IPv4 のみを使用）にアクセスできるインターネットへの IPv4 ルートが必要です。また、次の DNS リゾルバへのルートも必要となるほか、アクセスルールでこれらのホストに DNS トラフィックを許可する必要があります。これらのルートは、データインターフェイスまたは管理インターフェイスのいずれかを通過できます。有効なルートが登録と DNS 解決の両方で機能します。システムで使用する

デフォルトのサーバーを示しています。Umbrella のグローバル設定でリゾルバを設定すると他のサーバーを使用できます。

- 208.67.220.220 (IPv4 のシステム デフォルト)
 - 208.67.222.222
 - 2620:119:53::53 (IPv6 のシステム デフォルト)
 - 2620:119:35::35
- システムは Umbrella FamilyShield サービスをサポートしていません。FamilyShield リゾルバを設定すると、予期しない結果が発生する可能性があります。
 - フェールオープンにするかどうかを評価する場合、システムは、Umbrella リゾルバがダウンしているかどうか、または仲介デバイスが要求の送信後の応答待機時間に基づいて DNS 要求または応答をドロップするかどうかを考慮します。Umbrella リゾルバへのルートなしなど、他の要因は考慮されません。
 - デバイスの登録を解除するには、Umbrella の設定を削除した後で Cisco Umbrella ダッシュボードからデバイスを削除します。
 - FQDN ではなく IP アドレスを使用するすべての Web 要求では、Cisco Umbrella がバイパスされます。また、ローミングクライアントは、Umbrella がイネーブルになっているデバイスを通過せずに別の WAN 接続から DNS 解決を取得した場合、この DNS 解決を使用する接続で Cisco Umbrella をバイパスします。
 - ユーザーに HTTP プロキシがある場合は、プロキシで DNS 解決を実行し Cisco Umbrella を通過しない可能性があります。
 - NAT DNS46 および DNS64 はサポートされていません。IPv4 アドレスと IPv6 アドレスの間で DNS 要求を変換することはできません。
 - EDNS レコードには、IPv4 と IPv6 の両方のホストアドレスが含まれます。
 - クライアントが HTTPS 経由で DNS を使用している場合、クラウドセキュリティサービスでは DNS および HTTP/HTTPS トラフィックが検査されません。

Cisco Umbrella Connector の設定

クラウドで Cisco Umbrella と対話するようにデバイスを設定できます。システムは DNS ルックアップ要求を Cisco Umbrella にリダイレクトします。次に、クラウドベースのエンタープライズセキュリティの完全修飾ドメイン名 (FQDN) ポリシーを適用します。悪意のあるトラフィックまたは疑わしいトラフィックにおいては、ユーザーがサイトからブロックされるか、クラウドベースのポリシーに基づいて URL フィルタリングを実行するインテリジェントプロキシにリダイレクトされます。

次の手順では、Cisco Umbrella コネクタの設定におけるエンドツーエンドのプロセスについて説明します。

始める前に

マルチコンテキストモードでは、Cisco Umbrella を使用する必要のある各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1 Cisco Umbrella のアカウント (<https://umbrella.cisco.com>) を確立します

ステップ 2 [Cisco Umbrella 登録サーバーからの CA 証明書のインストール \(6 ページ\)](#)。

デバイスの登録では HTTPS を使用します。これによりルート証明書をインストールするように要求されます。

ステップ 3 イネーブルになっていない場合は、DNS サーバーを設定してインターフェイス上で DNS ルックアップをイネーブルにします。

[**Configuration**] > [**Device Management**] > [**DNS**] > [**DNS Client**] ページで構成を設定します。

自分のサーバーを使用することも、Cisco Umbrella サーバーを設定することもできます。別のサーバーを設定する場合でも、DNS インスペクションによって Cisco Umbrella リゾルバへ自動的にリダイレクトされます。

- 208.67.220.220
- 208.67.222.222
- 2620:119:53::53
- 2620:119:35::35

ステップ 4 [Umbrella Connector のグローバル設定 \(7 ページ\)](#)。

ステップ 5 [DNS インスペクション ポリシー マップでの Umbrella のイネーブル化 \(9 ページ\)](#)。

ステップ 6 [Umbrella の登録確認 \(10 ページ\)](#)。

Cisco Umbrella 登録サーバーからの CA 証明書のインストール

Cisco Umbrella 登録サーバーとの間で HTTPS 接続を確立するために、ルート証明書をインポートする必要があります。システムは、デバイスを登録するときに、HTTPS 接続を使用します。Cisco Umbrella で、[**展開 (Deployments)**] > [**構成 (Configuration)**] > [**ルート証明書 (Root Certificate)**] を選択し、証明書をダウンロードします。

