Device Management を使用するための CSS の設定

WebNS Device Management ユーザ インターフェイス ソフトウェアを使用するには、まずここで説明する作業を行う必要があります。

- WebNS Device Management ユーザ インターフェイスのクイック スタート
- WebNS Device Management ユーザ インターフェイスの有効化
- 強度の高い SSL 暗号化を行うためのセキュア管理ライセンス キーの入力（オプション）
- アイドル タイムアウトの設定（オプション）
- イーサネット ポートの設定
- SNMP コミュニティの設定
- Device Management ユーザ インターフェイスへのアクセス制限（オプションですが、推奨します）
- ブラウザの設定
- SSL セキュリティ証明書の表示とインストール

WebNS Device Management ユーザ インターフェイスのクイック スタート

表 2-1 に、CSS で Device Management ユーザ インターフェイスを設定するために必要な手順の概要を示します。それぞれの手順に、作業を行うために必要な CLI コマンドも示します。CLI コマンドに関する各機能とすべてのオプションの詳細については、表以降の項を参照してください。

表 2-1　Device Management 設定のクイック スタート

作業とコマンドの例

1. 設定モードに入ります。
`# config`
`(config)#`

2. Device Management ユーザ インターフェイスを有効にします。「WebNS Device Management ユーザ インターフェイスの有効化」を参照してください。 `(config)# no restrict web-mgmt`

3. イーサネット ポート（たとえば、管理ポート）の IP アドレスとサブネット マスクを指定して、イーサネット ポートを設定します。「イーサネット ポートの設定」を参照してください。
`(config)# boot`
`(config-boot)#`
`(config-boot)# ip address 192.168.16.2`
`(config-boot)# subnet mask 255.255.255.0`

4. SNMP コミュニティを設定します。「SNMP コミュニティの設定」を参照してください。 `(config)# snmp community sqa read-write`
5. Device Management ユーザ インターフェイスへのアクセスを制限して、ユーザ アクセス特権をもつユーザ、および ACL に指定されたユーザだけが Device Management を使用できるようにします。「Device Management ユーザ インターフェイスへのアクセス制限」を参照してください。
6. SSL セキュリティ証明書を確認してインストールします。「SSL セキュリティ証明書の表示とインストール」を参照してください。

WebNS Device Management ユーザ インターフェイスの有効化

WebNS Device Management ユーザ インターフェイスを有効にするには、CLI コマンド **no restrict web-mgmt** を使用します。Device Management ユーザ インターフェイスは、デフォルトでは無効になっています。

CSS の Device Management ユーザ インターフェイスを有効にするには、次のコマンドを入力します。

```
(config)# no restrict web-mgmt
```

（注） Device Management ユーザ インターフェイスにアクセスするには、仮想認証を有効にし、使用する認証方法に応じて設定する必要があります。仮想認証はデフォルトで有効にされており、ローカルの CSS データベースを使用してユーザを認証します。仮想認証を無効にした場合、Device Management にアクセスするには、再度有効にする必要があります。仮想認証の設定の詳細については、『*Cisco Content Services Switch Security Configuration Guide*』を参照してください。

CSS の Device Management ユーザ インターフェイスを無効にするには、次のコマンドを入力します。

```
(config)# restrict web-mgmt
```

CSS の Device Management ユーザ インターフェイスの状態を確認するには、次のコマンドを入力します。

```
# show running-config
!************************ Global ***************************
virtual authentication
no restrict web-mgmt
```

Device Management ユーザ インターフェイスが有効になっている場合は、実行設定に **no restrict web-mgmt** コマンドが表示されます。

（注）　Device Management ユーザ インターフェイス ソフトウェアは、デフォルトで、強度の低い SSL 暗号化が有効な状態で実行されます。強度の高い SSL 暗号化を有効にする方法については、この章で後述する 「強度の高い SSL 暗号化を行うためのセキュア管理ライセンス キーの入力」を参照してください。

強度の高い SSL 暗号化を行うためのセキュア管理ライセンス キーの入力

Device Management ソフトウェアで 強度の高い SSL 暗号化を有効にするには、セキュア管理ソフトウェア オプションを購入する必要があります。セキュア管理ソフトウェア オプションを購入すると、次のいずれかの方法で権利証明書を入手できます。

- CSS　本体とともに発注した場合、ソフトウェアの権利証明書はアクセサリ キットに同梱されています。
- CSS をすでに購入している場合、権利証明書は郵送でお手元に届きます。

