トラブルシューティング

CiscoWorks Common Services は、Security Manager に、サーバー上でのインストール、アンインストール、および再インストール用のフレームワークを提供します。Security Manager サーバーソフトウェアのインストールまたはアンインストールでエラーが発生した場合は、Common Services のオンラインヘルプの「Troubleshooting and FAQs」[英語] を参照してください。

次のトピックは、スタンドアロンバージョンの Cisco Security Agent を含む、クライアントシステムまたはサーバー上に Security Manager 関連ソフトウェアアプリケーションをインストール、アンインストール、または再インストールしたときに発生する可能性のある問題の解決に役立ちます。

- トラブルシューティング （2 ページ）
- Cisco Security Manager サービスの起動要件 （2 ページ）
- 必要な TCP ポートと UDP ポートの包括的リスト （3 ページ）
- Security Manager サーバのトラブルシューティング （5 ページ）
- Security Manager クライアントのトラブルシューティング （17 ページ）
- サーバ セルフテストの実行 （25 ページ）
- サーバ トラブルシューティング情報の収集 （26 ページ）
- サーバ プロセス ステータスの表示と変更 （27 ページ）
- サーバ上の全プロセスの再起動 （27 ページ）
- サーバ インストール ログ ファイルの確認 （27 ページ）
- Symantec の共存問題 （28 ページ）
- Windows アップデートのインストール後の問題 （28 ページ）
- Cisco Security Manager サーバーのバックアップ （29 ページ）
- 高度な暗号化による ASA デバイスへの接続の問題 （29 ページ）
- インストール時に使用する Activation.jar のポップアップ表示 （30 ページ）
- Windows の既定のユーザーテンプレートのロケールを米国英語に設定する方法 （31 ページ）
- RMI レジストリポートを無効にする方法 （34 ページ）

トラブルシューティング

CiscoWorks Common Services は、Security Manager に、サーバー上でのインストール、アンインストール、および再インストール用のフレームワークを提供します。Security Manager サーバーソフトウェアのインストールまたはアンインストールでエラーが発生した場合は、Common Services のオンラインヘルプの「Troubleshooting and FAQs」[英語] を参照してください。

次のトピックは、スタンドアロンバージョンの Cisco Security Agent を含む、クライアントシステムまたはサーバー上に Security Manager 関連ソフトウェアアプリケーションをインストール、アンインストール、または再インストールしたときに発生する可能性のある問題の解決に役立ちます。

- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF

Cisco Security Manager サービスの起動要件

Cisco Security Manager サービスは、特定の順序で起動しなければ、Security Manager が正しく機能しません。これらのサービスの初期化は、Cisco Security Manager Daemon Manager サービスによって制御されます。Cisco Security Manager サービスの起動タイプは変更しないでください。また、Cisco Security Manager サービスは手動で停止または開始しないでください。特定のサービスを再起動しなければならない場合は、Cisco Security Manager Daemon Manager を再起動して、すべての関連サービスが正しい順序で停止および開始する必要があります。

必要な TCP ポートと UDP ポートの包括的リスト

Cisco Security Management Suite アプリケーションは、クライアントや他のアプリケーションと通信する必要があります。その他のサーバ アプリケーションは別のコンピュータ上にインストールできます。通信を成功させるためには、特定の TCP ポートと UDP ポートを開いて、トラフィック送信に使用できるようにする必要があります。通常は、必要なサービスとポートに記載されているポートを開くだけで十分です。ただし、アプリケーションが通信不能なことを検出した場合は、次の表内のポートも開く必要もあります。リストはポート番号順に並んでいます。

表 *1*: 必要なサービスとポート

サービス	対象または使用アプリケーション	ポート番号/ポートの範囲	プロトコル	着信	発信
FTP	Security Manager と TMS サーバ間の通信	21	TCP	—	X
SSH	Common Services	22	TCP	—	X
	セキュリティ マネージャ	22	TCP	—	X
Telnet	セキュリティ マネージャ	23	TCP	—	X
SMTP	Common Services	25	TCP	—	X
TACACS+（ACS の場合）	Common Services	49	TCP	—	X
TFTP	Common Services	69	UDP	X	X
HTTP	Common Services	80	TCP	—	X
	セキュリティ マネージャ		TCP	—	X
SNMP（ポーリング）	Common Services	161	UDP	—	X
	パフォーマンス モニター（Performance Monitor）	161	UDP	—	X
SNMP（トラップ）	Common Services	162	UDP	—	X
	パフォーマンス モニター（Performance Monitor）	162	UDP	X	—

サービス	対象または使用アプリケーション	ポート番号/ポートの範囲	プロトコル	着信	発信
HTTPS（SSL）	Common Services	443[1]	TCP	X	—
	セキュリティ マネージャ		TCP	X	X
	パフォーマンス モニター（Performance Monitor）		TCP	X	—
	Syslog[2]		セキュリティ マネージャ	514	UDP X —
Common Services（Security Manager がインストールされていない場合）		514 または 49514（この行の脚注を参照）	UDP	X	—
Performance Monitor（Security Manager がインストールされていない場合）		514	UDP	X	—
Remote Copy Protocol; リモート コピー プロトコル	Common Services	514	TCP	X	X
HTTP	Common Services	1741	TCP	X	—
	セキュリティ マネージャ		TCP	X	—
	パフォーマンス モニター（Performance Monitor）		TCP	X	—
	RADIUS LDAP Kerberos		Security Manager（外部 AAA サーバへ）	1645、1646、1812（新規）、389、636（SSL）、88	TCP — X
Access Control Server HTTP/HTTPS	セキュリティ マネージャ	2002	TCP	—	X
CiscoWorks ゲートキーパー用の HIPO ポート	Common Services	8088	TCP	X	X
Tomcat シャットダウン	Common Services	9007	TCP	X	—
Tomcat Ajp13 コネクタ	Common Services	9009	TCP	X	—

サービス	対象または使用アプリケーション	ポート番号/ポートの範囲	プロトコル	着信	発信
データベース	セキュリティ マネージャ	10033 および 10034	TCP	X	—
ライセンス サーバ	Common Services	40401	TCP	X	—
Daemon Manager	Common Services	42340	TCP	X	X
Osagent	Common Services	42342	UDP	X	X
データベース	Common Services	43441	TCP	X	—
パフォーマンスモニター（Performance Monitor）	43453	TCP	X	X	
DCR と OGS	Common Services	40050 ～ 40070	TCP	X	—
Event Services	Software Service	42350/44350	UDP	X	X
	Software Listening	42351/44351	TCP	X	X
	Software HTTP	42352/44352	TCP	X	X
	Software Routing	42353/44353	TCP	X	X
転送メカニズム（CSTM）	Common Services	50000 ～ 50020	TCP	X	—

[1] Cisco Security Monitoring, Analysis, and Response System（Cisco Security MARS）アプライアンスと情報を共有または交換するために、Security Manager はデフォルトでポート 443 上の HTTPS を使用します。この目的で別のポートを使用するかどうかを選択できます。

[2] Security Manager のインストールまたはアップグレード時に、Common Services syslog サービスポートが 514 から 49514 に変更されます。あとで Security Manager がアンインストールされた場合、ポートは 514 に戻されません。

Security Manager サーバのトラブルシューティング

この項では、次の疑問にお答えします。

- インストール中のサーバ障害　（6 ページ）
- インストール後のサーバ障害　（11 ページ）
- アンインストール中のサーバ障害　（15 ページ）

インストール中のサーバ障害

Q. サーバ ソフトウェアのインストール時に表示されたこのインストール エラー メッセージはどういう意味ですか。

A：サーバーソフトウェアのインストールエラーメッセージと説明を表2:インストールエラーメッセージ（サーバ） に示します。この表は先頭の文字のアルファベット順に並べられています。

