



Cisco Umbrella

Cisco Umbrella で定義されている FQDN ポリシーをユーザ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 の例 \(13 ページ\)](#)
- [Umbrella Connector のモニタリング \(17 ページ\)](#)
- [Cisco Umbrella Connector の履歴 \(20 ページ\)](#)

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 でブラックリストまたはグレーリストの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 ポリシーを適用することができます。

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。

- **ホワイトリスト**：FQDN に対するブロック ルールがなく、Cisco Umbrella で悪意のないサイトに属していると判断した場合は、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。
- **グレーリスト**：FQDN に対するブロック ルールがないが、Cisco Umbrella で疑わしいサイトに属していると判断した場合は、DNS 応答が Umbrella インテリジェントプロキシの IP アドレスを返します。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。
- **ブラック リスト**：FQDN が明示的にブロックされているか、Cisco Umbrella で悪意のあるサイトに属していると判断した場合は、DNS 応答が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 アドレスを返します。

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。

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 マスターでは、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 となったりすることはありません。

- 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、ブラックリストおよびグレーリストのアクションは 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）。ブラックリストまたはグレーリストにある非 HTTP/HTTPS 接続のアドレスは、失敗するか誤った方法で完了します。たとえば、ブラックリストにある 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。グレーリストにあるドメイン名の 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。

- 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спек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спек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спек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спек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、DNSscrypt では、IPv4 と IPv6 の両方のトラフィックを暗号化します。
- Cisco Umbrella と ASA FirePOWER の処理は、特定の接続に対して互換性がありません。両方のサービスを利用する場合は、ASA FirePOWER の処理から UDP/53 と UDP/443 を除外する必要があります。たとえば、現在すべてのトラフィックを ASA FirePOWER モジュールにリダイレクトしている場合、クラスを更新してアクセスリストを照合する必要があります。アクセスリストは宛先ポート UDP/53 および UDP/443 の Umbrella サーバに対する接続を拒否し、次にすべての宛先に対する送信元を許可してから開始する必要があります。ACL と一致するステートメントは、次のようになります。

```
access-list sfr extended deny udp any host 208.67.220.220 eq domain
access-list sfr extended deny udp any host 208.67.220.220 eq 443
access-list sfr extended permit ip any any
```

```
class-map sfr
  match access-list sfr
policy-map global_policy
  class sfr
    sfr fail-open
```

- 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さずに別の 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。

自分のサーバを使用することも、Cisco Umbrella サーバを設定することもできます。別のサーバ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

例：

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220
```

ステップ 4 [Umbrella Connector のグローバル設定 \(8 ページ\)](#)。

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 \(10 ページ\)](#)。

ステップ 6 [Umbrella の登録確認 \(12 ページ\)](#)。

Cisco Umbrella 登録サーバからの CA 証明書のインストール

Cisco Umbrella 登録サーバとの間で 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。

インポートする必要のある PEM 証明書を次に示します。

```

-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNLcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWwNcnQuY29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAEFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzA1BgNVBAMTHkRrZ21lZDZlZDZlZDZlZDZl
U2VjdXJlIFNlcnZlcjBDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8z15CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPdkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDog5B6TXvi/TC2rSsd9f
/lD0Uzs1gN2ujkSYs58009rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARfDRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmr7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKfCs/mC/bdFWJsCAwEAAsCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVFR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWwNcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGmWh0dHA6
Ly9jc2w0LmRrZ21jZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
oDOGmWh0dHA6Ly9jc2w0LmRrZ21jZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
ZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
ZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
xtniMB8GA1UdIwQYMBAAFAPEUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHg14+mUwnNqipl
5TlPHo0lbyYoiQm5vuh7ZPHLgLTUq/sELfeNqzqPlt/yGFUzZgThb07DjcllGA
8MXW5dRNJ2Srm8c+cftI17gzbcTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdc
2iDj6m6K7hQGrn2iWziIqBtvLfTyyRRfJs8sjX7tN8CplTm5gr8ZDoo0rwaAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJes4d60tbvVS3br0
j6tJlp07kzQoH3jOlOrHvdPjRzeXDLz
-----END CERTIFICATE-----

```

手順

ステップ 1 Cisco Umbrella 登録サーバのトラストポイントを作成します。

crypto ca trustpoint name

トラストポイントには、最大 128 文字の任意の名前（ctx1 or または umbrella_server など）を使用できます。

例：

