



インストール後のサーバタスク

次のトピックは、Security Manager またはその関連アプリケーションをサーバー上にインストールしてから実行すべきタスクです。

- [すぐに実行すべきサーバタスク \(1 ページ\)](#)
- [必要なプロセスが動作しているかどうかの確認 \(2 ページ\)](#)
- [MRF を使用した Security Manager プロセスのヒープサイズの設定 \(3 ページ\)](#)
- [現行のサーバセキュリティに関するベストプラクティス \(9 ページ\)](#)
- [インストールまたはアップグレードの確認 \(10 ページ\)](#)
- [\(任意\) Security Manager サーバーのホスト名の変更 \(10 ページ\)](#)
- [CSM ログビューアの確認と検証 \(11 ページ\)](#)
- [関連情報 \(12 ページ\)](#)

すぐに実行すべきサーバタスク

インストール直後に次のタスクを実行してください。

✓	タスク
□	<p>1. アンチウイルススキャナと同等の製品を再イネーブルまたは再インストールします。アンチウイルスツールなどのサーバーセキュリティソフトウェアをアンインストールまたは一時的にディセーブルにした場合は、今すぐ、そのソフトウェアを再インストールまたは再起動して、必要に応じてサーバーを再起動します。Security Manager がサーバーにインストールされている場合は、NMSROOT ディレクトリとイベントフォルダをスキャンから除外してください。</p> <p>(注) アンチウイルスソフトウェアが原因で Security Manager サーバーの効率性や応答性が損なわれていることが判明した場合は、アンチウイルスソフトウェアのマニュアルで推奨設定を確認してください。</p>
□	<p>1. インストール中にディセーブルにしたサービスとサーバプロセスを再イネーブルします。IIS は再イネーブルしないでください。</p>

✓	タスク
☐	1. サーバ上で、自己署名証明書を信頼できる証明書のリストに追加します。手順については、ブラウザのマニュアルを参照してください。
☐	1. Cisco.com 上で Security Manager とその関連アプリケーションのアップデートをチェックします。アップデートが入手可能なことがわかった場合は、組織やネットワークに関連するアップデートをインストールします。

必要なプロセスが動作しているかどうかの確認

Windows のコマンドプロンプト ウィンドウから **pdshow** コマンドを実行して、インストールする Cisco サーバアプリケーションに必要なプロセスのすべてが正しく動作していることを確認できます。プロセス要件はアプリケーションによって異なります。



ヒント **pdshow** の詳細については、Common Services のマニュアルを参照してください。

表 7-1 を使用して、どのアプリケーションにどのプロセスが必要かを確認してください。

表 1: アプリケーション プロセス要件

アプリケーション	必要な Daemon Manager プロセス
Common Services	Apache CmfDbEngine CmfDbMonitor CMFOGSServer CSRegistryServer DCRServer diskWatcher EDS EDS-GCF ESS EssMonitor jrm LicenseServer Proxy Tomcat TomcatMonitor NameServer NameServiceMonitor EventFramework

アプリケーション	必要な Daemon Manager プロセス
Cisco Security Manager	AthenaOGSServer ccrWrapper CsmReportServer rptDbEngine rptDbMonitor VmsBackendServer vmsDbEngine vmsDbMonitor VmsEventServer CsmHPMServer ProcessManager

MRF を使用した Security Manager プロセスのヒープ サイズの設定

Security Manager 4.1 で導入された機能である Memory Reservation Framework (MRF) は、Cisco Security Manager 管理者に、主要プロセスのヒープ サイズを変更する機能を提供します。それにより、サーバのパフォーマンスを向上させることができます。MRF を使用すると、プロセスは、サーバに搭載された RAM の容量に基づいてヒープ サイズを調整できるようになります。