表 *2:*インストール エラー メッセージ（サーバ）

メッセージ	メッセージの理由	ユーザのアクション
License file failed. ERROR: The file with the name c:\progra~1\CSCOpx\setup does not exist	先に Common Services 依存アプリケーションをアンインストールしようとして失敗しました。	**1.** サーバをシャットダウンしてから、再起動します。 **2.** レジストリエディタを使用して、このエントリ（$HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432N 削除します。 **3.** Security Manager をインストールしたディレクトリで します。 **4.** CMFLOCK.TXT を削除します（存在する場合）。 **5.** Security Manager を再インストールします。
`Corrupt License file. Please enter a valid License file.`	ライセンス ファイルが破損しているか、ライセンス ファイルの内容が無効です。	ライセンスに関する支援を参照してください。

メッセージ	メッセージの理由	ユーザのアクション
`Corrupt License file entered for 5 tries. Install will proceed in EVAL mode. Press OK to proceed.`	5 回連続で無効なライセンス ファイルへのパス名を入力した可能性があります。試行が 5 回失敗したら、インストールが評価モードに変わります。	[OK（OK）] をクリックして、ライセンスエラーのダ面に進みます。

メッセージ	メッセージの理由	ユーザのアクション
Windows 2012 R2 Server には、次の Microsoft Windows パッチが適用されていない可能性があります。 a. KB2919442 b. clearcompressionflag.exe c. KB2919355、KB2932046、KB2959977、KB2937592、KB2938439、KB2934018 d. KB2999226 これらのパッチは、このサーバーに重要な Cisco Security Manager サービスを登録するために必要です。これらのパッチは前述の順序でインストールしてください。 Cisco Security Manager をインストールする前に、これらのパッチをインストールすることを推奨します。または、Cisco Security Manager のインストール後にこれらのパッチをインストールしてから、"<CSMInstalledDirectory>\CSCOpx\bin\RegisterApache.bat" CSM スクリプトを使用してサービスを登録することもできます。 詳細については、『Installation Guide for Cisco Security Manager』[英語] を参照してください。 インストールを続行するには、[OK（OK）] をクリックします。 インストールを中止するには、[キャンセル（Cancel）] をクリックします。	推奨される Windows Update パッチが Windows 2012 R2 Server にない可能性があります。	Cisco Security Manager のインストールを開始する前に、必 いることを確認してください。 Cisco Security Manager のインストールを続行してから、こ し、Windows サービスに Apache サービスを登録する必要 詳細については、インストール準備状況チェックリスト
One instance of CiscoWorks Installation is already running. If you are sure that no other instances are running, remove the file C:\CMFLOCK.TXT. This installation will now abort.	先に Common Services 依存アプリケーションをインストールしようとして失敗した可能性があります。	C:\CMFLOCK.TXT ファイルを削除してから、もう一度試

メッセージ	メッセージの理由	ユーザのアクション
`Severe` `Failed on call to FileInsertLine.`	サーバがハード ドライブ スペースに関する要件を満たしていません。	サーバの要件および推奨事項を参照してください。
`Temporary directory used by installation has reached _istmp9x. If _istmp99 is reached, no more setups can be run on this computer, they fail with error -112.`	サーバ上で、ソフトウェア インストール中に自動的に削除される予定の一時ファイルが残っています。	サーバー上の一時ディレクトリで名前に「_istmp」文字のようなサブディレクトリをすべて削除します。
`Windows cannot find 'C:\Documents and Settings\Administrator\WINDOWS\System32\cmd.exe'. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.`	サポートされていないにもかかわらず、Terminal Services をインストール中にイネーブルにした可能性があります。XREF を参照してください。	**1.** Terminal Services をディセーブルにします。 この手順については、次の URL にある『*Installing and Solution 3.1*』の「Terminal Server Support for Windows 2 参照してください。 http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_la **1.** Security Manager をもう一度インストールしてみて

メッセージ	メッセージの理由	ユーザのアクション
`Setup has detected that unInstallShield is in use. Close unInstallShield and restart setup. Error 432.`	インストール中に Windows アカウント権限がチェックされます。CiscoWorks Common Services をインストールしている Windows アカウントがローカル管理者特権を持っていない場合は、InstallShield にこのエラー メッセージが表示されます。	**1.** %WINDIR% に書き込むための適切な権限が付与され はアンインストールは、ローカル管理者グループのメ **2.** [OK（OK）] をクリックしてエラーメッセージを閉じ 理者特権を持つアカウントを使用して Windows に再

Q. サーバ インストーラが処理を中断（ハングアップ）した場合はどうしたらいいですか。

A：リブートしてもう一度試してみてください。

Q. Cisco Security Manager と Cisco Secure Access Control Server の両方を 1 つのシステム上にインストールできますか。

A：インストールしないことを推奨します。同じサーバ上での Security Manager と Cisco Secure ACS for Windows の共存はサポートされていません。

Q. Security Manager データベースのバックアップが失敗するのはなぜですか。

A：Tivoli などのネットワーク管理アプリケーションを使用して、Security Manager がインストールされたシステム上に Cygwin をインストールした場合は、Security Manager データベースのバックアップに失敗します。Cygwin をアンインストールしてください。

インストール後のサーバ障害

Q. Security Manager サーバーのホスト名を変更する必要があります。どうすれば実行できますか。

A：（任意）Security Manager サーバーのホスト名の変更で説明されている手順を実行することで、Security Manager サーバーのホスト名を変更できます。

Q. Security Manager インターフェイスが表示されない、または正しく表示されない、あるいは特定のインターフェイス要素が欠けています。原因は何でしょうか。

A：いくつかの可能性が考えられます。このリスト内のシナリオを参照して、インターフェイスに影響を与える可能性のある単純な問題を特定し、対処してください。

- 必要なサービスのいくつかがサーバ上で動作していません。サーバーの Daemon Manager を再起動して、すべてのサービスの起動が完了するのを待ってから、Security Manager クライアントを再起動して接続し直してみてください。
- サーバに十分な空きディスク スペースがありません。サーバー上の Security Manager パーティションの空き容量が 500 MB 以上あることを確認してください。
- 基本ライセンス ファイルが破損しています。ライセンスに関する支援を参照してください。
- サーバで使用されている Windows 言語が間違っています。米国英語バージョンの Windows 上の英語と、日本語バージョンの Windows 上の日本語しかサポートされていません（サーバの要件および推奨事項 を参照。）他の言語はインストールされたバージョンの Security Manager に悪影響を与える可能性があります。また、GUI 要素の欠落は可能性のある症状の 1 つです。サポートされていない言語を使用している場合は、サポートされている言語を選択してから、Security Manager をアンインストールして再インストールしてください。サーバ アプリケーションのアンインストールを参照してください。
- ネットワーク接続上で Security Manager インストールユーティリティを実行しましたが、このユースケースはサポートされていません（、Common Services、および のインストールを参照）。サーバ ソフトウェアをアンインストールして再インストールする必要があります。サーバ アプリケーションのアンインストールを参照してください。
- クライアント システムが最小限の要件を満たしていません。クライアントの要件を参照してください。
- HTTP を使用しようとしましたが、必要なプロトコルは HTTPS です。
- ボタンだけが表示されません。Security Manager クライアントを使用している最中に、クライアントシステム上で [表示プロパティ（Display Properties）] コントロールパネルを開いて、[外観（Appearance）] タブでいくつかの設定を変更した可能性があります。この問題に対処するには、Security Manager クライアントを終了してから、再起動してください。
- 間違ったグラフィックス カードのドライバ ソフトウェアがクライアント システム上にインストールされています。クライアントの要件を参照してください。

問題：Web ブラウザを使用して Security Manager への Web インターフェイスを開こうとしたときに、Security Manager サーバー上の /cwhp/LiaisonServlet にアクセスするための権限がないことを伝えるメッセージが表示されました。What does this mean?