API と秘密鍵を使用して Cisco Umbrella に登録する場合は、ISRG ルート X1 の自己署名証明書 pem ファイルをインストールする必要があります。 <https://letsencrypt.org/certs/isrgrootx1.pem> からこの証明書を取得できます。

始める前に

Umbrella が証明書を更新する場合は、新しい証明書をダウンロードする必要があります。ルート証明書も変更される場合があります。正しいルート証明書がアップロードされていることを確認します。

証明書を更新する場合は、Umbrella を無効化してから再度有効にする必要があります。これにより、システムは新しい証明書を取得し、Umbrella に正しく登録されます。

手順

ステップ 1 [Configuration] > [Firewall] > [Advanced] > [Certificate Management] > [CA Certificates] を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 トラストポイント名 (ctx1 または umbrella_server など) を入力します。

ステップ 4 [Paste Certificate in PEM Format] を選択し、証明書をボックスに貼り付けます。

BEGIN CERTIFICATE 行および END CERTIFICATE 行は、含めても含めなくても構いません。

ステップ 5 [Install Certificate] をクリックします。

証明書はデバイスで作成されます。ビューを更新してリストされたトラストポイントを表示する必要があります。

Umbrella Connector のグローバル設定

Cisco Umbrella グローバル設定は、主に、Cisco Umbrella にデバイスを登録するために必要な API キーと秘密鍵またはレガシー API トークンを定義します。

グローバル設定が Umbrella を有効にするために十分ではありません。[DNS インспекションポリシー マップでの Umbrella のイネーブル化 \(9 ページ\)](#) の説明に従って、DNS インспекションポリシー マップでも Umbrella をイネーブルにする必要があります。

始める前に

- Cisco Umbrella ダッシュボードにログインして、API キーと秘密鍵を生成します。Cisco Umbrella で [管理 (Admin)] > [API キー (API Keys)] からキーを生成します。キーを生成するときは、後で秘密を取得できないため、API と秘密鍵をコピーして保存する必要があります。キーの範囲は読み取り/書き込みである必要があります。
- (レガシー、非推奨。) Cisco Umbrella ネットワーク デバイス ダッシュボード (<https://login.umbrella.com/>) にログインし、組織の従来のネットワークデバイスの API トークンを取得します。トークンは、16 進数の文字列、たとえば、AABBA59A0BDE1485C912AFE になります。従来のネットワークデバイスの API キーを Umbrella ダッシュボードから生成します。

- Cisco Umbrella 登録サーバーの証明書をインストールします。

手順

ステップ 1 Cisco Umbrella への登録に必要な API キーおよび秘密を設定します。

token-request-credential api-key key_value secret secret_value

キーの有効期限が切れ、新しいキーを適用するときに Cisco Umbrella を無効にして新しいキー/秘密を追加し、Cisco Umbrella を再度有効にする必要があることに注意してください。

例 :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token-request-credential
api-key f817feb474d94c56b3448bcd08edc11 secret 4afe58df5c454161a10a172145cb1456
```

ステップ 2 **[Configuration] > [Firewall] > [Objects] > [Umbrella]** を選択します。

ステップ 3 **[Enable Umbrella]** を選択します。

ステップ 4 Cisco Umbrella に登録するときに使用する方法を選択します。

- **[Token] (レガシー、非推奨)** : [トークン (Token)] フィールドに API トークンを入力します。
- **[Token-Request-Credential]** : 以下を設定します。
 - **[API-Key]** : Cisco Umbrella から生成した API キーを入力します。
 - **[Secret-Key]** : API キーに指定された秘密鍵を入力します。

ステップ 5 (任意) DNS インспекション ポリシー マップで DNSCrypt をイネーブルにする場合は、必要に応じて証明書の検証に DNSCrypt プロバイダーの公開キーを設定できます。キーを設定しない場合は、現在配布されているデフォルトの公開キーが検証に使用されます。

キーは 32 バイトの 16 進数値です。2 バイトごとにコロンで区切った ASCII の 16 進数値を入力します。キー長は 79 バイトです。このキーは Cisco Umbrella から取得します。

デフォルト キーは