MRF を使用して設定可能な Security Manager プロセスを表 7-2 に示します。

表 2: MRF を使用して設定可能な Security Manager プロセス

プロセス	pdshow で表示される名前	説明
バックエンドプロセス	VmsBackendServer	デバイス検出操作と展開操作を実行します。
Tomcat	Tomcat	ポリシーなどの編集および検証を行うためのアプリケーションをホストします。
レポート サーバ	CsmReportServer	レポート データを生成します。
イベント サーバ	VmsEventServer	デバイスから送信されているイベントを収集します。



(注) 設定の負荷に基づいて、パフォーマンス向上のために、環境に応じた Tomcat およびバックエンドサーバーのヒープサイズを常に特定することを推奨します。



(注) HPM (Health and Performance Monitor) サーバの MRF 設定はありません。



(注) pdshow コマンドの詳細については、前述の [必要なプロセスが動作しているかどうかの確認 \(2 ページ\)](#) および Common Services のマニュアルを参照してください。

デフォルト設定

表 3 : Security Manager プロセスに対して事前に設定されるデフォルトのヒープ サイズ に示されているプロセス (MRF を使用して設定可能な Security Manager プロセス) は、ヒープサイズに対してデフォルト値が事前に設定されています。表 3 : Security Manager プロセスに対して事前に設定されるデフォルトのヒープ サイズ には、MRF を使用して設定可能な Security Manager プロセスごとに、サーバーで使用可能なさまざまな RAM 容量に応じたデフォルトの最小および最大ヒープサイズが MB 単位で示されています。

表 3 : Security Manager プロセスに対して事前に設定されるデフォルトのヒープ サイズ

サーバ上の物理 RAM (GB)	VmsBackendServer	Tomcat	CsmReportServer	VmsEventServer	CsmHPMServer
< 8	1024、2048	512、1024	1024、1024	1024、2048	512、1024
8	1024、3072	1024、2048	1024、1024	1024、3072	512、1024
12	2048、4096	2048、3072	1024、2048	2048、4096	512、1024
16	2048、4096	2048、4096	1024、4096	4096、4096	512、1024
24	4096、8192	4096、4096	1024、4096	4096、8192	512、1024
>= 28	8192、8192	4096、4096	1024、4096	4096、8192	512、1024

一定量の RAM がオペレーティングシステム用とその他のプロセス用に予約されていますが、この表には示されていません。たとえば、表 3 : Security Manager プロセスに対して事前に設定されるデフォルトのヒープ サイズ の RAM が 16 GB の場合について考えてみます。4 つすべてのプロセスに対する最大ヒープ サイズの合計は、 $(4096 + 4096 + 1024 + 4096) = 13312$ MB、つまり 13 GB です。残りの 3 GB の RAM がオペレーティングシステム用とその他のプロセス用に使用できます。



- (注) 導入モデルガイドを参照し、環境に応じてそれぞれの RAM を使用してください。メモリ関連の遅延が観察された場合は、上記のパラメータを微調整してパフォーマンスを向上させることができます。

コンフィギュレーション コマンド

MRF では、1つのコマンドと一連のサブコマンドが提供され、Security Manager サーバプロセスのヒープサイズの読み取りや変更に使われます。各プロセスの最小および最大ヒープサイズは、`mrf` コマンドを使用して設定できます。次のようにこのコマンドを実行すると、このコマンドの使用方法に関する情報が表示されます。

```
> mrf
mrf help          Prints this message.
mrf backup        Backup existing configuration
mrf revert        Restores backed up configuration
mrf set_heap_params process X-Y [min],[max]
                  Sets minimum and maximum heap sizes
                  process -> process name
                  X-Y -> Memory Range in MB to which heap sizes apply
                  [min],[max] -> minimum and maximum heap sizes in MB. These are optional but
                  atleast one should be specified.
mrf get_heap_params process [memory]
                  Prints minimum and maximum heap sizes in MB
                  process -> process name
                  [memory] -> memory size in MB for which heap sizes are to be printed. If not
                  specified heap sizes are to be printed for current system memory.
```

`mrf` コマンドを実行する際は、有効なプロセス名のみを使用してください。無効なプロセス名を指定しても、エラーは発生しません。有効なプロセス名は、表 7-2 に示されています。プロセス名は大文字と小文字が区別されます。