解決策：下の表に、この問題の一般的原因と提案されている対処法を示します。

表 *3 : LiaisonServlet* エラーの原因と対処法

原因	回避策
サーバ上にアンチウイルス アプリケーションがインストールされている	アンチウイルス アプリケーションをアンインストールします。
サーバ上に IIS がインストールされている	IIS は Security Manager と互換性がないため、アンインストールする必要があります。
Security Manager に必要なサービスが正しい順序で開始されていない	自動に設定する必要があるサービスは Cisco Security Manager Daemon Manager だけです。他の CiscoWorks サービスは手動に設定する必要があります。Daemon Manager が他の Ciscoworks サービスを起動するまでに数分かかる場合があることに注意してください。これらのサービスは、正しい順序で起動する必要があります。手動でサービスを起動した場合はエラーを引き起こす可能性があります。

原因	回避策
casuser パスワード	次の 5 つの権限は Security Manager のインストール時に自動的に割り当てられ、設定されます。 • ネットワークからこのコンピュータにアクセスする：casusers • ネットワークからこのコンピュータへのアクセスを拒否する：casuser • ローカルのログオンを拒否する：casuser • バッチ処理としてログオンする：casuser、casusers • サービスとしてログオンする：casuser casuser ログインは、Windows 管理者と同じで、すべての Common Services タスクと Security Manager タスクにアクセスできます。次のように casuser パスワードをリセットします。 **1.** [管理者として実行（Run as administrator）] オプションを使用して、サーバーでコマンドプロンプトを開きます。 **2.** NMSRoot\setup\support\resetCasuser.exe と入力し、**Enter** を押します。 （注） 場所 NMSROOT は Security Manager インストールディレクトリへのパスです。デフォルトは **C:\Program Files (x86)\CSCOpx** です。 **3.** 表示された 2 つのオプションのうち、オプション 2 - [casuserのパスワードを入力（Enter casuser password）] を選択します。casuser のパスワードの入力を求められ、入力後、確認のためにパスワードを再入力するように求められます。 **4.** ローカル セキュリティポリシーが設定されている場合は、ローカル セキュリティポリシーの「サービスとしてログオン（Log on as a service）」操作に casuser アカウントを追加します。 **5.** 次のコマンドを実行して、*NMSROOT* に casuser 権限を適用します。C:\Windows\System32\cacls.exe “NMSROOT” /E /T /G Administrators:F casusers:F **6.** 次のコマンドを実行して、casuser をデータベースサービスに設定します。NMSROOT\bin\perl NMSROOT\bin\ChangeService2Casuser.pl "casuser" "casuserpassword"

Q. Security Manager を使用してサーバー上のディレクトリを参照したときに、ローカルボリュームだけが表示され、マップされたドライブは表示されません。どうしてですか。

A：Microsoft はサーバ セキュリティを強化するために Windows の設計にこの機能を組み込みました。Security Manager で選択する必要のあるすべてのファイル（ライセンス ファイルなど）をサーバ上に配置する必要があります。

Q. 日本語バージョンの Windows の [スタート（Start）] メニューに Security Manager が表示されないのはなぜですか。

A：サーバ上の地域と言語のオプションを、英語を使用するように設定した可能性があります。日本語バージョンの Windows 内の言語として英語はサポートされていません（サーバの要件および推奨事項を参照）。コントロールパネルを使用して、言語を日本語にリセットしてください。

Q. サーバの SSL 証明書が無効になっています。また、DCRServer プロセスが開始しません。原因は何でしょうか。

A：サーバの日付または時刻が SSL 証明書の有効範囲外にリセットされています。インストール準備状況チェックリストを参照してください。この問題に対処するには、サーバの日付/時刻の設定をリセットしてください。

Q. サーバとクライアント間の通信に使用されるプロトコルの入力が要求されませんでした。デフォルトで使用されるプロトコルは何ですか。他のモードを使用してこの設定を手動で変更する必要がありますか。

A：サーバのインストール中にクライアントをインストールした場合は、デフォルトで、サーバとクライアント間の通信プロトコルとして HTTPS が使用されます。通信はデフォルト プロトコルを使用して保証されているため、この設定を手動で変更する必要はありません。

プロトコルとして HTTP を選択するオプションは、サーバインストーラとは別に、クライアント インストーラを実行して Security Manager クライアントをインストールした場合にのみ使用できます。ただし、サーバとクライアント間の通信プロトコルとして HTTP を使用しないことを推奨します。クライアントは、サーバが使用するように設定されたプロトコルを使用する必要があります。

Q. VMware セットアップを使用しているとシステムのパフォーマンスが受け入れられないほど低下します。たとえば、システムのバックアップに 2 時間もかかります。

A：Security Manager を実行している VM に複数の CPU が割り当てられていることを確認してください。1 つの CPU しか割り当てられていないシステムでは、一部のシステム アクティビティに対して受け入れられないほどのパフォーマンスを示すことがわかっています。

Q. 検証などのいくつかの操作が、MariaDB 例外の SQL クエリーをログに出力して失敗します。原因は何でしょうか。

A：TMPDIR、TEMP、または TMP が設定されていない場合、Maria DB の MySQL は Windows システムのデフォルト（通常、**C:\windows\temp**）を使用します。一時ファイルディレクトリを含むファイルシステムが小さすぎる場合は、mysqld--tmpdir オプションを使用して、十分なスペースがあるファイルシステム内のディレクトリを指定できます。

Q. Diffie-Hellman の 2048 ビットを有効にする必要がありますが、その方法が見つかりません。

A：Apache はデフォルトで 512 ビットをサポートしていますが、この Dhparam は CSM で実行できないコンパイル時のパラメータ変更が必要なため、2048 ビットはサポートしていません。したがって、CSM 4.22 で Diffie-Hellman の 2048 ビットを有効にすることはできません。

アンインストール中のサーバ障害

Q. このアンインストール エラー メッセージはどういう意味ですか。

A：アンインストール エラーメッセージと説明を表 4 : アンインストール エラー メッセージに示します。この表は先頭の文字のアルファベット順に並べられています。アンインストール エラーメッセージに関するその他の情報については、Security Manager のインストールの Common Services のマニュアルを参照してください。

表 *4*:アンインストール エラー メッセージ

メッセージ	メッセージの理由	ユーザのアクション
C:*NMSROOT* \MDC\msfc-backend refers to a location that is unavailable. It could be on a hard drive on this computer, or on a network. Check to make sure that the disk is properly inserted, or that you are connected to the Internet or your network, and then try again. If it still cannot be located, the information might have been moved to a different location.	このメッセージは害がない可能性があります。[OK] をクリックしてメッセージを消去する以外は何もする必要がありません。そうしなかった場合は、次の条件の一方または両方が適用されるサーバ上でメッセージが表示される可能性があります。 - 簡易ファイル共有が Windows 上でイネーブルになっている。 - オフライン ファイル同期が Windows 上でイネーブルになっている。	メッセージを消去してアンインストールが失敗した場合は、次の可能性のある対処法の一方または両方を試して、もう一度アンインストールを行ってみてください。 **簡易ファイル共有** **1.** [スタート（Start）] > [設定（Settings）] > [コントロール パネル（Control Panel）] > [フォルダオプション（Folder Options）] を選択します。 **2.** [表示（View）] タブをクリックします。 **3.** [Advanced Settings] ペインの一番下までスクロールします。 **4.** [簡易ファイル共有（推奨）（Use simple file sharing (Recommended)）] チェックボックスをオフにしてから、[OK（OK）] をクリックします。 **オフラインファイル同期** **1.** [スタート（Start）] > [設定（Settings）] > [コントロールパネル（Control Panel）] > [フォルダオプション（Folder Options）] を選択します。 **2.** [オフラインファイル（Offline Files）] タブをクリックします。 **3.** [オフラインファイルの有効化（Enable Offline Files）] チェックボックスをオフにしてから、[OK（OK）] をクリックします。
C:\temp\<*subdirectory* >\setup.exe - Access is denied. The process cannot access the file because it is being used by another process. 0 file(s) copied.1 file(s) copied.	アンインストールが失敗しました。	サーバをリブートしてから、サーバアプリケーションのアンインストールに記載されている手順を実行してください。

メッセージ	メッセージの理由	ユーザのアクション
Windows Management Instrumentation (WMI) is running. The setup program has detected Windows Management Instrumentation (WMI) services running. This will lock some Cisco Security Manager processes and may abort uninstallation abruptly. To avoid this, uninstallation will stop and start the WMI services. Do you want to proceed? Click Yes to proceed with this uninstallation. Click No to exit uninstallation.	組織で WMI が使用されているか、誰かが誤ってサーバ上の WMI サービスをイネーブルにした可能性があります。	[Yes] をクリックします。