```

ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)#

```

ステップ 2 これは、証明書を貼り付けて手動で登録することを示しています。

enrollment terminal

例：

```

ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)#

```

ステップ 3 証明書をインポートします。

crypto ca authenticate name

この証明書で作成したトラストポイントの名前を入力します。指示に従い、base64 でエンコードされた証明書を貼り付けます。貼り付ける証明書には、BEGIN CERTIFICATE 行および END CERTIFICATE 行を含めないでください。

```
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
MIIEIDCCA3ygAwIBAgIQAF2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWN1cnQuY29tMSAwHgYDVQDExdEaWdpQ2VydCBHbG9iYWwum9vdCBD
QTAEFw0xMzAzMDgxmMjAwMDBaFw0yMzAzMDgxmMjAwMDBaME0xCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbMxkZjZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
U2VjdXJlIFN1cnZlcjBDQTCASlWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyUwJBNwCQwFZA1W248ghX1LFy949v/cUP6ZCWA104Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8z15CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDog5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2uJkSYs58009rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdrRdNzGX
kujNVA075ME/OV4uuPNcfhCOhKEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKkFfCs/mC/bdFWJsCAwEAAaOCAVowggFwMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWN1cnQuY29tMHsGAlUdHwR0MHIwN6A1oDOGMMWh0dHA6
Ly9jcmwzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwzLmRp
oDOGMMWh0dHA6Ly9jcmwzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwzLmRp
Z21jZXJ0LmNvbS9DUFMwHQYDVR0OBjEFAA+AYRyCMWHVLYjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHg14+mUwnNqip1
5TlPHoO1blyYoiQm5vuh7ZPHLgLTUq/sELfeNqzqPlt/yGFUzZgTHb07Djc11GA
8MXW5dRNJ2Srm8c+cftI17gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGzn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPi
t c+LJMto4JQvtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3j01OrHvdPJbrZeXDLz
quit

INFO: Certificate has the following attributes:
Fingerprint:      345eff15 b7a49add 451b65a7 f4bdc6ae
Do you accept this certificate? [yes/no]: yes

Trustpoint 'ctx1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported
ciscoasa(config)#
```

Umbrella Connector のグローバル設定

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 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 \(10 ページ\)](#) 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 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 登録サーバの証明書をインストールします。

手順

ステップ 1 Umbrella コンフィギュレーション モードを開始します。

umbrella-global

例 :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)#
```

ステップ 2 Cisco Umbrella への登録に必要な API トークンを設定します。

token api-token

例 :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
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
```

ステップ 3 (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。

public-key hex_key

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、**no public-key** と入力します。設定したキーは、省略することも、コマンドの **no** バージョンに追加することもできます。

例 :

```
ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
```

ステップ 4 (任意) アイドルタイムアウトを設定します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。

```
timeout edns hh:mm:ss
```

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。

例 :

```
ciscoasa(config-umbrella)# timeout edns 00:01:00
```

ステップ 5 (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。

ローカルドメイン名を直接入力できます。必要に応じて名前を定義する正規表現を作成し、次に正規表現クラス マップを作成して次のコマンドで指定します。

```
local-domain-bypass {regular_expression | regex class regex_classmap}
```

例 :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

ステップ 6 (任意) 使用する DNS 要求を解決する、デフォルト以外の Cisco Umbrella DNS サーバのアドレスを設定します。

```
resolver{ipv4 | ipv6} ip_address
```

コマンドを個別に入力して、デフォルト以外の Umbrella リゾルバの IPv4 および IPv6 アドレスを定義できます。

例 :

```
ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222
ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