```
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
```

です。

デフォルトの公開キーの使用に戻すには、キーを **[Public Key]** フィールドから削除します。

ステップ 6 (任意) **[EDNS Timeout]** を選択してアイドルタイムアウトを変更します。その時間が経過するまでサーバーからの応答がない場合、クライアントから Umbrella サーバーへの接続は削除されます。

タイムアウトは hours:minutes:seconds の形式で、0:0:0 ~ 1193:0:0 の範囲で指定できます。デフォルトは 0:02:00 (2 分) です。

ステップ7 (任意) リゾルバ IPv4 およびリゾルバ IPv6 で、使用する DNS 要求を解決するデフォルト以外の Cisco Umbrella DNS サーバーのアドレスを設定します。

これらのオプションを設定しない場合、システムはデフォルトのサーバーを使用します。

ステップ8 (任意) Umbrella のバイパスに必要なローカルドメイン名を設定します。

Cisco Umbrella をバイパスする必要がある DNS 要求でローカルドメインを特定し、代わりに設定済みの DNS サーバーに直接移動することができます。たとえば、すべての内部接続が許可されることを想定して、内部 DNS サーバーで組織のドメイン名のすべての名前を解決できます。

ローカルドメインを定義する正規表現オブジェクトを含む、1つの正規表現クラスを指定することも、正規表現オブジェクトとして直接名前を入力することもできます。これらのクラスを組み合わせることもできますが、指定できるのは1つまでです。

ローカルドメインバイパス正規表現クラスオプションの横にある [Manage] ボタンをクリックしてクラスを作成します。また、正規表現の場合は [Add/Edit] ダイアログボックスで [Manage] ボタンをクリックして、これらのオブジェクトを作成することもできます。

DNS インスペクションポリシーマップでの Umbrella のイネーブル化

グローバル Umbrella 設定の構成は、デバイスの登録および DNS ルックアップリダイレクトの有効化において十分ではありません。アクティブな DNS インスペクションの一部として Umbrella を追加する必要があります。

Umbrella を `preset_dns_map` DNS インスペクションポリシーマップに追加して、グローバルにイネーブルにすることができます。

ただし、カスタマイズされた DNS インスペクションを使用して、異なるインスペクションポリシーマップを異なるトラフィッククラスに適用する場合は、Umbrella をサービスを必要とするクラスごとにイネーブルにする必要があります。

次の手順では、Umbrella をグローバルに実装する方法について説明します。カスタマイズされた DNS ポリシーマップがある場合は、[DNS インスペクションポリシーマップの設定](#) を参照してください。

手順

ステップ1 [Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [DNS] を選択します。

ステップ2 `preset_dns_map` インスペクションマップをダブルクリックして編集します。

ステップ3 [Umbrella Connections] タブをクリックして、クラウドでの Cisco Umbrella への接続を有効にします。

- [Umbrella] : Cisco Umbrella を有効にします。必要に応じて、デバイスに適用する Cisco Umbrella ポリシーの名前を [Umbrella Tag] フィールドに指定します。ポリシーを指定しな

い場合は、デフォルトの ACL が適用されます。登録が完了すると、Umbrella のデバイス ID がタグの横に表示されます。

- **[Enable Dnsrypt]** : DNSCrypt を有効にしてデバイスと Cisco Umbrella 間の接続を暗号化します。DNSCrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。DNSCrypt では UDP/443 を使用するため、そのポートが DNS インспекションに使用するクラス マップに含まれていることを確認する必要があります。デフォルトのインспекションクラスには DNS インспекションに UDP/443 がすでに含まれています。
- **フェールオープン** : Umbrella DNS サーバーが使用できない場合に DNS 解決を動作させるには、フェールオープンをイネーブルにします。フェールオープン状態で Cisco Umbrella DNS サーバーが使用できない場合は、このポリシー マップで Umbrella 自体がディセーブルになり、DNS 要求をシステム上に設定された他の DNS サーバー（存在する場合）に移動できるようになります。Umbrella DNS サーバーが再度使用可能になると、ポリシーマップはそれらの使用を再開します。このオプションを選択しない場合、DNS 要求はアクセスできない Umbrella リゾルバへ移動し続けるので、応答は取得されません。

ステップ 4 [OK] をクリックします。

Umbrella の登録確認

Umbrella のグローバル設定を実行し、DNS インспекションで Umbrella をイネーブルにしたら、デバイスから Cisco Umbrella に接続して登録を行う必要があります。Cisco Umbrella にデバイス ID が指定されているかどうかを確認することで、登録が正常に完了したかどうかをチェックできます。

コマンドを入力するには、**[Tools] > [Command Line Interface]** または SSH セッションを使用します。

最初にサービスポリシーの統計情報を確認し、Umbrella の登録回線を検出します。ここでは、Cisco Umbrella によって適用されたポリシー（タグ）、接続の HTTP ステータス、およびデバイス ID が示されます。

ステータスは 200（成功）である必要があります。エラーコード：401 は API トークンが正しくなかったこと、403 はキーの範囲が読み取り/書き込みではなかった（アクセスをブロックしていた）こと、405 は API キーの有効期限が切れていること、409 はデバイスが Cisco Umbrella にすでに存在することを示します。

ステータスが UNKNOWN の場合は、syslog メッセージを確認します。メッセージ 339011 : 「Cisco Umbrella API トークン要求で応答を受信しませんでした（Umbrella API token request received no response）」は、api.umbrella.com に到達するためのルーティングの問題があるか、必要な証明書をアップロードしなかったことを示します。

Umbrella のリゾルバ回線では、リゾルバが無応答であることを示すことはできません。無応答の場合は、アクセス制御ポリシーでこれらの IP アドレスに対する DNS 通信が開いていること

を確認します。これは一時的な状況の可能性もありますが、ルーティングの問題を示している場合もあります。

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      message-length maximum client auto, drop 0
      message-length maximum 512, drop 0
      dns-guard, count 0
      protocol-enforcement, drop 0
      nat-rewrite, count 0
    umbrella_registration: mode: fail-open tag: default, status: 200 success,
device-id: 010a13b8fbd9c9aa
      Umbrella ipv4 resolver: 208.67.220.220
      Umbrella ipv6 resolver: 2620:119:53::53
      Umbrella: bypass 0, req inject 0 - sent 0, res rcv 0 - inject 0
local-domain-bypass 10
      DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
      DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
      DNScrypt: Certificate Update: completion 10, failure 1
```