Q. アンインストーラがハングアップした場合はどうしたらいいですか。

A：リブートしてからもう一度試してみてください。

Q. アンインストーラに *crmdmgtd* サービスが応答していないという内容のメッセージが表示され、「待機を続けますか？（Do you want to keep waiting?）」と尋ねられた場合はどうしたらいいですか。

A：アンインストール スクリプトには、スクリプトがタイムアウトする前に命令に応答しなかった crmdmgtd サービスを停止する命令が含まれています。[Yes] をクリックします。ほとんどの場合、crmdmgtd サービスは、その後、予想どおりに停止します。

Security Manager クライアントのトラブルシューティング

この項では、次の疑問にお答えします。

- インストール中のクライアント障害　（17 ページ）
- インストール後のクライアント障害　（21 ページ）

インストール中のクライアント障害

Q. クライアント ソフトウェアのインストール時に表示されたこのインストール エラー メッセージはどういう意味ですか。

A：クライアントソフトウェアのインストール エラーメッセージと説明を表 5 : インストール エラー メッセージ（クライアント） に示します。この表は先頭の文字のアルファベット順に並べられています。

表 *5:* インストール エラー メッセージ（クライアント）

メッセージ	メッセージの理由	ユーザのアクション
`Could not install engine jar`	以前のソフトウェアインストールとアンインストールが原因で InstallShield が正しく動作していません。	1. **C:\Program Files (x86)\Common Files\InstallShield\Universal\common\Gen1** に移動します。 2. Gen1 フォルダの名前を変更してから、もう一度 Security Manager クライアントのインストールを試してみてください。 Gen1 が存在しない場合は、代わりに **common** の名前を変更します。

`Error - Cannot Connect to Server`
`The client cannot connect to the server. This can be caused by one of the following reasons:`
`The server name is incorrect.`
`The protocol (http, https) is incorrect.`
`The server is not running.`
`Network access issues. Please confirm that the server name and protocol are correct.`
`The server is running and you are not experiencing network connectivity issues by loading the CS Manager home page in your browser.`
	サーバが誤って HTTPS トラフィック用に設定されている可能性があります。	1. ブラウザから、**https://***<server>***/CSCOnm/servlet/login/login.jsp** にある Cisco Security Management Suite デスクトップにログインします。
		2. [サーバー管理（Server Administration）] をクリックします。
		3. [管理者（Admin）] ウィンドウで、[サーバー（Server）]>[セキュリティ（Security）] を選択します。
		4. TOC で、[単一サーバー管理（Single Server Management）]>[ブラウザ-サーバーセキュリティモードの設定（Browser-Server Security Mode Setup）] を選択してから、[有効（Enable）] オプションボタンが選択されていることを確認します。
		
		オプションボタンが選択されていなかった場合は、それを選択してから、[適用（Apply）] をクリックします。
		1. プロンプトが表示されたら、Cisco Security Manager Daemon Manager を再起動します。
		2. 5 分待ってから、もう一度 Security Manager クライアントを使用してみてください。
		
		それでも接続できない場合は、エラーメッセージが示している他の可能性のある問題を検討してください。

メッセージ	メッセージの理由	ユーザのアクション

`Error - Cisco Security Agent Running`
`Installation cannot proceed while the Cisco Security Agent is running`
`Do you want to disable the Cisco Security Agent and continue with the installation?`
	クライアントのインストール中は、Cisco Security Agent を停止する必要があります。	• Cisco Security Agent をディセーブルにする場合は、[はい（Yes）] をクリックします。
		• 操作をキャンセルして、Cisco Security Agent を手動で停止する場合は、[いいえ（No）] をクリックします。
		• Security Manager クライアントのオンラインヘルプにアクセスする場合は、[ヘルプ（Help）] をクリックします。

`Error - Cisco Security Agent not Stopped`
`The installation will be aborted because the Cisco Security Agent could not be stopped.`
`Please attempt to disable Cisco Security Agent before repeating the installation process.`
	Security Manager クライアントから Cisco Security Agent を停止できませんでした。	[OK（OK）] をクリックして、このエラーメッセージを閉じ、インストールを中断します。もう一度インストールを試す前に、Cisco Security Agent を手動でディセーブルにします。

`Error occurred during the installation: null.`	以前のソフトウェアインストールとアンインストールが原因で InstallShield が正しく動作していません。	**1.** C:\Program Files (x86)\Common Files\InstallShield\Universal\common\Gen1 に移動します。 **2.** Gen1 フォルダの名前を変更してから、もう一度 Security Manager クライアントのインストールを試してみてください。 Gen1 が存在しない場合は、代わりに **common** の名前を変更します。
`Errors occurred during the installation.` • null	ログインアカウントに管理特権が付与されている Windows ユーザーだけが、Security Manager Client をインストールできます。	Windows 管理者としてログインしてから、もう一度 Security Manager クライアントのインストールを試してみてください。

メッセージ	メッセージの理由	ユーザのアクション
`Internet Explorer cannot download CSMClientSetup.exe from <server>. Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.`	クライアントシステム上の OS が Windows 2008 の場合は、Internet Explorer セキュリティ強化のデフォルト設定が原因で、サーバーからクライアントソフトウェアインストールユーティリティをダウンロードできない可能性があります。	**1.** [スタート（Start）] > [コントロールパネル（Control Panel）] > [プログラムの追加と削除（Add or Remove Programs）] の順に選択します。 **2.** [Windows コンポーネントの追加と削除（Add/Remove Windows Components）] をクリックします。 **3.** Windows コンポーネントウィザードウィンドウが開いたら、[Internet Explorerセキュリティ強化の構成（Internet Explorer Enhanced Security Configuration）] チェックボックスをオフにして、[次へ（Next）] をクリックし、[完了（Finish）] をクリックします。

`Please read the information below.`
`The following errors were generated:`
• [警告：選択した項目をインストールするには<ドライブ>パーティションの空きスペースが不足しています。（WARNING: The <*drive*> partition has insufficient space to install the items selected.）]
	空きスペースが不十分なドライブまたはパーティション上に Security Manager クライアントをインストールしようとした可能性があります。	[戻る（Back）] をクリックしてから、Security Manager クライアントをインストールする別の場所を選択してください。

`Unable to Get Data` `A database failure prevented successful completion of this operation.`	サーバデータベースが完全に稼働する前に、クライアントを使用してサーバに接続しようとした可能性があります。	数分待ってから、もう一度ログインしてみてください。問題が解決されない場合は、必要なすべてのサービスが実行していることを確認してください。

Q. クライアント インストーラが処理を中断（ハングアップ）した場合はどうしたらいいですか。

A：次の手順を試してみてください。いずれかの手順で問題が解決される可能性があります。

- クライアント システム上にアンチウイルス ソフトウェアがインストールされている場合は、それをディセーブルにしてから、もう一度インストーラを実行してみてください。
- クライアント システムをリブートしてから、もう一度インストーラを実行してみてください。
- クライアントシステム上でブラウザを使用して、**http://**<*server_name*>**:1741** にある Security Manager サーバーにログインします。「禁止（Forbidden）」または「内部サーバーエラー

（Internal Server Error）」というエラーメッセージが表示された場合は、必要な Tomcat サービスが実行していません。最近サーバをリブートして、Tomcat の稼働までに十分な時間がなかったことがない場合は、サーバログを確認するか、その他のステップを実行して、Tomcat が動作していない理由を調査する必要があります。

Q. インストーラに、以前のバージョンのクライアントがインストールされているためアンインストールされるという内容のメッセージが表示されます。しかし、以前のバージョンのクライアントはインストールされていません。これは障害ですか。

A：クライアントのインストールまたは再インストール中に、インストーラがインストールされていないクライアントを検出して、そのクライアントがアンインストールされるという内容の誤ったメッセージを表示することがあります。このメッセージは、システム内に特定の古いレジストリエントリが残っていることが原因で表示されます。このメッセージが表示されてもクライアントのインストールは正常に進行しますが、レジストリエディタを使用して次のキーを削除し、今後のインストールでこのメッセージが表示されないようにします。HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Cisco Security Manager Client （レジストリエディタを開くには、[開始（Start）] > [実行（Run）] を選択して **regedit** と入力します）。また、C:\Program Files (x86)\Zero G Registry\.com.zerog.registry.xml ファイルの名前を変更します（任意の名前を指定できます）。