（注）　ライセンス　キーの権利証明書が見つからない場合は、製品をお買い上げの弊社販売代理店にお問い合せください。

ライセンス キーの権利証明書に記載されている手順に従って、セキュア管理ソフトウェアのライセンス キーを入手します。

セキュア管理ライセンス キーを入力して、CSS の強度の高い SSL 暗号化を有効にするには、次の操作を行います。

1. CSS にログインして、**license** コマンドを実行します。

   ```
   # license
   ```

2. セキュア管理ライセンス キーを入力します。

   ```
   Enter the Software License Key (q to quit): nnnnnnnnnnnn
   ```

これで、セキュア管理ライセンス キーが正常にインストールされ、強度の高い SSL 暗号化が有効になりました。

（注）　**restrict web-mgmt** コマンドを使用して Device Management ソフトウェアを無効にした後、**no restrict web-mgmt** コマンドで再度有効にすると、強度の高い SSL 暗号化に使用する暗号スイートが内部の Web サーバから自動的に読み込まれます。

アイドル タイムアウトの設定

アイドル タイムアウトは、デフォルトで、すべてのアクティブな Web 管理セッションに対して無効になっています（0 に設定されています）。アクティブな Web 管理セッションがログアウトされるまでの最大アイドル時間を設定するには、**idle timeout web-mgmt** コマンドを使用します。0 ～ 65535 分のタイムアウト値を入力します。

たとえば、すべてのアクティブな Web 管理セッションに対するアイドル タイムアウト値を 15 分に設定するには、次のように入力します。

```
(config)# idle timeout web-mgmt 15
```

Web 管理セッションのタイムアウト値を無効にするには、次のように入力します。

```
(config)# no idle timeout web-mgmt
```

イーサネット ポートの設定

WebNS Device Management ユーザ インターフェイスにアクセスするには、最初に CSS の CLI から適切なイーサネット インターフェイス ポート（イーサネット管理ポートなど）を設定する必要があります。

1. CSS にログインします。
2. CLI で **config** と入力して設定モードに入ります。

   ```
   # config
   (config)#
   ```

3. **boot** と入力してブート モードに入ります。

   ```
   (config)# boot
   (config-boot)#
   ```

4. 管理ポートの IP アドレスとサブネット マスクを入力します。

   ```
   (config-boot)# ip address 192.168.16.2
   (config-boot)# subnet mask 255.255.255.0
   ```

SNMP コミュニティの設定

snmp community コマンドを使用すると、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）のコミュニティ名を設定または変更して、SNMP にアクセスすることができます。コミュニティ名はいくつでも指定できます。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

snmp community *community_name* [**read-only**|**read-write**]

変数とオプションは次のとおりです。

- *community_name*：システムの SNMP コミュニティ名です。スペースを含まない 12 文字以内のテキスト文字列を引用符で囲まずに入力します。
- **read-only**：このコミュニティに対する読み取り専用アクセスを許可します。
- **read-write**：このコミュニティに対する読み取りと書き込みアクセスを許可します。

たとえば、次のように入力します。

```
(config)# snmp community sqa read-write
```

SNMP の詳細については、『*Cisco Content Services Switch Administration Guide*』を参照してください。

Device Management ユーザ インターフェイスへのアクセス制限

WebNS Device Management ユーザ インターフェイスには、CSS の設定を変更する権限を持つユーザだけがアクセスできるように、アクセスを制限することをお勧めします。アクセスの制限には、次の 2 種類の方法があります。

- 特権によるアクセス制限
- アクセス コントロール リストの設定

特権によるアクセス制限

WebNS Device Management Configuration ツリーの HTML ページにアクセス（SNMP GET および SET）できるのは、CSS の特権ユーザ（スーパーユーザ アクセス権を持つユーザ）だけです。これは、第 1 レベルの設定ページからアクセスするすべての第 2 レベルの設定ページでも同様です。

特権を持たないユーザ（ユーザ アクセス権を持つユーザ）は、モニタ ページとサマリー ページに読み取り専用でアクセス（SNMP GET）できますが、設定ページにはアクセスできません。特権を持たないユーザが設定ページにアクセスしようとすると、アクセス制限を示すページに次のメッセージが表示されます。

```
You do not have the appropriate privileges to access the configuration
page.
```

（注）　Device Management ソフトウェアにログインするには、使用するブラウザで Coockie を有効にする必要があります。

ユーザ アクセス権およびスーパーユーザ アクセス権を持つユーザの作成方法については、『*Cisco Content Services Switch Administration Guide*』の第 1 章「Getting Started」を参照してください。

