CTA システムにログ ファイルをアップロードするための Blue Coat ProxySG の設定

最終更新日:2015 年 10 月 23 日

目次

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	どれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングと見なされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符(!)またはポンド記号(#)がある場合には、コメント行であることを示します。

メモ:*読者に留意していただきたいこと*を示します。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意:**注意が必要なことを*示しています*。機器の損傷またはデータ損失を予防するための注意事項が記述されています。**

警告:**安全上の重要事項です。**

危険があることを示します。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。警告の各国語版については、各警告文の末尾に提示されている番号をもとに、この機器に付属している各国語で記述された安全上の警告を参照してください。

これらの注意事項を保存しておいてください。

規制:追加情報および規制要件または顧客要件に準拠するために定められています。

はじめに

このドキュメントでは、Cisco Cognitive Threat Analytics（CTA）システムにログ ファイルをアップロードするように Blue Coat ProxySG を設定する方法について説明します。ログ ファイルがシステムにアップロードされると、CTA はデータを分析し、その結果を CTA ポータルに報告します。

前提条件

要件

Cisco ScanCenter は、Cisco Cloud Web Security の管理ポータルです。最初に、Blue Coat ProxySG 用のデバイス アカウントを Cisco ScanCenter に作成する必要があります。

- Cisco ScanCenter にログインします。
- [脅威（Threats）] タブをクリックします。
- ページの右上の隅にあるグローバル設定メニューのアイコンをクリックします。
- [デバイス アカウント（Device Accounts）] をクリックします。
- アップロード方法として [自動（Automatic）] を選択します。

詳細については、『Cisco ScanCenter Administrator Guide（Cisco ScanCenter 管理ガイド）』の「Proxy Device Uploads（プロキシ デバイスのアップロード）」のセクションを参照してください。

デバイス アカウントを作成したら、Cisco ScanCenter の [デバイス アカウントを追加（Add Device Account）] ページからプロキシ設定に次の情報をコピーする必要があります。

- HTTPS ホスト：`etr.cloudsec.sco.cisco.com`
- HTTPS パス
- プロキシ デバイス用に生成されたユーザ名。大文字と小文字が区別され、プロキシ デバイスごとに異なります。
- デバイス パスワード（大文字、小文字を区別）

Blue Coat ProxySG にアクセスするには、以下が必要です。

- Blue Coat ProxySG のホスト名または IP アドレス
- Blue Coat ProxySG へのログイン クレデンシャル
    - デフォルトのユーザ名は admin です。
    - デフォルトのパスワードはありません。設定する必要があります。
- Java™ プラグインが搭載された Web ブラウザ。Blue Coat は Google Chrome、Opera、または Safari をサポートしていません。

注意：このドキュメントの情報は、ラボ環境にあるデバイスに基づいて作成されたものです。対象のネットワークが実稼働中である場合には、どのようなコンフィギュレーション コマンドについても、その潜在的な影響力を理解しておいてください。

