Security Manager の管理設定値の設定

Security Manager には、数多くのシステム機能に対してデフォルト設定が用意されています。組織のニーズに合わない場合は、これらの設定を変更できます。これらの設定を表示および変更するには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択します。次に、ウィンドウの左側にあるコンテンツテーブルから項目を選択して、その項目に関するデフォルト設定を表示できます。

ほとんどのページで、設定を変更する場合は、[Save] をクリックして変更を保存する必要があります。間違えた場合は、[リセット（Reset）] をクリックして、以前に保存した値に戻すことができます。また、[デフォルトを復元（Restore Defaults）] をクリックして、Security Manager のデフォルト設定に戻すこともできます。

[Security Manager管理（Security Manager Administration）] ウィンドウには、システムのデフォルトが含まれたページ以外に、システム管理アクティビティに関連する項目（別のユーザの作業を引き継ぐ、サーバーセキュリティ作業を実行するために Common Services 内のページにアクセスするなど）が含まれています。

次の項では、[Security Manager Administration] ウィンドウで使用できる各ページ上で使用可能な設定とアクションについて説明します。

[API設定（API Settings）] ページ

Cisco Security Manager の [API設定（API Settings）] ページでは、API サービスを有効または無効にして、サービスの設定を変更できます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [API] を選択します。

フィールド リファレンス

表 1 : [API設定（API Settings）] ページ

要素	説明
API サービスの有効化	API サービスを有効にするか無効にするかを指定します。

要素	説明
結果セットのページサイズ（Result Set Page Size）	許容値は 100 から 1000 までです。
アクティブクライアントセッション数（Active client sessions）	許容値は 1 から 10 までです。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[自動リンク設定（AutoL-ink Settings）] ページ

Security Manager のマップ ビューでは、VPN およびレイヤ 3 ネットワーク トポロジのグラフィカル ビューが提供されます。管理対象デバイスを表すデバイス ノード、および管理対象外のオブジェクト（デバイス、クラウド、ネットワークなど）を表すマップ オブジェクトを使用して、ネットワークの調査に使用するトポロジマップを作成できます。自動リンク設定を使用すると、5つのプライベート ネットワークまたは予約済みネットワークのいずれかをマップ ビューから除外できます。たとえば、Security Manager を使用して実行する管理タスクとは関係ないテスト ネットワークを除外する必要がある場合があります。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [自動リンク（AutoLink）] を選択します。

関連項目

- マップにおけるレイヤ 3 リンクの追加と管理
- マップでのネットワークの表示

フィールド リファレンス

表 2 : [AutoLink] ページ

要素	説明
Enable AutoLink for 10.0.0.0/8 Enable AutoLink for 172.16.0.0/12 Enable AutoLink for 192.168.0.0/16	作成したマップで、これらのプライベート ネットワークを自動的に含めるか、または除外する（選択解除する）かを指定します。

要素	説明
Enable AutoLink for 127.0.0.0/8	作成したマップで、このループバック ネットワークを自動的に含めるか、または除外する（選択解除する）かを指定します。
Enable AutoLink for 224.0.0.0/4	作成したマップで、マルチキャスト ネットワークを自動的に含めるか、または除外する（選択解除する）かを指定します。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[ACLヒットカウント設定（ACL Hit Count Settings）] ページ

Security Manager の [ACLヒットカウント設定（ACL Hit Count Settings）] ページでは、ヒットカウントの設定を構成および変更できます。この機能は、ASA および ASASM デバイスの Security Manager バージョン 4.9 以降で使用できます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Managerの管理（Cisco Security Manager Administration）] をクリックし、コンテンツテーブルから [ACLヒットカウント設定（ACL Hit Count Settings）] を選択します。

フィールド リファレンス

表 *3:* ヒットカウント設定

要素	説明
[ヒットカウント履歴の持続制限（ACE単位）（Hit Count History Persist Limit (per ACE)）]	[ヒットカウント履歴の持続制限（ACE単位）（Hit Count History Persist Limit (per ACE)）] は、データベース内の特定の ACE に関して保存できるヒットカウント履歴の詳細情報に対する制限です。デフォルト値は 5 で、入力可能な最大値は 10 です。
[消去スケジューラの処理時間（Purge Scheduler Process Time）]	[消去スケジューラの処理時間（Purge Scheduler Process Time）] は、ヒットカウントスケジューラによって、毎日指定された時刻にヒットカウント消去ジョブをスケジュールするために使用されます。ドロップダウンリストから時刻を選択します。デフォルトは [12 AM] です。

（注） 画面間を移動した後に ACL ポリシーページに移動すると、すべての ACL ルールについて、[HitCount] および [LastHitTime] の値にそれぞれ [0] および [なし（Never）] が表示されます。実際の [HitCount] および [LastHitTime] の値を取得するには、ACL ポリシーページの [ヒットカウントの更新（Refresh Hit Count）] ボタンをクリックします。値はデータベースから取得され、すべての ACL ルールに表示されます。

[CCO設定（CCO Settings）] ページ

[CCO設定（CCO Settings）] ページを使用して、Cisco.com への接続に使用する設定を構成します。

証明書の信頼管理にも [CCO設定（CCO Settings）] ページを使用します（Security Manager は、HTTPS 経由で Cisco.com から ASA イメージをダウンロードし、信頼を確立するために証明書を使用します）。[Image Manager] ページの証明書信頼管理機能は、Security Manager 4.4 の新機能です。この機能は、ASA イメージのダウンロードに向けた Cisco.com 証明書の処理を改善するのに役立ちます。

- この機能を使用して証明書を表示できます。証明書を受け入れるかどうか慎重に検討してください。
- 証明書を受け入れると、証明書は Security Manager サーバーに保存されます。
- [Image Manager] ページの概要テーブルにすべての証明書が表示され、そのテーブルを使用して証明書を表示または削除できます。

ヒント 下のテーブルの [証明書の取得（Retrieve Certificate）] を必ず確認してください。

証明書信頼管理機能の詳細については、証明書信頼管理を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [CCO設定（CCO Settings）] を選択します。

フィールド リファレンス

表 *4 : [CCO*設定（*CCO Settings*）*]* ページ

要素	説明
[IPS更新設定を使用（Use IPS Updates Settings）]	オンにすると、このページの他の設定が無効になり、デフォルトが優先されるようになります（[IPSの更新（IPS Updates）] ページの Cisco.com ログイン情報が適用されます）。 **注意** オンにした場合、[IPSの更新（IPS Updates）] ページの Cisco.com ログイン情報が正しく設定されていることを確認してください。ページ上の [更新元：（Update From:）] のデフォルト値は [ローカルサーバー（Local Server）] です。証明書の設定を表示するには、[Cisco.com] を選択する必要があります。証明書の設定が不適切または不完全な場合、Cisco.com への接続が妨げられ、このエリアでの Cisco.com 関連のすべての操作が失敗します。
ユーザー名	Security Manager が Cisco.com にログインするときに使用するユーザー名。
パスワード 確認（Confirm）	ユーザー名のパスワード。両方のフィールドにパスワードを入力します。
プロキシ サーバーの設定	
[プロキシの有効化（Enable Proxy）]	Image Manager が Web プロキシサーバー経由で Cisco.com に接続できるようにします。[プロキシの有効化（Enable Proxy）] を選択すると、他のプロキシフィールド（[IP] または [ホスト名（Hostname）]、[ポート（Port）]、[ユーザー名（Username）]、および[パスワード（Password）] など）が有効になり、Web プロキシへの接続に使用されます。
テスト接続（Test Connection）	Cisco.com の接続とログイン情報をテストするために使用されます。
証明書	

要素	説明
[連絡先URL（Contact URL）]	• 選択すると、[イメージメタデータロケータ（Image Meta-data Locator）] が使用されます。これは、イメージに関するメタデータ情報の取得に使用される Cisco.com の URL です。メタデータ情報は、特定の製品に該当するイメージ、名前、サイズ、チェックサム、および各イメージをダウンロードする URL で構成されます。 • 選択すると [その他（Other）] が使用されます。任意の有効な HTTPS URL を入力できます。この URL は、主に、イメージに関するメタデータ情報から取得したイメージをダウンロードするための HTTPS URL を対象としています。この URL は、前の段落で説明したイメージメタデータロケータの URL とは異なる場合があります。証明書も異なる場合があります。 **注意** [その他（Other）] を選択した場合は、明示的に "https://dl.cisco.com" を追加する必要があります（引用符は不要）。[その他（Other）] ボタンの隣のテキストフィールドに入力します。これを追加しないと、Cisco.com に接続できなくなり、このエリアでの Cisco.com 関連のすべての操作が失敗します。

要素	説明
[証明書の取得（Retrieve Certificate）]	選択した [連絡先URL（Contact URL）] に接続して証明書を取得するために使用されます。証明書を取得すると、[証明書の検証（Certificate Verification）] ダイアログが開きます。証明書の簡単な概要、つまり、証明書の発行対象、発行者、証明書の有効期間が表示されます。さらに、次の選択肢が表示されます。 • [証明書の表示（View Certificate）]：証明書ビューアを開いて、証明書のすべての詳細（認証局、バージョン、シリアル番号、サムプリント、その他の詳細）を表示できます。ルート発行認証局までの完全な証明書チェーン情報が表示されます。 • [承認（Accept）]：証明書を承認して、Cisco Security Manager に追加します。 • [拒否（Reject）]：証明書を拒否します。アクションは実行されません。 • [キャンセル（Cancel）]：アクションを実行せずに [証明書の検証（Certificate Verification）] ダイアログを閉じます。 次の推奨される証明書を表示して承認する必要があります。 • https://www.cisco.com/ • https://www.dl3.cisco.com • https://www.cloudsso.cisco.com • https://www.api.cisco.com • https://www.download-ssc.cisco.com （注） Ciscoから一度に最大2つのファイルをダウンロードできます。3つ以上のファイルをダウンロードしようとすると、エラーメッセージが表示されます。
証明書	Security Manager インストールの各証明書について、[情報カテゴリ（Subject）]、[発行者（Issued By）]、および [承認者（Accepted By）] を表示するテーブル。
表示（View）	[証明書（Certificate）] テーブルで選択した証明書の証明書ビューアを開きます。
削除（Remove）	[証明書（Certificate）] テーブルで選択した証明書を削除します。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。

要素	説明
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Configuration Archive] ページ

[Configuration Archive] ページを使用して、Configuration Archive ツールのデフォルト設定（保存する設定バージョンの数、Cisco IOS ソフトウェア デバイス設定のロールバックに使用する TFTP サーバなど）を定義します。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [設定アーカイブ（Configuration Archive）] を選択します。

関連項目

- [Configuration Archive] ウィンドウ
- 設定のロールバック

フィールド リファレンス

表 5 : [Configuration Archive] ページ

要素	説明
[デバイスごとの最大バージョン数（Max. Versions per Device）] [Purge Now] ボタン Enable Configuration Archive Versions Auto Purge	各管理対象デバイスで維持する設定バージョン数（1 ～ 100）。この数を減らした場合は、[今すぐ消去（Purge Now）] をクリックして、余分なバージョンをすぐに削除できます。 このオプションを使用してファイルを消去すると、**C:\Program Files (x86)\CSCOpx\MDC\tomcat\vms\athena\transcript** フォルダから、追加の設定バージョンに対応するトランスクリプトファイルが削除されます。ただし、消去後は、削除されたバージョンに関連するトランスクリプトファイル（対応する展開ジョブにも関連）は表示できません。トランスクリプトファイルを表示しようとすると、それらが削除されているため、「**Unable to Display Transcript（トランスクリプトを表示できません）**」というエラーが表示されます。 。 [設定アーカイブバージョンの自動消去を有効にする（Enable Configuration Archive Versions Auto Purge）] オプションを指定している場合、Security Manager は、通常のクリーンアップサイクル中に余分なバージョンを自動的に削除します。

要素	説明
TFTP Server for Rollback	TFTP ファイル転送に使用するサーバの完全修飾 DNS ホスト名または IP アドレス。TFTP は、設定を更新できなかった場合に、**configure replace** コマンドを使用して IOS をロールバックするときに使用されます。このとき、システムのリロードは発生しません。Security Manager サーバーを使用するには、**localhost** を入力します。 TFTP サーバは、Security Manager サーバ上でデフォルトでイネーブルになっています。リモート TFTP サーバを指定する場合は、TFTP サービスを適切に提供するように、そのサーバを設定する必要があります。
TFTP Root Directory	Security Manager サーバを TFTP サーバとして使用している場合の、設定ファイル転送用のルート ディレクトリ。[参照（Browse）] をクリックして、Security Manager サーバー上のディレクトリを選択します。 Security Manager サーバ以外のサーバを TFTP ホストとして指定する場合、Security Manager は、その TFTP サーバのルート ディレクトリを常に使用します。リモート TFTP サーバのルート以外のディレクトリは指定できません。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[CS-MARS] ページ

[CS-MARS] ページを使用して、Cisco Security Monitoring, Analysis and Response System サーバを登録します。このサーバは、Security Manager を使用してデバイスをモニタします。CS-MARS サーバーを登録すると、Security Manager で設定されているデバイスのファイアウォール アクセス ルールまたは IPS シグニチャルールに基づいて CS-MARS でキャプチャされたメッセージとイベントを表示できます。CS-MARS サーバを登録しないと、ユーザは CS-MARS から収集されたイベントを表示できません。

ヒント CS-MARS Global Controller を使用している場合は、個別の Local Controller ではなく Global Controller を追加します。Global Controller を追加することによって、各 Local Controller を追加しなくても、Security Manager でデバイスの正しい Local Controller を識別できます。これにより、Security Manager における CS-MARS の設定が簡素化されます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [CS-MARS] を選択します。

関連項目

- Security Manager での CS-MARS サーバの登録

フィールド リファレンス

表 *6 : [CS-MARS]* ページ

要素	説明
CS-MARS Devices	Security Manager に登録する CS-MARS サーバ。 • サーバを追加するには、[Add]（+）ボタンをクリックし、[New CS-MARS Device]/[Edit CS-MARS Device] ダイアログボックス （12 ページ）に入力します。 • サーバを編集するには、サーバを選択し、[Edit]（鉛筆）ボタンをクリックします。 • サーバを削除するには、そのサーバを選択し、[Delete]（ゴミ箱）ボタンをクリックします。サーバを削除すると、そのサーバを使用するすべてのデバイスのデバイス プロパティが更新され、そのサーバ接続が削除されます。リスト上の別のCS-MARSサーバもデバイスをモニタしている場合は、別のサーバを指し示すようにデバイスのプロパティが更新されます。
When Launching CS-MARS Allow User to Save Credentials	Security Manager が、イベント情報の取得時に CS-MARS にログインするために使用するクレデンシャルのタイプ： • [ユーザーのプロンプト（Prompt users）] : ユーザーは、CS-MARS からイベント情報を取得しようとするときに、CS-MARS にログインするように要求されます。このオプションを選択する場合は、[ユーザーによるクレデンシャルの保存を許可（Allow User to Save Credentials）] も選択する必要があります。選択すると、ユーザーのクレデンシャルを保存するオプションがユーザーに表示されるため、ユーザーは、次回イベントステータスを要求したときにCS-MARSに再度ログインする必要がなくなります。 • [CS-Managerクレデンシャルを使用（Use CS-Manager Credentials）] : ユーザーは、CS-MARS からイベント情報を取得しようとするときに、Security Manager へのログインに使用しているのと同じユーザー名とパスワードを使用して CS-MARS にログインします。
[Save] ボタン	変更を保存して適用します。

要素	説明
リセット ボタン	変更を前回保存した値にリセットします。

[New CS-MARS Device]/[Edit CS-MARS Device] ダイアログボックス

[New CS-MARS Device] または [Edit CS-MARS Device] ダイアログボックスを使用して、Security Manager に CS-MARS サーバを登録します。ユーザーは、デバイスをモニターしている CS-MARS サーバーから、デバイスのファイアウォールまたは IPS ポリシーのメッセージやイベントステータスを取得できます。詳細については、Security Manager での CS-MARS サーバの登録を参照してください。

ナビゲーション パス

[CS-MARS] ページ （10 ページ）で、[Add] ボタンをクリックして新しいサーバを追加するか、またはサーバを選択して [Edit] ボタンをクリックします。

フィールド リファレンス

表 7 : [Add CS-MARS Device]/[Edit CS-MARS Device] ダイアログボックス

要素	説明
CS-MARS Hostname/IP	CS-MARS サーバの IP アドレスまたは完全修飾 DNS ホスト名。 ヒント CS-MARS Global Controller を追加する場合は、その Global Controller によってモニタされる Local Controller は追加しないでください。Security Manager によって、特定のデバイスをモニタしている Local Controller が自動的に識別されます。Global Controller を追加することによって、CS-MARS の設定が簡素化されます。
ユーザ名 パスワード ユーザー タイプ（User Type）	CS-MARS サーバが適切なソフトウェア バージョンを実行していることを検証し、その他の基本情報を取得するために、サーバにログインするときのユーザ名とパスワード。また、Security Manager では、このアカウントを使用して、特定のデバイスをモニタしている CS-MARS サーバも識別します。 CS-MARS Local Controller の場合は、グローバル ユーザ アカウントまたはローカル ユーザ アカウントを入力できます。Global Controller の場合は、グローバル アカウントを入力する必要があります。アカウントのタイプを [User Type] フィールドで指定します。

要素	説明
Certificate Thumbprint [Retrieve From Device] ボタン	CS-MARS サーバ証明書（デバイス固有の 16 進ストリング）。[デバイスから取得（Retrieve From Device）] をクリックして、Security Manager が証明書を CS-MARS サーバーから取得するようにします。 証明書は、正常に取得されると表示されます。証明書を確認した後に、[承認（Accept）] をクリックして、Security Manager サーバーにその証明書を保存します。Security Manager から CS-MARS サーバを使用するには、正しい証明書を取得している必要があります。

[CSM Mobile] ページ

[Security Manager管理（Security Manager Administration）] ウィンドウの [CSM Mobile] ページを使用して、Cisco Security Manager の CSM Mobile 機能をイネーブルまたはディセーブルにします。CSM Mobile 機能がイネーブルになっている場合、ユーザは次のリンクに移動して、モバイルデバイスからデバイスの正常性と概要の情報にアクセスできます。ここで、<SecManServer> は Security Manager サーバーの DNS 名または IP アドレスです。

https://<*SecManServer*> /mobile/

または

https://<*SecManServer*> /mobile

提供される情報のタイプの詳細については、ダッシュボードの概要を参照してください。

CSM Mobile の詳細については、CSM Mobileを参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [CSM Mobile] を選択します。

フィールド リファレンス

表 8 : [CSM Mobile] ページ

要素	説明
CSM モバイル機能の有効化（Enable CSM Mobile Feature）	CSM Mobile 機能をイネーブルまたはディセーブルにできます。この機能をディセーブルにすると、モバイルデバイスからデバイスの正常性の概要情報にアクセスできなくなります。
[Save] ボタン	変更を保存して適用します。 サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。進捗インジケータが表示されます。

要素	説明
リセット ボタン	変更を前回保存した値にリセットします。

[Customize Desktop] ページ

[デスクトップのカスタマイズ（Customize Desktop）]ページを使用して、Security Managerアプリケーションが、指定した時間アイドル状態であったあとに自動的に閉じられるかどうかを制御し、特定の状況におけるアクションを確認するようにユーザに要求するかどうかをリセットします。また特定のファイル操作を Security Manager クライアントで実行できるかどうかを制御します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デスクトップのカスタマイズ（Customize Desktop）] を選択します。

関連項目

- Security Manager のライセンス ファイルのインストール
- ポリシーまたはデバイスのインポート
- コマンドラインからのデバイス インベントリのエクスポート
- 共有ポリシーのエクスポート
- IPS ライセンス ファイルの選択 （86 ページ）

フィールド リファレンス

表 9 : [Customize Desktop] ページ

要素	説明
[警告の「Do Not Ask」のリセット（Reset "Do Not Ask" on Warnings）] ボタン	このボタンをクリックして、「Are you sure...?」ポップアップ警告を再設定します。一部のアクションを実行すると、結果に関する警告が表示され、警告が再度表示されないようにするオプションが提示されます。これらの警告のいずれかに対して [Do Not Ask Me Again] を選択している場合、このボタンをクリックすると、警告が再度イネーブルになります。

要素	説明
Enable Idle Timeout Idle Timeout (minutes)	指定した期間、Security Manager クライアント アプリケーションを使用しなかった場合に、クライアントを自動的に終了するかどうかを指定します。タイムアウトはすべてのアプリケーションにわたって適用され、1 つのアプリケーションで操作するとすべてのアプリケーションのタイマーがリセットされます。 このオプションを選択する場合は、クライアントを閉じるまでに経過する必要がある時間を分単位で [Idle Timeout] フィールドに入力します。デフォルトでは、クライアントは、非活動状態が 120 分続いたあとに閉じられます。
Enable Client side file browser	Security Manager クライアントでファイル操作を許可するかどうか。このオプションが選択されている場合、次のファイル操作を実行するときに、クライアント ファイル システムとサーバ ファイル システムを選択できます。 • Security Manager のライセンス ファイルのインストール • IPS ライセンスファイルのインストール • デバイス インベントリ ファイルのインポート/エクスポート • 共有ポリシーのインポート/エクスポート • 次のファイル オブジェクトの作成 • Cisco Secure Desktop Package • Plug-In：ブラウザ プラグイン ファイル用。 • セキュアクライアント プロファイル • セキュアクライアント イメージ • Hostscan Image このオプションは、デフォルトで有効です。
[グローバル検索（Global Search）]	
グローバル検索の有効化	グローバル検索機能を有効にするか無効にするか。この機能はデフォルトでイネーブルになっています。 **ヒント** パフォーマンスを向上させるために、デバイスの一括検出または再検出を実行する前にグローバル検索を無効にすることができます。検出が完了した後、またはユーザーがシステムを使用する可能性が最も低いときに、グローバル検索を再度有効にしてインデックスを再作成できます。

要素	説明
インデックスの再作成	このボタンをクリックして、検索インデックスを再生成します。インデックスの再作成中は、グローバル検索機能を使用できません。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Debug Options] ページ

[Debug Options] ページを使用して、デバッグ ログに含めるメッセージの重大度を設定し、収集するその他のデバッグ情報を指定します。

デバッグ レベルは、Cisco Technical Assistance Center（TAC）から変更を指示された場合にだけ変更してください。これにより、より詳細な情報を CSMDiagnostics.zip ファイルに含めることができるようになります。

該当するサブコンポーネントのメッセージ レベルを変更したあと、システムの問題を引き起こすアクションを再実行します。問題が発生した後、次の順番で選択して、CSMDiagnostics.zip ファイル（または CSMDiagnostics_light.zip ファイル）を作成します。**[ツール（Tools）] > [Cisco Security Managerの診断...（Security Manager Diagnostics,,,）] > [一般的な診断...（General Diagnostics...）]**（または **[ツール（Tools）] > [Cisco Security Managerの診断...（Security Manager Diagnostics...）] > [Light Diagnostics...]**。次に、デバッグ オプションをデフォルト レベルにリセットして、Security Manager サーバが、余分なデバッグ情報の収集が原因でダウンしないようにします。CSMDiagnostics.zip ファイルの生成の詳細については、Cisco Technical Assistance Center 用の診断ファイルの作成を参照してください。

デフォルトでは、重大度がエラーであるか、より高いメッセージがログに含められます。重大度（重大度の高い順）：

- [Severe]：システムが使用できなくなる問題。
- [Error]：Security Manager によって復元できない問題。
- [Warning]：Security Manager による復元が可能な、予期しない状況。
- [Info]：情報メッセージ。
- [Debug]：内部ステータス情報。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [デバッグオプション（Debug Options）] を選択します。