インストール後のクライアント障害

Q. インターフェイスが正しく表示されないのはなぜですか。

A：古いビデオ（グラフィックス）カードは、ドライバソフトウェアをアップグレードしなければ、Security Manager GUI を正しく表示しない可能性があります。この問題がクライアントシステムに影響するかどうかをテストするには、[マイコンピュータ（My Computer）] を右クリックして、[プロパティ（Properties）] を選択し、[ハードウェア（Hardware）] を選択して、[デバイスマネージャ（Device Manager）] をクリックしてから、[ディスプレイアダプタ（Display adapters）] エントリを展開します。アダプタのエントリをダブルクリックして、使用されているドライバのバージョンを確認します。その後で、次のいずれかを実行できます。

- クライアント システムで ATI MOBILITY FireGL ビデオ カードが使用されている場合は、カードに付属していたビデオ ドライバ以外のドライバを入手しなければならない場合があります。使用するドライバは、手動で Direct 3D が設定できる必要があります。このような機能のないドライバは、Security Manager GUI 内の要素をクライアントシステムに表示できない可能性があります。
- ビデオ カードの場合は、PC メーカとカード メーカの Web サイトにアクセスして、最新の Java2 グラフィックス ライブラリの表示との非互換性をチェックしてください。既知の非互換性が残っているほとんどのケースで、半分以上のメーカが互換性のあるドライバを入手してインストールするための手段を提供しています。

Q. 日本語バージョンの Windows の [スタート（Start）] メニューに Security Manager クライアントが表示されないのはなぜですか。

A：クライアントシステム上で英語を使用するように、地域と言語のオプションを設定している可能性があります。日本語バージョンの Windows 内の言語として英語はサポートされていません。コントロール パネルを使用して、言語を日本語にリセットしてください。

Q. Security Manager クライアントがインストールされたワークステーション上で一部または全部のユーザの [Start] メニューに Security Manager クライアントが表示されないのはなぜですか。

A：クライアントをインストールするときに、製品をインストールしているユーザ専用のショートカットを作成するのか、すべてのユーザ用のショートカットを作成するのか、どのユーザ用のショートカットも作成しないのかを選択します。インストール後にこの選択を変更する場合は、Cisco Security Manager Client フォルダを Documents and Settings\<user>\Start Menu\Programs\Cisco Security Manager から Documents and Settings\All Users\Start Menu\Programs\Cisco Security Manager にコピーすることによって、手動で変更できます。ショートカットを作成しないことにした場合は、指定された All Users フォルダ内にショートカットを手動で作成する必要があります。

Q. クライアント システムとサーバ間の接続が異常に遅いと感じる場合、または、ログイン時に DNS エラーが表示される場合はどうしたらいいですか。

A：クライアントシステム上の **hosts** ファイル内に Security Manager サーバー用のエントリを作成しなければならない場合がありますこのようなエントリは、ネットワーク用の DNS サーバに登録されていない場合にサーバへの接続の確立に役立つ可能性があります。クライアントシステム上でこの有効なエントリを作成するには、メモ帳またはその他のプレーン テキスト エディタを使用して、C:\WINDOWS\system32\drivers\etc\hosts を開きます（ホストファイル自体にエントリの追加方法に関する詳細な手順が保存されています）。

（注） （Security Manager クライアント アプリケーションの [サーバー名（Server Name）] フィールドで使用される）同じ IP アドレスをポイントする DNS 追加エントリを *NMSROOT~/MDC/Apache/conf/* の下の httpd.conf 構成ファイルに作成して、Daemon Manager を再起動しなければならない場合があります。このエントリは、サーバーへの接続を確立するのに役立ちます。ServerName、foo.example.com など（**ヒント**：場所 *NMSROOT* は Security Manager インストールディレクトリへのパスです。デフォルトは **C:\Program Files (x86)\CSCOpx** です）。

Q. Security Manager クライアントを使用してログインしようとしたときにエラーメッセージが表示されることなくログイン情報が受け入れられましたが、Security Manager デスクトップが空の状態で使用できません。認証セットアップの何が間違っているのでしょうか（また、Security Manager サーバー上の Common Services でログイン情報が受け入れられましたが、Web ブラウザ上で Cisco Security Management Suite デスクトップのロードに失敗します。これも同じ原因でしょうか）。

A：Security Manager と Common Services に対してログイン認証サービスを提供するための Cisco Secure ACS に必要なステップが完了していない可能性があります。ACS でログイン情報を入力しましたが、Security Manager サーバーを AAA クライアントとして定義していません。この定義を行わなければ、ログインできません。詳しい手順については、ACS のマニュアルを参照してください。

Q. Security Manager クライアントを使用してサーバにログインできず、次のようなメッセージが表示されます。どうしたらいいですか。

... repeatedly that the server is checking its license.	サーバが最小限のハードウェア要件とソフトウェア要件を満たしていることを確認してください。サーバの要件および推奨事項を参照してください。
`Synchronizing with DCR.`	2 通りの可能性が考えられます。 • サーバーの再起動直後に Security Manager クライアントを起動した可能性があります。その場合は、サーバーが完全に使用可能になるまで数分待ってから、Security Manager クライアントを使用してみてください。 • CiscoWorks 管理パスワードにアンパサンド（&）などの特殊文字が含まれている可能性があります。その結果、Security Manager のインストール時にサーバー上の *NMSROOT*\lib\classpath サブディレクトリで comUser.dat ファイルを作成できませんでした。ここで、*NMSROOT* は Common Services をインストールしたディレクトリです（デフォルトは C:\Program Files (x86)\CSCOpx です）。 1. Cisco TAC に連絡して、**comUser.dat** の交換または Security Manager の再インストールに関する支援を要請してください。 2. または、特殊文字を含まない Common Services パスワードを作成します。
`Error - Unable to Check License on Server. An attempt to check the license file on the Security Manager server has failed. Please confirm that the server is running. If the server is running, please contact the Cisco Technical Assistance Center.`	次のサービスのいずれかが正しく起動していない可能性があります。サーバー上で、[スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [サービス（Services）] を選択して、次の名前のサービスを右クリックし、ショートカットメニューから [再起動（Restart）] を選択します。 • Cisco Security Manager Daemon Manager • Cisco Security Manager Database Engine • Cisco Security Manager Tomcat Servlet Engine • Cisco Security Manager VisiBroker Smart Agent • Cisco Security Manager Web Engine 5 分待ってから、もう一度 Security Manager クライアントを起動してみてください。

Q. デフォルト ブラウザとして Internet Explorer を使用しているときにアクティビティ レポートが表示されないのはなぜですか。

A：この問題は、無効なレジストリ キー値、または Internet Explorer に関連付けられた DLL ファイルの場所に関する間違いが原因で発生します。この問題の対処法については、http://support.microsoft.com/kb/281679/EN-US から入手可能な Microsoft サポート技術情報の記事 281679 [英語] を参照してください。

Q. どうすれば、ログイン ウィンドウの [Server Name] フィールドからサーバ リストを消去できますか。

A：csmserver.txt を編集して必要のないエントリを削除します。このファイルは、Security Manager クライアントをインストールしたディレクトリ内にあります。デフォルトの場所は、C:\Program Files (x86)\Cisco Systems\Cisco Security Manager Client です。

Q. バージョン ミスマッチが原因で Security Manager クライアントがロードされなかった可能性があります。What does this mean?

A：Security Manager サーバのバージョンとクライアントのバージョンが一致していません。これを修正するには、最新のクライアント インストーラをサーバからダウンロードしてインストールします。

Q. クライアント ログ ファイルはどの場所にありますか。

A：クライアントログファイルは、C:\Program Files (x86)\Cisco Systems\Cisco Security Manager Client\logs に配置されています。GUI セッションごとに専用のログ ファイルが作成されます。