使用されるコンポーネント

このドキュメントの情報は、次のハードウェアでテストされています。

- Blue Coat ProxySG 600

このドキュメントの情報は、次のソフトウェアのバージョンでテストされています。

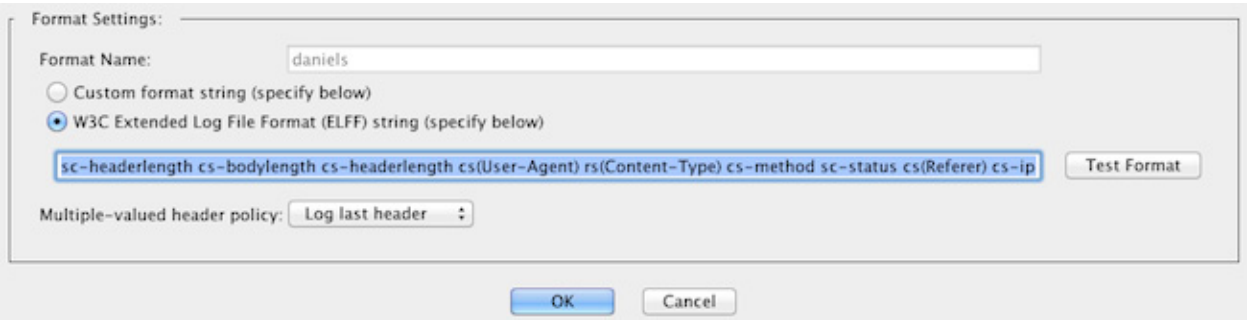
- SGOS 6.5.7.5
- SGOS 6.5.6.1

メモ：他のバージョンは CTA へのアップロー時に正しく動作*しない*可能性があるため、現在サポートされて*いません*。

設定

プロキシの設定

1. Web ブラウザで次のように指定し、Blue Coat ProxySG に移動します。
   a. https://sg_600.*hostname*:8082/ または
   b. https://*a.b.c.d*:8082/。ここで、*a.b.c.d* はプロキシの IP アドレスです。
2. 必要に応じて、セキュアではない HTTPS 証明書を承認し、続行します。
3. admin としてログインします。
4. 必要に応じて、Java™ のセキュリティ警告を承認し、続行します。
5. [設定（Configuration）] > [アクセスログ（Access Logging）] > [全般（General）] に移動します。
6. [アクセスログを有効にする（Enable Access Logging）] チェックボックスをオンにし、[適用（Apply）] ボタンをクリックします。
7. [設定（Configuration）] > [アクセスログ（Access Logging）] > [形式（Formats）] に移動します。
8. [新規（New）] ボタンをクリックして新しい形式エントリを作成します。
9. [形式名（Format Name）] フィールドに一意の名前を入力します。この例では、`daniels` を使用しています。

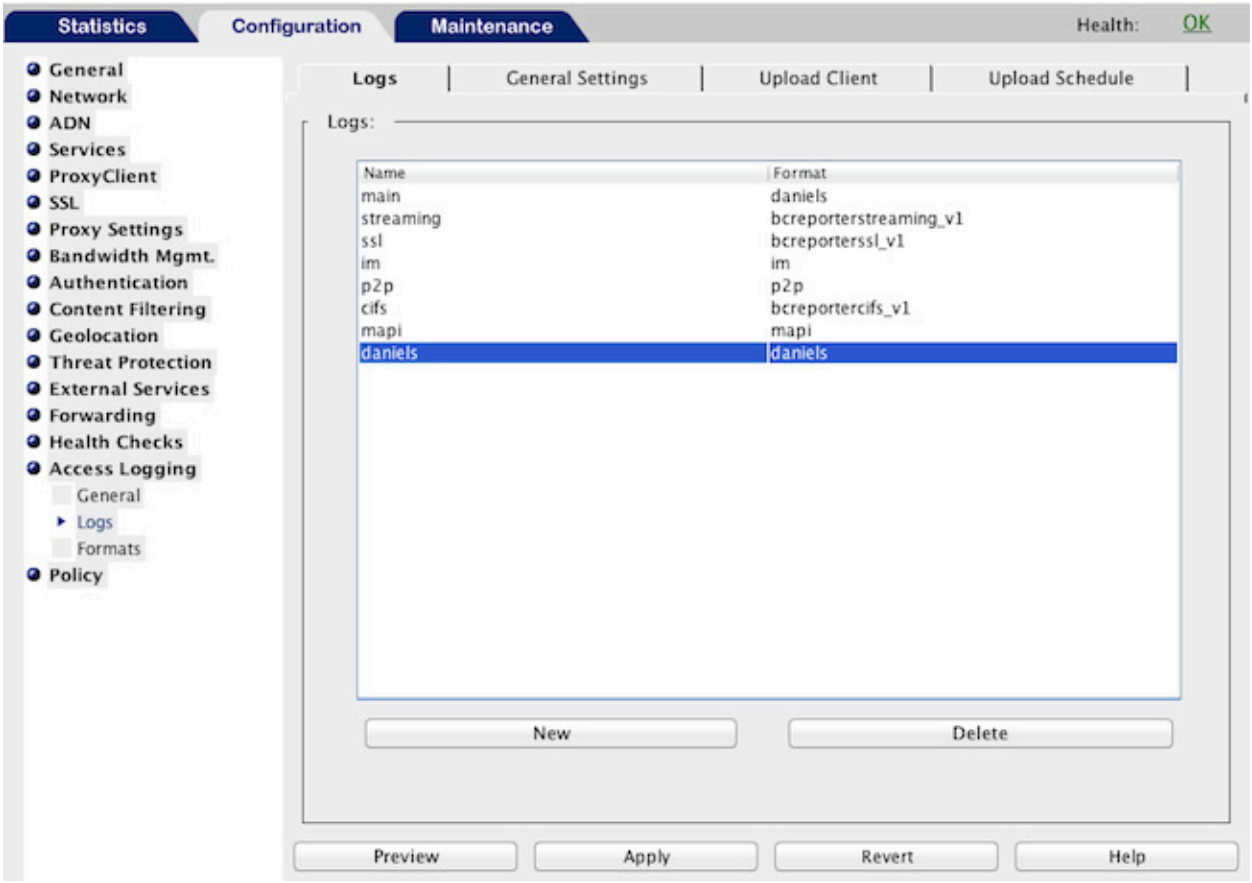


10. [W3C拡張ログファイル形式（ELFF)の文字列（W3C Extended Log File Format (ELFF) string）] のオプション ボタンをクリックし、次の文字列をフィールドに貼り付けます。

```
timestamp time-taken c-ip cs-username s-ip s-port c-port cs-uri cs-bytes
sc-bytes sc-bodylength sc-headerlength cs-bodylength cs-headerlength
cs(User-Agent) rs(Content-Type) cs-method sc-status cs(Referer) cs-ip r-ip
r-port rs(Location)
```