フィールド リファレンス

表 *10 : [Debug Options]* ページ

要素	説明
Capture Discovery/Deployment Debugging Snapshots to File	Security Managerが、設定の生成、展開、および検出が実行されたときに、これらの機能に関するデータ ファイルを生成するかどうかを指定します。一時的なデータ ファイルが、サーバ上の Security Managerインストール フォルダ内の MDC\temp ディレクトリに格納されます。これらのファイルをデバッグに使用できます。 展開または検出に関する問題が発生した場合に、この設定をイネーブルにします。 （注） このチェックボックスをオンにすると、Security Manager の応答時間が遅くなります。このオプションは、限られた状況でだけイネーブルにします。 これらのファイルをデバッグのために Cisco TAC に送信する場合は、パスワードなどの機密データが含まれている可能性があるため、暗号化します。 （注） 検出（または）展開の進行中は、Cisco Security Manager インストールフォルダの MDC\temp ディレクトリにあるスナップショットファイルを削除しないでください。スナップショットファイルは、Cisco Security Manager がアイドル状態のときに削除できます。また、デフォルトのファイルを削除していないことを確認してください。
Deployment Debug Level	展開関連のアクション（デバイス通信など）のメッセージの重大度。
Event Manager Debug Level	Event Manager サブシステムのメッセージの重大度。
Health and Performance Monitor のデバッグレベル（Health and Performance Monitor Debug Level）	Health and Performance Monitor サブシステムのメッセージ重大度レベル。
Image Managerのデバッグレベル（Image Manager Debug Level）	Image Manager サブシステムのメッセージの重大度。
Firewall Services Debug Level	ファイアウォール関連ポリシーのメッセージの重大度。

要素	説明
IOS Platform Debug Level	Cisco IOS ソフトウェア プラットフォーム ポリシーのメッセージの重大度。
PIX Platform Debug Level	PIX、ASA、および FWSM プラットフォーム ポリシーのメッセージの重大度。
Report Manager Debug Level	Report Manager サブシステムのメッセージの重大度。
VPN Services Debug Level	VPN サービス ポリシーのメッセージの重大度。
APIのデバッグレベル（API Debug Level）	アプリケーション プログラミング インターフェイス サブシステムのメッセージ重大度レベル。
[Save] ボタン	変更内容を保存します。
リセット ボタン	すべてのフィールドを以前の値に復元します。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Deployment] ページ

[Deployment] ページを使用して、Security Manager がデバイスに設定を展開するデフォルトの方式を定義します。展開ジョブの作成時に、これらの設定の一部をオーバーライドできます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [展開（Deployment）] を選択します。

関連項目

- 展開の管理
- ポリシー オブジェクトの管理

フィールド リファレンス

表 *11 : [Deployment]* ページ

要素	説明
一般的なパラメータ	

要素	説明
スナップショットパージ設定 Purge Debugging Files Older Than (days)	システムがデバッグ ファイルを保持する最大日数。デバッグ ファイルは自動的に削除されます。この日数を減らした場合、[今すぐパージする（Purge Now）] をクリックして、指定した日数よりも古いすべてのデバッグファイルをすぐに削除できます。 （注） パージする場合、Security Manager は、[デバッグオプション（Debug Options）] ページの [検出/展開デバッグスナップショットのファイルへのキャプチャ（Capture Discovery/Deployment Debugging Snapshots to File）] チェックボックスが有効になった後に作成されたデバッグファイルのみを考慮します。
Default Deployment Method ディレクトリ	デバイスに設定を展開するためのデフォルト方式として使用する方式。 • [Device]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。詳細については、デバイスへの直接展開を参照してください。 • [File]：Security Manager サーバ上のディレクトリに設定ファイルを展開します。[File] を選択する場合は、設定ファイルの展開先ディレクトリを [Destination] カラムで指定します。ファイルをデフォルトとして選択しても、IPS デバイスには設定が適用されません。IPS デバイスについては、デバイス展開だけを使用できます。詳細については、ファイルへの展開を参照してください。 展開ジョブを作成するときに、この方式をオーバーライドできます。

要素	説明
When Out of Band Changes Detected	Security Manager が、設定がデバイスに最後に展開されたあとに、デバイスの CLI で変更が直接行われたことを検出したときに、対応するかどうかを指定します。アウトオブバンド変更の検出は、ファイルではなくデバイスに展開するときにだけ正しく機能し、デバイスから参照設定を取得するように設定された展開方式に対してだけ適用されます（参照設定の設定値については、後述の説明を参照してください）。 この設定によって、デフォルトのアクションが指定されます。デフォルトのアクションは、展開ジョブの作成時にオーバーライドできます。次のいずれかを選択できます。 • [変更を上書きして警告を表示（Overwrite changes and show warning）]（デフォルト）：デバイスに対して手動で変更を行った場合、Security Manager は、展開を続行し、変更を上書きし、このアクションを通知する警告を表示します。 • [展開をキャンセル（Cancel deployment）]：デバイスに対して手動で変更を行った場合、Security Manager は展開をキャンセルし、このアクションを通知する警告を表示します。 • [変更を確認しない（Do not check for changes）]：Security Manager は、変更内容を確認せずにデバイスに展開し、ローカルの変更を上書きします。 アウトオブバンド変更の処理の詳細な説明については、アウトオブバンド変更の処理方法についてを参照してください。 （注） フェールオーバーが設定されていないデバイスの場合、帯域外の変更が検出されたときに[展開をキャンセル（Cancel Deployment）]オプションを選択すると、ブートストラップ設定によって展開が失敗する可能性があります。展開を成功させるには、Security Manager でデバイスを検出する前にフェールオーバーを設定する必要があります。
Deploy to File Reference Configuration	Security Manager サーバ上のファイルに設定を展開するときに、Security Manager が、デバイスの以前の設定と新しいポリシーを比較するために使用する設定。 • [Archive]（デフォルト）：最後にアーカイブされた設定。 • [Device]：現在実行中のデバイスの設定。デバイスから取得されます。 設定を比較したあとで、Security Manager によって、展開する適切な CLI が生成されます。

要素	説明
Deploy to Device Reference Configuration	デバイス（または転送サーバ）に設定を直接展開するときに、Security Manager が、デバイスの以前の設定と新しいポリシーを比較するために使用する設定。 • [Archive]：最後にアーカイブされた設定。 • [Device]（デフォルト）：現在実行中のデバイスの設定。デバイスから取得されます。 設定を比較したあとで、Security Manager によって、展開する適切な CLI が生成されます。
Allow Download on Error	軽微なデバイス設定エラーがある場合でも、デバイスへの展開を継続するかどうかを指定します。
Save Changes Permanently on Device	設定をデバイスに展開したあとに（**write memory** コマンドを使用して）、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するかどうか。これは、PIX、FWSM、ASA、または Cisco IOS の各デバイスに適用されます。このチェックボックスをオフにすると、スタートアップ コンフィギュレーションは変更されません。これは、デバイスが何らかの理由でリロードされると設定の変更内容が失われることを意味します。
Preselect Devices with Undeployed Changes	展開ジョブの作成時に確認する、変更されたデバイスのリストで、変更されたすべてのデバイスを選択済みとするかどうかを指定します。このオプションの選択を解除すると、ユーザは、デバイスを手動で選択して展開ジョブに含める必要があります。
Enable Auto Refresh in Deployment Main Panel	展開ジョブおよびスケジュール ステータス情報が、[Deployment Manager] ウィンドウで自動的にリフレッシュされるかどうかを指定します。このオプションの選択を解除すると、[Refresh] ボタンをクリックして、情報を手動でリフレッシュする必要があります。
Remove Unreferenced SSL VPN Files on Device （ASA のみ）	SSL VPN 設定に関連するファイルが、デバイスの SSL VPN 設定によって現在は参照されていない場合に、Security Manager がこれらのファイルを削除するかどうか。このオプションの選択を解除すると、使用されていないファイルは、展開後にデバイス上に残ります。

要素	説明
Mask Passwords and Keys When Viewing Configs and Transcripts Mask Passwords and Keys When Deploying to File	Security Managerが、次の項目をマスクして、読み取られないようにする条件（ある場合）：ユーザ、イネーブル モード、Telnet、およびコンソールのパスワード。SNMP コミュニティ ストリング。TACACS+、事前共有キー、RADIUS サーバ、ISAKMP、フェールオーバー、Web VPN 属性、ロギング ポリシー属性、AAA、AUS、OSPF、RIP、NTP、ロギング FTP サーバ、ポイントツーポイント プロトコル、ストレージ キー、シングル サインオン サーバ、ロード バランシング、HTTP/HTTPS プロキシ、および IPSEC 共有キーなどのキー。 • [Mask Passwords and Keys When Viewing Configs and Transcripts]：このオプションは、クレデンシャルの画面表示だけに影響します。これにより、未認可ユーザによるクレデンシャルの表示を防ぐことができます。このオプションを選択しない場合でも、デバイスがクレデンシャルを処理する方法によっては、完全なトランスクリプトのクレデンシャルが引き続きマスクされる場合があります。 • [Mask Passwords and Keys When Deploying to File]：このオプションは、ファイルに展開される設定ファイルの内容に影響し、設定ファイルが実際のデバイスに展開できなくなります。このオプションは、これらの設定を現実のデバイスに実際に展開する必要がない場合にだけ選択します。このオプションを選択しても、クレデンシャルが表示されるときにマスクされるかどうかに影響はありません。
新規または変更されたFlexconfig のみを展開する	FlexConfig の作成または変更後に FlexConfig を 1 回だけ展開するか、展開ごとにすべての FlexConfig を展開するか。このオプションは、デフォルトで選択されます。 （注） 展開ごとに展開する必要がある FlexConfig がある場合は、このオプションを無効にする必要があります。この設定を変更した後は、展開後に 1 回限りの FlexConfig を削除して管理する必要があります。
ACL パラメータ	

要素	説明
Optimize the Deployment of Access Rules For （IPv4 および IPv6 のアクセス ルール）。	ファイアウォール ルールが展開される方法。次のいずれかを選択できます。 • [Speed]（デフォルト）：新しい ACL と古い ACL 間のデルタ（差分）だけを送信することで、展開速度を高速化します。これは推奨オプションです。この方法では、ACL 行番号を利用することで、特定の位置にある ACE を選択して追加、更新、または削除します。ACL 全体の再送信は実行されません。編集されている ACL は使用中であるため、ACE が削除され、新しい位置に追加されるまでの間に、一部のトラフィックが不適切に処理される可能性がわずかにあります。この ACL 行番号機能は、Cisco IOS、PIX、および ASA のほとんどのバージョンでサポートされており、FWSM の場合は FWSM 3.1(1) から使用できるようになりました。 • [Traffic]：この方法によって、ACL がシームレスに切り替えられ、トラフィックの中断が回避されます。ただし、展開タスクに時間がかかり、一時 ACL が削除されるまではより多くのデバイス メモリが使用されます。最初に、一時コピーが、展開するための ACL で構成されます。この一時 ACL が、ターゲット インターフェイスにバインドされます。次に、古い ACL が元の名前を使用して再作成されますが、その内容は新しい ACL になります。この ACL も、ターゲット インターフェイスにバインドされます。この時点で、一時 ACL が削除されます。 （注） FWSM デバイスの場合は、[Let FWSM Decide When to Compile Access Lists] オプションも選択している場合にだけ、このオプションが処理に影響します。
Firewall Access-List Names （IPv4 および IPv6 のアクセス ルール）。	アクセス ルールに Security Manager での名前がない場合に、ACL 名がデバイスに展開される方法。 • [Reuse existing names]：参照設定で設定されている ACL 名を再利用します（通常は、デバイスからの名前）。 • [Reset to CS-Manager generated names]：Security Manager が自動生成した ACL 名に名前をリセットします。

要素	説明
Enable ACL Sharing for Firewall Rules （IPv4 および IPv6 のアクセス ルール）。	Security Manager が、アクセス ルール ポリシー用の単一アクセス コントロール リスト（ACL）を複数のインターフェイスと共有するかどうかを指定します。このオプションを選択しない場合、Security Manager は IPv4 および IPv6 のアクセス ルール ポリシーを適用する各インターフェイス固有の ACL を作成します。ACL の共有は、アクセス ルール ポリシーによって作成された ACL の場合にだけ行われます。 このオプションを選択すると、Security Manager は、各インターフェイスのアクセス ルール ポリシーを評価し、ポリシーの実行に必要な最小数を展開する一方で、ACL 命名要件を維持します。たとえば、1 つのインターフェイスロールを使用して 4 つのインターフェイスに同じルールを割り当てる場合は、[ファイアウォールアクセスリスト名（Firewall Access-List Names）] プロパティの [CS-Managerが生成した名前にリセット（Reset to CS-Manager generated names）] を指定し、アクセス制御設定ポリシーでインターフェイスの ACL 名は指定せずに、1 つの ACL だけを展開し、各インターフェイスでその ACL を使用するようにします。 このオプションを選択する場合は、次の点に注意してください。 • インターフェイスで、別のインターフェイスの名前が付いた ACL が使用される場合があります。 • アクセス コントロール設定ポリシーで ACL の名前を指定すると、その名前の ACL は、別のインターフェイスによって使用されている名前と同じ場合でも作成されます。このポリシーで指定された名前は、他のいずれの設定よりも優先されます。 • [ファイアウォールアクセルリスト名（Firewall Access-List Names）] プロパティの [既存の名前を再利用（Reuse Existing Names）] を選択すると、既存の名前は保存されます（アクセス制御設定ポリシーで名前をオーバーライドした場合を除く）。つまり、重複する ACL がデバイスにすでに存在する場合は、異なる名前で ACL が重複して作成されます。 • ヒット カウント統計は、インターフェイスではなく ACL に基づくため、共有 ACL により、その ACL を共有するすべてのインターフェイスから結合された統計情報が提供されます。 • ACL の共有は、FWSM など、デバイスにメモリの制約がある場合に有用です。

要素	説明
Let FWSM Decide When to Compile Access Lists （IPv4 のアクセス ルールのみ）。	Firewall Services Module（FWSM; ファイアウォール サービス モジュール）で、アクセス リストをコンパイルするタイミングを自動的に決定するかどうかを指定します。このオプションを選択すると、展開が高速化される可能性がありますが、トラフィックが中断し、システムが ACL コンパイルのエラー メッセージを報告できなくなる場合があります。このオプションを選択すると、[Optimize the Deployment of Access Rules For Traffic] 設定を使用して、トラフィックの中断の可能性を低減できます。 選択を解除すると、Security Manager は、ACL コンパイルを制御して、トラフィックの中断を回避し、デバイスにおけるピーク時のメモリ使用率を最小限に抑えます。 **注意** このオプションは、展開の問題が発生し、かつ自分が上級ユーザである場合を除き、選択しないでください。
Remove Unreferenced Access-lists on Device （IPv4 および IPv6 のアクセス ルール）。	展開時に、Security Manager が管理する他の CLI コマンドで使用されていないアクセスリストをデバイスから削除するかどうかを指定します。 （注） このオプションを有効にすると、Security Manager は、Security Manager によって管理または検出されたポリシーで使用されていないアクセスリストを、展開中に削除します。Security Manager によって検出または管理されていないポリシーがそのようなアクセスリストを使用している場合、Security Manager は展開中にそのオブジェクトを削除しようとします。これは、FlexConfig で使用され、Security Manager によって管理される他のポリシーでは使用されないアクセスリストにも適用されます。 **警告** [管理設定（Administrative Settings）] から [デバイスで参照されていないアクセスリストを削除（Remove Unreferenced Access-lists on Device）] オプションを有効にすると、Cisco Security Manager は、Security Manager によって管理または検出されたポリシーで使用されていないアクセスリストを自動的に削除します。ただし、グループポリシーの VPN フィルタが使用されている場合、[デバイスで参照されていないアクセスリストを削除（Remove Unreferenced Access-lists on Device）] オプションが有効になっていない場合でも、Security Manager は参照されていないアクセスリストを削除します。
Generate ACL Remarks During Deployment （IPv4 および IPv6 のアクセス ルール）。	展開時に、ACL の警告メッセージおよび備考を表示するかどうかを指定します。

要素	説明
Preserve Sections for Access Rules	アクセスルールを編成するセクション名を展開するかどうかを指定します。このオプションにより、デバイスが検出または再検出された場合にセクション名が失われません。
Generate CSM Rule Number	Cisco Security Manager ユーザーインターフェイスで使用されるルール番号を展開するかどうかを指定します。このオプションは、デバイス設定内のアクセスルールをルールテーブル内の位置に関連付けるのに役立ちます。
オブジェクト グループ パラメータ	
Remove Unreferenced Object Groups from Device (PIX, ASA, FWSM, IOS 12.4(20)T+) （IPv4 オブジェクトおよび IPv6 オブジェクト）。	Security Manager が、Security Manager が管理する他の CLI コマンドで使用されていないオブジェクトグループを、展開中にデバイスから削除するかどうかを指定します。オブジェクトグループには、ネットワーク/ホスト、サービス、およびIDユーザーグループが含まれます。 （注） このオプションを有効にすると、Security Manager は、Security Manager によって管理または検出されたポリシーで使用されていないオブジェクトを、展開中に削除します。Security Manager によって検出または管理されていないポリシーがそのようなオブジェクトを使用している場合、Security Manager は展開中にそのオブジェクトを削除しようとします。このような場合、オブジェクトを削除できなかったことを示すトランスクリプトエラーが表示されて、展開が失敗します。 ヒント ASA 8.3+ デバイス上のオブジェクト NAT 設定を含む、ネットワーク/ホスト オブジェクトは、参照されないとは見なされません。

要素	説明
Create Object Groups for Policy Objects (PIX, ASA, FWSM, IOS 12.4(20)T+) Create Object Groups for Multiple Sources, Destinations or Services in a Rule (PIX, ASA, FWSM, IOS 12.4(20)T+) Optimize Network Object Groups During Deployment (PIX, ASA, FWSM, IOS 12.4(20)T+) （IPv4 オブジェクトおよび IPv6 オブジェクト）。	Security Manager が、ネットワークオブジェクトやサービス グループ オブジェクトなどのオブジェクトグループを作成して、ユーザー グループ オブジェクトを識別し、指定されたデバイスの規則テーブルセル内のカンマ区切りの値を置換するかどうかを指定します。選択を解除すると、Security Managerは、オブジェクトグループをフラット化して、これらのデバイスの IP アドレス、送信元と宛先、ユーザ、ポート、およびプロトコルを表示します。 **ヒント** これらのオプションは、常にオブジェクトとして作成されるホスト、ネットワーク、またはアドレス範囲ネットワーク/ホストの各オブジェクト、あるいはサービス オブジェクト（サービス グループ オブジェクトではありません）には適用されません。複数の FQDN ネットワーク オブジェクトを単一のネットワーク オブジェクトにグループ化できます。 このオプションを選択すると、次のオプションも選択できます。 • [ルール内の複数の送信元、宛先、またはサービスのオブジェクトグループを作成（Create Object Groups for Multiple Sources, Destinations or Services in a Rule）]：ネットワークオブジェクトおよびサービスオブジェクトを自動的に作成して、ユーザー グループ オブジェクトを識別し、規則テーブルセル内の、複数のルールが結合された結果であるカンマ区切りの複数の値を置換するかどうかを指定します。オブジェクトは展開中に作成され、「CSM_INLINE...」の形式で、たとえば「CSM_INLINE_src_rule_8589960758」のようになります。詳細については、ルールの結合を参照してください。 **重要** [ルール内の複数の送信元、宛先、またはサービスのオブジェクトグループを作成（Create Object Groups for Multiple Sources, Destinations or Services in a Rule）] を有効にすると、それらの ACL のヒットカウントプロセスが影響を受け、データの入力に失敗します。これは、CSM が生成したオブジェクトグループと、デバイスと CSM 間の ACL ハッシュの不一致が原因です。 • [Optimize Network Object Groups During Deployment]：ネットワーク オブジェクト グループをより簡潔にして、最適化するかどうかを指定します。ポリシー オブジェクトの簡潔化の詳細については、ファイアウォール ルールの展開時のネットワーク オブジェクト グループの最適化を参照してください。
IPS パラメータ	

要素	説明
Generate transcripts for IPS Auto-Update Jobs	
Attach transcripts to email for IPS Auto-Update Jobs	
Remove Unreferenced Signature and Event Action Variables from IPS Device (IPS Parameters object group)	次回の展開中に、センサー（IPS デバイス）設定から未使用の変数を削除するかどうかを指定します。IPS のイベントおよびシグニチャ変数は、Security Manager のポリシーオブジェクトとして定義されています。 デフォルトでは無効になっています（チェックボックスはデフォルトでオフになっています）。つまり、参照されていない変数を削除しません。 次の変数に適用されます。 IPv4 と IPv6 の両方に適用されます。 • signature source と destination addresses • シグネチャ エンジン パラメータの signature service port 変数 • イベントアクションフィルタの victim and attacker addresses • network information target addresses 次の変数には適用されません。 • signature source port • OS identification address • signature destination port
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Device Communication] ページ

[Device Communication] ページを使用して、デバイスと通信する場合のデフォルト設定を定義します。これらの設定は、主に、デバイスインベントリ、ポリシー検出、および設定の展開に影響します。デバイスのデバイスプロパティにおける個々のデバイスに関する転送設定をオーバーライドできます。

トランスポートプロトコルの設定を変更する場合は、使用しているデバイスが、それらの接続タイプを受け入れるように適切に設定されていることを確認してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します。

関連項目

- デバイス インベントリへのデバイスの追加
- デバイス インベントリの管理
- デバイスを管理するための準備
- デバイス プロパティの表示または変更

フィールド リファレンス

表 12 : [Device Communication] ページ

要素	説明
Device Connection Parameters	
Device Connection Timeout	Security Manager がデバイスとの接続を何秒の間に確立する必要があるか。この秒数を超過すると、タイムアウトします。
再試行回数（Retry Count）	Security Manager がデバイスへの接続の確立を何回試行するか。この試行回数を超過すると、接続を実行できないと判断されます。デフォルト値は 3 です。
Socket Read Timeout	SSH セッションと Telnet セッションの場合に、接続が失われたと結論付ける前に、Security Manager が着信データを待機する最大の秒数。
Transport Protocol (IPS)	IPS 機能を備えた IPS センサーとルータのデフォルト トランスポート プロトコル。デフォルトは HTTPS です。
Transport Protocol (IOS Routers 12.3 and above)	Cisco IOS ソフトウェア Release 12.3 以上を実行するルータのデフォルト トランスポート プロトコル。デフォルトは HTTPS です。
Transport Protocol (Catalyst Switch/7600)	Catalyst 6500/7600 デバイスおよびその他のすべての Catalyst スイッチのデフォルト トランスポート プロトコル（これらのデバイス上で実行されている Cisco IOS ソフトウェア バージョンは関係ありません）。デフォルトは SSH です。
Transport Protocol (IOS Routers 12.2, 12.1)	Cisco IOS ソフトウェア Release 12.1 および 12.2 を実行するルータのデフォルト トランスポート プロトコル。デフォルトは Telnet です。