プロセスに対するヒープサイズの設定

Security Manager プロセスに対するヒープサイズの設定は、次の主要な 3 つの手順で構成されます。

1. 既存の設定の保存
2. 既存の設定の読み取り
3. 設定の変更 (6 ページ)

1. 既存の設定の保存

プロセスのヒープサイズの設定は、Security Manager のパフォーマンスに影響する可能性のある重要な手順であるため、アプリケーションの専門家の指示の下でのみ実施することを推奨します。

2. 既存の設定の読み取り

また、予防措置として、プロセスの既存のメモリ設定を変更する前に、それらを保存しておくことも推奨します。MRF では、2 種類の保存方法が用意されています。

1. 1 つ目の方法は、設定変更をテストする場合に使用できます。この場合、次に示す 2 つのコマンドを使用して、それぞれ、古い設定を保存すること、および新しい変更を古い設定に戻すことができます。

```
mrf backup
mrf revert
```

2. 2 つ目の方法は、新しい設定をしばらく使用した後に、古い値に戻す場合に役立ちます。これには 2 つの方法があり、次のうちのいずれか一方を使用できます。
 1. 設定変更を行った後に **mrf backup** を実行していなければ、**mrf revert** を実行できます。
 2. Cisco Security Manager サーバのバックアップを取ってから、設定変更を行います。変更を元に戻すときは、バックアップを復元します。この場合、バックアップ後に行われたデータの変更は失われます。

2. 既存の設定の読み取り

データの保存が完了しましたので、次のコマンドを使用して、プロセスの既存の値を問い合わせることができます。

```
mrf get_heap_params [process name] [memory]
```

このコマンドで **memory** 値を指定しなければ、現在の RAM サイズが使用されます。一般に関心があるのは、現在の RAM サイズに対する情報です。パラメータ [process name] は、表 7-2 に示されている値のいずれかになります。プロセス名は大文字と小文字が区別されます。

このコマンドの出力は、次のように表示されます。値の単位は MB です。

```
Minimum Heap Size = 1024
Maximum Heap Size = 2048
```

3. 設定の変更

現在の設定を確認した後、この項に記載された説明に従って設定を変更することができます。

ヒープサイズを設定するには、次のコマンドを使用します。

```
mrf set_heap_params [process name] [X-Y] [min] [,max]
```

パラメータ [process name] は、表 7-2 に示されているプロセスのいずれかにすることができます。プロセス名は大文字と小文字が区別されます。

このコマンドを実行した後、Security Manager サーバを再起動して変更を反映させる必要があります。



(注) **mrf set_heap_params** を使用して行われた変更は、ヒープパラメータの変更前に取られたバックアップが復元されると、失われる可能性があります。この場合、新しい値を保持する必要があるときは、次の手順を実行できます。

1. **mrf backup** を実行します。
2. アプリケーションの復元を行います。
3. **mrf revert** を実行します。

このコマンドでは、次の構文が使用されます。

mrf set_heap_params [*process name*] [*X-Y*] [*min*],[*max*]

最小および最大ヒープサイズを設定します。

[*X-Y*] : ヒープサイズを適用するメモリ範囲 (単位は MB)

[*min*],[*max*] : 最小および最大ヒープサイズ (単位は MB)。これらはオプションですが、少なくとも 1 つは指定する必要があります。

パラメータ [*process name*] は、表 7-2 に示されている値のいずれかになります。プロセス名は大文字と小文字が区別されます。

設定変更の例

次に、ヒープサイズの設定変更の例を示します。

- **mrf set_heap_params Tomcat 7372-8192 2048,4096**

RAM サイズが 7372 ~ 8192 MB の範囲内のときの Tomcat プロセスに対して最小および最大ヒープサイズをそれぞれ 2048 MB と 4096 MB に設定します。