11. [OK] ボタンをクリックします。

12. [適用(Apply)] ボタンをクリックします。
13. [設定(Configuration)] > [アクセスログ(Access Logging)] > [ログ(Logs)] に移動します。
14. [新規(New)] ボタンをクリックして新しいログエントリを作成します。
15. [ログ名(Log Name)] と [ログ形式(Log Format)] の両方にステップ 9 で作成した形式名を選択します。この例では、`daniels` を使用しています。

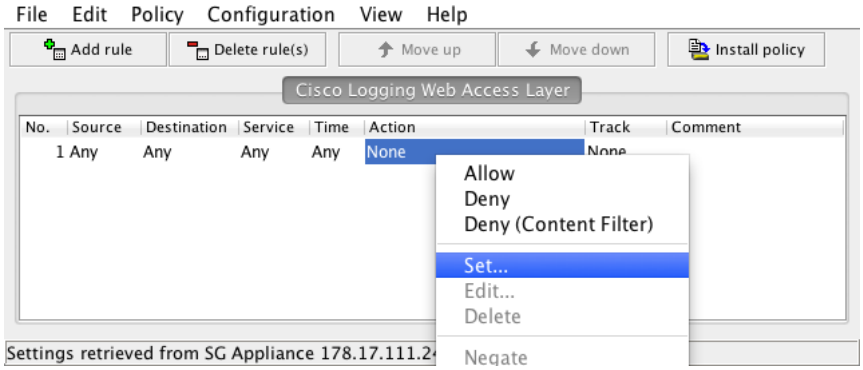


16. [OK] ボタンをクリックします。
17. [適用(Apply)] ボタンをクリックします。
18. 警告のポップアップ メッセージが表示される場合がありますが、無視しても安全です。メッセージには、同じログ ファイル内に以前の形式のログ エントリと現在の形式のエントリが混在する可能性があると示されています。
19. [アップロード クライアント(Upload Client)] タブをクリックします。
20. [ログ(Log)] プルダウンで、ステップ 15 のログを選択します。
21. [クライアント タイプ(Client type)] プルダウンで、[HTTP クライアント(HTTP Client)] を選択します。
22. [クライアント タイプ(Client type)] の横にある [設定(Settings)] ボタンをクリックして新しいウィンドウを表示します。
23. [ホスト(Host)] フィールドに、Cisco ScanCenter で指定したホストを入力します。次に例を示します。`etr.cloudsec.sco.cisco.com`
24. [ポート(Port)] フィールドに、`443` と入力します。
25. [パス(Path)] フィールドに、Cisco ScanCenter で指定したパスを入力します。次に例を示します。`/upload/`*`username`*

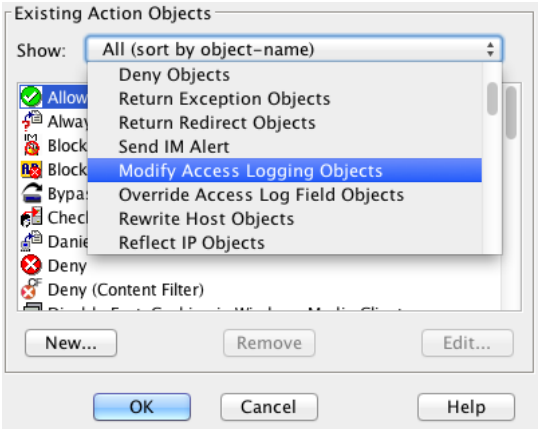
26. [ユーザ名（Username）] フィールドに、Cisco ScanCenter のデバイス用に生成されたユーザ名を入力します。デバイス ユーザ名は大文字と小文字が区別され、プロキシ デバイスごとに異なります。
27. この時点では、[ファイル名（Filename）] フィールドを変更しないでください。
28. [セキュアな接続（SSL）を使用する（Use secure connections (SSL)）] チェックボックスをオンにします。
29. [プライマリ パスワードを変更（Change Primary Password）] ボタンをクリックして新しいウィンドウを表示します。
30. パスワード フィールドに、Cisco ScanCenter のデバイス用に生成されたパスワードを入力します。デバイス パスワードは大文字と小文字が区別されます。
31. [OK] ボタンをクリックします。
32. [アップロード スケジュール（Upload Schedule）] タブをクリックします。
33. [ログ（Log）] プルダウンで、ステップ 9 で作成した形式名を選択します。
34. [ログ ファイルをアップロード（Upload the log file）] セクションで、ログ ファイルをアップロードする [間隔（Every）] として 0 時間と 55 分を選択します。