要素	説明
Connect to Device Using	Security Manager がデバイスにアクセスするときに使用するクレデンシャルのタイプ。詳細については、デバイス クレデンシャルについてを参照してください。 • [Security Managerのユーザ ログイン クレデンシャル（Security Manager User Login Credentials）]：Security Manager は、ユーザが Security Manager にログインしたときに入力したクレデンシャルを使用して、デバイスに接続します。[Device Credentials] ページで各デバイスに設定されたクレデンシャルに関係なく、同じクレデンシャル セットがすべてのデバイスに使用されます。 • [Security Managerデバイスのクレデンシャル（Security Manager Device Credentials）]：Security Manager は、[デバイスプロパティのクレデンシャル（Device Properties Credentials）]ページで指定したクレデンシャルを使用して、デバイスに接続します。これがデフォルトです。 **注意** IPS センサーへの接続が含まれる場合は、[Security Manager User Login Credentials] ではなく [Security Manager Device Credentials] を使用する必要があります。Security Manager が IPS センサーに接続するとき、Security Manager にユーザがログインしているかどうかにかかわらず、デバイス クレデンシャルを使用する必要があります。
SSL Certificate Parameters	

要素	説明
Device Authentication Certificates (IPS) Device Authentication Certificates (Router) PIX/ ASA/ FWSM Device Authentication Certificates [Add Certificate] ボタン	SSL（HTTPS）通信用のデバイス認証証明書の処理方法。さまざまなデバイス タイプごとに異なる動作を設定できますが、次の設定は同じ意味を持ちます。 • [デバイスの追加時に取得（Retrieve while adding devices）]：Security Manager は、ユーザがネットワークまたはエクスポートファイルからデバイスを追加するときに、これらのデバイスの証明書を自動的に取得します。 • [証明書を手動で追加（Manually add certificates）]：Security Manager は、デバイスから証明書を自動的に受け取りません。[証明書の追加（Add Certificate）] をクリックして、[Add Certificate] ダイアログボックスを開きます（[Add Certificate] ダイアログボックス （33 ページ）を参照）。このダイアログボックスで、ネットワークまたはエクスポートファイルからのデバイスの追加を試行する前に、サムプリントを手動で追加できます。[Device Properties Credentials] ページで手動による作成に成功したデバイスの証明書を追加することもできます。詳細については、HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加を参照してください。 • [証明書認証を使用しない（Do not use certificate authentication）]：Security Manager は、デバイス認証証明書を無視します。このオプションを使用すると、第三者によるデバイス検証の妨害に対してシステムが脆弱になります。このオプションは使用しないことを推奨します。
Accept Device SSL Certificate after Rollback	SSL を使用するデバイスの場合、デバイス上の設定をロールバックするときに、IPS デバイス、ファイアウォールデバイス、FWSM、ASA、または Cisco IOS ルータにインストールされている証明書をデバイスから取得するかどうかを指定します。

要素	説明
HTTPS Port Number	デバイスが、Security Manager（および、これらのプロトコルを使用するその他の管理アプリケーション）とのセキュアな通信に使用するデフォルトのポート番号。この値によって、デバイスの HTTP ポリシーで設定した HTTPS ポート番号がオーバーライドされます。 （注） ローカル HTTP ポリシーを共有ポリシーとして設定し、その HTTP ポリシーを複数のデバイスに割り当てると、このポリシーが割り当てられているすべてのデバイスに関して、[Device Properties Credentials] ページで設定されたポート番号が、このポリシーの HTTPS ポート番号設定で上書きされます。 この HTTPS ポート番号は、Cisco Web ブラウザのユーザ インターフェイスを介してデバイスへのアクセスを提供する以外に、Cisco Router and Security Device Manager（SDM）などのデバイス管理アプリケーションや、デバイスと通信するモニタリング ツールで使用されます。 （注） セキュリティアプライアンスでは、同じインターフェイス上のデバイス マネージャ管理セッションの SSL VPN 接続と HTTPS 接続の両方を同時にサポートできます。HTTPS と SSL VPN は両方とも、デフォルトでポート 443 を使用します。このため、HTTPS と SSL VPN の両方を同じインターフェイスでイネーブルにする場合は、HTTPS または WebVPN に対して異なるポート番号を指定する必要があります。代替方法は、SSL VPN と HTTPS を異なるインターフェイスに設定することです。
Overwrite SSH Keys	Security Manager が、デバイスの SSH キーがデバイス上で変更された場合に、そのキーを上書きできるかどうかを指定します。SSH 接続の場合、通信を正常に実行するには正しいキーが必要です。 このチェックボックスは、慎重に検討し、より高いレベルのセキュリティが必要な場合にだけ、オフにしてください。キーがデバイス上で変更されると、Security Manager はそのデバイスと通信しなくなります。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Add Certificate] ダイアログボックス

[Add Certificate] ダイアログボックスを使用して、SSL トランスポート プロトコルを使用するデバイス（ファイアウォール デバイス、FWSM、ASA、IPS デバイス、および Cisco IOS デバイス）にデバイス証明書を手動で追加します。デバイス証明書を手動で追加すると、侵入者が不正な証明書サムプリントを追加できなくなるため、最高レベルのセキュリティがもたらされます。デバイス証明書は、デバイス認証に使用されるデータベースに格納されます。

SSL 証明書の手動による追加の詳細については、HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択し、[証明書の追加（Add Certificate）] をクリックします。

フィールド リファレンス

表 *13 : [Add Certificate]* ダイアログボックス

要素	説明
ホスト名またはIPアドレス	証明書を追加するデバイスのホスト名または IP アドレス。
Certificate Thumbprint	デバイス固有の16進数文字列である、証明書サムプリント。

[Device Groups] ページ

[Device Groups] ページを使用して、デバイス インベントリで定義されているデバイス グループおよびグループ タイプを管理します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイスグループ（Device Groups）] を選択します。

関連項目

- デバイスのグループ化について
- デバイス グループの使用

フィールド リファレンス

表 14 : [Device Groups] ページ

要素	説明
Groups	デバイス グループとグループ タイプを表示します。 グループ名またはタイプ名を変更するには、グループまたはタイプを選択し、もう一度クリックしてテキストを編集可能にします。新しい名前を入力し、Enter を押します。
[Add Type] ボタン	新しいグループ タイプを作成するには、このボタンをクリックします。タイプはデフォルト名で追加されます。名前を上書き入力し、Enter を押します。
[Add Group to Type] ボタン	デバイス グループを選択したデバイス グループまたはグループ タイプに追加するには、このボタンをクリックします。
[Delete] ボタン（ゴミ箱）	選択したデバイス グループまたはグループ タイプとその中に含まれているすべてのデバイス グループを削除するには、このボタンをクリックします。デバイス グループまたはグループ タイプを削除しても、その中に含まれているデバイスは削除されません。
[Save] ボタン	変更内容を保存します。
リセット ボタン	すべてのフィールドを以前の値に復元します。

[Discovery] ページ

[Discovery] ページを使用して、Security Manager が、インベントリおよびポリシーの検出時に特定のタイプのオブジェクトまたはイベントを処理する方法を定義します。Security Manager が検出タスクを保持する時間を制御することもできます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [検出（Discovery）] を選択します。

フィールド リファレンス

表 *15 : [Discovery]* ページ

要素	説明
Prepend Device Name when Generating Security Context Names	セキュリティコンテキストが含まれているデバイスの名前を、そのセキュリティコンテキスト名の先頭に追加するかどうかを指定します。たとえば、セキュリティ コンテキストが admin という名前で、表示名が 10.100.15.16 であるデバイスに含まれている場合、デバイス セレクタに表示される名前は 10.100.15.16_admin になります。 デバイス名をプリペンドしない場合は、セキュリティ コンテキスト名がそのままインベントリに表示されます。Security Manager では、親デバイスに関連するフォルダにセキュリティ コンテキストが配置されないため、デバイスに関連するコンテキストを簡単に確認する唯一の方法が、デバイス名のプリペンドです。 デバイス名をプリペンドしない場合、Security Manager は、同じ名前のデバイスを区別するために番号のサフィックスを追加します。たとえば、admin コンテキストが複数のファイアウォールに存在する場合、デバイス セレクタでは admin_01、admin_02、というように表示されます。
Purge Discovery Tasks Older Than	検出タスクおよびデバイス インポート タスクを保存する日数。入力した日数よりも古いタスクは削除されます。
[ドメインあたりのマルチコンテキスト ASAの最大数（Maximum Number of Multi context ASA per domain）]	1 ドメインに追加できるコンテキストの数。マルチコンテキスト ASA では、ドメインごとに同じ名前のコンテキストを作成できます。デフォルト値は 20 で、必要に応じて 20 を超える任意の値を入力できます。 （注） コンテキスト名では大文字と小文字が区別されません。たとえば、Test、test、および TEST で作成されたコンテキスト名は、同じコンテキスト名と見なされます。
Reuse Policy Objects for Inline Values	Security Manager ですでに定義されているネットワーク/ホスト オブジェクト、アイデンティティ ユーザ グループ オブジェクトなど、名前の付いているポリシー オブジェクトを、CLI のインライン値に置き換えるかどうかを指定します。ポリシー オブジェクトの詳細については、ポリシー オブジェクトの管理を参照してください。 ヒント このオプションは通常、ネットワーク/ホストオブジェクトに適用されますが、完全修飾ドメイン名（FQDN）はインライン値として指定できないため、FQDN ネットワーク/ホストオブジェクトには適用されません。

要素	説明
Allow Device Override for Discovered Policy Objects	オーバーライドが可能なオブジェクトタイプについて、ユーザーが、検出されたポリシーオブジェクトの親オブジェクトの値をデバイスレベルでオーバーライドできるようにするかどうかを指定します。たとえば、このオプションを選択すると、デバイスに Security Manager の ACL ポリシー オブジェクトと同じ名前の ACL があるデバイス上でポリシー検出を実行した場合、検出されたポリシー オブジェクトの名前が再利用されますが、このオブジェクトのデバイス レベルのオーバーライドが作成されます。このオプションの選択を解除すると、新しいポリシー オブジェクトが、名前に番号が付加されて作成されます。 **ヒント** ネットワーク/ホストやサービスなど、サブタイプを持つオブジェクトの場合、オーバーライドはタイプ内に限定されます。たとえば、同じ名前のネットワーク/ホスト グループが検出されると、ネットワーク/ホスト グループのオーバーライドが作成されますが、同じ名前のネットワーク/ホスト アドレス範囲が検出されても、オーバーライドは作成されません。代わりに、新たに検出されたオブジェクトの名前に番号が付加されます。 詳細については、個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。
On Error, Rollback Discovery for Entire Device	Security Manager が、ポリシー検出時に、単一ポリシーで 1 つのエラーが発生した場合でも、検出されたすべてのポリシーをロールバックするかどうかを指定します。選択を解除すると、Security Manager は、正常に検出されたポリシーを保持し、エラーが発生したポリシーだけを廃棄します。ポリシー検出の詳細については、ポリシーの検出を参照してください。
Auto-Expand Object Groups with Prefixes	デバイスインポートプロセス時に、リストに表示されているプレフィックスを使用して、ネットワーク グループやアイデンティティ ユーザ グループなどのオブジェクト グループを拡張します。複数のプレフィックスはカンマで区切ります。この拡張によって、オブジェクト グループの要素が、検出されたポリシーにおける個別の項目として表示されます。詳細については、検出中のオブジェクト グループの展開を参照してください。 **ヒント** このオプションは、**object network** コマンドまたは **object service** コマンドを使用して ASA 8.3+ デバイスから作成されたポリシーオブジェクトには適用されません。これらのコマンドによって、ホスト、ネットワーク、FQDN、またはアドレス範囲ネットワーク/ホストの各オブジェクトや、サービス オブジェクトが作成されます。
[Save] ボタン	変更内容を保存します。

要素	説明
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Event Management] ページ

[Event Management] ページを使用して、イベント管理をイネーブルにします。イベント管理では、Event Viewer を使用して、ASA イベント、FWSM イベント、および IPS イベントを表示できます。イベント収集に必要な設定値を設定することもできます。

Event Manager サービスは Report Manager アプリケーションにも必要です。Report Manager アプリケーションでは、このサービスによって収集された情報を集約したレポートを参照できます。

ヒント　このページで [イベント管理の有効化（Enable Event Management）] オプションが選択されているにもかかわらず、[起動（Launch）] > [イベントビューア（Event Viewer）] を選択したときに Event Viewer が使用不可能であるというメッセージが表示される場合には、Event Manager サービスをもう一度開始してみてください。まず、[Enable] オプションの選択を解除し、[Save] をクリックします。サービスが停止するまで待ちます。次に、[Enable] オプションを選択し、[Save] をクリックし、サービスが再び開始されるまで待機します。その後、Event Viewer を再度開いてみます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] をクリックし、コンテンツテーブルから [イベント管理（Event Management）] を選択します。

フィールド リファレンス

表 16 : [Event Management] ページ

要素	説明
Event Management Options	

要素	説明
Enable Event Management	Event Manager サービスをイネーブルにするかどうかを指定します。このサービスを使用すると、Security Manager はイベント情報を収集できます。この機能をディセーブルにすると、Event Viewer アプリケーションまたは Report Manager アプリケーションを使用できません。 **ヒント** この設定を変更し、[保存（Save）] をクリックすると、Event Manager サービスを起動または停止してもよいかどうかの確認を求められます。[Yes] をクリックするとすぐにサービスが開始または停止し、進捗インジケータが表示されて変更が完了したときに通知されます。ステータス変更が完了するまで待ってから続行します。
Event Data Store Location	イベント情報の収集に使用するディレクトリ。これはプライマリ イベント ストアと呼ばれます。[参照（Browse）] をクリックして、Security Manager サーバー上のディレクトリを選択します。 まだ存在していないディレクトリを指定する場合は、Windows エクスプローラで作成します。Security Manager からディレクトリを作成することはできません。 **ヒント** Event Manager サービスを使用して起動したあとに場所を変更した場合、古いイベントのクエリーは実行できなくなります。
Event Data Store Disk Size	イベント データを格納するために割り当てるディスク スペースの容量（GB 単位）。拡張ストアのサイズが指定した容量の 90％に達すると、増分に応じて（循環的に）ストアからイベントが削除されるようになります。この設定を変更する場合は、次のことを考慮してください。 • イベント データによってすでに使用されているディスク スペース容量よりもサイズを少なくすると、新たに設定したサイズになるまで、古いものから順にイベントが削除されます。 • イベントデータに現在使用されているスペース量の視覚的表示を確認できます。Event Viewer を開き（**[起動（Launch）] > [Event Viewer]**）、次にイベントビューアで **[ビュー（Views）] > [イベントストアディスク使用状況の表示（Show Event Store Disk Usage）]** を選択します。

要素	説明
Event Syslog Capture Port	syslogイベントキャプチャをイネーブルにするポート。デフォルトは514 です。 Security Manager サーバおよび介在するファイアウォールで、イベントを収集するために、Security Manager のこのポート上で着信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。管理対象デバイスは、Security Manager サーバ上のこのポートに syslog 情報を送信するように設定されている必要があります。 **ヒント** このポートを変更した場合は、Security Manager にイベントを送信するすべてのASAデバイスおよびFWSMデバイスと、それらのセキュリティコンテキストのSyslog Serversポリシーも変更する必要があります。詳細については、[Syslog Servers] ページを参照してください。
Event Data Pagination Size	各クエリー応答の各ページに含めることができる最大イベント数。デフォルトは20000ですが、サポートされている値のリストから異なるサイズを選択できます。 （注） Security Manager 4.10 では、ページあたりのイベントの最大数が 100000 に増えました。
Extended Store Management Options	
Auto Copy Events to Extended Store	イベントを格納する拡張保管場所を定義するかどうかを指定します。通常のイベント保管場所から拡張保管場所にイベントをコピーして、引き続き使用できるようにします。Event Viewer で履歴イベントのクエリーを実行すると、必要に応じて、拡張保管場所にあるイベントが自動取得されます。 **ヒント** この拡張サービスを開始して拡張保管場所に変更を加えてもよいかどうかの確認が求められます。

要素	説明
Extended Data Store Location	イベントの拡張データ ストアの場所。サーバ上のドライブとして表示される、DASプロトコルを使用する直接接続ストレージを指定できます。たとえば、ファイバ チャネルを介して接続された SAN ストレージなどです。CIFS ストレージはサポートされていません。[参照（Browse）] をクリックして、目的のドライブとディレクトリを選択します。 **ヒント** • 拡張保管場所を選択して変更を保存すると、Security Managerは、その場所にアクセスできるかどうか、また書き込み権限があるかどうかをチェックします。プライマリ保管場所は参照として使用され、プライマリ保管場所にあって、拡張保管場所にはないデータがあった場合、そのデータは拡張保管場所にコピーされます。すでに拡張保管場所にあるデータは評価されず、そのまま残りますが、あとで削除して新しいデータ用のスペースを確保できます。 • 拡張データ ストアの場所を変更した場合、変更前の拡張データ ストアの場所だけに存在するイベント（プライマリ ロケーションからすでに削除されていて照会できないイベント）に対してクエリーを実行することはできません。このようなイベントを保持するには、以前の場所から新しい場所にデータをコピーしてください。
Extended Data Store Disk Size	イベントの拡張保管場所に割り当てるスペース量（GB 単位）。拡張ストアのサイズが指定した容量の90%に達すると、増分に応じて（循環的に）ストアからイベントが削除されるようになります。サイズは、イベントデータのプライマリ保管場所のサイズ以上にする必要があります。 イベントデータに現在使用されているスペース量の視覚的表示を確認できます。Event Viewerを開き（**[起動（Launch）] > [Event Viewer]**）、次にイベントビューアで **[ビュー（Views）] > [イベントストアディスク使用状況の表示（Show Event Store Disk Usage）]** を選択します。

要素	説明
Error Notification Email IDs	拡張保管場所の使用で問題が発生した場合に、通知を受信する電子メールアドレス。カンマで複数のアドレスを区切ります。通知が正常に送信されるように、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定で説明しているように SMTP サーバも設定する必要があります。 メッセージには、問題、原因、および推奨アクションが示されます。たとえば、頻繁に拡張ストレージが到達不能になる場合、データのコピーが繰り返し失敗する場合、または拡張保管領域にコピーできるようになる前にプライマリ保管領域からパーティションが削除された場合（頻繁にストレージが到達不能になるか、コピーに永続的な問題があると発生する可能性がある）などに通知を受信します。
フェールオーバーデバイスの Syslog	
フェールオーバースタンバイデバイスからの Syslog の処理（Process Syslogs from Failover Standby Device）	スタンバイ ASA からの syslog メッセージの処理をイネーブルまたはディセーブルにします。イネーブルにすると、スタンバイ ASA またはフェールオーバー ASA によって生成された syslog メッセージが、[イベントモニタリング（Event Monitoring）] ウィンドウの [デバイス ID（Device Identifier）] 列に表示されます。 （注） デフォルトでは、スタンバイ ASA からの syslog メッセージの処理は無効になっています。
Syslogリレーサービス（Syslog Relay Service） （注） バージョン 4.13 以降、Cisco Security Manager は Event Viewer で IPv6 経由の syslog をサポートしますが、syslog リレーサービスは IPv6 経由の syslog ではサポートされません。	
Syslogリレーサービスの有効化（Enable Syslog Relay Service）	Syslog リレーサービスをイネーブルまたはディセーブルにします。[Syslogリレーサービスの有効化（Enable Syslog Relay Service）] チェックボックスをオンにして、Syslog リレーサービスの構成に必要なフィールドを有効にします。

要素	説明
Syslogリレーキャプチャポート（Syslog Relay Capture Port）	Syslog リレーサービスが syslog をリッスンする UDP ポートを指定します。デフォルトは 514 です。 Syslog リレーサービスが有効になっている場合、デバイスはSyslog リレーキャプチャポートに Syslog を送信して、ローカルコレクタとリモートコレクタに転送できるようにする必要があります。Syslog リレーサービスがオフになっている場合、デバイスはSyslogをイベント Syslog キャプチャポートに送信する必要があります。 （注） Syslog リレーキャプチャポートとイベント Syslog キャプチャポートを同じにすることはできません。Syslogリレーサービスを有効にするときに、デバイスが現在 Syslog をイベント Syslog キャプチャ ポートに送信するように設定されている場合は、代わりにそのポート番号を Syslog リレーキャプチャポートに使用してから、イベント Syslog キャプチャポートを別のポートに変更する必要があります。 Security Manager サーバおよび介在するファイアウォールで、イベントを収集するために、Security Manager のこのポート上で着信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。管理対象デバイスは、Security Manager サーバ上のこのポートに syslog 情報を送信するように設定されている必要があります。 ヒント このポートを変更した場合は、Security Manager にイベントを送信するすべてのASAデバイスおよびFWSMデバイスと、それらのセキュリティ コンテキストのSyslog Servers ポリシーも変更する必要があります。詳細については、[Syslog Servers] ページを参照してください。
ローカルイベントコレクタへのリレー（Relay to Local Event Collector）	ローカルイベントコレクタの syslog リレーを有効または無効にします。
リモートコレクタ1へのリレー（Relay to Remote Collector 1）	リモートコレクタ 1 の syslog リレーを有効または無効にします。
コレクタ1のIPアドレス（Collector 1 IP address）	リモートコレクタ 1 の syslog 送信先 IP アドレスを指定します。
コレクタ1 Syslogキャプチャポート（Collector 1 Syslog Capture Port）	リモートコレクタ 1 がリレーされた syslog をリッスンする UDP ポートを指定します。

要素	説明
リモートコレクタ2へのリレー（Relay to Remote Collector 2）	リモートコレクタ 2 の syslog リレーを有効または無効にします。
コレクタ2のIPアドレス（Collector 2 IP address）	リモートコレクタ 2 の syslog 送信先 IP アドレスを指定します。
コレクタ2 Syslogキャプチャポート（Collector 2 Syslog Capture Port）	リモートコレクタ 2 がリレーされた syslog をリッスンする UDP ポートを指定します。

要素	説明
デバイス フィルタ	特定のコレクタについて、syslog をリレーする必要があるデバイスをフィルタできます。この機能を使用すると、あるデバイスセットの syslog を 1 つのコレクタに送信し、別のデバイスセットの syslog を別のコレクタに送信するように構成できます。 **1.** デバイスをフィルタリングする対象のタブ（ローカルコレクタ、リモートコレクタ 1、またはリモートコレクタ 2）を選択します。 **2.** このコレクタに対して syslog をリレーするデバイスを指定するには、[リレーを許可（Permit Relay）] を選択します。逆に、このコレクタに対する syslog リレーを無効にするデバイスを指定する場合は、[リレーを許可（Permit Relay）] チェックボックスをオフにします。[リレーを許可（Permit Relay）] チェックボックスがオンになっていない場合、フィルタに追加したデバイスの syslog はリレーされません。一方、他のすべてのデバイスの syslog はリレーされます。 （注） 有効になっている各コレクタについて、すべてのデバイスからの syslog リレーがデフォルトで有効になっています。 （注） クラスタをフィルタリストに追加すると、クラスタ管理プールの IP アドレスがフィルタ構成の一部として含まれます。 **3.** フィルタに追加するデバイスまたはデバイスグループを [使用可能なデバイス（Available Devices）] リストから選択し、[>>] をクリックして [選択されたデバイス（Selected Devices）] リストに移動します。デバイスの選択の詳細については、セレクタの使用を参照してください。 **4.** Security Manager の管理対象外デバイスを追加するには、[特別なデバイスの追加（Add Special Device）] フィールドにデバイスの IP アドレスを入力し、下部の [>>] をクリックして、デバイスを [選択されたデバイス（Selected Devices] リストに移動します。
再起動（Restart）	Syslog リレーサービスを再起動します。
CPUスロットル設定（CPU Throttle Settings）	Syslog リレーサービスに使われる CPU 負荷を制御できる [CPUスロットリングポリシー（CPU Throttling Policy] ダイアログボックスを開きます。詳細については、[CPU スロットリング ポリシー] ダイアログボックス （46 ページ）を参照してください。