また、実行コンフィギュレーション（ポリシーマップでのフィルタ処理）も確認できます。ポリシーマップの `umbrella` コマンドを更新して、デバイス ID を表示します。このコマンドをイネーブルにしても、デバイス ID を直接設定することはできません。次の例で、出力を編集して関連する情報を表示します。Umbrella に使用される DNS インスペクション マップを編集して ASDM のデバイス ID を表示することもできます。ID は、[Umbrella Connections] タブに表示されます。

```
ciscoasa(config)# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnsencrypt
  umbrella device-id 010a3e5760fdd6d3
no tcp-inspection
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
```

Umbrella Connector のモニタリング

ここでは、Umbrella Connector をモニターする方法について説明します。

Umbrella サービス ポリシーの統計情報のモニタリング

Umbrella をイネーブルにすると、DNS インスペクションの統計情報の概要と詳細を両方表示できます。

コマンドを入力するには、[Tools]>[Command Line Interface] または SSH セッションを使用します。

show service-policy inspect dns [detail]

detail キーワードを使用しないと、すべての基本的な DNS インспекションカウンタと Umbrella の設定情報が表示されます。ステータス フィールドに、システムで Cisco Umbrella への登録を試行するための HTTP ステータス コードを指定します。

リゾルバ回線は、使用中の Umbrella サーバーを示します。これらの回線によって、サーバーが応答なしかどうか、または現在サーバーが使用可能かどうかを判断するためにシステムでサーバーをプローブ中かどうかわかります。フェール オープン モードの場合、システムで DNS 要求が許可され他の DNS サーバー（設定されている場合）に移動します。それ以外のモードの場合、Umbrella サーバーが無応答の間は DNS 要求で応答を取得できません。