Q. Security Manager が HTTPS モードで動作中かどうかはどうすれば確認できますか。

A：次のいずれかを実行します。

- ブラウザを使用してサーバにログインしたら、アドレス フィールド内の URL を調査します。URL が https で始まっていれば、Security Manager が HTTPS モードで動作しています。
- [Common Services] > [Server] > [Security] > [Single Server Management] > [Browser-Server Security Mode Setup] に移動します。[Current Setting] が [Enabled] になっていれば、Security Manager が HTTPS モードで動作しています。この設定が [Disabled] の場合は、HTTP を使用します。
- クライアントを使用してログインするときに、まず、HTTPS モードを試してみてください（[HTTPS] チェックボックスをオンにします）。「ログインURLへのアクセスは禁止されています。プロトコル(HTTP、HTTPS)が正しいことを確認してください（Login URL access is forbidden; Please make sure your protocol (HTTP, HTTPS) is correct）」というメッセージが表示されたら、サーバーは HTTP モードで動作している可能性があります。[HTTPS] チェックボックスをオフにして、もう一度試してみてください。

Q. どうすれば、クライアント デバッグ ログ レベルをイネーブルにできますか。

A：デフォルトで C:\Program Files (x86)\Cisco Systems\Cisco Security Manager Client\jars に配置されている client.info ファイル内で、DEBUG_LEVEL パラメータに DEBUG_LEVEL=ALL を追加してから、Security Manager クライアントを再起動します。

Q. 2 画面構成で作業している場合は、Security Manager クライアントが第 2 画面上で動作していても、必ず、特定のウィンドウとポップアップ メッセージが第 1 画面に表示されます。たと

えば、クライアントが第 2 画面上で動作しているときに、必ず、Policy Object Manager などのウィンドウが第 1 画面に表示されます。これを修正できますか。

A：これは、特定のオペレーティング システムにおける 2 画面サポートの実装方法に伴う既知の問題です。Security Manager クライアントを第 1 画面上で動作させることを推奨します。クライアントは、2 画面構成の設定後に起動する必要があります。

他の画面でウィンドウが開いた場合は、Alt + スペースバーを押した後に M を押すことによってそのウィンドウを移動できます。その後で、矢印キーを使用してウィンドウを移動します。

Q. クライアント システム上でソフトウェアをインストールまたはアンインストールできません。どうしてですか。

A：クライアントシステム上でインストールとアンインストールを同時に実行した場合は、それらが別々のアプリケーションに対するものであっても、クライアントシステムの InstallShield データベースエンジンに悪影響を与え、ソフトウェアのインストールまたはアンインストールができなくなります。詳細については、Cisco.com アカウントにログインしてから、Bug Toolkit を使用して CSCsd21722 と CSCsc91430 を確認してください。

サーバ セルフテストの実行

Security Manager サーバーが正しく動作していることを確認するセルフテストを実行するには、次の手順を実行します。

ステップ 1 Security Manager クライアントが Security Manager サーバーに接続されているシステムから、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択します。

ステップ 2 [管理（Administration）] ウィンドウで、[サーバーセキュリティ（Server Security）] をクリックしてから、任意のボタンをクリックします。新しいブラウザが開いて、クリックしたボタンに対応する Common Services GUI のセキュリティ設定ページが表示されます。

ステップ 3 [Common Services（Common Services）] ページの [サーバー（Server）] タブで、[管理者（Admin）] を選択します。

ステップ 4 [管理者（Admin）] ページの TOC で、[セルフテスト（Selftest）] をクリックします。

ステップ 5 [作成（Create）] をクリックします。

ステップ 6 *<MM-DD-YYYY HH:MM:SS>* リンクで [セルフテスト情報（SelfTest Information）] をクリックします。ここで、

MM-DD-YYYY は、現在の月、日、年です。

HH:MM:SS は、[セルフテスト（Selftest）] をクリックした時、分、秒を表すタイムスタンプです。

ステップ 7 [Server Info] ページでエントリを読み取ります。

サーバ トラブルシューティング情報の収集

Security Manager で問題が発生しており、エラー メッセージ内の推奨事項のすべてを試し、このマニュアル内の可能性のある解決策を確認したにもかかわらず、問題が解決されない場合は、Security Manager Diagnostics ユーティリティを使用してサーバ情報を収集します。

Security Manager Diagnostics ユーティリティは、ZIP ファイルの CSMDiagnostics.zip からサーバー診断情報を収集します。このファイル名を変更しなかった場合は、Security Manager Diagnostics を実行するたびに新しい情報でファイルが上書きされます。CSMDiagnostics.zip ファイル内の情報は、サーバー上の Security Manager または関連アプリケーションで発生した問題のシスコのテクニカルサポート エンジニアによる解決を支援します。

ヒント　Security Manager には、アプリケーションによって実施された設定変更に関する情報を収集する高度なデバッギング オプションも用意されています。このオプションをアクティブにするには、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デバッグオプション（Debug Options）] を選択してから、[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）] チェックボックスをオンにします。診断ファイルに保存されたその他の情報はトラブルシューティングの試みに役立つ可能性がありますが、ファイルにはパスワードなどの機密情報が書き込まれている場合があることに注意してください。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。

Security Manager Diagnostics は次のいずれかの方法で実行できます。

Security Manager クライアントシステムから	**Security Manager サーバーから**
1. サーバーへの Security Manager クライアント セッションを確立したら、[ツール（Tools）]> [Security Managerの管理（Security Manager Administration）] をクリックして [OK（OK）] をクリックします。 CSMDiagnostics.zip ファイルは、サーバー上の *NMSROOT* \MDC\etc\ ディレクトリに保存されます。ここで、*NMSROOT* は、Common Services をインストールしたディレクトリです（C:\Program Files (x86)\CSCOpx など）。 **1.** [閉じる（Close）] をクリックします。 （注）　このユーティリティを実行するたびに上書きされないようにこのファイルの名前を変更することを推奨します。	**1.** Windows のコマンドウィンドウを開きます。それには、たとえば[スタート（Start）] > [実行（Run）] を選択し、**command** と入力します。 **2.** **C:\Program Files (x86)\CSCOpx\MDC\bin\CSMDiagnostics** と入力します。または、このZIPファイルを *NMSROOT* \MDC\etc\ とは別の場所に保存するには、**CSMDiagnostics** *drive:\path* と入力します。たとえば、CSMDiagnostics D:\temp と入力します。

サーバ プロセス ステータスの表示と変更

Security Manager のサーバープロセスが正しく動作していることを確認するには、次の手順を実行します。

ステップ 1 CiscoWorks のホームページで、[Common Services（Common Services）] > [サーバー（Server）] > [管理者（Admin）] を選択します。

ステップ 2 [管理者（Admin）] ページの TOC で、[プロセス（Processes）] をクリックします。

[Process Management] テーブルにすべてのサーバ プロセスが表示されます。[ProcessState] カラム内のエントリが、プロセスが正常に動作しているかどうかを示します。

ステップ 3 必要なプロセスが動作していない場合は、それを再起動します。サーバ上の全プロセスの再起動 （27 ページ）を参照してください。

（注） ローカル管理者特権を持つユーザのみがサーバ プロセスを起動または停止できます。

サーバ上の全プロセスの再起動

（注） すべてのプロセスを停止してから、それらを再起動しなければ、この方法は機能しません。

ステップ 1 コマンドプロンプトで、**net stop crmdmgtd** と入力してすべてのプロセスを停止します。

ステップ 2 **net start crmdmgtd** と入力してすべてのプロセスを再起動します。

ヒント または、[スタート（Start）] > [設定（Settings）] > [コントロールパネル（Control Panel）] > [管理ツール（Administrative Tools）] > [サービス（Services）] を選択してから、Cisco Security Manager Daemon Manager を再起動できます。