要素	説明
統計情報の表示（View Statistics）	[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックスを開いて、syslog リレーサービスプロセスの平均CPUとメモリ使用量、およびさまざまなコレクタのトラフィックレートを表示できます。詳細については、[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス （48 ページ）を参照してください。
[Save] ボタン	変更を保存して適用します。 ほとんどの場合、Event Viewer 設定に関連する変更を反映するには、Event Manager サービスを一時的に停止し、再起動することが必要となります。サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。進捗インジケータが表示されます。 Syslog リレーサービス設定の変更を反映するには、Syslog リレーサービスを一時的に停止してから再起動する必要があります。サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

Syslog リレーサーバーのトラブルシューティング

Syslog リレーサービスが有効になっている場合、デバイスはSyslog リレーキャプチャポートにSyslogを送信して、ローカルコレクタとリモートコレクタに転送できるようにする必要があります。Syslog リレーサービスがオフになっている場合、デバイスは Syslog をイベント Syslog キャプチャポートに送信する必要があります。

Syslog リレーサーバーは、デバイスイベントと Security Manager イベント マネージャ アプリケーション間の中間接続として機能します。デバイスイベントのパケットを受信し、ローカルコレクタとリモートコレクタに転送します。

IP によるデバイス管理

IP を介して（IPv4 または IPv6 を使用して）Security Manager でデバイスを管理するには、デバイス管理インターフェイスに適切な IP 情報が必要です。

たとえば、次のサンプル設定を参照してください。

!

interface Management1/1

management-only

nameif management

security-level 100

ip address 10.197.87.95 255.255.255.0

ipv6 address 2016::b2aa:77ff:fe7c:a068/64

ipv6 enable

この設定では、デバイス管理 IP アドレスに IPv4 と IPv6 の両方の管理アドレスがあります。したがって、IPv4 または IPv6 を介してデバイスを管理できます。

問題：

デバイスが Security Manager の IPv6 管理アドレスを介して管理されている場合、Security Manager とデバイス間の通信は、IPv4 アドレスではなく IPv6 アドレスのみを介して行われます。

ただし、Event Syslog サーバーは引き続き Event Syslog パケットを IPv4 アドレスにのみ送信するため、このシナリオでは、Security Manager は受信した IPv4 Event Syslog パケットに対応するデバイスをマッピングできません。

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [イベント管理（Event Management）] > [Syslogリレーサービス（Syslog Relay Service）] で、Syslog リレーサービスのローカルコレクタまたはリモートコレクタにフィルタデバイスを追加すると、Security Manager は、IPv6 管理アドレスではなくデバイス管理 IPv4 アドレスを抽出しようとします。

ただし、デバイスには IPv4 管理インターフェイスが設定されていません。したがって、Security Manager は次のエラーを表示します。

デバイスの選択 – デバイスの IPv4 アドレスが見つかりません（Device selection – Ipv4 address not found for device(s)）

ソリューション：

[デバイスビュー（Device View）] > [ポリシー（Policies）] > [インターフェイス（Interfaces）] に移動して、IPv4 アドレスを使用してデバイス管理インターフェイスを設定します。

[CPU スロットリング ポリシー] ダイアログボックス

[CPUスロットリングポリシー（CPU Throttling Policy] ダイアログボックスを使用して、Syslog リレーサービスに使われる CPU 負荷を制御するための設定を指定します。

CPU スロットリングをイネーブルにした後で、[最大CPU使用率平均の時間（Average Max CPU Usage Time）] フィールドで選択されている期間中の syslog リレーサービスの平均 CPU 使用率が [最大CPU使用率（Maximum CPU Usage）] しきい値より大きい場合、[転送の中止期間（Stop Forwarding For）] で指定された期間、CPU スロットリングが [次への転送を中止（Stop Forwarding To）] で指定されたコレクタに対して実行されます。

（注） [Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックスを使用して、スロットルポリシーのためにコレクタごとにドロップされた syslog パケットの数を確認できます（[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス （48 ページ）を参照）。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント管理（Event Management）] を選択して、[CPUスロットル設定（CPU Throttle Settings）] をクリックします。

フィールド リファレンス

表 *17 : [CPU* スロットリング ポリシー*]* ダイアログボックス

要素	説明
CPUスロットリングを有効にする（Enable CPU Throttling）	syslog リレーサービスに対するスロットリングをイネーブルにするかどうかを指定します。デフォルトでは、syslog リレーサービスに対する CPU スロットリングはディセーブルになっています。
最大CPU使用率（Maximum CPU Usage）	Syslog リレーサービス用の最大 CPU 使用率を、合計 CPU 容量のパーセンテージとして指定します。これは、CPU スロットリングが開始されるしきい値です。
最大CPU使用率平均の時間 (分)（Average Max CPU Usage Time (Minutes)）	syslog リレーサービスによる CPU 使用率が計算される時間を分単位で指定します。オプションは、1 分、5 分、および 15 分です。この平均値は、最大 CPU 使用率の値と比較されて、スロットルを実行する必要があるかどうかが判断されます。
[次への転送を中止（Stop Forwarding To）]	スロットリングが行われているときに syslog の転送を停止するコレクタを指定します。
転送の中止期間（Stop Forwarding For）	しきい値に達したときにスロットルをイネーブルにする時間を分単位で指定します。指定された時間が経過した後も、CPU 使用率が最大 CPU 使用率のしきい値を超えている場合、スロットリングは引き続きイネーブルです。
電子メール通知の有効化	syslog リレーサービスがスロットルモードを開始または終了したときに電子メール通知を送信するかどうかを指定します。電子メール通知は、デフォルトではディセーブルです。 電子メールを送信するには、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定の説明に従って SMTP サーバを設定する必要があります。
通知電子メールID（Notification Email IDs）	[通知電子メールID（Notification Email IDs）] フィールドに、有効なアドレスを 1 つ以上入力します。複数のアドレスはコンマで区切ります。

要素	説明
電子メールの送信	通知メールを送信する頻度を指定します。 • [毎回（Every time）]：このオプションを選択すると、syslog リレーサービスがスロットルモードを開始または終了するたびに通知が送信されます。転送の中止期間タイマーが経過した後も CPU 使用率が最大 CPU 使用率のしきい値を超えている場合、スロットリングは継続され、追加の通知が送信されます。 • [指定した期間ごと（Every）]：このオプションを選択すると、syslog リレーサービスが特定の期間にスロットルモードを開始または終了したときに、最大 1 つの通知が送信されます。このオプションを選択する場合は、分数または時間数を入力して期間を指定し、ドロップダウンリストから対応するオプション（分/時間）を選択します。

[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス

[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックスを使用して、syslog リレーサービスプロセスの平均 CPU とメモリ使用量、およびさまざまなコレクタのトラフィックレートを表示します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [イベント管理（Event Management）] を選択して、[統計情報の表示（View Statistics）] をクリックします。

フィールド リファレンス

表 18 : [Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス

要素	説明
ログリレーサービス（Log Relay Service）	
平均メモリ使用量（過去1分間）（Memory Usage Average (last 1 min.)）	過去 1 分間に平均して syslog リレーサービスによって使用されたメモリの量を示します。

要素	説明
平均CPU使用率（過去1分間）（CPU Usage Average (last 1 min.)）	過去 1 分間に平均して syslog リレーサービスによって使用された CPU 容量の割合を示します。 ヒント　平均 CPU 使用率が高すぎる場合は、syslog リレーサービスの CPU スロットリングを有効にすることを検討してください（[CPU スロットリング ポリシー] ダイアログボックス （46 ページ）を参照）。
受信syslogパケットの総数（Total sylog packets received）	サービスの開始以降、syslog リレーサービスによって受信された syslog パケットの総数を示します。
開始以降に受信した1秒あたりの平均syslog数（Average syslog received per second since start）	サービスの開始以降、syslog リレーサービスによって受信された 1 秒あたりの syslog パケットの平均数を示します。
過去1分間に受信した1秒あたりの平均syslog数（Average syslog received per second for last 1 minute）	過去 1 分間に syslog リレーサービスによって受信された 1 秒あたりの syslog パケットの平均数を示します。
過去5分間に受信した1秒あたりの平均syslog数（Average syslog received per second for last 5 minute）	過去 5 分間に syslog リレーサービスによって受信された 1 秒あたりの syslog パケットの平均数を示します。
過去15分間に受信した1秒あたりの平均syslog数（Average syslog received per second for last 15 minute）	過去 15 分間に syslog リレーサービスによって受信された 1 秒あたりの syslog パケットの平均数を示します。
スロットルポリシーがアクティブな期間（分単位）（Period (in mins.) for which throttle policy is active）	syslog リレーサービスの CPU スロットルポリシーがアクティブであった時間を分単位で示します。詳細については、[CPU スロットリング ポリシー] ダイアログボックス （46 ページ）を参照してください。
ローカルコレクタ/リモートコレクタ 1/リモートコレクタ 2	
正常に送信されたsyslogパケットの総数（Total syslog packets sent successfully）	サービスの開始以降、syslog リレーサービスによって送信された syslog パケットの総数を示します。
ドロップされたsyslogパケットの総数（フィルタポリシー）（Total syslog packets dropped (filter policy)）	サービスの開始以降、定義されたフィルタポリシーに従って syslog リレーサービスによってドロップされた syslog パケットの総数を示します。
ドロップされたsyslogパケットの総数（スロットルポリシー）（Total syslog packets dropped (throttle policy)）	サービスの開始以降、スロットルポリシーに従って syslog リレーサービスによってドロップされた syslog パケットの総数を示します。

要素	説明
送信中に失敗したsyslogパケットの総数（Total syslog packets failed during transmit）	サービスの開始試行、syslog リレーサービスで転送できなかった syslog パケットの総数を示します。
開始以降に送信した1秒あたりの平均syslog数（Average syslog sent per second since start）	サービスの開始以降、syslog リレーサービスによって送信された 1 秒あたりの syslog パケットの平均数を示します。
過去1分間に送信した1秒あたりの平均syslog数（Average syslog sent per second for last 1 minute）	過去 1 分間に、syslog リレーサービスによって 1 秒あたりに送信された syslog パケットの平均数を示します。
過去5分間に送信した1秒あたりの平均syslog数（Average syslog sent per second for last 5 minute）	過去 5 分間に、syslog リレーサービスによって 1 秒あたりに送信された syslog パケットの平均数を示します。
過去15分間に送信した1秒あたりの平均syslog数（Average syslog sent per second for last 15 minute）	過去 15 分間に、syslog リレーサービスによって 1 秒あたりに送信された syslog パケットの平均数を示します。
更新	[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックスに表示される統計を更新します。

[Health and Performance Monitor] ページ

[Cisco Security Manager管理（Cisco Security Manager Administration）] ウィンドウの [Health and Performance Monitor] ページを使用して、ネットワーク全体の Health and Performance Monitoring を有効にします。Health and Performance Monitor（HPM）はスタンドアロン アプリケーションであり、デバイスステータスやトラフィック情報をネットワークレベルで可視化することにより、ASA デバイス、IPS デバイス、および VPN サービスの主要な正常性データとパフォーマンスデータを監視できます。

ヒント　Health and Performance Monitor の起動を試みたときにアプリケーションが使用できないというメッセージが表示された場合でも、このページで [Health and Performance Monitorの有効化（Enable Health and Performance Monitor）] オプションを選択している場合は、Health and Performance Monitoring を再起動してみてください。まず、[Enable] オプションの選択を解除し、[Save] をクリックします。サービスが停止するまで待ちます。次に、[Enable] オプションを選択し、[Save] をクリックし、サービスが再び開始されるまで待機します。その後、HPM アプリケーションを再度開いてみてください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] をクリックし、目次から [Health and Performance Monitor] を選択します。

フィールド リファレンス

表 19 : [Health and Performance Monitor] ページ

要素	説明
Health and Performance Monitorの有効化（Enable Health and Performance Monitor）	Cisco Security Manager がイベント情報を収集できるようにする Health and Performance Monitoring サービスを有効化または無効化できます。この機能を無効にすると、HPM アプリケーションを使用できません。 **ヒント** この設定を変更し、[保存（Save）] をクリックすると、Health and Performance Monitoring サービスの起動または停止の確認を求められます。[Yes] をクリックするとすぐにサービスが開始または停止し、進捗インジケータが表示されて変更が完了したときに通知されます。ステータス変更が完了するまで待ってから続行します。
OOB 通知設定 **（注）** 電子メール通知を受信するには、SMTP サーバーが Cisco Security Manager サーバーで設定されている必要があります。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定を参照してください。 Cisco Security Manager は、アウトオブバンド（OOB）変更を手動で、または Cisco Security Manager の管理外でデバイスに加えられた変更であると見なします。たとえば、（監視対象）デバイスに直接ログインし、CLI を介してコンフィギュレーション コマンドを入力した場合です。HPM アプリケーションによって監視されるデバイスの場合、Cisco Security Manager は、HPM によって定期的に検出される OOB の変更を監視します。アウトオブバンド変更が検出された場合、HPM は [デバイスステータスビュー（Device Status View）] ページに表示されるアラートを生成し、設定済みの受信者に電子メールを送信します。 **（注）** 更新時間中に Cisco Security Manager が再起動した場合、OOB の変更が検出され、電子メール通知が送信された後、Cisco Security Manager の起動後に同じ電子メールが再度送信される可能性があります。	

要素	説明
OOB電子メール通知の有効化（Enable OOB Email Notification）	アウトオブバンド変更に関する電子メール通知を有効化または無効化できます。 （注） 電子メール通知が無効になっている場合、[デバイスステータスビュー（Device Status View）] ページにはアラートのみが表示されます。 （注） HPM が OOB の変更を検出し、Configuration Manager と同期すると、監視対象のデバイスごとに個別の電子メールアラート通知が送信されます。重複を防ぐために、OOB 変更ごとに送信される電子メールは追跡され、5 分に 1 回ファイルに保存されます。 ヒント デフォルトの追跡時間は、Cisco Security Manager プロパティファイルで 5 分に設定されています。時間は必要に応じて更新できます。
受信者の電子メール（Recipient E-mail(s)）	OOB の変更を通知する必要がある受信者を指定します。
[Save] ボタン	変更を保存して適用します。 ほとんどの場合、Health and Performance Monitoring サービスを一時的に停止して、再起動する必要があります。サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。進捗インジケータが表示されます。
リセット ボタン	変更を前回保存した値にリセットします。

[Report Manager] ページ

[Security Manager管理（Security Manager Administration）] ウィンドウの [Report Manager] ページを使用して、Cisco Security Manager の Report Manager 機能をイネーブルまたはディセーブルにします。Report Manager は、デバイス、およびリモートアクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示できるスタンドアロンアプリケーションです。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] をクリックし、コンテンツテーブルから [Report Manager] を選択します。

フィールド リファレンス

表 *20 : [*ヘルスとパフォーマンスのモニタリング（*Health and Performance Monitoring***）*]* ページ**

要素	説明
Report Manager を有効にする（Report Manager）	Report Manager サービスをイネーブルまたはディセーブルにすることができます。この機能をディセーブルにすると、Report Manager アプリケーションを使用できません。 ヒント　この設定を変更し、[保存（Save）] をクリックすると、Report Manager サービスを起動または停止してもよいかどうかの確認を求められます。[Yes] をクリックするとすぐにサービスが開始または停止し、進捗インジケータが表示されて変更が完了したときに通知されます。ステータス変更が完了するまで待ってから続行します。
[Save] ボタン	変更を保存して適用します。 サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。進捗インジケータが表示されます。
リセット ボタン	変更を前回保存した値にリセットします。

[Identity Settings] ページ

[Identity Settings] ページを使用して、NetBIOS ドメインが ASA デバイスの ID 認証ファイアウォール ポリシーを使用するように、Active Directory（AD）サーバ グループを設定します。これらの設定によって、ID認証ポリシーのユーザまたはユーザ グループ、またはアイデンティティ ユーザ グループ ポリシー オブジェクトを選択するときに、検索機能を使用できるようになります。

ヒント　ASA で [Identity Options] ポリシーを設定することで、エントリを追加することもできます。ポリシーを保存するときに、アイデンティティ設定管理ページを更新するかどうかを確認します。1 つのドメインに対して異なるサーバ グループを使用するように複数の ASA を設定できますが、設定ページでのドメインと AD サーバの組み合わせは 1 つであることに注意してください。ユーザー名のルックアップでは、設定している個々の ASA にどのサーバーグループが設定されているかに関係なく、常に ID 設定管理ページで定義された AD サーバーが選択されます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ID設定（Identity Settings）] を選択します。

関連項目

- アイデンティティ ユーザ グループ オブジェクトの作成
- ポリシーでのアイデンティティ ユーザの選択

フィールド リファレンス

表 21 : [Identity Settings] ページ

要素	説明
ドメイン - AD サーバー グループ マッピング テーブル。	テーブルの各行によって、NetBIOS ドメインが ASA デバイスの ID 認証ファイアウォール ポリシーを使用するように、Active Directory（AD）サーバ グループが定義されます。 • エントリを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[ADドメインサーバーの追加（Add AD Domain Server）] ダイアログボックスに入力します。[Domain AD Server] ダイアログボックスを参照してください。ドメイン名を入力し、LDAP AD サーバーを指定する AAA サーバー グループ オブジェクトを選択する必要があります。 • エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[行の削除（ゴミ箱）（Delete Row (trash can)）] ボタンをクリックします。 • Security Manager がサーバーグループで定義されたサーバーに正常に接続できるかどうかをテストするには、行を選択して [テスト（Test）] をクリックします。
デフォルト ドメイン	ファイアウォール ポリシーまたはアイデンティティ ユーザ グループ ポリシー オブジェクトのユーザ名またはグループ名を指定するときにドメインを入力しなかった場合に使用する NetBIOS ドメイン。 デフォルトは LOCAL であり、これは名前が ASA 自体で定義されることを意味します（ローカルユーザーとして、またはドメイン名に関連付けられた LDAP サーバーグループ以外の手段で認証された VPN ユーザーとして）。 LOCAL 以外は、[Domain-AD Server Group Mapping] テーブルで設定されたドメインだけがこのリストに表示されます。 **ヒント** この設定は、user-identity default-domain コマンドで設定されたデフォルト ドメインとは関係ありません。この設定は、ドメイン名を必ずしも含めなくてもユーザー名を入力できるようにする便利な設定です。ユーザー名を最も頻繁に入力するドメインを選択します。

要素	説明
ルートクエリの経由元	ユーザまたはユーザ グループを選択するときに検索機能を使用する場合、Security Manager から AD サーバにクエリーを送信する必要があります。クエリが Security Manager クライアント（クライアントを実行しているワークステーション）からのものか、サーバーからのものかを選択します。 デフォルトでは、LDAP クエリはクライアントから送信されます。
ドメインのないユーザー文字列の場合	デフォルト ドメインに LOCAL 以外を選択した場合、ドメイン名なしで入力されたユーザ名またはユーザ グループ名の処理方法を指定します。 • [ADからユーザー/ユーザーグループを自動判断（Auto determine user/user-group from AD）]：デフォルトドメインに関連付けられている AD サーバーをチェックして、名前がユーザーかユーザーグループかを判断し、適切な文字列（Default-Domain\user または Default-Domain\\user-group）を追加します。名前が見つからない場合は、ドメイン名と 1 つか 2 つの \ 文字を手動で入力して、その名前がユーザーのものかグループのものかを示す必要があります。 • [Default-Domain/userに変更（Change it to Default-Domain/use）]：入力された名前がユーザーグループ名ではなくユーザー名であると想定し、デフォルトドメイン（Default-Domain\user）を追加します。 ヒント　入力する場合は、名前の前に \ または \\ を付けると、デフォルトドメインが自動的に追加されます。そのため、[Change it to Default-Domain/user] オプションを選択した場合でも、最初に \\ を入力すれば、ドメインを入力せずにグループ名を入力できます。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Image Manager] ページ

[Image Manager] ページを使用して、Cisco Security Manager 内の Image Manager の管理設定を制御します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [Image Manager] を選択します。

フィールド リファレンス

表 22 : [Image Manager] ページ

要素	説明
CCO設定の編集（Edit CCO Settings）	[CCO設定の編集（Edit CCO Settings）] リンクを使用して、[CCO設定（CCO Settings）] ページに迅速に移動できます。[CCO設定（CCO Settings）] ページの詳細については、[CCO設定（CCO Settings）] ページ （5 ページ）を参照してください。
より古いジョブを削除（Purge Jobs Older Than）	Image Manager ジョブを削除する前に保持する期間（日数）を入力します。デフォルトは365 日です。[今すぐ削除（Purge Now）] を選択して、以前の Image Manager ジョブの仕様をすぐにクリアします。
リポジトリを含める（Include Repository）	オンにすると、イメージリポジトリは Cisco Security Manager バックアップの一部になります。デフォルトではイメージは除外されます。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[IPインテリジェンス設定（IP Intelligence Settings）] ページ

[IPインテリジェンス設定（IP Intelligence Settings）] ページを使用して、Cisco Security Manager 内の IP インテリジェンス機能の管理設定を制御します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [IPインテリジェンス設定（IP Intelligence Settings）] を選択します。

フィールド リファレンス

表 *23 : [IP*インテリジェンス設定（*IP Intelligence Settings*）*]* ページ

要素	説明
CCO設定の編集（Edit CCO Settings）	GeoIP データベースを自動更新するには、Cisco.com に接続するためのログイン情報が必要です。[CCO設定の編集（Edit CCO Settings）] リンクを使用して、ログイン情報が設定されている [CCO設定（CCO Settings）] ページに迅速に移動できます。[CCO設定（CCO Settings）] ページでプロキシサーバーの設定を設定することもできます。[CCO設定（CCO Settings）] ページの詳細については、[CCO設定（CCO Settings）] ページ （5 ページ）を参照してください。
逆引き DNS（FQDN）	
逆引きDNS（FQDN）ルックアップサービスの有効化（Enable Reverse DNS (FQDN) Lookup Service）	逆引きDNS（FQDN）ルックアップサービスを有効にするか無効にするかを指定します。IP インテリジェンスツールを使用して IPv4 アドレスの完全修飾ドメイン名（FQDN）を特定できるようにする場合は、このサービスを有効にします。
CSMサーバーのDNSサーバーを使用（Use CSM Server's DNS Server）	逆引き DNS ルックアップ要求に Cisco Security Manager サーバーで定義された DNS サーバーを使用するには、このオプションを選択します。
カスタムDNSサーバーを使用（Use custom DNS servers）	逆引き DNS ルックアップ要求に使用する DNS サーバーを手動で指定するには、このオプションを選択します。表示されるフィールドには、最大 3 つの DNS サーバーアドレスを入力できます。 （注） Cisco Security Manager は、仮想マシンの内部に構成された外部 DNS サーバーの使用をサポートしていません。
ロード バランシングの有効化（Enable Load Balancing）	複数の DNS サーバーが使用可能な場合に、DNS サーバー間で逆引き DNS ルックアップ要求を分散するかどうかを指定します。
デフォルトのブロッキング範囲（Default Blocking Ranges）	デフォルトで逆引き DNS ルックアップから除外される IP アドレスの範囲を一覧表示します。 0.0.0.0、255.255.255.255、127.0.0.1、169.254.0.0 ～ 169.254.255.255、224.0.0.0 ～ 239.255.255.255