プロキシの背後のユーザ数	推奨アップロード期間
2000 人未満	55 分
不明または 2000 ～ 4000	30 分
4000 ～ 6000	20 分
6000 超	10 分

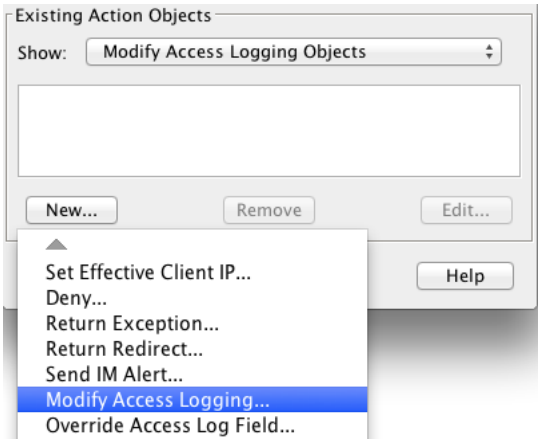
35. [適用（Apply）] ボタンをクリックします。
36. [設定（Configuration）] > [ポリシー（Policy）] > [Visual Policy Manager] に移動します。
37. [起動（Launch）] ボタンをクリックして新しいウィンドウを表示します。
38. [ポリシー（Policy）] > [Web アクセス レイヤを追加（Add Web Access Layer）] に移動します。
39. レイヤに Cisco Logging Web Access Layer という名前を付け、[OK] をクリックします。
40. カーソルを [アクション（Action）] 列に移動して右クリックし、[設定（Set）] を選択します。



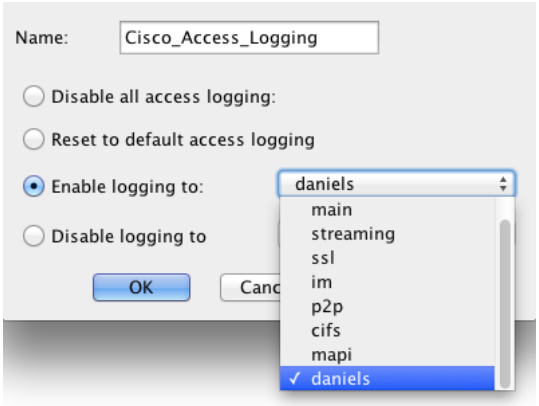
41. [表示（Show）] プルダウンで、[アクセス ログ オブジェクトを変更（Modify Access Logging Objects）] を選択します。



42. [新規（New）] ボタンをクリックし、[アクセス ログを変更（Modify Access Logging）] を選択します。



43. 名前を入力します。この例では、`Cisco_Access_Logging` を使用しています。
44. [ロギングを有効にする（Enable logging to）] のオプション ボタンをクリックし、プルダウンでステップ 15 のログを選択します。この例では、`daniels` を使用しています。



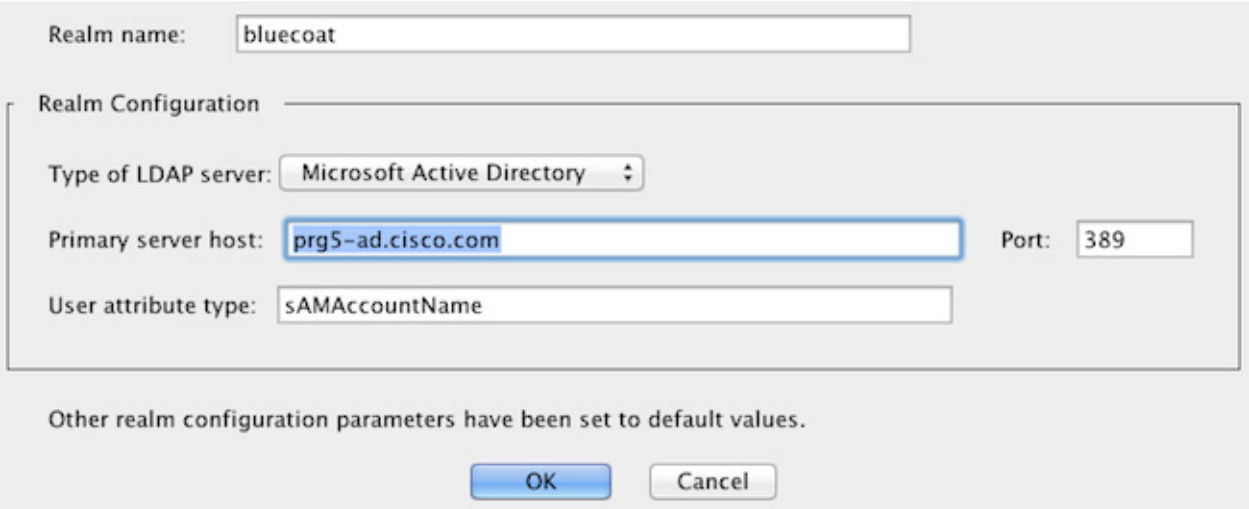
45. [OK] ボタンをクリックします。
46. もう 1 つの [OK] ボタンをクリックします。
47. [ポリシーをインストール（Install Policy）] ボタンをクリックします。