サーバ インストール ログ ファイルの確認

サーバからの応答が期待していたものと違っていた場合は、サーバ インストール ログ ファイルでエラー メッセージと警告メッセージを確認できます。

テキストエディタを使用して、**Cisco_Prime_install_*.log** を開きます。

ほとんどの場合、確認すべきログファイルは、ファイル名に最大の番号が付けられたファイルか、作成日が最新のファイルです。

たとえば、ログ ファイルでは、次のようなエラー エントリと警告エントリが確認できます。

```
ERROR: Cannot Open C:\PROGRA~1\CSCOpx/lib/classpath/ssl.properties at
C:\PROGRA~1\CSCOpx\MDC\Apache\ConfigSSL.pl line 259.
INFO: Enabling SSL....
WARNING: Unable to enable SSL. Please try later....
```

インストールログと同じように、アンインストールログのエラーを確認できます。

テキストエディタを使用して、**Cisco_Prime_uninstall_*.log** を開きます。

Symantec の共存問題

Symantec Antivirus Corporate Edition 10.1.5.5000 と Security Manager を同じシステムで使用し、Security Manager 起動中に問題が発生した場合は、次の手順に従ってください。

手順

ステップ 1 Symantec Antivirus を完全にディセーブルにします。

ステップ 2 Security Manager サービスを再起動します。（サーバ上の全プロセスの再起動 （27 ページ） を参照。）

ステップ 3 Symantec Event Manager を最後に起動したような方法で、Symantec サービスのセット（Symantec Antivirus、Symantec Antivirus Definition Watcher、Symantec Settings Manager、および Symantec Event Manager）を再起動します。

Windows アップデートのインストール後の問題

Microsoft Windows アップデートをインストールした後に、Security Manager Daemon Manager に関する問題が発生する可能性があります。原因は、Windows アップデートのインストールにより、*.dll ファイルが更新される場合があり、これに依存する Common Services などのアプリケーションの機能に影響する可能性があることです。

この問題は、次の症状で認識できます。Windows アップデートの後、Security Manager によってすべてのプロセスを開始しますが、Security Manager に HTTPS を介して到達できません。このため、Security Manager クライアントから HTTPS を使用します。

この問題が生じるのは、Common Services が Windows 内のファイルおよび関連付けに依存するためです。これらのファイルは、脆弱性を修正し、不正利用から Windows を保護するために変更できます。ただし、意図しない副作用として再起動した場合はこれらの変更により、Security Manager サーバの異常動作が起きる可能性があります。

この問題は、Windows アップデート、またはその他のアプリケーションが、*.dll ファイル、実行可能ファイル、起動プロセス、Windows コンポーネント、またはパーティション サイズに影響する Windows に変更を加えると、いつでも発生する可能性があります。

Windows で変更が行われ、その再起動で Security Manager が異常動作した場合に、この問題を解決するには、Security Manager を再インストールする必要があります。

Windows Update またはその他のインストーラパッケージを実行する前に、必ず Security Manager サーバーをバックアップしてください。

Cisco Security Manager サーバーのバックアップ

シスコは Security Manager サーバーを定期的にバックアップすることを推奨します。特に、定期的なバックアップが行われていない場合、または Security Manager インストールに対して多数の変更を行う場合は、Security Manager サーバーをバックアップする必要があります。

問題：手動またはスケジュールバックアップを実行すると、完了に失敗することがあります。このエラーは、「情報：ファイルが存在しません。SQL（INFO: File not exists.SQL）」または検証エラーが原因で発生する可能性があります。

解決策：dbbackup_timestamp.log を添付し、Tac ケースを作成します。

高度な暗号化による ASA デバイスへの接続の問題

このトラブルシューティングの項目は、高度な暗号化を使用して ASA デバイスを追加および検出できない場合に役立ちます。特に AES-282 を使用する場合は、Java Cryptography Extension（JCE）Unlimited Strength Jurisdiction Policy File をダウンロードしてインストールする必要があります。Security Manager はこの拡張を含みませんが、これをサポートします。

問題：証明書に含まれるキーが 1024 ビットを超える場合に問題が発生します。Java ランタイム環境（JRE）に含まれているデフォルト ポリシー ファイルによって設定される暗号化強度の制限は、すべての国へのインポートが可能な、最高強度暗号化アルゴリズムとキー長を提供します。

解決策：当該国で暗号化のインポートに制限が定められていなければ、無制限強度ポリシー ファイルをダウンロードできます。

ステップ 1 http:// java.sun.com/javase/downloads/index.jsp に移動します。

ステップ 2 「Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6」をダウンロードします。

ステップ 3 ダウンロードしたパッケージの README.txt ファイルの説明に従ってください。

インストール時に使用する Activation.jar のポップアップ表示

このトラブルシューティング項目は、インストール中に「Activation.jarはその他のサービスで使用されています（Activation.jar being used by some other service）」というメッセージがポップアップウィンドウで表示される場合に役立ちます。

ヒント この問題はきわめてまれにしか起こりません。

はじめる前に

サーバのすべてのアンチウイルスまたはモニタリング エージェント プロセスは、インストール前にシャットダウンする必要があります。詳細については、インストール準備状況チェックリストを参照してください。

問題

「Activation.jarはその他のサービスで使用されています（Activation.jar being used by some other service）」というメッセージがポップアップウィンドウで表示されます。

解決方法

次の手順を使用してください。

ステップ 1 ポップアップで [OK] をクリックして、インストールを完了します。

ステップ 2 Security Manager をアンインストールし、サーバを再起動します。

ステップ 3 Security Manager を再インストールします。

ステップ 4 インストールを開始した直後に、「services.msc」をコマンドプロンプトに入力し、Enter キーを押します。

ステップ 5 [サービス（Services）] メニューを開くと、「Cisco Security Manager Daemon Manager」が表示されるまで更新が続きます。

ステップ 6 [CSM Daemon Manager] を右クリックして、[Properties] > [Startup type] > [Disabled] の順にクリックします。

ステップ 7 [CWCS syslog service] を右クリックして、[Properties] > [Startup type] > [Disabled] の順にクリックします。

ステップ 8 インストールの完了後、サーバーの再起動時に、「無効（Disabled）」から「自動（Automatic）」モードに上記のサービスの両方の起動タイプを変更します。

Windowsの既定のユーザーテンプレートのロケールを米国英語に設定する方法

通常、英語（米国）以外の Windows ロケールを使用する場合は、Security Manager をインストールする前にデフォルトのシステム ロケールを米国英語に変更する必要があります。デフォルト システム ロケールを変更し、サーバをリブートしても、デフォルト プロファイルは変更されません。現在のユーザーは、適切な設定をするだけでは十分ではありません。これは、Security Manager はすべての Security Manager サーバープロセスを実行する新しいアカウント（「casuser」）を作成するためです。