- **mrf set_heap_params Tomcat 7372-8192 2048**

RAM サイズが 7372 ~ 8192 MB の範囲内のときの Tomcat プロセスに対して最小ヒープサイズを 2048 MB に設定します。

- **mrf set_heap_params Tomcat 7372-8192,4096**

RAM サイズが 7372 ~ 8192 MB の範囲内のときの Tomcat プロセスに対して最大ヒープサイズを 4096 MB に設定します。

- **mrf set_heap_params Tomcat 8080-8080 2048,4096**

RAM サイズが 8080 MB ときの Tomcat プロセスに対して最小および最大ヒープサイズをそれぞれ 2048 MB と 4096 MB に設定します。**getramsize** コマンドを実行すると、既存の RAM サイズを MB 単位で取得できます。

設定変更の確認

ヒープパラメータを設定した後、`mrf get_heap_params` コマンドを実行して変更を確認できます。

プロセスに対するヒープサイズの設定の要約

ここで説明した、Security Manager プロセスに対するヒープサイズの設定のための3つの主要手順は、次のように要約されます。これらのコマンドは、実行順で示されています。

```
mrf backup
mrf get_heap_params process
mrf set_heap_params Tomcat 7372-8192 2048,4096
mrf revert #if required to revert changes
```

ユーザがヒープサイズの再設定を必要とする一般的なシナリオ

シナリオ 1

ある Security Manager 4.0 ユーザが、バックエンドプロセス (VmsBackendServer) に対して 4 GB の最大ヒープサイズを使用しています。これは、8 GB RAM に対して Security Manager 4.1 で割り当てられるデフォルトの最大ヒープサイズである 3 GB を超えています。このシナリオのユーザは、バックエンドプロセスのヒープサイズを 4 GB に再設定する必要があります。イベント管理 (Event Server プロセス (VmsEventServer) を使用) がイネーブルになっていなければ、そうすることができます。

シナリオ 2

Security Manager が設定専用モードで使用されています (イベント管理とレポートがディセーブルになっている)。このシナリオでは、バックエンドプロセスと Tomcat のヒープサイズを増やすことができます。

シナリオ 3

Security Manager が設定専用モードで使用されており (イベント管理とレポートがディセーブルになっている)、イベント管理をイネーブルにする必要があります。このシナリオでは、すべての Security Manager プロセスのヒープサイズの合計がサーバで使用可能な RAM サイズを超えないように、バックエンドプロセスと Tomcat のヒープサイズを減らしてから、イベント管理をイネーブルにする必要があります。

シナリオ 4

イベント管理とバックエンドプロセスは、メモリを大量に消費するため、より多くの RAM 割り当てを必要とします。(イベント管理が使用されない場合は、その分の RAM がバックエンドプロセスに割り当てられるように、バックエンドプロセスの最大ヒープサイズを増やすことができます)。

現行のサーバセキュリティに関するベストプラクティス

システムの最小限のセキュアコンポーネントによってシステムの安全性が定義されます。下のチェックリスト内のステップは、Security Manager のインストール後のサーバーとその OS のセキュリティ保護に役立ちます。