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
  Class-map: inspection_default
  Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
  message-length maximum client auto, drop 0
  message-length maximum 512, drop 0
  dns-guard, count 0
  protocol-enforcement, drop 0
  nat-rewrite, count 0
  umbrella registration: mode: fail-open tag: default, status: 200 success,
device-id: 010a13b8fbdfc9aa
  Umbrella ipv4 resolver: 208.67.220.220
  Umbrella ipv6 resolver: 2620:119:53::53
  Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0
local-domain-bypass 10
  DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
  DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
  DNScrypt: Certificate Update: completion 10, failure 1
```

詳細な出力では、DNScrypt 統計情報と使用されるキーが表示されます。

```
asa(config)# show service-policy inspect dns detail
Global policy:
  Service-policy: global_policy
  Class-map: inspection_default
  Class-map: dnscrypt30000
  Inspect: dns dns_umbrella, packet 12, lock fail 0, drop 0, reset-drop 0,
  5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
  message-length maximum client auto, drop 0
  message-length maximum 1500, drop 0
  dns-guard, count 3
  protocol-enforcement, drop 0
  nat-rewrite, count 0
  Umbrella registration: mode: fail-open tag: default, status: 200 SUCCESS,
device-id: 010af97abf89abc3, retry 0
  Umbrella ipv4 resolver: 208.67.220.220
  Umbrella ipv6 resolver: 2620:119:53::53
  Umbrella: bypass 0, req inject 6 - sent 6, res recv 6 - inject 6
local-domain-bypass 10
  Umbrella app-id fail, count 0
  Umbrella flow alloc fail, count 0
```

