



Service Monitor を使用する前に

ここでは、次の内容について説明します。

- 「[セキュリティの設定](#)」(P.3-1)
- 「[Service Monitor の設定](#)」(P.3-3)

セキュリティの設定

Service Monitor は Common Services を使用して設定するセキュリティに依存しています。設定するには、以下のトピックを参照してください。

- 「[ユーザの設定 \(ACS および非 ACS\)](#)」(P.3-1)
- 「[ブラウザとサーバ間の SSL のイネーブル化](#)」(P.3-2)

詳細については、Common Services オンラインヘルプの「[Setting Up Security](#)」を参照してください。

ユーザの設定 (ACS および非 ACS)

Service Monitor ユーザが何を表示および実行できるかは、ユーザ ロールによって決まります。Service Monitor では、ユーザ認証に次の 2 つの Common Services モードがサポートされています。

- 非 ACS : 認証および認可を提供するには、サポートされているログイン モジュールを選択します。Common Services はデフォルトで Local ログイン モジュールを使用して、ロールとそれらのロールに関連付けられた特権を割り当てます。詳細については、「[Common Services Local ログイン モジュールを使用したユーザの設定](#)」(P.3-2) を参照してください。
- ACS : ACS モードでは、認証および認可は Cisco Secure Access Control Server (ACS) によって実現されます。Cisco Secure ACS は、ロールに関連付けられた特権を特定し、ユーザが特定のタスクだけを実行するようにするものです。

ACS モードを使用するには、Cisco Secure ACS がネットワークにインストールされ、Service Monitor が Cisco Secure ACS に登録されている必要があります。詳細については、「[Cisco Secure ACS によるセキュリティの設定](#)」(P.C-1) を参照してください。



(注) Operations Manager が認証および認可に ACS モードを使用する場合に、同一システム上で Service Monitor が実行されているとき、Service Monitor も ACS モードを使用する必要があります。そうでなければ、Service Monitor ユーザはどのような権限も与えられません。

Common Services Local ログイン モジュールを使用したユーザの設定

-
- ステップ 1 [Administration] > [Server Administration (Common Services)] > [Security] > [Local User Setup] の順に選択します。[Local User Setup] ページが表示されます。
 - ステップ 2 [Add] をクリックします。[User Information] ページが表示されます。
 - ステップ 3 ユーザ情報を入力します。
 - ステップ 4 [OK] をクリックします。
-

各ユーザ ロールと Service Monitor のタスクとの関連付けを確認するには、Permission Report を表示します。

-
- ステップ 1 [Administration] > [Server Administration (Common Services)] > [Reports] > [Permission Report] > [Generate Report] の順に選択します。新しいウィンドウが開きます。
 - ステップ 2 [Go to] リストから [Cisco Unified Service Monitor] を選択し、Service Monitor のタスク一覧を表示します。
-

ブラウザとサーバ間の SSL のイネーブル化

Service Monitor を起動すると、ログイン ページは常にセキュア モードで開かれ、クライアント ブラウザと Service Monitor サーバとの間で安全に通信できます。セキュア モードでは、ブラウザとサーバ間の転送チャンネルを暗号化するのに、Secure Socket Layer (SSL) が使用されます。Service Monitor 全体でセキュア モードを使用するには、Common Services の SSL をイネーブルにします。



-
- (注) Service Monitor と Operations Manager がインストールされているシステムで SSL をイネーブルにすると、SSL は両方のアプリケーションに対してイネーブルにされます。
-

-
- ステップ 1 [Administration] > [Server Administration (Common Services)] > [Security] > [Browser-Server Security Mode Setup] の順に選択します。[Browser-Server Security Mode Setup] ダイアログ ボックスが表示されます。
 - ステップ 2 [Enable] オプション ボタンを選択します。
 - ステップ 3 [Apply] をクリックします。
 - ステップ 4 Service Monitor をログアウトし、すべてのブラウザ セッションを終了します。
 - ステップ 5 コマンド ラインから以下のコマンドを入力して、デーモン マネージャを再起動します。

```
net stop crmdmgtd
net start crmdmgtd
```

- ステップ 6 ブラウザを再起動し、以下の安全な URL を使用して、Service Monitor を再起動します。

```
https://<servername>:<https port>
```



-
- (注) ブラウザで「http://<servername>:1741」と入力した場合に SSL がイネーブルにされていると、セキュア URL に転送されます。
-

Service Monitor の設定

Service Monitor CDR Call Report は、システム定義データとユーザ定義ダイヤルプランに依存しています。ダイヤルプランおよびコールカテゴリを定義するには、『*User Guide for Cisco Unified Service Monitor*』の「Configuring Call Classification」を参照してください。



(注)

Service Monitor データの長期レポートのため Service Statistics Manager を使用する場合、以下のことに留意します。

- Service Statistics Manager は Service Monitor に依存してコールデータを分類しています。
- Service Monitor のコール分類の設定は、Service Statistics Manager 1.3 のインストールまたはアップグレードインストールの前に実行します。

Service Monitor を設定するには、『*User Guide for Cisco Unified Service Monitor*』の付録「Configuration Checklists and Tips」を参照してください。