アクセス コントロール リストの設定

ACL を使用すれば、WebNS Device Management ユーザ インターフェイスへのアクセスを、特定の IP アドレスまたはサブネットだけに制限することができます。ACL には、CSS のインターフェイスでパケットの通過 / 遮断を制御するネットワーク トラフィック フィルタ機能があります。ACL でルーティング対象ネットワーク プロトコルを、そのプロトコルのパケットが CSS を通過するときにフィルタリングされるように設定できます。

CSS のイーサネット管理ポートを使用して Device Management ソフトウェアにアクセスする場合には、ACL による制御は無効です。ACL でアクセスを制御するには、別のイーサネット ポートから Device Management ソフトウェアにアクセスする必要があります。

ACL は、ユーザ定義の句から構成されます。CSS では、これらの句を使用して各パケットの処理方法を決定します。各パケットを調べ、パケットが ACL の句に一致するかどうかに基づいて、そのパケットを転送またはブロックします。

注意　ACL は一種のファイアウォールとして機能し、セキュリティを確保します。ACL を有効にすると、ACL の permit 句で設定されていないトラフィックはすべて拒否されます。ACL を有効にする前に、まずトラフィックを許可する ACL を 1 つ設定することが非常に重要です。トラフィックを一切許可しないと、ネットワークに接続できなくなります。ただし接続が失われても、コンソール ポートには影響しません。

ACL の設定に応じて、permit all 句または deny all 句を設定することをお勧めします。たとえば、最初に permit all 句を設定した後、拒否するトラフィックだけを対象に deny 句を設定します。または、デフォルトの deny all 句を使用した後、許可するトラフィックだけを対象に permit 句を設定します。

ACL 句を定義して ACL オプションを設定する方法については、『*Cisco Content Services Switch Security Configuration Guide*』を参照してください。

ブラウザの設定

Device Management ソフトウェアにアクセスするには、使用する Web ブラウザで次の項目を有効にする必要があります。

- Cookie：Device Management ソフトウェアは、Cookie を使用して認証を行います。ブラウザで Cookie を有効にしないと、Device Management ページにアクセスできません。ログイン ページを使用してログインすると、Cookie が作成されます。Cookie は、現在のブラウザ セッションの間だけ有効です。Cookie が見つからないと、CSS はページへのアクセスをまったく許可しません。Cookie が見つかると、ユーザの権限が SuperUser であるか、または User であるかを判断します。すべてのページにアクセスできるのは、SuperUser 特権を持つユーザだけです。User 特権を持つユーザは、設定以外のページだけにアクセスできます。SuperUser 特権および User 特権を設定するには、**username** コマンドを使用します。「特権によるアクセス制限」を参照してください。
- JavaScript：Device Management ソフトウェアでは、ナビゲーション ツリーおよびオンライン ヘルプに JavaScript が必要です。

SSL セキュリティ証明書の表示とインストール

WebNS Device Management ユーザ インターフェイスと Web ブラウザとの間のデータ転送（パスワードを含む）を保護するために、通信を保護するための標準インターネット プロトコルである Secure Socket Layer（SSL）を提供しています。SSL では、証明書を使用した認証と公開鍵暗号を使って、クライアントと WebNS Device Management ユーザ インターフェイスとの暗号化通信を確立します。トラフィックは、CSS を設定または監視するユーザの識別（認証）、および認証後のデータの暗号化により保護されます。

CSS に常駐する HTTP Web サーバは、SSL を使用して、Web ブラウザと CSS との間の接続を保護します。SSL が有効になっている場合、Web ブラウザの各 Device Management フォームの一番下に「ロックされた状態の錠前」アイコン（または類似のアイコン）が表示されます。

WebNS Device Management ユーザ インターフェイスは、SSL バージョン 3.0 をサポートしています。また、SSL バージョン 2.0 の ClientHello メッセージを解釈し、受け入れます。したがって、SSL 2.0 と SSL 3.0 の両方をサポートするクライアントが CSS と通信できます。この場合、クライアントは、SSL 2.0 の ClientHello 内に SSL バージョン 3.0 を示し、SSL 3.0 に対応していることを WebNS Device Management ユーザ インターフェイスに通知します。WebNS Device Management ユーザ インターフェイスは、バージョン 3.0 の ServerHello メッセージを返します。

（注）　現在の市場では、SSL バージョン 2.0 だけをサポートするクライアントはほとんどありません。WebNS Device Management ユーザ インターフェイスは、バージョン 2.0 だけをサポートするクライアントとは通信できません。

Device Management ユーザ インターフェイスに最初にアクセスする際には、シスコが発行したセキュリティ証明書のインストールと確認を求める **Security Alert** メッセージ ボックスが表示されます。ユーザのセキュリティ要件に応じて、証明書をインストールして確認するか、**Security Alert** メッセージ ボックスをスキップして CSS の操作を継続するかを選択します。**Security Alert** メッセージ ボックスをスキップしても、Device Management ユーザ インターフェイス使用時の通信のセキュリティには影響しません。**Security Alert** メッセージ ボックスは、