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** `preset_dns_map` インスペクション ポリシーマップを編集し、パラメータ設定モードを入力します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)#
```

- ステップ 2** Umbrella をイネーブルにし、必要に応じてデバイスに適用する Cisco Umbrella のポリシー名を指定します。

umbrella [*tag umbrella_policy*] [*fail-open*]

タグは、Cisco Umbrella で定義されたポリシーの名前です。登録中に Cisco Umbrella によってデバイスにポリシーが割り当てられます（ポリシー名が存在する場合）。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。

Umbrella DNS サーバが使用できない場合に DNS 解決を動作させるには、**fail-open** キーワードを追加します。フェールオープン状態で Cisco Umbrella DNS サーバ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（存在する場合）に移動できるようになります。Umbrella DNS サーバ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。このオプションが含まれていない場合、DNS 要求は到達不能の Umbrella リゾルバへ移動し続けるので、応答は取得されません。

例：

```
ciscoasa(config-pmap-p)# umbrella fail-open
```

- ステップ 3** （任意）DNSCrypt をイネーブルにしてデバイスと Cisco Umbrella 間の接続を暗号化します。

dnscrypt

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 インスペクション

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。デフォルトのインスペクションクラスには DNS インスペクションに UDP/443 がすでに含まれています。

例：

```
ciscoasa(config-pmap-p)# dnscrypt
```

例

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

Umbrella の登録確認

Umbrella のグローバル設定を実行し、DNS インスペクションで 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。

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。ここには、Cisco Umbrella で適用されるポリシー（タグ）、接続の HTTP ステータス（401 は API トークンが正しくないことを示し、409 はデバイスがすでに Cisco Umbrella に存在することを示します）、およびデバイス ID が示されている必要があります。

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: 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
```



```
Ly9jcmwzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwvN6A1
oDOGmWh0dHA6Ly9jcmw0LmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwvPQYDVR0gBDYwNDAYBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ21jZXJ0LmNvbS9DUFMwHQYDVR0OBByEFA+AYRyCMWHVlyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqip1
5TlPHo0lblyYoiQm5vuh7ZPHLgLTUq/sELfeNqzqPlt/yGFUzZgTHb07Djc1lGA
8MXW5dRNJ2Srm8c+cftI17gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGGrn2iWziIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BN098pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3j0L0rHvdPJbRzeXDLz
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint:      345eff15 b7a49add 451b65a7 f4bdc6ae
Do you accept this certificate? [yes/no]: yes
```

Trustpoint 'ctx1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

```
% Certificate successfully imported
ciscoasa(config)#
```

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220
```

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
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
```

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

例：カスタムインスペクションポリシーを使用したインターフェイス上での Umbrella のイネーブル化

次に、特定のトラフィッククラスで Umbrella をイネーブルにする例を示します。Umbrella は DNS/UDP のトラフィックの内部インターフェイスでのみイネーブルになります。DNSCrypt がイネーブルになっているため、トラフィッククラスに UDP/443 を追加する必要があります。

「Mypolicy」（Cisco Umbrella で定義）という名前のエンタープライズセキュリティポリシーが適用されます。

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
MIIE1DCCA3ygAwIBAgIQAF2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
```



```
ciscoasa(config)#

ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
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

ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt

ciscoasa(config)# access-list sfr extended deny udp any host 208.67.220.220 eq domain
ciscoasa(config)# access-list sfr extended deny udp any host 208.67.220.220 eq 443
ciscoasa(config)# access-list sfr extended permit ip any any

ciscoasa(config)# class-map sfr
ciscoasa(config-cmap)# match access-list sfr

ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class sfr
ciscoasa(config-pmap-c)# sfr fail-open

ciscoasa(config)# service-policy global_policy global
```

Umbrella Connector のモニタリング

ここでは、Umbrella Connector をモニタ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спекションの統計情報の概要と詳細を両方表示できます。

```
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 サーバを示します。これらの回線によって、サーバが応答なしかどうか、または現在サーバ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（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できます。

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

Umbrella サーバ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ある場合があります。

- 「%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、修正する必要の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。

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>umbrella、umbrella-global、token、public-key、timeout edns、dnscrypt、show service-policy inspect dns detail の各コマンドが追加または変更されました。</p>

機能名	プラットフォーム リリース	説明
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 サーバも特定できるようになりました。さらに、Umbrella サーバ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спек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>local-domain-bypass、resolver、umbrella fail-open の各コマンドが追加または変更されました。</p>