✓	タスク
□	<p>1. サーバセキュリティを定期的にモニタします。 システム アクティビティを記録して確認します。Microsoft Security Configuration Tool Set (MSCTS) や Fport などのセキュリティツールを使用して、サーバのセキュリティ設定を定期的に確認します。Security Manager サーバー上にインストールされたスタンドアロンバージョンの Cisco Security Agent に関するログファイルを確認します。</p> <p>ヒント MSCTS は Microsoft の Web サイトから、Fport は Foundstone/McAfee の Web サイトから入手できます。</p>
□	<p>1. サーバへの物理アクセスを制限します。 サーバに取り外し可能なメディアドライブが接続されている場合は、ハードドライブから起動するようにサーバを設定します。誰かが取り外し可能なメディアドライブからサーバを起動した場合に、データが侵害されるおそれがあります。通常は、システム BIOS 内で起動順序を設定できます。BIOS が強力なパスワードで保護されていることを確認します。</p>
□	<p>1. リモートアクセス ツールやリモート管理ツールをサーバ上にインストールしないでください。 このようなツールは、サーバへのエントリ ポイントを提供するセキュリティ リスクになります。</p>
□	<p>1. サーバ上で自動的かつ継続的に動作するようにウイルス スキャン アプリケーションを設定します。 ウイルススキャンアプリケーションは、トロイの木馬アプリケーションのサーバへの侵入を阻止できます。ウイルス署名を定期的に更新します。</p>
□	<p>1. サーバデータベースを頻繁にバックアップします。 すべてのバックアップをアクセスが制限されたセキュアな場所に保管します。</p> <p>(注) ハードディスクに常に十分な空き領域を確保するために、ログ/データベースのバックアップファイルを定期的に削除してください。10GB 以上のハードディスク空き容量を確保することをお勧めします。</p>
□	<p>1. Security Manager サーバーを定期的にバックアップしてください。 定期的なバックアップが行われていない場合、または Security Manager インストールに対して複数の変更が行われている場合は、Windows アップデートを実行する前に Security Manager サーバーをバックアップします。</p>

インストールまたはアップグレードの確認

Common Services を使用して、Security Manager のインストールまたはアップグレードが成功したかどうかを確認できます。Security Manager インターフェイスが表示されない、または、正しく表示されないことが原因でインストールを確認する場合は、XREF を参照してください。

ステップ 1 クライアントシステム上のブラウザを使用して、次のいずれかを使用している Security Manager サーバーにログインします。

- HTTP サービスの場合 : **http://<server_name>:1741**
- SSL サービスの場合 : **https://<server_name>:443**

サポートされているブラウザとブラウザのバージョンを確認するには、[クライアントの要件](#)を参照してください。

ステップ 2 Cisco Security Management Suite ページから、[サーバー管理 (Server Administration)] パネルをクリックして [サーバー (Server)] > [管理 (Admin)] ページで Common Services を開きます。

ステップ 3 [プロセス管理 (Process Management)] ページを表示するには、[プロセス (Processes)] をクリックします。

結果のリストには、すべてのサーバプロセスの名前とプロセスごとの動作ステータスの説明が表示されません。次のプロセスが正常に動作している必要があります。

- vmsDbEngine
- vmsDbMonitor
- EDS

(任意) Security Manager サーバーのホスト名の変更

Security Manager サーバーのホスト名を変更する必要がある場合は、次の手順に従います。

ステップ 1 OS でホスト名を変更します。

- [コンピュータ (Computer)] を右クリックして [プロパティ (Properties)] を選択するか、[コントロールパネル (Control Panel)] を開いて [システム (System)] を選択します。
- [コンピュータ名、ドメイン、ワークグループ設定 (Computer name, domain, and workgroup settings)] の下で、[設定の変更 (Change settings)] をクリックします。
- [変更 (Change)] をクリックして、[コンピュータ名 (Computer Name)] (ホスト名) を変更します。
- コンピュータを再起動します。

ステップ2 コマンドウィンドウで **net stop crmdmgtd** と入力して、Security Manager Daemon Manager を停止します。

ステップ3 コマンドウィンドウで次のコマンドを実行して、Security Manager Server ホスト名変更スクリプトを実行します。

例：

```
NMSROOT\bin\perl NMSROOT\bin\hostnamechange.pl
```

このコマンド内の NMSROOT は、Security Manager のインストール ディレクトリへのパスです。

ヒント **hostnamechange.pl** は、OS でホスト名が変更された後、Common Services に関連したディレクトリ、ファイル、データベースエントリ、およびレジストリエントリにホスト名の変更を反映するユーティリティです。

ステップ4 コンピュータを再起動します。

(注) このステップでは、コンピュータを再起動する必要があります。Security Manager Daemon Manager の再起動では不十分です。

CSM ログビューアの確認と検証

Cisco Security Manager 4.24 以降では、CSM ソフトウェアのインストールまたはアップグレード後に、CSM ログビューアを使用して、サポートされているオプションを確認および検証できます。