証明書をインストールして確認するか、またはこのメッセージ ボックスを無効にするまで、Device Management ユーザ インターフェイスにアクセスするたびに表示されます。

SSL セキュリティ証明書をインストールして確認するには、次の操作を行います。

1. Web ブラウザの［アドレス］または［場所］フィールド（ブラウザによって異なります）に CSS の IP アドレスを入力します。WebNS Device Management ユーザ インターフェイスにアクセスするときに、安全な接続を行うには、URL に「s」を付ける必要があります（https://）。

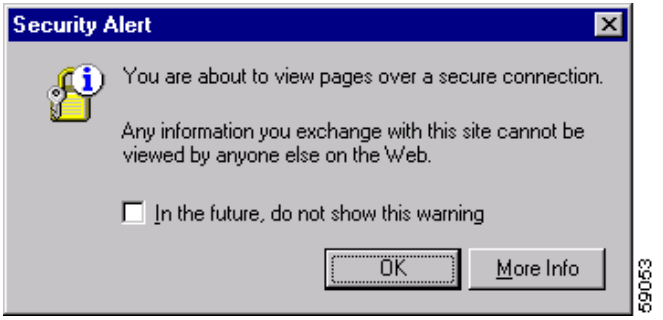
   例

   ```
   https://192.168.16.2
   ```

   （注）　WebNS Device Management ユーザ インターフェイス（WebNS バージョン 4.10 以前）へのブックマークとして、末尾にコロン（:）と TCP 8081 管理ポート番号を付加した IP アドレスを Web ブラウザに登録している場合、この要求は WebNS ソフトウェアによって拒否されます。ブラウザはページが表示できないことを通知します。

2. 最初の **Security Alert** メッセージ ボックスが表示され、保護された接続でページを表示しようとしていることが通知されます。これは、インターネット上の保護されたページに接続しようとするときに表示される Web ブラウザ標準のメッセージ ボックスです。

図 2-1　最初の Security Alert メッセージ ボックス

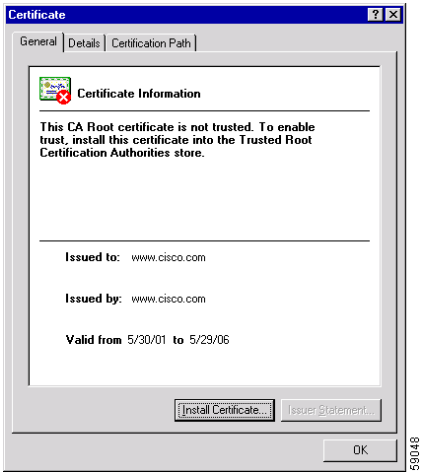


3. **OK** をクリックします。2 つ目の **Security Alert** メッセージ ボックスが表示されます。

図 2-2　　2 つ目の Security Alert メッセージ ボックス

4. **View Certificate** をクリックします。**Certificate** ダイアログボックスが表示されます。

図 2-3　　Certificate ダイアログボックスの General プロパティ タブ



5. **Install Certificate** をクリックします。**Certificate Manager Import Wizard** が表示されます。

図 2-4　Certificate Manager Import Wizard

6. **Next** をクリックします。表示される指示に従ってウィザードを進め、certificate store（証明書が格納される場所）を選択して、証明書をインポートします。ウィザードを使用して、シスコシステムズが作成した証明書をコンピュータの certificate store にコピーします。
7. 証明書のインポートが完了すると、図 2-3 に示す **Certificate** ダイアログボックスに戻ります。

8. **OK** をクリックして、**Security Alert** メッセージ ボックスに戻ります。リストの最初の項目が変わり、セキュリティ証明書が信頼できる発行元から発行されたものであることが示されています。

図 2-5　証明書情報を示す Security Alert メッセージ ボックス

9. **View Certificate** をクリックします。**Certificate** ダイアログボックスが開き、インポートした証明書の詳細が表示されます。

図 2-6　証明書情報を示す Certificate ダイアログボックス

10. **OK** をクリックします。Device Management ユーザ インターフェイスのログイン フォームが表示されます。

図 2-7 は、Device Management のログイン フォームです。Device Management ソフトウェアへのログインについては、第 3 章「Device Management ユーザ インターフェイスの使用」の「WebNS Device Management ユーザ インターフェイスへのアクセスとログイン」を参照してください。

図 2-7　WebNS Device Management ユーザ インターフェイスのログイン フォーム