48. 「ポリシーが正常にインストールされました（policy installation was successful）」というメッセージが表示されたら、Visual Policy Manager ウィンドウを閉じます。

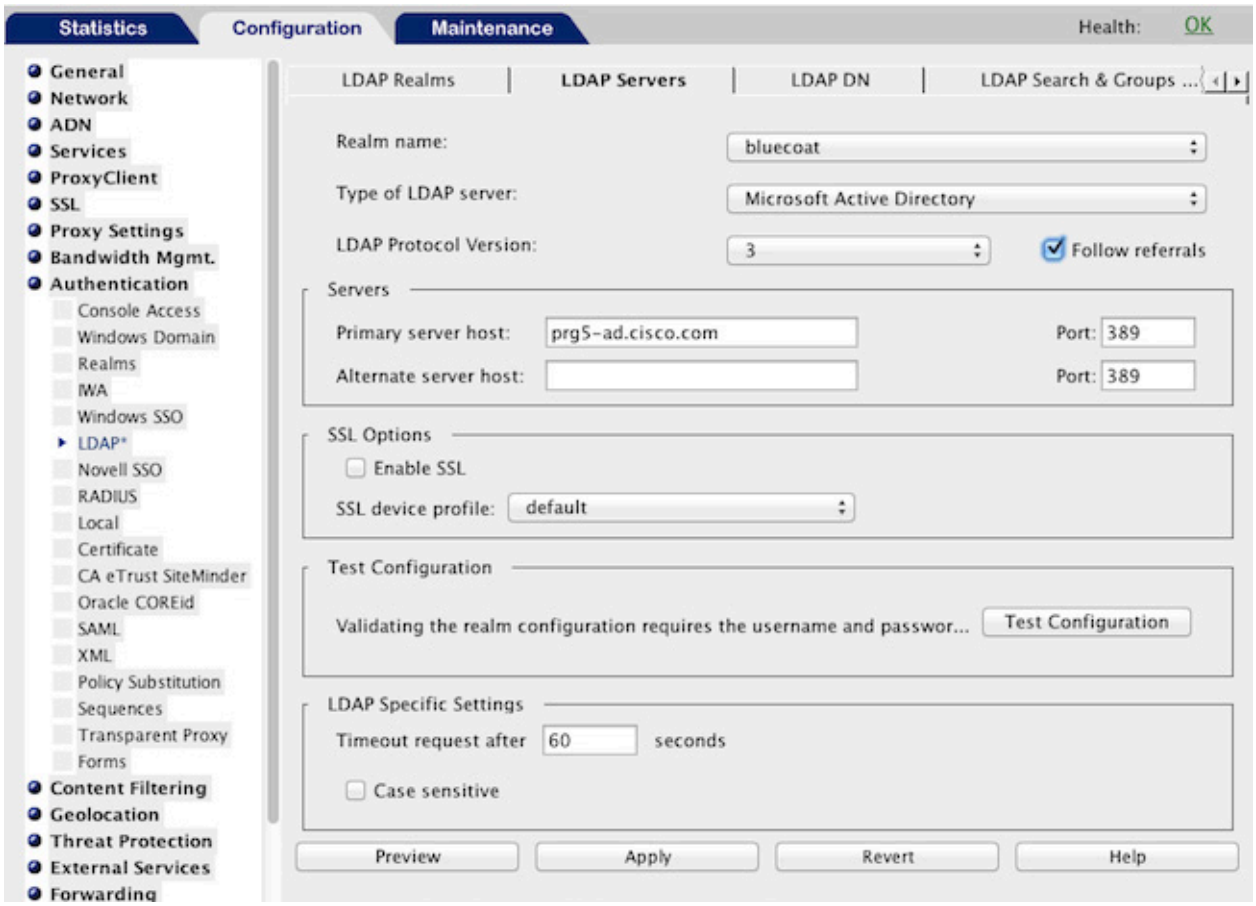
User Authentication

アクセス ログのユーザ詳細情報を取得するには、ユーザが認証されている必要があります。次のステップに従って、LDAP 認証をセットアップします。

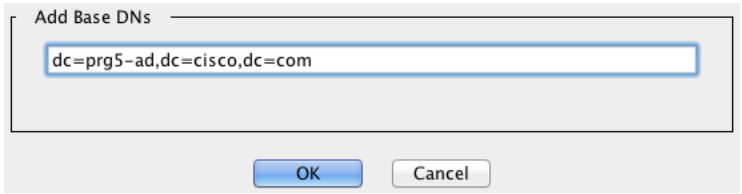
1. [設定（Configuration）] > [認証（Authentication）] > [LDAP] に移動します。
2. [LDAP レルム（LDAP Realms）] タブで [新規（New）] ボタンをクリックし、LDAP レルムを作成します。
3. レルムの名前とレルム設定パラメータを入力します。次に例を示します。



4. [OK] ボタンをクリックします。
5. [LDAP サーバ（LDAP Server）] タブをクリックします。
6. [レルム名（Realm name）] プルダウンで、以前に作成した LDAP レルムを選択します。
7. [リファーラルに従う（Follow referrals）] チェックボックスをオンにします。
8. [LDAP サーバのタイプ（Type of LDAP server）] を選択し、[プライマリ サーバのホスト（Primary server host）] に入力します。次に例を示します。