要素	説明
ユーザー定義のブロッキング範囲（User-defined Blocking Ranges）	逆引き DNS ルックアップ要求から除外する必要がある追加の IP アドレスまたはアドレスの範囲を指定します。[編集（Edit）]（鉛筆）ボタンをクリックして [IPv4ブロック範囲アドレスの編集（Edit IPv4 Blocking Range Addresses）] ダイアログボックスを開き、除外する IPv4 アドレスまたはアドレスの範囲を指定できます。複数のエントリを指定する場合は、カンマ「,」で区切ります。
GeoIP	
GeoIPルックアップサービスの有効化（Enable GeoIP Lookup Service）	GeoIP ルックアップサービスを有効にするか無効にするかを指定します。IP インテリジェンスツールを使用して IPv4 アドレスの地理的位置情報を取得できるようにする場合は、このサービスを有効にします。 （注） GeoIP 情報を IP インテリジェンスデータに含めるには、Cisco.com から地理的位置データベースをダウンロードする必要があります。また、バックアップから Cisco Security Manager データベースを復元した後、Cisco.com から地理的位置データベースをダウンロードする必要があります。バージョン 4.9 以降、Cisco Security Manager では、cisco.com からアップデートをダウンロードする前に、シスコ エンドユーザー ライセンス契約（EULA）を読んで同意することが義務付けられています。 Cisco Security Manager の以前のバージョンでは、すべてのイメージのダウンロードに対して、シスコ エンド ユーザー ライセンス契約（EULA）と K9 プロンプトに同意する必要がありました。バージョン 4.23 以降では、イメージをダウンロードするたびに EULA および K9 のプロンプトは表示されません。
GeoIP手動アップロード（GeoIP Manual Upload） [GeoIP手動アップロード（GeoIP Manual Upload）] フィールドを使用して、Cisco.com からダウンロードした MaxMind GeoLite City 更新パッケージを使用して、Cisco Security Manager の地理的位置データベースを更新します。 （注） 新しい更新パッケージは、Cisco.com で毎月提供されます。	

要素	説明
GeoIPデータベースアーティファクトの場所（GeoIP Database Artifact Location）	[参照（Browse）] をクリックし、Cisco.com からダウンロードした MaxMind GeoLite City 更新パッケージに移動して選択します。次に、[アップロード（Upload）] をクリックして、選択したデータベースを Cisco Security Manager にアップロードします。 （注） MaxMind 社またはその他のソースから直接取得した位置情報の更新は、Cisco Security Manager ではサポートされていません。
GeoIP Maxmindデータベースの更新設定（GeoIP Maxmind Database Update Settings） MaxMind GeoLite City 更新パッケージは、Cisco.com で毎月更新されます。[GeoIP Maxmind データベースの更新設定（GeoIP Maxmind Database Update Settings）] を使用して、更新パッケージを Cisco.com から自動的にダウンロードし、スケジュールされた更新を設定します。 （注） 地理的位置データベースを自動更新するには、Cisco.com に接続するためのログイン情報が必要です。[CCO設定の編集（Edit CCO Settings）] リンクを使用して、ログイン情報が設定されている [CCO設定（CCO Settings）] ページに迅速に移動できます。[CCO設定（CCO Settings）] ページの詳細については、[CCO設定（CCO Settings）] ページ （5 ページ）を参照してください。	
即時データベース更新を実行する（Run immediate database update）	[今すぐ更新（Update Now）] をクリックして、Cisco.com にある最新の更新パッケージを使用して、Cisco Security Manager の地理的位置データベースを更新します。

要素	説明
スケジュールされた更新の有効化（Enable scheduled update）	地理的位置データベースの自動更新を定期的なスケジュールで有効にするか無効にするかを指定します。スケジュールされた更新を有効にしたら、[設定の編集（Edit Settings）] をクリックして、更新を実行するスケジュールを指定します。 [毎週（Weekly）] オプションを使用して、自動更新を実行する曜日を指定できます。[毎月（Monthly）] オプションを使用して、自動更新を実行する日付を指定できます。いずれのオプションでも、更新の実行時刻を指定できます。 ヒント　地理的位置データベースは、毎月第 1 火曜日に MaxMind 社によって更新されます。新しい更新パッケージは、通常、MaxMind 社が発行してから約 1 週間後に Cisco.com で入手可能になるため、毎月 15 日以降に更新スケジュールを設定することを推奨します。ただし、更新されたデータベースが Cisco.com で利用可能になる時刻にできるだけ近い時刻に Cisco Security Manager で利用可能にする場合は、更新をより頻繁に実行するようにスケジュールできます。 （注）　バージョン 4.9 以降、Cisco Security Manager では、cisco.com からアップデートをダウンロードする前に、シスコ エンド ユーザー ライセンス契約（EULA）を読んで同意することが義務付けられています。 Cisco Security Manager の以前のバージョンでは、すべてのイメージのダウンロードに対して、シスコ エンド ユーザー ライセンス契約（EULA）と K9 プロンプトに同意する必要がありました。バージョン 4.23 以降では、イメージをダウンロードするたびに EULA および K9 のプロンプトは表示されません。
デフォルトのブロッキング範囲（Default Blocking Ranges）	デフォルトで GeoIP ルックアップから除外される IP アドレスの範囲を一覧表示します。 0.0.0.0、255.255.255.255、127.0.0.1、10.0.0.0 ～ 10.255.255.255、169.254.0.0 ～ 169.254.255.255、172.16.0.0 ～ 172.31.255.255、192.168.0.0 ～ 192.168.255.255、224.0.0.0 ～ 239.255.255.255

要素	説明
ユーザー定義のブロッキング範囲（User-defined Blocking Ranges）	GeoIP ルックアップ要求から除外する必要がある追加の IP アドレスまたはアドレスの範囲を指定します。[編集（Edit）]（鉛筆）ボタンをクリックして [IPv4ブロック範囲アドレスの編集（Edit IPv4 Blocking Range Addresses）] ダイアログボックスを開き、除外する IPv4 アドレスまたはアドレスの範囲を指定できます。複数のエントリを指定する場合は、カンマ「,」で区切ります。
[Whois]	
Whoisルックアップサービスの有効化（Enable Whois Lookup Service）	Whois ルックアップサービスを有効にするか無効にするかを指定します。IP インテリジェンスツールを使用して IPv4 アドレスの WHOIS 情報を取得できるようにする場合は、このサービスを有効にします。
外部プロキシの有効化（Enable External Proxy）	Whois リクエストに対して外部プロキシの使用を有効にするか無効にするかを指定します。プロキシサーバーの設定は、[CCO設定（CCO Settings）] ページで指定します。 ヒント [CCO設定の編集（Edit CCO Settings）] リンクを使用して、プロキシサーバー設定が設定されている [CCO設定（CCO Settings）] ページに迅速に移動できます。[CCO設定（CCO Settings）] ページの詳細については、[CCO設定（CCO Settings）] ページ（5 ページ）を参照してください。
デフォルトのブロッキング範囲（Default Blocking Ranges）	デフォルトで Whois ルックアップから除外される IP アドレスの範囲を一覧表示します。 0.0.0.0、255.255.255.255、127.0.0.1、10.0.0.0 ～ 10.255.255.255、169.254.0.0 ～ 169.254.255.255、172.16.0.0 ～ 172.31.255.255、192.168.0.0 ～ 192.168.255.255、224.0.0.0 ～ 239.255.255.255
ユーザー定義のブロッキング範囲（User-defined Blocking Ranges）	Whois ルックアップ要求から除外する必要がある追加の IP アドレスまたはアドレスの範囲を指定します。[編集（Edit）]（鉛筆）ボタンをクリックして [IPv4ブロック範囲アドレスの編集（Edit IPv4 Blocking Range Addresses）] ダイアログボックスを開き、除外する IPv4 アドレスまたはアドレスの範囲を指定できます。複数のエントリを指定する場合は、カンマ「,」で区切ります。

要素	説明
統計情報の表示（View Statistics）	IP インテリジェンス機能の統計を表示する [IPインテリジェンス統計（IP Intelligence Statistics）] ダイアログボックスを開きます。[IPインテリジェンス統計（IP Intelligence Statistics）] ダイアログボックスに表示される情報は次のとおりです。 • 過去 5 分間および過去 15 分間の IP インテリジェンス ルックアップ リクエストの平均数 • すべての IP インテリジェンス サービス リクエストの平均ルックアップ時間 • 現在有効になっている個々のサービスの平均ルックアップ時間 • 現在有効になっている個々のサービスに対して成功および失敗したルックアップの数 • 現在有効になっている個々のサービスのキャッシュヒット率 • GeoIP 更新のアップロード情報：更新の最終更新時刻、ステータス、およびバージョン情報 [更新（Refresh）] をクリックして、[IPインテリジェンス統計（IP Intelligence Statistics）] ダイアログボックスのデータを更新します。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[イベント通知設定（Eventing Notification Settings）] ページ

[イベント通知設定（Eventing Notification Settings）] ページを使用して、IPS イベントおよび重要な ASA イベントの電子メール通知を受信します。電子メール通知を受信する時間間隔を設定できます。

イベントは、.zip ファイル形式内の .CSV ファイルの形式で送信されます。デフォルトでは、電子メール通知はディセーブルになっています。電子メール通知を有効にすると、IPS イベントの通知のみが有効になります。重要なイベントの電子メール通知を受信するには、重要なイベント用の追加設定をイネーブルにする必要があります。

（注） Security Manager により通知が正常に送信されるように、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定で説明しているように SMTP サーバーを設定する必要があります。

ヒント Security Manager Event Viewer アプリケーションまたはダッシュボードを使用して、すべてのイベントを表示および監視することもできます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント通知設定（Eventing Notification Settings）] を選択します。

フィールド リファレンス

表 *24 : [イベント通知設定（Eventing Notification Settings）] ページ*

要素	説明
イベント電子メール通知の有効化（Enable Eventing Email Notification）	電子メールによる IPS イベントの通知を有効にする場合に選択します。
通知間隔（Notification Interval）（15 ～ 60 分）	Security Manager が IPS イベントまたは重要なイベントの電子メール通知を送信する間隔を入力します。 （注） Security Manager が設定された時間間隔中に 50000 を超えるイベントを受信した場合、最初の 50000 件のイベントのみが選択され、電子メールで送信されます。
通知設定（IPS）	
電子メールID（IPS イベント用）（Email IDs (for IPS Events)）	電子メールアドレスを1つ以上入力します（コンマ区切り）。
イベント重大度の選択（Select Severity of Events）	IPS シグニチャによってレポートされる重大度レベル（[高（High）]、[中（Medium）]、[低（Low）]、または [情報（Informational）]）。デフォルトでは、[高（High）] と [中（Medium）] の重大度が選択されています。

要素	説明
通知の内容	要約通知と詳細通知のどちらを電子メールで送信するかを指定します。[詳細な通知（Detailed Notifications）] を選択した場合は、電子メール通知に含める必要がある情報のフィールドを選択します。一部のフィールドは、デフォルトで選択されています。
フィールド	
イベント ID（Event ID）	内部で各イベントに割り当てられる一意の連続番号。
重大度	ファイアウォールまたは IPS の重大度の値。
デバイス	イベントの送信元。通常はデバイス ID です。 Not Available と識別されたデバイスは、Security Manager インベントリから削除されています。
アプリケーション	イベントを発生させているアプリケーションの名前。
Receive Time	イベントが Security Manager によって受信された時刻。
イベント時間	デバイスによりイベントが生成された時間。
センサーのローカル時刻（Sensor Local Time）	イベントが発生したセンサーの現地時刻。
Sig ID	Sig ID 値は、アラート発信者がアクティビティを特定するために使用されます。この値により、アクティビティにあらかじめ定義されているシグニチャを識別できます。
サブシグニチャ ID（Sub Sig. ID）ID	このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャIDによって、広範なシグニチャのより詳細なバージョンが識別されます。
シグニチャ名（Sig. Name）名前	証明書に割り当てられる名前を示します。
シグニチャ詳細（Sig. Detail）詳細（Details）	レポートされたシグニチャの詳細。トリガーされて、アラートの生成を引き起こしたシグニチャです。
シグニチャバージョン（Sig. Version）バージョン	アラートの生成に使用されたシグニチャ定義のバージョン。
Attacker IP	攻撃パケットを送信するホストの IP アドレス。
Attacker Port	攻撃者ホストによって使用されるポート。これは、攻撃パケットの発信元のポートです。

要素	説明
攻撃者の所在（Attacker Locality）	攻撃者のアドレスが、侵入検知デバイスの設定で指定された特定のネットワークの内側に存在するか、外側に存在するかを識別します。
攻撃対象IP（Victim IP）	攻撃されているホストの IP アドレス。
攻撃対象のポート	攻撃されているホスト（攻撃パケットの受信者）のポート。これは、攻撃パケットの送信先のポートです。
攻撃対象の OS	攻撃されているホストの OS。
攻撃対象の所在地	攻撃対象のアドレスが、侵入検知デバイスの設定で指定された特定のネットワークの内側に存在するか、外側に存在するかを識別します。
サマリーカウント（Summary Count）	サマリーアラートであり、特性が共通する 1 つ以上のアラートを表したものです。数値は、「initialAlert」属性値との一致により、最後のサマリーアラート以降にシグニチャが発行された回数を示します。
初期アラート（Initial Alert）	このフィールドはサマリーアラートに適用され、特性が共通する 1 つ以上のアラートを表したものです。値 initialAlertは、特性（sigid/subsigid）が同じでサマリーアラートではない最後の evIdsAlert のイベント ID です。
Summary Type	サマリーアラートのすべてのアラートに共通する特性を定義します。
最後（Is Final）	サマリーアラートに適用され、特性が共通する 1 つ以上のアラートを表したものです。このアラートが、 initialAlert 属性に同じ値を含む最後のイベントアラートであるかどうかを示します。
インターフェイス	IPS インターフェイスの名前。
VLAN	アラートをトリガーしたアクティビティにかかわるパケットに関連付けられた VLAN 番号。
仮想センサー	イベントに関連付けられた仮想センサーの名前。
[実施アクション（Action Taken）]	フローに対して実行されるアクション。たとえば、終了や拒否。
アラート詳細（Alert Details）	アラートに関する詳細。
Risk Rating	イベントに関連付けられたリスクを計算した値。
Threat Rating	イベントの脅威レーティング（ある場合）。

要素	説明
レピュテーション	-10.0 ～ +10.0 で示される攻撃者のレピュテーションスコア。スコアが低い（負の値が大きい）ほど、ホストが悪意のあるホストである可能性が高くなります。
レピュテーションの詳細（Reputation Details）	攻撃者の拒否（Deny Attacker）：リスクレーティングを算出した結果、内部オーバーライドを超えたために、攻撃者拒否アクションが発生した（または発生することになっていた）のかどうかを示す true または false。
Protocol	Level-3 プロトコルまたは Level-4 プロトコル。
通知設定 （Notification Settings）（重要なイベントのみ）	
有効 電子メール ID（Email IDs）	重要なイベントについて電子メール通知を送信するかどうか。このオプションを選択した場合は、1 つ以上の電子メール アドレスも入力します（カンマ区切り）。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[IPS Updates] ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

[IPS Updates] ページを使用して、シグニチャ、マイナーなバージョン更新、およびサービス パックに関して、センサーを最新の状態に保持するための管理タスクを実行します。[IPS Updates] ページを使用して、次のことを実行できます。

- 更新ステータスをモニタする。
- 取得可能な更新を確認し、それらをダウンロードする。
- IPS 更新サーバを設定する。
- 自動更新の設定値を設定する。

（注） Security Manager バージョン 4.9 以降、IPS の最新のセンサーおよびシグネチャパッケージのみが CCO からダウンロードできます。古いパッケージは、CCO からダウンロードできません。

ヒント

- IPS 更新を手動で適用するには、[ツール（Tools）] > [IPS更新の適用（Apply IPS Update）] を選択します。詳細については、IPS 更新の手動適用を参照してください。
- 後にシグニチャの更新を適用する必要はなかったと判断した場合は、デバイスで [シグネチャ（Signatures）] ポリシーを選択し、[更新レベルの表示（View Update Level）] ボタンをクリックしてから [Revert] をクリックすることで、直前の更新レベルに戻すことができます。

バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、Cisco.com 証明書の処理改善に役立ちます。この機能の詳細については、証明書信頼管理を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [IPSの更新（IPS Updates）] を選択します。

関連項目

- IPS 更新サーバの設定
- IPS 更新の確認とダウンロード
- IPS 更新の自動化
- Cisco IOS IPS のシグニチャ カテゴリの選択

フィールド リファレンス

表 *25 : [IPS Updates]* ページ

要素	説明
[Update Status] グループ [Refresh] ボタン	次の項目を表示します。[更新（Refresh）]をクリックして、情報を更新してください。 • [Latest Available]：Cisco.com または最後に更新を確認したときのローカルHTTPサーバで取得可能な最新のシグニチャおよびセンサーの更新。 • [Latest Downloaded]：Security Manager にダウンロードされた、最新のシグニチャおよびセンサーの更新。 • [Latest Applied]：Security Manager でデバイスに適用された、最新のシグニチャおよびセンサーの更新。 • [Latest Deployed]：Security Manager でデバイスに展開された、最新のシグニチャおよびセンサーの更新。 • [Last Check On]：Cisco.com の確認を最後に実行した時間。 • [Last Download On]：最後の更新が Security Manager にダウンロードされた時間。 • [Last Deployed On]：いずれかのデバイスに最後の更新が展開された時間。

要素	説明
[Check for Updates] ボタン [Download Latest Updates] ボタン	これらのボタンによって、更新が確認されるか、またはSecurity Managerサーバにまだダウンロードされていないシグニチャおよびセンサー更新がIPS更新サーバからダウンロードされます。更新の確認またはダウンロードの前に、IPS更新サーバーを設定する必要があります（[サーバーの更新（Update Server）] グループで [設定の編集（Edit Settings）] をクリックします）。 これらのボタンのいずれかをクリックすると、ダイアログボックスが開き、操作の結果が表示されます。ユーザが [Download] ボタンをクリックすると、Security Manager は IPS 更新サーバにログインして更新を確認し、更新をダウンロードします。Cisco.com からのダウンロードに失敗する場合は、使用しているアカウントで強化暗号化ソフトウェアをダウンロードできることを確認してください。詳細については、[Edit Update Server Settings] ダイアログボックス （73 ページ）の [User Name] の説明を参照してください。 **ヒント** サーバーを設定し、次に更新を確認しようとしたときに、サーバーを設定していないと通知された場合は、このページの一番下にある [保存（Save）] をクリックして、再試行してください。 **（注）** バージョン 4.9 以降、Cisco Security Manager では、cisco.com からアップデートをダウンロードする前に、シスコ エンド ユーザー ライセンス契約（EULA）を読んで同意することが義務付けられています。 Cisco Security Manager の以前のバージョンでは、すべてのイメージのダウンロードに対して、シスコエンドユーザーライセンス契約（EULA）と K9 プロンプトに同意する必要がありました。バージョン 4.23 以降では、イメージをダウンロードするたびに EULA および K9 のプロンプトは表示されません。
[Update Server] グループ	Cisco.com、または IPS 更新パッケージが格納されているローカル サーバへのアクセスに使用する設定を表示します。これらのフィールドには、Update サーバが Cisco.com とローカルに設定された HTTP サーバのいずれであるか、ローカル サーバを使用する場合はローカル サーバの名前、サーバにログインするためのユーザ アカウント、およびプロキシ サーバの名前（ある場合）が示されます。IPS更新サーバーを設定または変更するには、[設定の編集（Edit Settings）] をクリックして [サーバー設定の更新の編集（Edit Update Server Settings）] ダイアログボックスを開きます（[Edit Update Server Settings] ダイアログボックス （73 ページ）を参照）。 詳細については、IPS 更新サーバの設定を参照してください。 バージョン4.4以降、Security Managerには証明書信頼管理機能があります。この機能は、Cisco.com 証明書の処理改善に役立ちます。この機能の詳細については、証明書信頼管理を参照してください。

要素	説明
シグニチャフィルタ設定グループ	IPS シグネチャアップデートを選択的にダウンロードできます。[設定の編集（Edit Settings）] をクリックして、[シグネチャダウンロードフィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログ ボックスを開きます（[シグネチャ ダウンロード フィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックス （77 ページ） を参照）。
[Auto Update Settings] グループ	自動更新に固有の設定が含まれています。詳細については、IPS 更新の自動化を参照してください。
Auto Update Mode	自動更新を実行するかどうか、およびどの程度実行するかを設定します。次のオプションがあります。 • Download, Apply, and Deploy Updates • Disable Auto Update • 更新の確認（Check for Updates） • Download Updates • Download and Apply Updates デフォルトでは、自動更新はディセーブルになっています。その他のオプションは、次のオプションを 1 つ以上組み合わせたものとなります。 • [Check for Updates]：Security Manager は、IPS 更新サーバに接続して更新を取得できるかどうかを確認し、電子メール通知が設定されている場合は、電子メールを送信します。ファイルはダウンロードされません。 • [Download Updates]：Security Manager は最新の更新を IPS 更新サーバからダウンロードし、電子メール通知が設定されている場合は、電子メールを送信します。 • [Apply Updates]：Security Manager は、ダウンロードされた更新パッケージに基づいて、[Apply Update To] リストで選択されているデバイスの設定を変更します。[Deploy Updates] も選択している場合を除き、これらの更新は個別に展開する必要があります。 • [Deploy Updates]：Security Manager は、展開ジョブを開始して、適用可能な更新パッケージを、[Apply Update To] リストで選択されているデバイスに送信します。デバイスは、シグニチャ更新の成功に必要なライセンスを取得している必要があります。

要素	説明
スケジュールの更新 [Edit Update Schedule] ボタン	[Auto Update Mode] フィールドで選択されたアクションのスケジュール。このスケジュールを変更するには、[更新スケジュールの編集（Edit Update Schedule）] をクリックし、[IPS更新スケジュールの編集（Edit IPS Updates Schedule）] ダイアログボックスでスケジュールを定義します。Security Managerが毎時間、毎日、毎週、または毎月のスケジュールに基づいて更新を実行することを指定したり、1 回かぎりのイベントを指定したりできます。開始時間を入力する場合は、24 時間制の *hh:mm* 形式を使用してください。 （注） Security Managerサーバーの時刻から10分以内に更新が行われるようにスケジュールすると、[次の更新（Next Update）] フィールドに明日の日付が表示され、それに応じてジョブが実行されます。これは、最初の実行を保証するために設計された安全機能です。 ヒント 自動ダウンロードを時間外にスケジュールして、デバイス検出などの他のユーザ操作と競合しないようにすることを推奨します。 ヒント 通常のユーザ操作には、管理者アカウント以外のアカウントを使用することをお勧めします。
Notify Email	自動更新の通知が送信される電子メール アドレス。複数のアドレスを入力する場合は、それらのアドレスをカンマで区切ります。通知は、更新が次の状態になると送信されます。 • ダウンロードが可能になった。 • ダウンロードされた。 • ダウンロードされ、適用された。 • ダウンロードされ、適用され、展開された。