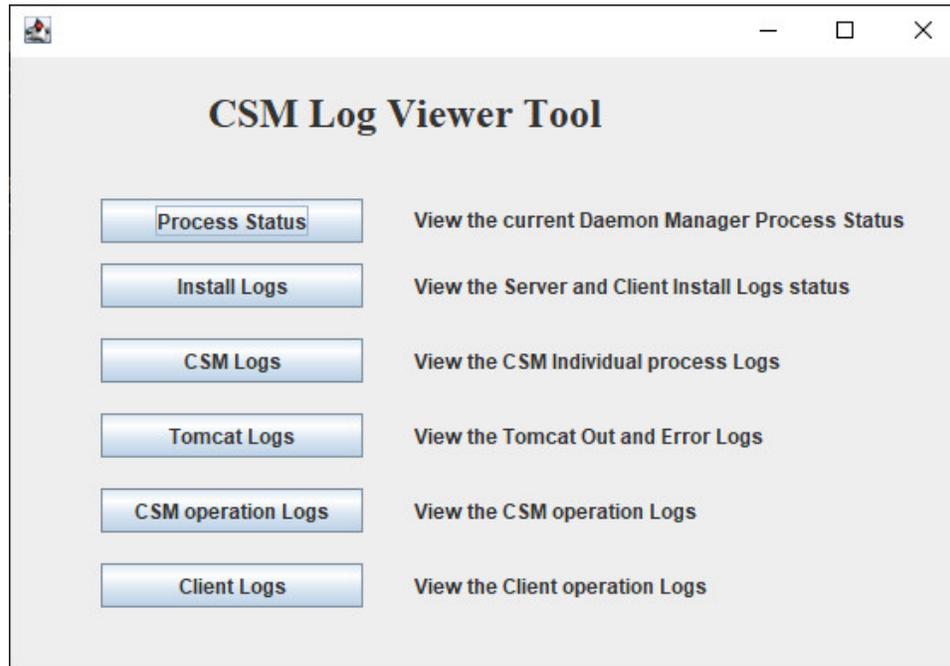
ステップ1 次の場所に移動します。 **C:\ProgramFiles(x86)\CSCOpX\bin**

ステップ2 バッチファイル **CsmLogViewer** を実行します。

次のサポートされているすべてのオプションを使用して、CSM ログビューアツールを表示できます。

- Process Status
- [インストールログ (Install Logs)]
- [CSMログ (CSM Logs)]
- [Tomcatログ (Tomcat Logs)]
- [CSM操作ログ (CSM operation Logs)]
- [クライアントログ (Client Logs)]

図 1: [CSMログビューア (CSM Log Viewer)]



ステップ3 [CSMログビューア (CSM Log Viewer)] ドロップダウンボックスから、情報またはエラーを確認し、データを検証するログを選択します。

関連情報

目的	操作手順
基本の理解	Security Manager を起動すると表示される対話形式の <i>JumpStart</i> ガイドを参照してください。
製品の迅速な稼働	オンラインヘルプの「Getting Started with Security Manager」トピック [英語] を参照するか、『 <i>User Guide for Cisco Security Manager</i> 』の第1章 [英語] を参照してください。
製品設定の実施	オンラインヘルプの「Completing the Initial Security Manager Configuration」トピック [英語] を参照するか、『 <i>User Guide for Cisco Security Manager</i> 』の第1章 [英語] を参照してください。

目的	操作手順
ユーザの認証と認可の管理	次のトピックを参照してください。 <ul style="list-style-type: none">• ユーザ権限• Security Manager と Cisco Secure ACS の結合
デバイスのブート	オンラインヘルプの「Preparing Devices for Management」トピック [英語] を参照するか、 http://www.cisco.com/it/enterprise/security/security-manager/products/userguide.html から入手可能な『 <i>User Guide for Cisco Security Manager 4.27</i> 』の第2章 [英語] を参照してください。

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。