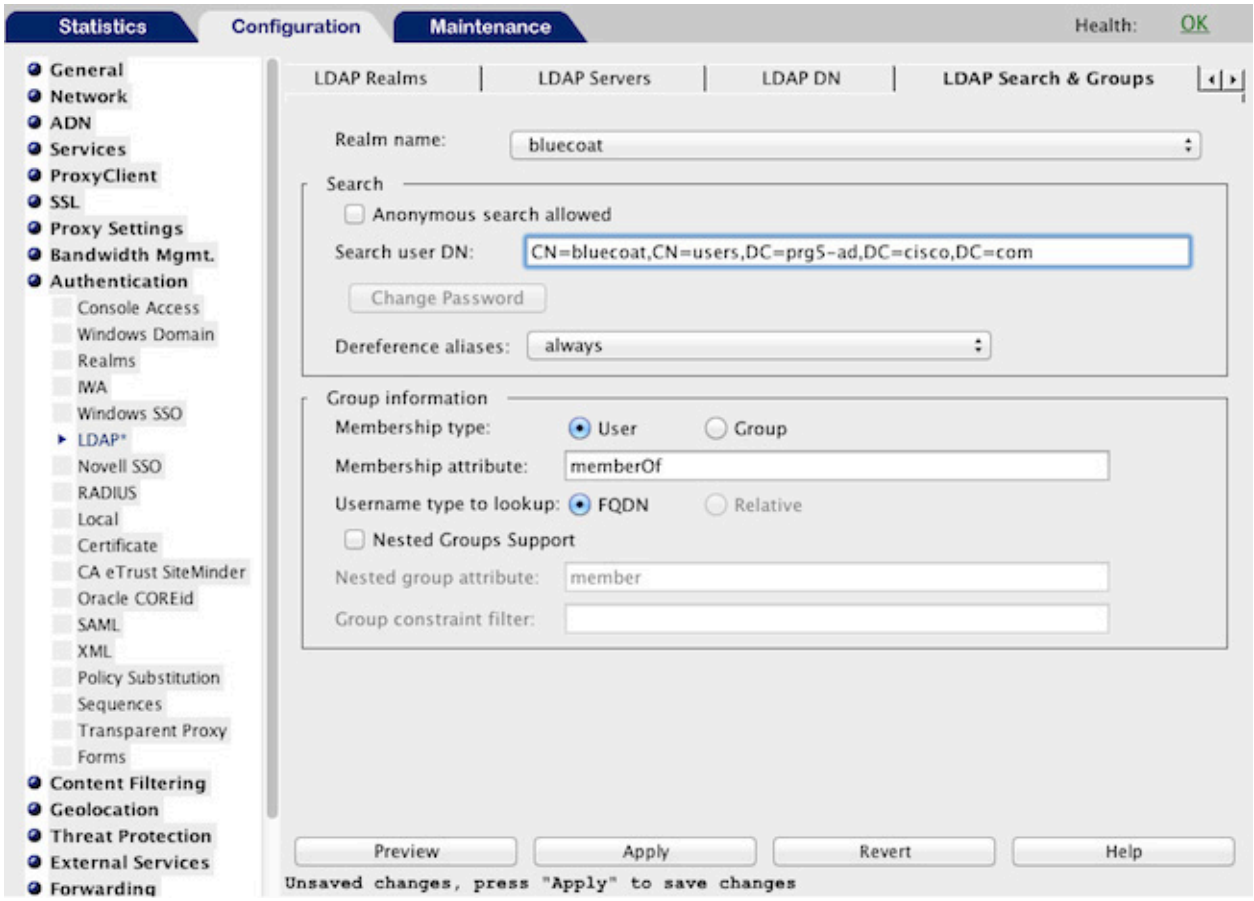


9. [適用（Apply）] ボタンをクリックします。
10. [LDAP DN] タブをクリックします。
11. [新規（New）] ボタンをクリックします。
12. [ベース DN を追加（Add Base DNs）] フィールドに識別名文字列を入力します。次に例を示します。



13. [OK] ボタンをクリックします。