要素	説明
Apply Update To タイプ（Type） [Edit Row] ボタン Devices to be Auto Updated	このセレクタには、Security Manager で定義されたローカル シグニチャ ポリシーおよび共有シグニチャ ポリシーを持つIPSデバイスが含まれています。セレクタのカラムは、ローカル デバイス ポリシーまたは共有ポリシーが、次の更新タイプに関して選択されているかどうかを示します。 • [Signature]：シグニチャ更新レベルの自動更新の場合。 • [Minor]：マイナー更新およびサービス パックの場合。 • [S.P.]：サービス パック更新の場合。 共有ポリシーの場合、一部がグレー表示になっているチェックボックスは、このポリシーを使用するデバイスの全部ではなく一部が選択されていることを示します。自動更新イベント中に、共有ポリシーに割り当てられているデバイスを変更すると、その共有ポリシーはグレー表示され、古い割り当てだけがこのページに表示されます。更新を実行したあとに、この割り当てリストは共有ポリシーのデバイス割り当てと同期されます。次の自動更新が実行される前に、このデバイス リストをプロアクティブに更新するには、ポリシーを選択して編集します（自動更新設定を選択します）。これで、デバイス割り当てリストが訂正されます。 （注） また、共有ポリシーの場合：デフォルトの仮想センサー（vs0）に割り当てられた共有ポリシーのみを選択できます。別の仮想センサーの共有ポリシーを選択しようとしても、変更は適用されず、エラーメッセージは受け取りません。 [Type] フィールドを使用して、ローカル ポリシーと共有ポリシーの表示を切り替えます。表示を変更しても、自動更新の選択内容は変更されません。 自動更新用のローカルまたは共有ポリシーを選択するには、このセレクタで選択し、セレクタの下にある [行の編集（Edit Row）] ボタンをクリックします。これにより、[Edit Auto Update Settings] ダイアログボックスが開きます。このダイアログボックスで、ポリシーの更新タイプを選択できます。いずれかの自動更新タイプをポリシーに選択すると、影響を受けるデバイスが、セレクタの右にある [自動更新されるデバイス（Devices to be Auto Updated）] リストに一覧表示されます。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Edit Update Server Settings] ダイアログボックス

[Edit Update Server Settings] ダイアログボックスを使用して、IPS 更新の取得に使用するサーバを設定します。必要に応じて、Update サーバと通信するためのプロキシ サーバを設定できます。

また、証明書の信頼管理には [更新サーバー設定の編集（Edit Update Server Settings）] ダイアログボックスを使用します（Security Manager は、HTTPS 経由で Cisco.com から IPS パッケージをダウンロードし、信頼を確立するために証明書を使用します）。[Image Manager] ページの証明書信頼管理機能は、Security Manager 4.4 の新機能です。この機能は、IPS パッケージのダウンロードに向けた Cisco.com 証明書の処理を改善するのに役立ちます。

- この機能を使用して証明書を表示できます。証明書を受け入れるかどうか慎重に検討してください。
- 証明書を受け入れると、証明書は Security Manager サーバーに保存されます。
- [Image Manager] ページの概要テーブルにすべての証明書が表示され、そのテーブルを使用して証明書を表示または削除できます。

ヒント　下のテーブルの [証明書の取得（Retrieve Certificate）] を必ず確認してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [IPS のアップデート（IPS Updates）] を選択し、[更新サーバー（Update Server）] グループで [設定の編集（Edit Settings）] をクリックします。

フィールド リファレンス

表 26 : [Edit Update Server Settings] ダイアログボックス

要素	説明
Update From	IPS 更新を Cisco.com から取得するか、ローカル HTTP/HTTPS サーバから取得するかを指定します。ダイアログボックスのフィールドは、選択に応じて変わります。 ローカルを選択した場合は、IPS 更新サーバとして使用するように HTTP または HTTPS サーバを設定する必要があります。 **注意**　[更新元：（Update From:）] のデフォルト値は [ローカル サーバー（Local Server）] です。証明書の設定を表示するには、[Cisco.com] を選択する必要があります。証明書の設定が不適切または不完全な場合、Cisco.com への接続が妨げられ、このエリアでの Cisco.com 関連のすべての操作が失敗します。

要素	説明
IP Address/ Host Name （ローカル サーバのみ）	ローカル IPS 更新 Web サーバのホスト名または IP アドレス。
Web サーバ ポート（Web Server Port） （ローカル サーバのみ）	ローカル サーバが接続要求をリスニングするポート番号。デフォルトは 80 です。
ユーザー名	IPS 更新サーバにログインするユーザ名。ユーザ ログインが不要なローカル サーバを設定する場合は、このフィールドを空白のままにしておきます。 Cisco.com ユーザ名を指定する場合、Cisco.com 上のユーザ アカウントは、強化暗号化ソフトウェアをダウンロードできる必要があります。アカウントが必要な権限を持っているかどうか不明な場合は、このアカウントを使用して Cisco.com にログインし、IPS 更新ファイルをダウンロードしてみます（http://www.cisco.com/cgi-bin/tablebuild.pl/ips5-system）。アカウントが適切な権限を持っていない場合は、必要な条件を読んで同意するように要求されます。適格要件を満たしている場合は、これらの条件を受け入れることができます。そうでない場合は、シスコの営業担当者にお問い合わせください。
パスワード 確認（Confirm）	両方のフィールドに入力される、指定したユーザ名のパスワード。パスワードが不要なローカル サーバを設定する場合は、これらのフィールドを空白のままにしておきます。
Path to Update Files （ローカル サーバのみ）	ローカル サーバ上の IPS 更新ファイルの場所へのパス。たとえば、更新ファイルに http://local-server-ip:port/update_files_path/ でアクセスできる場合、update_files_path をこのフィールドに入力します。
Connect Using HTTPS （ローカル サーバのみ）	ローカル IPS 更新サーバに接続する場合に、SSL を使用するかどうかを指定します。
Certificate Thumbprint	ローカル サーバ上の証明書から証明書サムプリントが計算されたあとに、この証明書サムプリントを表示します。
Retrieve From Server	ダイアログボックスで指定されたローカル サーバに接続し、所定のローカル サーバから証明書を取得し、[Certificate Thumbprint] フィールドに表示される証明書サムプリントを計算するために使用します。

要素	説明
[連絡先URL（Contact URL）]	• 選択すると、[イメージメタデータロケータ（Image Meta-data Locator）] が使用されます。これは、イメージに関するメタデータ情報の取得に使用される Cisco.com の URL です。メタデータ情報は、特定の製品に該当するイメージ、名前、サイズ、チェックサム、および各イメージをダウンロードする URL で構成されます。 • 選択すると [その他（Other）] が使用されます。任意の有効な HTTPS URL を入力できます。この URL は、主に、イメージに関するメタデータ情報から取得したイメージをダウンロードするための HTTPS URL を対象としています。この URL は、前の段落で説明したイメージメタデータロケータの URL とは異なる場合があります。証明書も異なる場合があります。 **注意** [その他（Other）] を選択した場合は、明示的に "https://dl.cisco.com" を追加する必要があります（引用符は不要）。[その他（Other）]ボタンの隣のテキストフィールドに入力します。これを追加しないと、Cisco.com に接続できなくなり、このエリアでの Cisco.com 関連のすべての操作が失敗します。
[証明書の取得（Retrieve Certificate）]	選択した [連絡先URL（Contact URL）] に接続して証明書を取得するために使用されます。証明書を取得すると、[証明書の検証（Certificate Verification）] ダイアログが開きます。証明書の簡単な概要、つまり、証明書の発行対象、発行者、証明書の有効期間が表示されます。さらに、次の選択肢が表示されます。 • [証明書の表示（View Certificate）]：証明書ビューアを開いて、証明書のすべての詳細（認証局、バージョン、シリアル番号、サムプリント、その他の詳細）を表示できます。ルート発行認証局までの完全な証明書チェーン情報が表示されます。 • [承認（Accept）]：証明書を承認して、Cisco Security Manager に追加します。 • [拒否（Reject）]：証明書を拒否します。アクションは実行されません。 • [キャンセル（Cancel）]：アクションを実行せずに [証明書の検証（Certificate Verification）] ダイアログを閉じます。
証明書	Security Manager インストールの各証明書について、[情報カテゴリ（Subject）]、[発行者（Issued By）]、および [承認者（Accepted By）] を表示するテーブル。

要素	説明
表示（View）	[証明書（Certificate）] テーブルで選択した証明書の証明書ビューアを開きます。
削除（Remove）	[証明書（Certificate）] テーブルで選択した証明書を削除します。
Proxy Server Group	
Enable Proxy Server	プロキシ サーバが、Cisco.com またはローカル サーバに接続するために必要であるかどうかを指定します。
IP Address/ Host Name	プロキシ サーバのホスト名または IP アドレス。 基本的なダイジェスト NT LAN Manager（NTLM）V1 または NTLM V2 認証を使用するように、プロキシ サーバを設定できます。NTLM V2 が、最もセキュアなスキームです。
[ポート（Port）]	プロキシサーバが接続要求をリッスンするポート番号。デフォルトは 80 です。
ユーザー名	プロキシ サーバにログインするユーザ名。プロキシ サーバでユーザ ログインが必要ない場合は、このフィールドを空白のままにしておきます。
パスワード 確認（Confirm）	両方のフィールドに入力される、指定したユーザ名のパスワード。プロキシサーバでパスワードが必要ない場合は、これらのフィールドを空白のままにしておきます。

[Edit Auto Update Settings] ダイアログボックス

[Edit Auto Update Settings] ダイアログボックスを使用して、[IPS Updates] ページの [Apply Update To] テーブルで選択したデバイスまたはポリシーの自動更新オプションを設定します。自動更新の設定については、IPS 更新の自動化を参照してください。

ナビゲーション パス

[IPS Updates] ページ（[IPS Updates] ページ （66 ページ）を参照）の [Apply Update To] テーブルで、デバイスまたはポリシーを選択し、[Edit Row] ボタンをクリックします。

フィールド リファレンス

表 27 : [Edit Auto Update Settings] ダイアログボックス

要素	説明
自動更新 （IPS センサーおよび共有ポリシーだけ）	選択したデバイスまたは共有ポリシーに適用する、センサー更新のタイプ。マイナー更新とサービス パックの両方を適用したり、サービス パックだけを適用したりできます。または、[None] を選択して、センサーの更新が自動的に適用されないようにできます。
Auto Update Signature Update Level	自動シグニチャ更新にデバイスまたはポリシーを選択するかどうかを指定します。

[シグネチャダウンロードフィルタ設定の編集（EditSignatureDownload Filter Settings）] ダイアログボックス

[シグネチャ ダウンロード フィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックスでは、IPS シグネチャの更新を選択的にダウンロードできます。これは、手動ダウンロードと自動ダウンロードの両方に適用されます。

（注） フィルタ処理は、IPS センサーパッケージまたは IPS エンジンパッケージには適用されません。IPS シグネチャパッケージのみに適用されます。Cisco.com またはローカルサーバー上の使用可能なすべてのセンサーパッケージが、シグニチャダウンロードの一部としてダウンロードされます。

選択的ダウンロードの利点は、必要なものだけをダウンロードできるため、ダウンロード時間が短縮され、ディスクストレージスペースが削減され、トラブルシューティングが迅速化されることです。

[シグネチャ ダウンロード フィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックスでは、次の 4 タイプのシグネチャダウンロードを使用できます。

- [フィルタなし（No filter）]
- [[E4、E3、E2、または E1 を選択] で始まるエンジンバージョンのすべてのシグネチャをダウンロード（Download all signatures for engine versions starting with [choose E4, E3, E2, or E1]）]
- [[1000 などのシグネチャバージョンを入力] で始まるすべてのシグネチャバージョンをダウンロード（Download all signature versions starting with [enter a signature version such as 1000]）]
- [単一のシグネチャバージョン番号 [1000 などのシグネチャ番号を入力] をダウンロード（Download a single signature version number [enter a signature number such as 1000]）]

デフォルトのシグネチャ設定では、E4 以降のエンジンバージョンのシグネチャがすべてダウンロードされます。

ヒント　このデフォルト値は、Security Manager 4.3 の新規インストールでも以前のバージョンからのアップグレードでも同じです。

ナビゲーション パス

[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] を選択し、目次で [IPS の更新（IPS Updates）] を選択します。その後、[シグネチャフィルタ設定（Signature Filter Settings）] グループの [設定の編集（Edit Settings）] をクリックします。

関連項目

- IPS 更新サーバの設定
- IPS 更新の確認とダウンロード
- IPS 更新の自動化

フィールド リファレンス

表 *28 : [シグネチャ ダウンロード フィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックス*

要素	説明
[フィルタタイプ（Filter Type）] : [フィルタなし（No filter）]	使用可能なすべてのエンジン用の使用可能なすべてのシグネチャがダウンロードされます。
[フィルタタイプ（Filter Type）] : [で始まるエンジンバージョンのすべてのシグネチャをダウンロード（Download all signatures for engine versions starting with）]	選択したエンジン（E4、E3、E2、または E1）用の使用可能なすべてのシグネチャがダウンロードされます。
[フィルタタイプ（Filter Type）] : [で始まるすべてのシグネチャバージョンをダウンロード（Download all signature versions starting with）]	入力した ID で始まる使用可能なすべてのシグネチャがダウンロードされます。
[フィルタタイプ（Filter Type）] : [単一のシグネチャバージョン番号をダウンロード（Download single signature version number）]	入力した ID を持つ単一のシグネチャがダウンロードされます。

[ISE設定（ISE Settings）] ページ

[ISE 設定（ISE Settings）] ページを使用して、Cisco Security Manager とTrustSec ファイアウォールポリシーで使用する Cisco Identity Services Engine（ISE）間の通信を設定します。

（注） Cisco Security Manager は、セキュリティグループの名前とタグを取得して解決するために、1 つの ISE アプライアンス/サーバーとの通信のみサポートします。

PCI に準拠するために、Cisco Security Manager 4.15 および 4.16 では、TLS 1.0 と TLS 1.1 がそれぞれ無効になりました。したがって、4.16 以降では、Cisco Security Manager は TLS 1.2 バージョンのみを使用していました。

ただし、ISE 1.3 サーバーおよびその下位バージョンは TLS 1.2 をサポートしていません。これは、リリース 4.15 以降の Cisco Security Manager でのレガシー ISE 設定に影響します。この非互換性により、ISE サーバーと Cisco Security Manager の統合が妨げられます。

Cisco Security Manager 4.15、4.16、または 4.17 バージョンで ISE サーバー（バージョン 1.3 以前）を使用して、ISE 1.3 以前のバージョンを Cisco Security Manager と正常に統合する必要がある場合は、リリース 4.17 用の『Cisco Security Manager User Guide』を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ISE設定（ISE Settings）] を選択します。

関連項目

- Trustsec ファイアウォールポリシーの管理
- セキュリティ グループ オブジェクトの作成
- ポリシーでのセキュリティグループの選択

フィールド リファレンス

表 29 : [Identity Settings] ページ

要素	説明
ISE 機能の有効化（Enable ISE feature）	ISE との通信をイネーブルにするかどうかを指定します。
ユーザー名	Security Manager が、ISE にログインするときに使用するユーザ名。
パスワード	ユーザー名のパスワード。

要素	説明
ISEサーバー（IPアドレス/ホスト名）（ISE Server (IP Address/Hostname)）	ISE の DNS ホスト名または IP アドレス
ISEバージョン（ISE Version）	バージョン 4.18 以降、Cisco Security Manager は ISE バージョン 2.3 の統合のみをサポートします。
接続のテスト	[接続のテスト（Test Connectivity）] をクリックして、入力した設定で Security Manager が ISE と通信できることを確認します。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

Licensing ページ

[Licensing] ページを使用して、Security Manager アプリケーションおよび IPS デバイス用のライセンスを管理します。詳細については、IPS ライセンスの管理を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ライセンス（Licensing）] を選択します。

フィールド リファレンス

表 *30 : Licensing* ページ

要素	説明
[CSM] タブ	Security Manager アプリケーションのライセンス設定。このタブの各フィールドの説明については、[CSM] タブ、[Licensing] ページ （81 ページ）を参照してください。
[IPS] タブ	Security Manager によって管理される IPS デバイスのライセンス設定。このタブの各フィールドの説明については、[IPS] タブ、[Licensing] ページ （81 ページ）を参照してください。

[CSM] タブ、[Licensing] ページ

[Licensing] ページの [CSM] タブを使用して、インストール済みの Security Manager ライセンスのリストを表示し、新しいライセンスをインストールします。詳細については、Security Manager のライセンス ファイルのインストールを参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ライセンス（Licensing）] を選択し、[CSM] をクリックします。

フィールド リファレンス

表 31 : [CSM] タブ、[Licensing] ページ

要素	説明
ライセンス情報	製品に登録されているライセンスに関する情報（エディション、ライセンス タイプ、有効期限、ライセンス対象デバイスの数、使用中のデバイス数、および使用されているデバイス数のパーセンテージ）を表示します。
ライセンスのインストール	インストールしたライセンスおよびそのインストール日のリスト。
Install a License button	このボタンをクリックして、ライセンス ファイルをインストールします。開いているこのダイアログボックスには、Cisco.com へのリンクが含まれています。ライセンスをまだ取得していない場合は、Cisco.com でライセンスを取得できます。ライセンス ファイルは、Security Manager サーバ上のローカル ドライブにコピーしてからインストールする必要があります。

[IPS] タブ、[Licensing] ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、拡張機能はサポートしていません。

[Licensing] ページの [IPS] タブを使用して、インストール済みの IPS デバイス ライセンスのリストを表示したり、新しいライセンスまたは更新されたライセンスをインストールしたり、ライセンスを再展開したりします。このライセンス リストには、現在のライセンス、ライセンスを取得していないデバイス、ライセンスの有効期限が切れているデバイス、およびライセンスが無効なデバイスが表示されます。また、このページの設定を使用して、ライセンスが指定された日数以内に期限切れになるすべての IPS デバイスのレポートを送信できます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ライセンス（Licensing）] を選択し、[IPS] をクリックします。

関連項目

- IPS ライセンス ファイルの更新
- IPS ライセンス ファイルの再展開
- IPS ライセンス ファイル更新の自動化
- [License Update Status Details] ダイアログボックス （86 ページ）
- テーブルのフィルタリング
- テーブル カラムおよびカラム見出しの機能

フィールド リファレンス

表 32 : [IPS] タブ、[Licensing] ページ

要素	説明
IPS License Table	情報を最後にリフレッシュした時点での、デバイスインベントリ内のすべての IPS デバイスおよびそのライセンス ステータスを表示します。[更新（Refresh）] ボタンをクリックして、デバイスから最新の情報を取得します。 情報には、デバイスのシリアル番号（ライセンスの登録に使用）、ライセンス ステータス、およびライセンスの有効期限が含まれます。このリストには、現在のライセンスだけでなく、ライセンスを取得していないデバイス、ライセンスの有効期限が切れているデバイス、およびライセンスが無効なデバイスも表示されます。 **ヒント** このリストには、Cisco IOS IPS デバイスは含まれていません。Security Manager は、IPS を実行しているルータのライセンス管理には使用できません。

要素	説明
[Update Selected via CCO] ボタン	このボタンをクリックして Cisco.com に接続し、新しいライセンスを取得して、選択したデバイスのライセンスファイルを更新します。このボタンをクリックすると、ダイアログボックスが表示され、Cisco.com から更新可能なデバイスが示されます。選択したすべてのデバイスが表示されるとはかぎりません。[OK] をクリックして、更新を実行します。正常に更新するために、更新されたファイルがデバイスに自動的に適用されます。 この方法でライセンスを更新するには、選択したデバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。 **ヒント** ライセンスが格納されたシスコのソフトウェア ライセンス サーバ（SWIFT）は、同じサーバから 3 分間に 10 ライセンス以上の要求があると、その要求をブロックする場合があります。そのため、手動でライセンス更新を実行するときは、一度に選択するデバイスを 8 つ以下にしてください。
[Redeploy Selected Licenses] ボタン	このボタンをクリックして、選択したデバイスにライセンスを再展開します。ライセンスの再展開は、更新されたライセンス ファイルを取得し、そのファイルが自動更新時にデバイスに正常に適用されなかった場合に必要となる場合があります。 このボタンをクリックすると、ダイアログボックスが開き、再展開するライセンスのデバイスが表示されます。[OK] をクリックして、更新を実行します。正常に更新するために、更新されたファイルがデバイスに自動的に適用されます。
[Update from License File] ボタン	このボタンをクリックし、Security Manager サーバからライセンス ファイルを選択して、ライセンスを更新します。このボタンをクリックすると、ダイアログボックスが開き、そこでライセンスファイルを指定できます。[参照（Browse）] をクリックして、ファイルを選択します。ファイルは、Cisco Security Manager サーバー上のローカルドライブに存在する必要があります。[OK] をクリックすると、更新されたファイルがデバイスに自動的に適用されます。
[名前を付けてエクスポート（Export As）] ボタン	リストから 1 つ以上の IPS デバイスを選択し、[名前を付けてエクスポート（Export As）] ボタンをクリックして、ライセンスを Portable Document Format（PDF）またはカンマ区切り値（CSV）ファイルにエクスポートします。Security Manager サーバ上のフォルダを選択し、ファイル名を指定するように要求されます。リストからデバイスを選択しない場合、使用可能なすべてのデバイスのライセンスがエクスポートされます。

要素	説明
[Refresh License] ボタン	選択したデバイスの IPS ライセンステーブルのデータをリフレッシュするには、このボタンをクリックします。更新された情報がデバイスから取得されます。デバイスを選択しないと、すべてのデバイスのデータがリフレッシュされるため、リストに含まれるデバイスの数によっては長時間かかる場合があります。
Download and apply licenses Days before the expiration date	IPS ライセンスを Cisco.com から自動的にダウンロードし、それらのライセンスをデバイスに自動的に適用するかどうかを指定します。自動更新を設定するには、IPS デバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。 このオプションを選択した場合は、ライセンスの有効期限が切れるまでの日数も指定して、その間にライセンスをダウンロードして適用できるようにします。Security Manager は、ライセンスのないデバイス、ライセンスの有効期限が切れたデバイス、またはライセンスは有効だが、ここで指定した日数以内に期限切れになるデバイスだけを評価します。有効期限が現在のライセンスより長いか、または異なるライセンス情報を持つ、有効なライセンスのみが適用されます。
Discover devices daily at	自動ライセンス更新を選択した場合に、Security Manager がデバイスに接続して現在のライセンスのステータスを確認し、指定した日数以内に期限切れになるデバイスがあるかどうかを評価する時刻を指定します。1 つ以上のデバイスが有効期限切れの条件を満たしている場合にだけ、Cisco.com に接続します。
Email License Update Results 電子メール通知	有効期限切れのアラートとライセンス更新ジョブの結果を通知する電子メールを送信するかどうかを指定します。このオプションを選択した場合は、1 つ以上の電子メールアドレスも入力します（カンマ区切り）。
ライセンス有効期限ステータスの電子メール送信（Email License Expiration Status） 電子メール通知	ライセンスが指定された日数以内に期限切れになる IPS デバイスの PDF レポートを送信するかどうかを指定します。このオプションを選択した場合は、次のようになります。 • Cisco Security Manager が PDF レポートを送信するデバイスライセンスの有効期限までの日数（100 以下）を入力します。 • Cisco Security Manager がライセンスの有効期限をチェックする日時を選択します。 • ライセンス有効期限ステータス PDF レポートの送信先となる 1 つ以上の電子メールアドレス（カンマ区切り）を入力します。
[Save] ボタン	自動ライセンス更新と電子メール通知設定の変更を保存します。

ライセンスを更新または再展開する IPS デバイスの確認

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

[ライセンス（Licensing）] > [IPS] タブでデバイスを選択し（[IPS] タブ、[Licensing] ページ（81 ページ）を参照）、Cisco.com（CCO）からライセンスを更新したり、ライセンスを再展開したりしようとすると、更新されるデバイスのリストが最初に表示されます。ダイアログボックスの名前は、実行するアクションによって異なります。

- [CCO経由でのライセンスの更新（Updating Licenses via CCO）] ダイアログボックス：Cisco.com から更新するために選択した IPS デバイスを確認します。このデバイス リストには、Cisco.com からライセンスを更新できる IPS デバイスが表示されます。選択したすべてのデバイスが表示されるとはかぎりません。