```

Umbrella block alloc fail, count 0
Umbrella client flow expired, count 0
Umbrella server flow expired, count 0
Umbrella request drop, count 0
Umbrella response drop, count 0
DNScrypt egress: rcvd 6, encrypt 6, bypass 0, inject 6
DNScrypt ingress: rcvd 18, decrypt 6, bypass 12, inject 6
DNScrypt length error, count 0
DNScrypt add padding error, count 0
DNScrypt encryption error, count 0
DNScrypt magic_mismatch error, count 0
DNScrypt disabled, count 0
DNScrypt flow error, count 0
DNScrypt nonce error, count 0
DNScrypt: Certificate Update: completion 1, failure 1
DNScrypt Receive internal drop count 0
DNScrypt Receive on wrong channel drop count 0
DNScrypt Receive cannot queue drop count 0
DNScrypt No memory to create channel count 0
DNScrypt Send no output interface count 1
DNScrypt Send open channel failed count 0
DNScrypt Send no handle count 0
DNScrypt Send dupb failure count 0
DNScrypt Create cert update no memory count 0
DNScrypt Store cert no memory count 0
DNScrypt Certificate invalid length count 0
DNScrypt Certificate invalid magic count 0
DNScrypt Certificate invalid major version count 0
DNScrypt Certificate invalid minor version count 0
DNScrypt Certificate invalid signature count 0
Last Successful: 01:42:29 UTC May 2 2018, Last Failed: None
Magic DNSC, Major Version 0x0001, Minor Version 0x0000,
Query Magic 0x714e7a696d657555, Serial Number 1517943461,
Start Time 1517943461 (18:57:41 UTC Feb 6 2018)
End Time 1549479461 (18:57:41 UTC Feb 6 2019)
Server Public Key
240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836
Client Secret Key Hash
48DD:E6D3:C058:D063:1098:C6B4:BA6F:D8A7:F0F8:0754:40B0:AFB3:CB31:2B22:A7A4:9CEE
Client Public key
6CB9:FA4B:4273:E10A:8A67:BA66:76A3:BFF5:2FB9:5004:CD3B:B3F2:86C1:A7EC:A0B6:1A58
NM key Hash
9182:9F42:6C01:003C:9939:7741:1734:D199:22DF:511E:E8C9:206B:D0A3:8181:CE57:8020

```

Umbrella の syslog メッセージのモニタリング

次の Umbrella 関連の syslog メッセージをモニターできます。

- 「%ASA-3-339001: DNSCRYPT certificate update failed for *number* tries.」

Umbrella サーバーへのルートが存在すること、および出力インターフェイスが表示され正常に機能していることを確認してください。また、DNScrypt 用に設定された公開キーが正しいことも確認してください。Cisco Umbrella から新しいキーを取得する必要が生じる場合があります。

- 「%ASA-3-339002: Umbrella device registration failed with error code *error_code*.」

各エラー コードの内容は、次のとおりです。

- 400 : 要求の形式またはコンテンツに問題があります。トークンが短すぎるか、破損している可能性があります。トークンが Umbrella ダッシュボードのトークンと一致していることを確認してください。
- 401 : API トークンが承認されていません。トークンを再設定してください。Umbrella ダッシュボードのトークンを更新する場合は、必ず新しいトークンを使用してください。
- 409 : デバイス ID が別の組織と競合しています。問題の内容について Umbrella 管理者に確認してください。
- 500 : 内部サーバー エラー。問題の内容について Umbrella 管理者に確認してください。

• 「%ASA-6-339003: Umbrella device registration was successful.」

• 「%ASA-3-339004: Umbrella device registration failed due to missing token.」

Cisco Umbrella から API トークンを取得し、Umbrella のグローバル設定で設定する必要があります。

• 「%ASA-3-339005: Umbrella device registration failed after *number* retries.」

syslog 339002 メッセージを確認し、修正する必要があるエラーを特定します。

• 「%ASA-3-339006: Umbrella resolver *IP_address* is reachable, resuming Umbrella redirect.」

このメッセージは、システムが再度正常に機能していることを示します。そのため、対処は必要ありません。

• 「%ASA-3-339007: Umbrella resolver *IP_address* is unresponsive and fail-close mode used, starting probe to resolver.」

フェールクローズモードを使用しているため、Umbrella DNS サーバーがオンラインに戻るまで DNS 要求に対する応答を取得できません。問題が解決しない場合は、システムから Umbrella サーバーへのルートが存在すること、およびアクセス制御ポリシーでサーバーへの DNS トラフィックが許可されていることを確認してください。

• API キー/秘密の登録に関するメッセージ :

- %ASA-6-339010 : Cisco Umbrella API トークンの要求が成功しました
- %ASA-3-339011 : Cisco Umbrella API トークンの要求で応答がありませんでした
- %ASA-3-339012 : Cisco Umbrella API トークンの要求がエラーコード %d で失敗しました
- %ASA-3-339013 : 応答処理で Cisco Umbrella API トークンの要求が失敗しました
- %ASA-3-339014 : %d の再試行後に Cisco Umbrella API トークンの要求が失敗しました。登録を中止します

Cisco Umbrella Connector の履歴

機能名	プラットフォームリリース	説明
Cisco Umbrella サポート。	9.10(1)	<p>Cisco Umbrella で定義されている エンタープライズセキュリティ ポリシーをユーザー接続に適用できるように DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。FQDNに基づいて接続を許可またはブロックできます。または、疑わしい FQDN の場合は Cisco Umbrella インテリジェント プロキシにユーザーをリダイレクトして URL フィルタリングを実行できます。Umbrella の設定は、DNS インスペクション ポリシーに含まれています。</p> <p>次の画面を追加または変更しました。[Configuration] > [Firewall] > [Objects] > [Umbrella]、[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > DNS。</p>
Cisco Umbrella の強化	9.12(1)	<p>Cisco Umbrella をバイパスする必要があるローカルドメイン名を特定できるようになりました。これらのドメインの DNS 要求は、Umbrella を処理せず DNS サーバーに直接送信されます。また、DNS 要求の解決に使用する Umbrella サーバーも特定できるようになりました。さらに、Umbrella サーバーを使用できない場合は、DNS 要求がブロックされないように、Umbrella インスペクション ポリシーをフェール オープンに定義することができます。</p> <p>次の画面が変更されました。[設定 (Configuration)] > [ファイアウォール (Firewall)] > [オブジェクト (Objects)] > [Cisco Umbrella (Umbrella)]、[設定 (Configuration)] > [ファイアウォール (Firewall)] > [オブジェクト (Objects)] > [マップの調査 (Inspect Maps)] > [DNS]。</p>
新しい Cisco Umbrella API。	9.23(1)	<p>秘密鍵を持つ API キーを使用する Cisco Umbrella オープン API を使用して、Cisco Umbrella を設定できるようになりました。</p> <p>次の画面が更新されました。[設定 (Configuration)] > [ファイアウォール (Firewall)] > [オブジェクト (Objects)] > [Cisco Umbrella (Umbrella)]。</p>

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。

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。

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。