14. [LDAP 検索およびグループ（LDAP Search & Groups）] タブをクリックします。
15. [レルム名（Realm name）] プルダウンで、以前に作成した LDAP レルムを選択します。

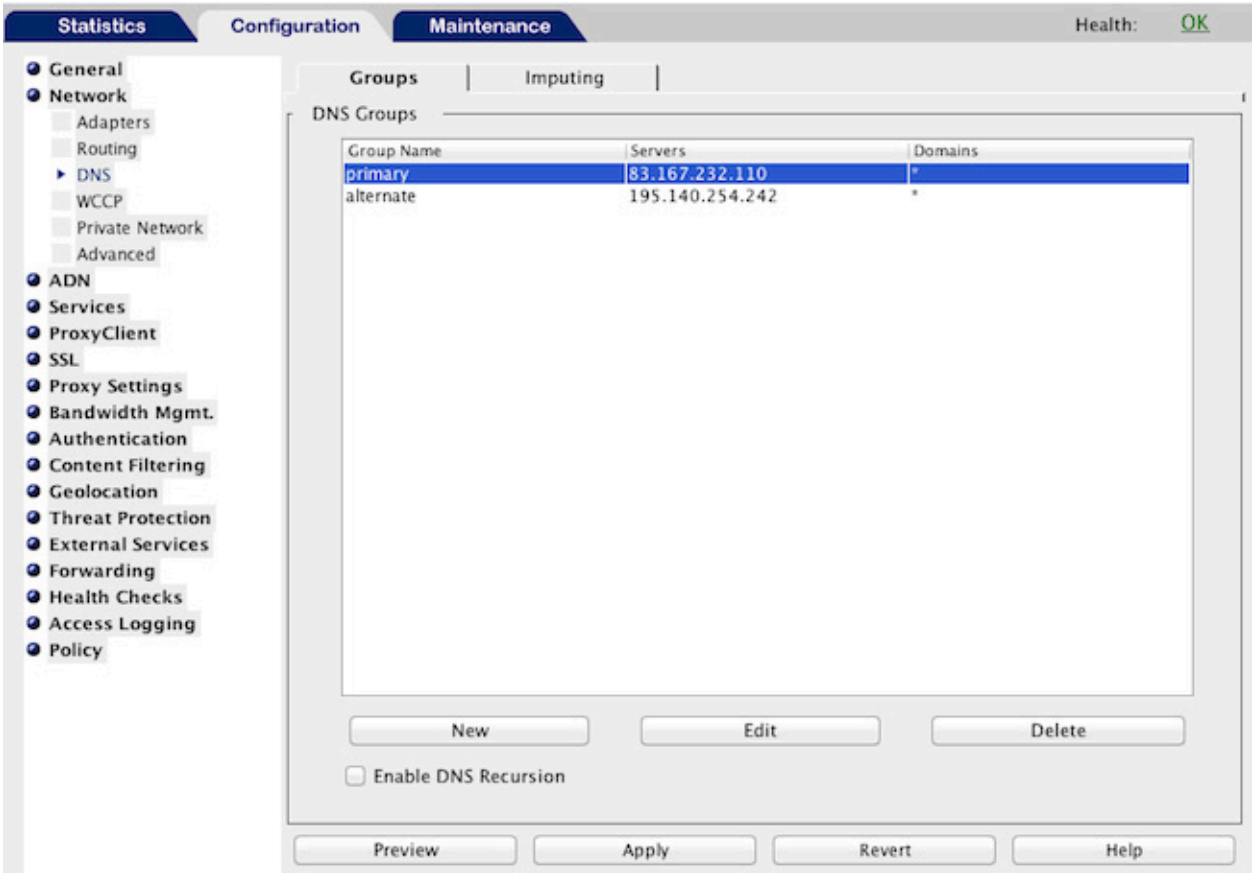
16. [ユーザ DN の検索（Search user DN）] に情報を入力します。次に例を示します。