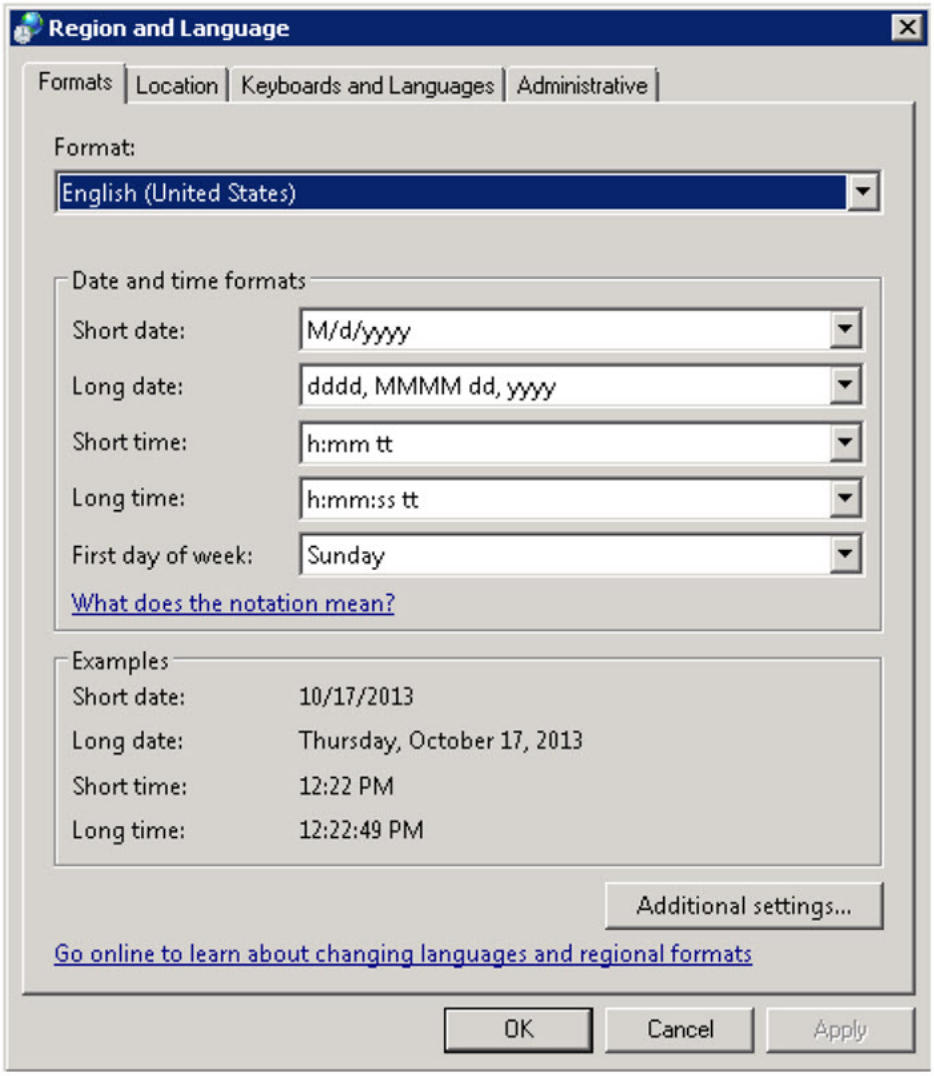
ここでは、特に、通常英語（米国）以外の Windows ロケールを使用する場合に、Security Manager サーバの地域と言語設定を設定する方法について説明します。具体的な詳細は、Microsoft Windows Server 2008 R2 with SP1 Enterprise（64 ビット）に適用されますが、その他のサポートされている以下のサーバー オペレーティングシステムに非常に似ています。

- Microsoft Windows Server 2019 Standard（64 ビット）
- Microsoft Windows Server 2019 Datacenter（64 ビット）
- Microsoft Windows Server 2012 Standard（64 ビット）
- Microsoft Windows Server 2012 Datacenter（64 ビット）

新たに作成されたすべてのユーザに現在のユーザと同じ設定を適用するには、新しいユーザアカウントに現在のユーザの設定をコピーする必要があります。これは、次に示す手順で実行できます。

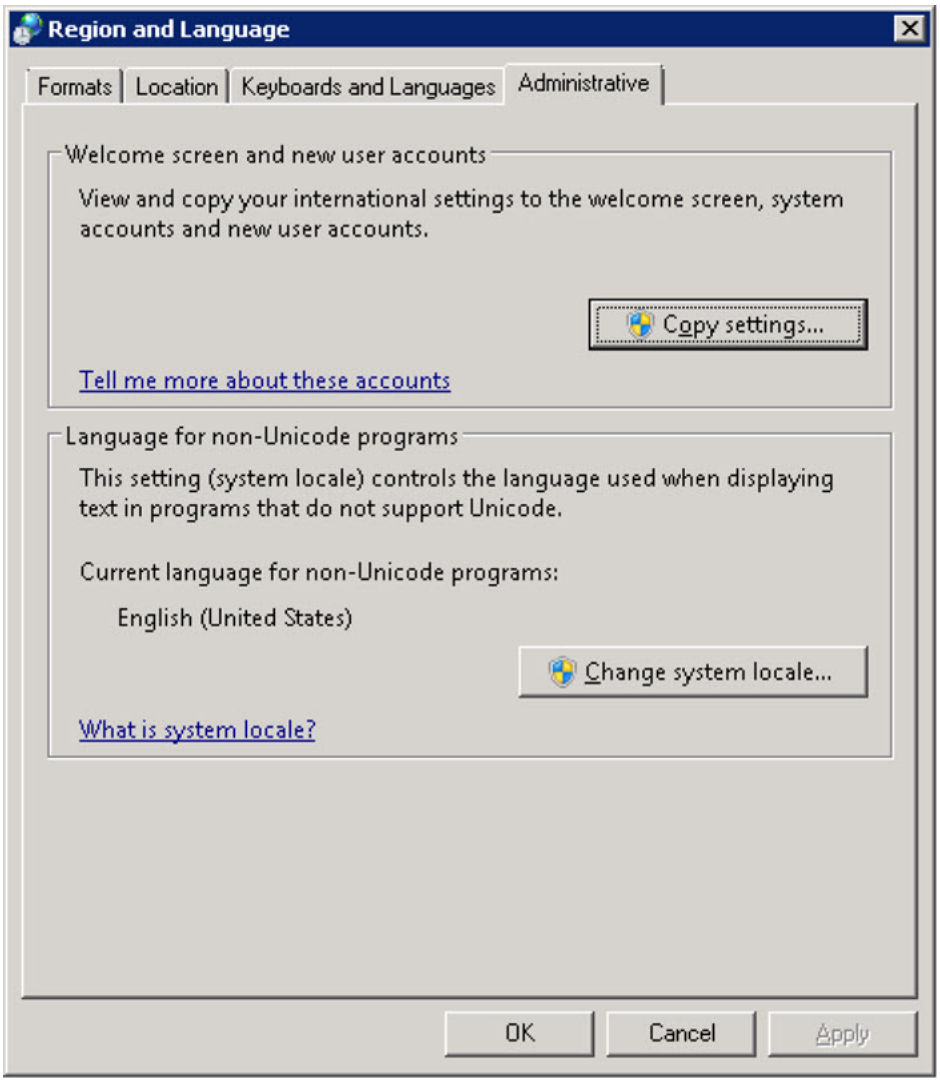
現在のユーザが、[Region and Language] ダイアログボックスで適切な米国英語に設定されていることを確認します。（このダイアログボックスのナビゲーション パスは [Start] > [Control Panel] > [Region and Language] です）。

図 A-1 Windows の [地域と言語（Region and Language）] ダイアログボックス



[管理（Administrative）] タブをクリックします。[設定のコピー...（Copy Settings...）] ボタンを見つけます。

図 A-2 [管理（Administrative）] タブ



[設定のコピー...（Copy Settings...）] ボタンをクリックします。[Welcome screen and new user account] 設定ダイアログボックスが表示されます。

[現在の設定のコピー先：（Copy your current settings to:）] で、[新しいユーザーアカウント（New user accounts）] ボックスをオンにします。これによって、新たに作成されたすべてのユーザに現在のユーザと同じ設定を適用します。

最後に、Cisco Security Manager サーバをインストール（または再インストール）します。新しいインストールでは、すべての Security Manager サーバープロセスを実行する新しいアカウント（「casuser」）には米国英語のデフォルトプロファイルが適用されます。

RMI レジストリポートを無効にする方法

一般的な Cisco Security Manager の設定では、RMI レジストリポートはデフォルトで開いています。一般的な Cisco Security Manager 設定では、これを無効にする必要がある場合があります。RMI レジストリポートを無効にするには、次の手順に従います。

問題

RMI レジストリポートの無効化

解決方法

次の手順を使用してください。

ステップ 1 Cisco Security Manager サーバーを停止します。

ステップ 2 Cisco Security Manager サーバーの次の Windows レジストリパスから ESS レジストリエントリをエクスポートします。

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Resource Manager\CurrentVersion\Daemons\ESS

（注） これは、バックアップを作成するために推奨されます。

ステップ 3 **ESS_Reg_Edit.bat** ファイルを実行します。このファイルは（障害 CSCvc21327 に添付されている）Bug Search Kit で入手できます。このファイルは、引数キーの JMX リモートモニタリング パラメータを削除することで、ESS レジストリエントリを更新します。

ステップ 4 ~CSCOpx\objects\ess\conf\activemq.xml 場所で **activemq.xml** ファイルを見つけます。

ステップ 5 次のように、「createConnector」の値を false に変更します。

<managementContext>

<managementContext createConnector="false"/>

</managementContext>

ステップ 6 **activemq.xml** を保存します。

ステップ 7 Cisco Security Manager を再起動します。

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。