この方法でライセンスを更新するには、選択したデバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。

ヒント ライセンスが格納されたシスコのソフトウェア ライセンス サーバ（SWIFT）は、同じサーバから 3 分間に 10 ライセンス以上の要求があると、その要求をブロックする場合があります。そのため、手動でライセンス更新を実行するときは、一度に選択するデバイスを 8 つ以下にしてください。

- [ライセンスの再展開（Redeploying Licenses）] ダイアログボックス：ライセンスを再展開するために選択した IPS デバイスを確認します。ライセンスをデバイスに再展開する場合は、そのライセンスが展開済みである必要があります。Security Manager は、すでに IPS デバイスと関連付けられているファイルを使用して、ライセンスを再展開します。

[OK] をクリックすると、[ライセンス更新ステータスの詳細（License Update Status Details）] ダイアログボックスが開き、ライセンス再展開タスクのステータスを表示できます。[License Update Status Details] ダイアログボックス （86 ページ）を参照してください。

ナビゲーション パス

これらのダイアログボックスを開くには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ライセンス（Licensing）] > [IPS]** タブで 1 つ以上のデバイスを選択し、[CCO経由で選択内容を更新（Update Selected via CCO）] または [選択したライセンスの再展開（Redeploy Selected Licenses）] をクリックします。

IPS ライセンス ファイルの選択

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [ライセンス（Licensing）] > [IPS] タブで 1 つ以上のデバイスを選択し、[ライセンスファイルからの更新（Update from License File）] をクリックすると、[ファイルからライセンスを更新（Updating Licenses from File）] ダイアログボックスで使用するライセンスファイルを選択するように要求されます。

ライセンスファイルはSecurity Managerサーバーのローカルドライブに保存することが可能で、Security Managerのバージョン4.5以降は、クライアントのローカルドライブに保存できます。

[参照（Browse）] をクリックしてライセンスファイルを選択します。Ctrl を押しながらクリックして複数のライセンス ファイルを選択したり、Shift を押しながらクリックしてファイルの範囲を選択したりできます。

（注） Security Manager サーバーがインストールされているマシンとは別のマシンに Security Manager クライアントをインストールした場合は、クライアントマシンまたはサーバーマシンのどちらからライセンスファイルを選択するかを選択できます。クライアントとサーバーの両方が同じマシンにインストールされている場合、Security Managerでは、ライセンスファイルをサーバーのみから選択できます。

使用するライセンスファイルを選択したら、[OK] をクリックして、それらのファイルを IPS デバイスに適用します。

（注） ライセンスファイルをクライアントマシンに保存する場合は、[デスクトップのカスタマイズ（Customize Desktop）] ページで [クライアント側のファイルブラウザを有効にする（Enable Client side file browser）] を選択する必要があります（[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）]）。

[License Update Status Details] ダイアログボックス

[License Update Status Details] ダイアログボックスを使用して、IPS ライセンス更新タスクのステータスを表示します。このダイアログボックスは、[Licensing] ページの [IPS] タブから更新タスクを起動するたびに開きます。詳細については、[IPS] タブ、[Licensing] ページ （81 ページ）を参照してください。

フィールド リファレンス

表 *33 : [License Update Status Details]* ダイアログボックス

要素	説明
進行状況バー	現在のデバイス上でライセンス更新タスクが何%完了したかを示します。
ステータス	更新タスクの現在の状態。
Devices to be updated	このタスク中に更新されるデバイスの総数。
Devices updated successfully	エラーが発生することなく更新されたデバイスの数。
Devices updated with errors	更新中にエラーが発生したデバイスの数。
Device list	更新されるデバイス。デバイス名、更新のステータス、および更新に関する概要情報が含まれます。デバイスを選択し、要約リストの下にあるメッセージリストで、そのデバイスの更新中に生成されたメッセージを確認します。
Messages list	ライセンス更新中に、選択したデバイスに関して生成されたメッセージ。メッセージを選択すると、リストの右側のフィールドに詳細情報が表示されます。
説明	[Message list] で選択されたメッセージに関する詳細情報。
操作	説明されている問題を解決するために実行する必要がある手順。
[Abort] ボタン	ライセンス更新タスクを中断します。

[Logs] ページ

[Logs]ページを使用して、監査ログおよび操作ログのデフォルト設定値を設定します。監査ログによって、Security Manager で発生したすべての状態変更の記録が保持されます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ログ（Logs）] を選択します。

関連項目

- [Audit Report] ウィンドウの使用
- 監査レポートについて
- 監査レポートの生成

- 監査ログ エントリのページ

フィールド リファレンス

表 *34 : [Logs]* ページ

要素	説明
手動削除	
監査ログをDBに保持する期間（日）（Keep Audit Log in DB For (days)）	削除する前にデータベースに保存する必要がある監査ログエントリの最大日数。
最後の監査ログをDBに保持する（エントリ）（Keep Audit Log in DB For Last (entries)）	データベースに保存される監査ログエントリの最大数。エントリが、[Keep Audit Log For] フィールドで指定した日数よりも古くなると、ログに含まれているエントリがこの最大エントリ数より少ない場合でも、そのエントリは削除されます。
Purge Now	データベースから古いエントリを削除するには、[今すぐ削除（Purge Now）] をクリックします。[過去（日）の監査ログをDBに保持する（Keep audit log in DB for Last (days)）] フィールドおよび [最後の監査ログをDBに保持する（エントリ）（Keep audit log in DB for Last (entries)）] フィールドに入力された値に基づいて、最大数の監査ログエントリが削除されます。 たとえば、[最後の監査ログをDBに保持する期間（日）（Keep audit log in DB for Last (days)）] の値が 5 で、[最後のの監査ログをDBに保持する（エントリ）（Keep audit log in DB for Last (entries)）] の値が 5000 で、過去 5 日間のログエントリが 5000 を超える場合、Cisco Security Manager は過去の 5000 エントリを保持し、古いエントリ（過去 5 日間のエントリも対象）を削除します。 （注） [Purge Now] ボタンは、データベースから監査レポートを削除するだけです。<install_dir>\CSCOpx\MDC\log\audit フォルダの *.csv ファイルは削除されません。これらの *.csv ファイルは、直接削除できます。
監査ログファイルの保存期間（日）（Keep Audit Log File For (days)）	監査ログファイルをシステムに保持する日数。

要素	説明
Purge Now	指定した古い監査ログファイルをすぐに削除するには、このボタンをクリックします。 （注） [今すぐ削除（Purge Now）] ボタンは、< install_dir >\MDC\log\CSDL 監査ログフォルダから CSDL 監査ログファイルを削除し、< install_dir >\MDC\log\audit フォルダから監査ログファイルを削除します。
操作ログファイルの保存期間（日）（Keep Operation Log Files For (days)）	操作ログが、削除されるまで Security Manager によって保持される日数。これらのログは、デバッグのために使用されます。
[Purge Now] ボタン	指定した古い監査ログファイルをすぐ削除するには、このボタンをクリックします。
スケジュールされた削除	
監査ログデータベースエントリのスケジュールされた削除の有効化（Enable Scheduled Purging for Audit Log Database Entries）	古いログエントリの削除をスケジュールするには、このチェックボックスをオンします。このチェックボックスをオンすると、スケジュールオプションが有効になります。
監査ログをDBに保持する期間（日）（Keep Audit Log in DB For (days)）	削除する前にデータベースに保存する必要がある監査ログエントリの最大日数。
最後の監査ログをDBに保持する（エントリ）（Keep Audit Log in DB For Last (entries)）	データベースに保存される監査ログエントリの最大数。エントリが、[Keep Audit Log For] フィールドで指定した日数よりも古くなると、ログに含まれているエントリがこの最大エントリ数より少ない場合でも、そのエントリは削除されます。
監査ログファイルのスケジュールされた削除の有効化（Enable Scheduled Purging for Audit Log Files）	システムの監査ログの削除をスケジュールするには、このチェックボックスをオンします。
監査ログファイルの保存期間（日）（Keep Audit Log File For (days)）	監査ログファイルをシステムに保持する日数。
操作ログファイルのスケジュールされた削除の有効化（Enable Scheduled Purging for Operation Log Files）	システムの操作ログの削除をスケジュールするには、このチェックボックスをオンにします。

要素	説明
操作ログファイルの保存期間（日）（Keep Operation Log Files For (days)）	操作ログが、削除されるまで Security Manager によって保持される日数。これらのログは、デバッグのために使用されます。
ログ レベル（Log Level）	操作ログで収集する必要がある、重大度に基づく情報レベル。各レベルでは、異なる量のデータが収集されます。たとえば、情報レベルでは、ほとんどのデータが収集され、重大レベルでは、収集されるデータが最も少なくなります。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Policy Management] ページ

[Policy Management] ページを使用して、Security Manager で管理するルータおよびファイアウォールのポリシータイプを選択します。これらの選択内容は、ルータおよびファイアウォールデバイスに適用されますが、IPS デバイスには適用されません。デフォルトでは、すべてのポリシーが管理対象として選択されています。

管理対象外のポリシーは、デバイス ビューとポリシー ビューの両方から削除されます。管理対象外のポリシー（ローカルまたは共有）は、Security Manager データベースから削除されます。唯一の例外は、インターフェイス ポリシーです。インターフェイス ポリシーは、Security Manager に引き続き表示されますが、読み取り専用ポリシーのマークが付けられます。ファイアウォール デバイスの場合、インターフェイスおよびフェールオーバーの設定は、1 つのユニットと見なされ、両方が管理対象となるか、または管理対象外となります。

ポリシータイプを管理する方法および管理対象外とする方法（これらの設定を変更する前後に実行する必要がある内容を含む）の詳細については、ルータおよびファイアウォールデバイスのポリシー管理のカスタマイズを参照してください。

注意 AUS または CNS を使用して設定を ASA または PIX デバイスに展開する場合は、デバイスが AUS または CNS から完全な設定をダウンロードする点に注意してください。そのため、Security Manager で管理されているポリシーを減らすと、実際にはデバイスから設定が削除されます。管理対象の一部の ASA/PIX ポリシーを選択解除し、Security Manager とともに他のアプリケーションを使用してデバイスを設定する場合は、AUS または CNS を使用しないでください。

ナビゲーション パス

[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ポリシー管理（Policy Management）] を選択します。

フィールド リファレンス

表 *35 : [Policy Management]* ページ

要素	説明
Policies to Manage	ポリシー タイプは、フォルダで整理されます。個別に処理されるルータとファイアウォール（すべての ASA、PIX、および FWSM デバイスを含む）別に整理され、次に、カテゴリ（[NAT]、[Interfaces]、および [Platform]）別に整理されます。必要に応じてポリシータイプを選択または選択解除し、[保存（Save）] をクリックします。ポリシーのグループのチェックボックスをオフにすると、そのグループのすべてのポリシーの選択が解除されます。デフォルトでは、すべてのポリシーが選択されています。 （注） バージョン 4.18 以降、Cisco Security Manager は、Cisco Umbrella サーバーで設定される ASA 9.10(1) デバイスのサポートを提供します。

要素	説明
Display a warning on all shared policies and imported objects	すべての共有ポリシーと、[ファイル（File）]>[インポート（Import）] コマンドでインポートされたオブジェクトに、メッセージを追加するかどうかを指定します。このオプションを選択すると、次のものにメッセージが表示されます。 • すべての共有ポリシー（インポートされたかローカルで作成されたかを問いません）。 • [ファイル（File）]>[インポート（Import）] コマンドを使用してデバイスまたは共有ポリシーをインポートすることで作成されたポリシーオブジェクト。PolicyObjectImportExport.pl コマンド（ポリシーオブジェクトのインポートおよびエクスポートを参照）によって作成され、インポートされたポリシーオブジェクトは含まれません。 共有ポリシーを定期的にインポートすると、インポートされたポリシーおよびオブジェクトによって同名のポリシーおよびオブジェクトが置換されて、ローカルで行った変更が削除されます。このメッセージは、ポリシーがインポートされる可能性があることをユーザに通知し、編集しないポリシー オブジェクトをユーザが識別するために役立ちます。 **ヒント** ポリシーまたはデバイスをインポートするとき、このオプションの設定を選択するように要求されます。そのため、ポリシーまたはデバイスをインポートするユーザは、必要な認可を受けていれば、このページにアクセスすることなくこの設定を変更できます。この変更は、インポートの実行者が変更を送信（必要に応じて承認）したあとにだけ、有効になります。詳細については、ポリシーまたはデバイスのインポートを参照してください。
[Save] ボタン	変更内容を保存します。 ポリシーを管理対象外とする場合、そのポリシーが割り当てられているデバイスのリストが表示されます。Security Manager は、ポリシーの割り当てを解除するために、すべてのデバイスから必要なロックを取得できる必要があります。そうでない場合、ポリシーを管理対象外とする前に、手動でポリシーの割り当てを解除（またはロックを削除）する必要があります。 前に管理対象外であったポリシーを管理対象にする場合は、影響を受けるすべてのデバイスを再検出して、既存の設定値を Security Manager に含める必要があります。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Policy Objects] ページ

[Policy Objects] ページを使用して、ポリシー オブジェクトの作成に関するシステム デフォルトを定義します。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ポリシーオブジェクト（Policy Objects）] を選択します。

関連項目

- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定
- ポリシー オブジェクトの管理

フィールド リファレンス

表 36 : [Policy Objects] ページ

要素	説明
When Redundant Objects Detected	既存のオブジェクトと同じ定義を持つポリシー オブジェクトを作成しようとしたときに、Security Manager で実行するアクション： • [Ignore]：同一の定義を持つオブジェクトを自由に作成できます。すべての競合は無視されます。 • [Warn]：既存のオブジェクトと同じオブジェクトを作成しようとすると、警告が表示されます。必要な場合は、オブジェクトの作成に進むことができます。 • [Enforce]：既存のオブジェクトと同じオブジェクトを作成することが禁止されます。エラー メッセージが表示されます。

要素	説明
Default Source Ports	サービス オブジェクトのデフォルト送信元ポート範囲として使用するポート範囲値。次のいずれかを選択できます。 • [Use all ports]：1 ～ 65535 のすべてのポートが含まれます。 • [Use secure ports]：1024 ～ 65535 のすべてのポートが含まれます。 デフォルトの送信元ポートを変更した場合は、影響を受ける可能性がある、以前展開されていたすべてのデバイスに手動で再展開する必要があります。これらの変更内容は、データをリフレッシュするまで、開いているアクティビティには反映されない場合があります。 ポート リスト オブジェクトの詳細については、ポート リスト オブジェクトの設定を参照してください。
Enable AutoComplete Dropdown Box	ユーザがサービスを作成するときに、ユーザの入力に一致するサービス名およびポート リスト名を Security Manager が表示するかどうかを指定します。これにより、すでに定義している名前から簡単に選択できるようになります。オートコンプリートの選択を解除すると、正確なサービス名およびポート リスト名を覚えておき、自分で入力する必要があります。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[プロセスモニタリングの設定（Process Monitoring Settings）] ページ

[プロセスモニタリングの設定（Process Monitoring Settings）] ページを使用して、プロセスモニタリングを有効にします。このページで、特定のプロセスのモニタリングを有効または無効にしたり、モニタリング間隔や電子メールアドレスなどの通知設定を行ったりすることができます。この設定により、プロセスが停止したときに、指定された受信者に電子メール通知が送信されます。

はじめる前に

電子メールアラートを受信できるようにするため、CS Web コンソールで SMTP サーバーと送信者メールを設定します。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [プロセスモニタリングの設定（Process Monitoring Settings）] を選択します。

フィールド リファレンス

表 *37 : [プロセスモニタリングの設定（Process Monitoring Settings）] ページ*

要素	説明
[プロセスモニタリングの有効化（Enable Process Monitoring）]	選択すると、Security Manager でモニタリングするプロセスを指定できます。続いて他のプロセスモニタリングの設定を行う必要があります。 デフォルトでは、プロセスモニタリング機能は Cisco Security Manager サーバーで無効になっています。 （注） プロセスモニタリングを有効または無効にすると、Windows レジストリが変更され、システムアラートが生成される場合があります。
[モニタリング間隔（分単位）（Monitor Interval (in Minutes)）]	プロセスをモニタリングする間隔を指定します。有効な値は 1 ～ 60 分です。デフォルトのモニタリング間隔は 5 分です。 （注） モニタリング間隔が変更されると、進行中のモニタリングタスクが停止し、新しいモニタリングタスクが更新された間隔で開始されます。
[通知受信者の電子メール（Notification Recipient(s) E-mail(s)）]	通知受信者の電子メール ID を入力します。複数の電子メール ID をカンマで区切って入力できます。通知受信者は、モニタリングされているプロセスが停止したときに通知される受信者です。
[最大メールアラート数（Maximum Mail Alerts）]	Security Manager の実行時に受信者に送信される電子メールの最大数を入力します。この項目のデフォルト値は 10 です。
[プロセスリスト（Process List）]	モニタリングするプロセスを 1 つ以上選択します。選択したプロセスのいずれかが停止すると、指定された受信者に通知メールが送信されます。 （注） [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] で、[イベント管理（Event Management）]、[正常性およびパフォーマンスのモニタリング（Health and Performance Monitor）]、[Report Manager] が無効になっている場合、[プロセスモニタリングの設定（Process Monitoring Settings）] ページで VmsEventServer、CsmHPMServer、および CsmReportServer の各プロセスが有効になっていても、電子メール通知は送信されません。

要素	説明
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[シングルサインオンの設定（Single Sign-on Configuration）] ページ

[Cisco Security Manager管理（Security Manager Administration）] ウィンドウの [シングルサインオンの設定（Single Sign-on Configuration）] ページを使用して、Cisco Prime Security Manager または FireSIGHT Management Center のクロス起動に使用する「シングルサインオン」（SSO）共有キーを有効にして設定します。

（注） シングルサインオンを使用することで、ユーザーは、Prime Security Manager や FireSIGHT Management Center に個別にログインすることなく、Cisco Security Manager から Prime Security Manager または FireSIGHT Management Center をクロス起動できます。ただし、Prime Security Manager や FireSIGHT Management Center をクロス起動するために SSO は必要ありません。

ヒント Cisco Prime Security Manager は、ASA CX モジュールの管理に使用されます。FireSIGHT Management Center は、ASA FirePOWER モジュールの管理に使用されます。

関連項目

- ASA CX モジュールおよび FirePOWER モジュールの検出
- Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動
- PRSM とのデバイスインベントリおよびポリシーオブジェクトの共有

ナビゲーション パス

1. **[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** を選択し、目次から [シングルサインオンの設定（Single Sign-on Configuration）] を選択します。
2. [Prime Security Managerの有効化（Enable for Prime Security Manager）] チェックボックスまたは [FireSIGHT Management Centerの有効化（Enable for FireSIGHT Management Center）] チェックボックスを選択します。

フィールド リファレンス

表 *38 : [*シングルサインオンの設定（*Single Sign-on Configuration***）*]* ページ**

要素	説明
Prime Security Managerの有効化（Enable for Prime Security Manager）	[チェックボックス] Prime Security Manager の SSO 機能を有効または無効にできます。無効の場合、共有キーが保持されます。
FireSIGHT Management Centerの有効化（Enable for FireSIGHT Management Center）	[チェックボックス] FireSIGHT Management Center の SSO 機能を有効または無効にできます。無効の場合、共有キーが保持されます。
シングルサインオンの共有キー（Shared Key for Single Sign-on）	このセクションの機能を使用して、Prime Security Manager または FireSIGHT Management Center をクロス起動するための暗号化キーを生成および表示します。 [生成（Generate）] ボタンをクリックして、128 ビットの AES キーをランダムに生成します。このキーは、[SSO共有キー（SSO Shared Key）] フィールドに 32 桁の 16 進数文字列として表示されます。 （注） このキーは、Prime Security Manager または FireSIGHT Management Center でシングルサインオンクロス起動を設定するときに指定する必要があります。また、許可された各 Cisco Security Manager ユーザーは、Prime Security Manager データベースまたは FireSIGHT Management Center ユーザーデータベースで、Cisco Security Manager ユーザーデータベースと同じユーザー名で設定する必要があります（パスワードは異なる場合があります）。 ヒント PRSM での SSO の設定については、ASA CX および Cisco Prime Security Manager のユーザーガイド [英語]（Cisco ASA CX Context-Aware Security End-User Guides）の「Configuring Single Sign-On for Cisco Security Manager」を参照してください。

[Rule Expiration] ページ

[Rule Expiration] ページを使用して、ポリシールールの有効期限のデフォルト値を定義します。一部のタイプのポリシールール（アクセス ルールなど）のポリシーを作成するときに、そのルールの有効期限を設定できます。また、Security Manager は、有効期限が近づくと電子メールで通知できます。

電子メール通知をイネーブルにするように、SMTP サーバを設定する必要があります。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [有効期限（Expiration）] を選択します。

フィールド リファレンス

表 39 : [Rule Expiration] ページ

要素	説明
Notify Email	ルールの有効期限の通知を受信する、デフォルトの電子メール アドレス。ユーザは、個々のルールを設定するときにこのアドレスをオーバーライドできます。
Notify Before Expiration	Security Manager が電子メール メッセージを送信する、ルールの有効期限が切れる前のデフォルト日数。ユーザは、個々のルールを設定するときにこの値をオーバーライドできます。
送信者（Sender）	Security Manager が電子メール通知を送信するために使用する電子メール アドレス。
Email Format	電子メール メッセージの形式： • [Text]：電子メールは、HTML 形式およびプレーン テキスト形式で送信されます。 • [XML]：電子メールは、XML マークアップを使用して送信されます。このオプションは、通知に対する処理および応答を自動的に行うプログラムを記述する場合に適しています。
[Save] ボタン	変更内容を保存します。
リセット ボタン	すべてのフィールドを以前の値に復元します。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Server Security] ページ

[Server Security] ページを使用して、CiscoWorks Common Services アプリケーションの特定のページを開きます。これらのページでは、Security Manager サーバでのさまざまなセキュリティ機能を設定できます。CiscoWorks Common Services によって、ユーザ アクセス コントロールやシステム セキュリティなど、Security Manager サーバの基本的な機能が制御されます。

Security Manager にログインするときに、ユーザ名とパスワードが、（インストール時に AAA プロバイダーとして設定したシステムに応じて）CiscoWorks または Cisco Secure Access Control Server（ACS）データベースに格納されているアカウント情報と比較されます。クレデンシャルの認証後、割り当てられているロールに応じたアクセスを実行できます。

Common Services ロールが、Security Manager におけるユーザー機能に変換される方法など、Security Manager のロールおよび権限の詳細については、『Installation Guide for Cisco Security Manager』を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager 管理（Security Manager Administration）] を選択し、目次から [サーバーセキュリティ（Server Security）] を選択します。

フィールド リファレンス

表 *40 : [Server Security]* ページ

要素	説明
[AAA Setup] ボタン	Common Services を開き、[AAA Mode Setup] ページを表示します。このページで、AAA をフォールバック サインオン方式として設定できます。AAA の詳細については、[AAA モードのセットアップ（AAA Mode Setup）] ページの [ヘルプ（Help）] をクリックして参照してください。
[Certificate Setup] ボタン	Common Services を開き、[Self-Signed Certificate Setup] ページを表示します。CiscoWorks を使用すると、自己署名セキュリティ証明書を作成できます。この証明書を使用して、クライアントブラウザと管理サーバ間の SSL 接続をイネーブルにできます。自己署名証明書の詳細については、[証明書のセットアップ（Certificate Setup）] ページの [ヘルプ（Help）] をクリックして参照してください。
[Single Sign On] ボタン	Common Services を開き、[Single Sign-On Setup] ページを表示します。Single Sign-On（SSO; シングル サインオン）を使用すると、ブラウザ セッションを使用して、複数の CiscoWorks サーバに透過的にナビゲートできます。各サーバで認証を受ける必要はありません。複数の CiscoWorks サーバ間の通信は、証明書と共有秘密キーによって対処されるトラスト モードでイネーブルになります。SSO のセットアップの詳細については、[シングルサイノン（Single Sign-On）] ページの [ヘルプ（Help）] をクリックして参照してください。
[Local User Setup]	Common Services を開き、[Local User Setup] ページを表示します。このページでは、ユーザを追加および削除したり、ユーザ設定を編集したり、ロールや権限を割り当てたりできます。詳細については、[ローカルユーザーのセットアップ（Local User Setup）] ページの [ヘルプ（Help）] をクリックし、『Installation Guide for Cisco Security Manager』を参照してください。