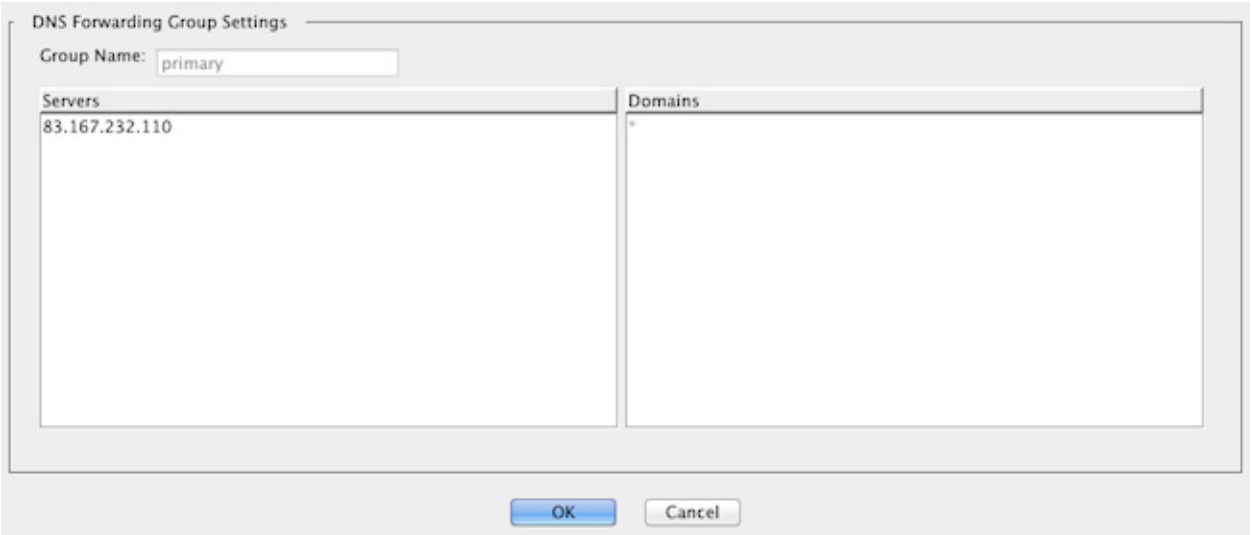


17. [パスワードの変更（Change Password）] ボタンをクリックします。
18. パスワード フィールドにパスワードを入力し、[OK] ボタンをクリックします。
19. [適用（Apply）] ボタンをクリックします。

DNS の設定

必要に応じて、次のセクションの設定を行います。変更を加える前に、IT 部門に問い合わせてください。Microsoft Active Directory を使用している場合は、そのアドレスを DNS サーバのリストに追加する必要がある場合があります。次に例を示します。





次のステップ

Cisco ScanCenter にログインし、[デバイス アカウント(DEVICE ACCOUNTS)] ページでアップロードが正常に行われていることを確認します。Blue Coat ProxySG の背後にあるデバイスから Web を参照すると、ファイルに記録されたテレメトリ データが分析のために CTA システムにアップロードされ、[脅威(Threats)] タブと CTA ポータルに表示されます。詳細については、『Cisco ScanCenter Administrator Guide, Release 5.2(Cisco ScanCenter 管理ガイド、リリース 5.2)』の第 32 章「Proxy Device Uploads(プロキシ デバイスのアップロード)」のセクションを参照してください。

トラブルシューティング

1. Blue Coat ProxySG にログインします。
2. [設定(Configuration)] > [アクセス ログ(Access Logging)] > [ログ(Logs)] > [アップロード クライアント(Upload client)] に移動します。
3. [アップロードのテスト(Test upload)] ボタンをクリックします。
4. [統計情報(Statistics)] > [詳細設定(Advanced)] > [イベント ログ(Event Log)] に移動してログ ファイルを表示します。
5. [更新時刻でイベント ログのテールを表示する(Show event log tail with refresh time)] をクリックします。

マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool(BST)の使用法、サービス要求の送信方法、および追加情報の収集方法については、「*What's New in Cisco Product Documentation*」(http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html)を参照してください。

「*What's New in Cisco Product Documentation*」に配信登録すると、新しい(または改訂された)シスコ技術情報のリストが RSS フィードとして提供され、リーダー アプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。RSS フィードは無料のサービスです。