要素	説明
[System Identity Setup]	Common Services を開き、[System Identity Setup] ページを表示します。複数の CiscoWorks サーバ間の通信は、証明書と共有秘密キーによって対処されるトラスト モードでイネーブルになります。システム ID を設定すると、複数サーバ セットアップの一部であるサーバ上に信頼ユーザを作成できます。システム ID の設定の詳細については、[システム ID のセットアップ（System Identity Setup）] ページの [ヘルプ（Help）] をクリックして参照してください。
[ネイティブ RBAC パラメータ（Native RBAC Parameters）]	
[ローカル ユーザー データベースで使用できないユーザー ID のログオンを許可（Allow logon for user ids not available in Local User Database）]	Active Directory、TACACS+、または RADIUS などの外部認証サーバーと統合された Security Manager インストールの場合、ユーザー名が Security Manager ユーザーリストで定義されていなくてもユーザーがログインできるかどうかを指定します。オンにすると、ユーザーはロール管理セットアップで指定されたデフォルトのロールを使用してログインできます。デフォルトのロールが設定されていない場合、ユーザーはログインを許可されません。

[Take Over User Session] ページ

[ユーザセッションの引き継ぎ（Take Over User Session）] ページを使用して、別のユーザの設定セッションを引き継ぎます。管理権限を持つユーザは、Workflow 以外のモードで別のユーザの作業を引き継ぐことができます。デバイスおよびポリシーが、ユーザによって操作されているためにロックされているが、別のユーザが同じデバイスおよびポリシーへのアクセスを必要としている場合、セッションの引き継ぎが役立ちます。ただし、別のユーザのセッションを引き継ぐと、現在のセッションは廃棄されるため、セッションを引き継ぐ前に、変更内容を必ず送信してください。

テーブルには、現在の設定セッションがすべて表示され、ユーザ名とセッションの状態、およびユーザが現在ログインしているかログアウトしているかが示されます。引き継ぐ設定セッションを選択し、[セッションの引き継ぎ（Take over session）] をクリックします。セッションは、ユーザがセッション中に保存した変更内容を含め、現在の状態で転送されます。

選択したユーザが、セッションを引き継ぐときにログインしている場合、そのユーザは、警告メッセージを受信し、進行中の保存していない変更内容は失われ、ログアウトされます。

詳細については、別のユーザの作業の引き継ぎを参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ユーザセッションの引き継ぎ（Take Over User Session）] を選択します。

[チケット管理（Ticket Management）] ページ

[チケット管理（Ticket Management）] ページを使用して、チケット管理をイネーブルにし、外部の変更管理システムと統合するためのチケット発行システムの URL を設定し、チケット情報の消去設定を構成します。

チケット管理がイネーブルになっている場合、すべてのイメージ管理インストールジョブにはチケットが割り当てられている必要があります。それ以外の場合、ジョブは実行されません。

ナビゲーション パス

[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [チケット管理（Ticket Management）] を選択します。

関連項目

- ワークフロー モードの変更
- Workflow モードの比較

フィールド リファレンス

表 *41 : [チケット管理（Ticket Management）] ページ*

要素	説明
チケットの有効化（Enable Ticketing）	チケット管理をイネーブルにするかどうかを指定します。
システム生成のデフォルトのチケット名（System Generated Default Ticket Name）	デフォルトでは、このチェック ボックスはオンになっています。チケット名にシステム生成のデフォルト名を付加しない場合は、チェックボックスをオフにします。アクティビティ作成ダイアログのチケット名フィールドは空白のままです。
チケットシステムURL（Ticketing System URL）	

要素	説明
チケットシステムURL（Ticketing System URL）	外部変更管理システムの起動に使用する URL。このフィールドが設定されている場合、チケット ID は、指定された URL を起動するハイパーリンクです。URL の形式は、チケット ID がURL の一部として組み込まれるテンプレートになっている必要があります。テンプレート形式では、実際のチケット ID の代わりに {0} を使用します。 たとえば、チケット ID が *TKT12345* のチケットの外部チケット管理システムを起動する URL が http://ticketsystem/displayticket?ticketid=TKT12345 である場合、使用するテンプレート URL は **http://ticketsystem/displayticket?ticketid={0}** となります。 チケットを作成すると、指定したチケット ID がハイパーリンクの {0} の代わりに使用されます。
生成	クリックすると、チケットシステム URL の作成に使用できる [テンプレートURLの生成（Generate Template URL）] ダイアログボックスが表示されます。 上記の例を使用すると、[チケット ID（Ticket ID）] フィールドに **TKT12345** と入力し、[チケット URL（Ticket URL）] フィールドに **http://ticketsystem/displayticket?ticketid=TKT12345** と入力します。[OK] をクリックすると、適切なテンプレート URL が作成され、[チケットシステムURL（Ticketing System URL）] フィールドに入力されます。
[チケット履歴（Ticket History）] チケット履歴の設定は、非ワークフローモードでのみ使用できます。ワークフローモードでは、消去設定はアクティビティの設定を介して制御されます（[Workflow] ページ （106 ページ）を参照）。	
次より古いチケット（変更レポートを含む）を消去（Purge Tickets (including change report) Older than）	チケット情報を Ticket Manager テーブルに保持する日数。デフォルトは 30 です。1 ～ 120 日まで指定できます。 [今すぐ消去（Purge Now）] をクリックすると、指定した日数よりも古いすべてのチケットが削除されます。
次より古い変更レポートを消去（Purge Change Report older than）	変更レポートが保持される日数。デフォルトは30です。[次より古いチケット（変更レポートを含む）を消去（Purge Tickets (including change report) Older than）] 設定よりも小さい値を指定できます。 [今すぐ消去（Purge Now）] をクリックすると、指定した日数よりも古いすべての変更レポートが削除されます。
[Save] ボタン	変更内容を保存します。

要素	説明
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Token Management] ページ

[Token Management] ページを使用して、Token Management System（TMS）を通信プロトコルとして使用している Cisco IOS ルータに設定を展開するために使用する TMS サーバを指定します。Security Manager は、このページ上の設定を使用して、TMS サーバに接続します。

Security Manager は、FTP を使用して、デルタ設定ファイルを TMS サーバに展開します。TMS サーバから eToken に設定ファイルをダウンロードし、暗号化できます。

Cisco IOS ルータで TMS を使用するには、TMS をトランスポート プロトコルとして指定する必要があります。すべてのルータの場合は [Device Communication] ページ（[Device Communication] ページ （28 ページ）を参照）で指定し、特定のルータの場合はそのデバイス プロパティ（[デバイスのプロパティ（Device Properties）] : [全般（General）] ページを参照）で指定できます。TMS サーバを FTP サーバとして設定する必要もあります。設定しないと、展開は失敗します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [トークン管理（Token Management）] を選択します。

関連項目

- Token Management Server への設定の展開
- 展開方法について

フィールド リファレンス

表 42 : [Token Management] ページ

要素	説明
[Server Name] または [IP Address]	TMS サーバの DNS ホスト名または IP アドレス。
ユーザー名	Security Manager が、TMS サーバにログインするときに使用するユーザ名。
Password Confirm Password	ユーザー名のパスワード。両方のフィールドにパスワードを入力します。

要素	説明
Directory in the TMS Server for Config Files	展開された設定ファイルがダウンロードされる、TMS サーバ上のディレクトリ。ルート FTP ディレクトリ（「.」）が、TMS サーバー上のデフォルトの FTP ロケーションです。
Public Key File Location	TMS サーバからコピーされた、Security Manager サーバ上の公開キー ファイルと秘密キー ファイルの場所。Security Manager は、この公開キーを使用して、TMS サーバに送信されるデータを暗号化します。次に、サーバはその秘密キーを使用してデータを復号化します。Security Manager には、サーバ上のデフォルトの秘密キーと一致する、デフォルトの公開キーが用意されています。 （注） 必要に応じて、TMS サーバを使用して、公開キーと秘密キーの新しいペアを生成できます。生成した場合は、新しい公開キーを Security Manager サーバにコピーする必要があります。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[VPN Policy Defaults] ページ

[VPN Policy Defaults] ページを使用して、Security Manager が各 IPsec テクノロジーに使用するデフォルトの VPN ポリシーを表示または割り当てます。ポリシーをデフォルトとして選択する前に、そのポリシーを共有ポリシーとして作成し、データベースに送信し、承認を受ける必要があります。このページからポリシーを作成することはできません。これらのデフォルトを設定する方法の詳細については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定を参照してください。

VPN トポロジに関連する各タブでは、各ポリシー タイプのドロップダウン リストに、選択可能な既存の共有ポリシーが示されます。ポリシーを選択して[コンテンツを表示（View Content）]ボタンをクリックすると、そのポリシーの定義を参照できます。場合によっては変更できますが、その変更は保存できません。

Security Manager は、VPN ポリシーのデフォルトを使用して、ポリシーの一貫性を維持すると同時に、VPN 設定を簡素化します。Security Manager は、必須ポリシー用に出荷時のデフォルト ポリシーを提供します。これにより、VPN が機能するために VPN トポロジ内のデバイスで設定する必要がある設定値が提供されます。必須ポリシーは、割り当てられている IPsec テクノロジーによって変わります。デフォルトの設定値を持つ出荷時のデフォルト ポリシーを使用すると、VPN トポロジの作成後すぐにデバイスに展開できます。デフォルト設定は、オプションのポリシーには提供されません。出荷時のデフォルト設定を使用する代わりに、異なるデフォルト設定を提供するために共有ポリシーを作成する必要がある場合があります。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [VPNポリシーのデフォルト（VPN Policy Defaults）] を選択します。

関連項目

- 新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス）

フィールド リファレンス

表 43 : [VPN Policy Defaults] ページ

要素	説明
[DMVPN] タブ	ダイナミック マルチポイント VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[Large Scale DMVPN] タブ	大規模ダイナミック マルチポイント VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[Easy VPN] タブ	Easy VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[IPsec/GRE] タブ	IPsec/GRE VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[GRE Dynamic IP] タブ	GRE ダイナミック IP VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[Regular IPsec] タブ	通常の IPsec VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[通常の IPSec VTI（Regular IPsec VTI）] タブ	通常の、トンネルベースの IPsec VPN テクノロジー用のデフォルトポリシーを設定できるポリシータイプが一覧表示されます。
GET VPN	Group Encrypted Transport（GET）VPN テクノロジー用のデフォルトポリシーを設定できるポリシータイプが一覧表示されます。
リモート アクセス VPN	IPsec リモート アクセス VPN 用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。

要素	説明
[S2S Endpoints] タブ	サイト間 VPN における内部インターフェイスと外部インターフェイスのデフォルトのエンドポイントを定義するインターフェイスロール。

[Workflow] ページ

[Workflow] ページを使用して、Security Manager が適用するワークフローモードを選択します。また、アクティビティおよび展開ジョブの通知とログのデフォルト設定を定義します。

ワークフローモードを変更する前に、次の項で、モードの相違、およびモード変更による影響を確認してください。

- Workflow モードの作業
- Workflow 以外のモードの作業
- Workflow モードの比較
- ワークフロー モードの変更

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ワークフロー（Workflow）] を選択します。

関連項目

- アクティビティの管理
- 展開の管理

フィールド リファレンス

表 44 : [Workflow] ページ

要素	説明
Workflow Control	
Enable Workflow	Workflow モードをイネーブルにするかどうかを指定します。Workflow モードをイネーブルにすると、アクティビティおよび展開ジョブのアプルーバを設定するかどうかを選択できます。

要素	説明
Require Activity Approval	アクティビティが、割り当てられたアプルーバによって明示的に承認される必要があるかどうかを指定します。アプルーバの有無による処理の違いについては、アクティビティの承認を参照してください。
提出者はアクティビティを承認できる（Submitter can Approve Activity）	アクティビティは提出者によって承認されます。
[展開とインストールイメージに承認が必要（Require Deployment & Install Image Approval）]	展開ジョブおよびインストールイメージジョブが、割り当てられたアプルーバによって明示的に承認される必要があるかどうかを指定します。アプルーバの有無による処理の違いについては、展開についてを参照してください。
提出者は展開ジョブを承認できる（Submitter can Approve Deployment Jobs）	展開ジョブは送信者が承認できます。
システム生成のデフォルトのアクティビティ名（System Generated Default Activity Name）	デフォルトでは、このチェックボックスはオンになっています。アクティビティ名にシステム生成のデフォルト名を付加しない場合は、チェックボックスをオフにします。アクティビティ作成ダイアログのアクティビティ名フィールドは空白のままになります。
電子メールの通知	
送信者（Sender）	Security Manager が電子メール通知を送信するために使用する電子メール アドレス。
Activity Approver	アクティビティの承認担当者のデフォルトの電子メール アドレス。ユーザは、承認のためにアクティビティを送信するときに、このアドレスをオーバーライドできます。詳細については、承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード）を参照してください。
Job/Schedule Approver	展開ジョブまたはスケジュールの承認担当者のデフォルトの電子メール アドレス。ユーザは、承認のためにジョブまたはスケジュールを送信するときに、このアドレスをオーバーライドできます。詳細については、展開ジョブの送信を参照してください。

要素	説明
Require Deployment Status Notification Include Job Deployer Job Completion Notification	展開ジョブのステータスが変更されるたびに、電子メール通知を送信するかどうかを指定します。このオプションを選択した場合は、通知を受信する電子メール アドレスを [Job Completion Notification] フィールドに入力します。カンマで複数のアドレスを区切ります。 [Include Job Deployer] を選択して、ジョブを展開した担当者の電子メール アドレスを通知電子メール メッセージに含めることもできます。
Workflow History	
Keep Activity for	アクティビティ情報を [Activity] テーブルで保持する日数。デフォルトは 30 です。1 ～ 180 日を指定できます。 [今すぐ消去（Purge Now）] をクリックして、指定した日数よりも古いすべてのアクティビティを削除します。 （注） Workflow 以外のモードでチケット発行が有効になっている場合、消去設定はチケットの設定を介して制御されます（[チケット管理（Ticket Management）] ページ （101 ページ）を参照）。
Keep Job for	展開ジョブ情報を [Deployment Job] テーブルで保持する日数。デフォルトは 30 です。1 ～ 180 日を指定できます。 [今すぐ消去（Purge Now）] をクリックして、指定した日数よりも古いすべてのジョブを削除します。 （注） Cisco Security Manager バージョン 4.22 以降では、このオプションを選択すると、指定された日数より古い展開トランスクリプトファイルが **C:\Program Files (x86)\CSCOpx\MDC\tomcat\vms\athena\transcript** フォルダからも削除されます。これは、古いエントリの蓄積を防ぎます。
Keep job per schedule for	展開ジョブ情報を、各ジョブ スケジュールの [Deployment Job] テーブルで保持する日数。この設定は、スケジュールを使用して開始されたジョブだけに適用されます。デフォルトは 30 です。1 ～ 180 日を指定できます。 [今すぐ消去（Purge Now）] をクリックして、指定した日数よりも古いすべてのジョブを削除します。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。

要素	説明
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[ウォール設定（Wall Settings）] ページ

Security Manager の [ウォール設定（Wall Settings）] ページでは、ウォール機能を有効または無効にできます。

「ウォール」機能は、「ShoutBox」機能とも呼ばれます。この機能を使用して、同じ Security Manager サーバーにログインしているすべてのユーザーにメッセージを送信できます。ただし、まず [ウォール設定（Wall Settings）] ページで機能を有効にする必要があります。

（注） 管理者ユーザーのみがウォール機能を有効または無効にする権限を持っていますが、すべてのユーザーはメッセージを送信する権限を持っています。

たとえば、ウォール機能を使用して、Security Manager のインストールでいくつかの変更を行いながら、他のユーザーと対話することができます。対話の内容は、多くの場合、行われている変更や、変更に対して実行される特定の即時アクションに関するものです。送信されるメッセージは、ログインしているすべてのユーザーにブロードキャストされます。ウォール機能を使用すると、ユーザーは、ログイン時に他のユーザーが表示できる基本的なプロファイル情報を入力できます。ウォール機能の重要な用途の 1 つは、現在ログインしているすべてのユーザーのリストを表示することです（ユーザーは、アイドルタイムアウトの後、または Security Manager クライアントを介してログアウトした後、[ウォール（Wall）] ウィンドウから削除されます）。

ウォール機能を使用して、*.pdf、*.xls、またはその他のファイルを添付送信することはできません。

ナビゲーション パス

[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] をクリックし、コンテンツテーブルから [ウォール設定（Wall Settings）] を選択します。

フィールド リファレンス

表 *45 : [ウォール設定（Wall Settings）] ページ*

要素	説明
ユーザーが他のユーザーにメッセージを送信できるようにします。	ウォール機能を有効にするか無効にするかを指定します。
[Save] ボタン	変更を保存して適用します。

要素	説明
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

ウォール機能が有効になっている場合、[ツール（Tool）] > [壁...（Wall...）] をクリックするか、Configuration Manager で [ウォール（Wall）] アイコンをクリックして、[ウォール（Wall）] ウィンドウを開くことができます。

Health and Performance Monitor または Image Manager で [ウォール（Wall）] アイコンをクリックして、[ウォール（Wall）] ウィンドウを開くこともできます。イベントビューアまたは Report Manager で [ウォール（Wall）] ウィンドウを開くことはできません。

ヘルプアイコンをクリックすると、[ウォール（Wall）] で詳細なウォール機能のヘルプを利用できます。

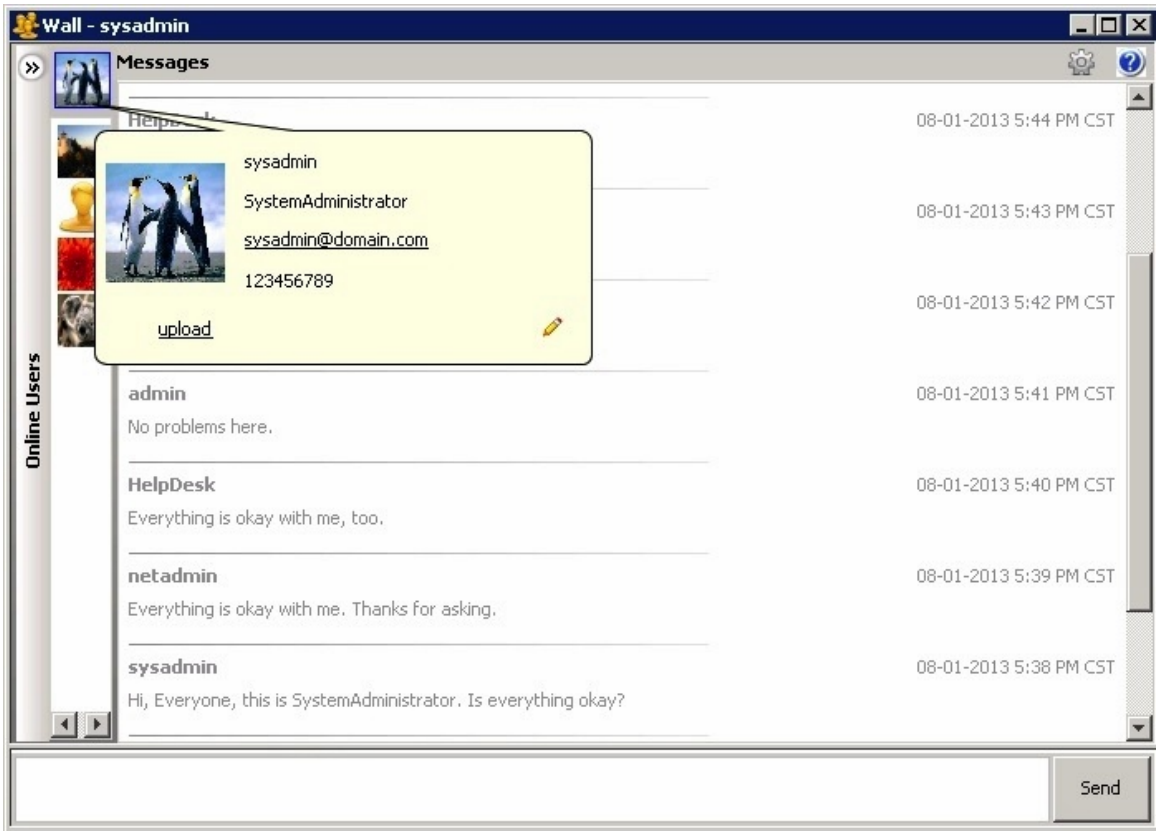
[ウォール（Wall）] ウィンドウには、次の要素が含まれています。

- 左側ペイン。同じ Security Manager サーバーにログインしているユーザーと展開/折りたたみボタンを表示します。
- 右側ペイン。ページの大部分を占めており、ユーザーが送信したメッセージのテキストが含まれます。右側ペインには、ウォールアラートを有効または無効にするボタンと、クリックして詳細なヘルプを表示できるヘルプアイコンもあります。

[ウォール（Wall）] ウィンドウの概要	
メッセージの表示	メッセージは、[ウォール（Wall）] ウィンドウの右側ペインに表示されます。常に最新のメッセージが最上部に表示されます。メッセージからテキストを選択してコピーすることができます。 メッセージパネルには最大 280 文字を入力することが可能で、この文字数に達すると、ビープ音で警告されます。
Message Log	過去のメッセージのログを表示できます。メッセージログには 100 件のメッセージが保持されます。[ウォール（Wall）] ウィンドウを起動すると、メッセージが表示されます。
プロファイル画像	プロフィール用の写真をアップロードできます。JPG、PNG、BMP、GIF などの有効な画像タイプがサポートされています。 写真をアップロードするには、ユーザー プロファイル ウィンドウの [アップロード（upload）] リンクを使用します。ユーザー プロファイル ウィンドウを開くには、[ウォール（Wall）] ウィンドウでユーザー名またはユーザーの写真をクリックします。 ユーザープロファイル ウィンドウには、プロファイル情報の編集機能とプロファイル情報の保存機能を切り替えるアイコンもあります。

ユーザー プロファイル ウィンドウ	ユーザー プロファイル ウィンドウを開くには、[ウォール（Wall）] ウィンドウでユーザー名またはユーザーの写真をクリックします。ユーザー プロファイル ウィンドウには、次の情報が含まれています。 • プロファイル名（最大 20 文字） • 職名（最大 15 文字） • 電子メール（最大 15 文字） • 電話 対応するメールリンクをクリックしてメールを送信します。
通知アラート	新しいメッセージを受信した時点で [ウォール（Wall）] ウィンドウがフォーカスされていない場合、新しい通知アラートポップアップが表示されます。通知をクリックするだけで [ウォール（Wall）] ウィンドウを起動できます。 通知アラートポップアップが表示されると、[ウォール（Wall）] ウィンドウのアイコンも点滅し、メッセージ数が表示されます。 アラートポップアップまたは [ウォール（Wall）] ウィンドウに表示される設定オプションから、通知アラートをオフにすることができます。

図 *1* : *[ウォール（Wall）]* ウィンドウ



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。