Prime Infrastructure サーバーを設定する

サーバーの構成の表示

現在のサーバー時間、カーネル バージョン、オペレーティング システム、ハードウェア情報などの サーバーの構成情報を表示するには、以下の手順を使用します。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム監視ダッシュボード（System Monitoring Dashboard）]** を選択します。

ステップ 2 [概要（Overview）] タブをクリックします。

ステップ 3 ダッシュボードの左上にある [システム情報（System Information）] をクリックして、[システム情報（System Information）] フィールドを展開します。

使用可能なシステム設定

[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] メニューには、Cisco Prime Infrastructure 設定値を設定または変更するためのオプションが含まれています。これらの設定値の多くは、最初に Prime Infrastructure を実装する際にカスタマイズできますが、実稼働に移した後に変更することは、ほとんどありません。

次の表に、[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] メニューから設定または変更できる設定値のタイプを一覧表示します。

表 *1* : 使用可能な *Prime Infrastructure* システム設定オプション

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Cisco.com へのログオンに使用するために保管されている Cisco.com クレデンシャル（ユーザー名とパスワード）を変更し、次の操作を行います。 • シスコ ソフトウェア イメージ アップデートの有無の確認 • シスコ サポート ケースの登録または確認 このページへは、[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ソフトウェア更新（Software Update）] ページのリンクからもアクセスできます。	[一般（General）] > [アカウント クレデンシャル（Account Credentials）]	Prime Infrastructure アプライアンス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Prime Infrastructure サーバーとそのローカル認証サーバーのプロキシを設定します。	[一般（General）] > [アカウント クレデンシャル（Account credentials）] > [プロキシ（Proxy）] 「プロキシ サーバーの設定」を参照してください。	N/A
テクニカル サポート リクエストを作成するための設定値を設定します。	[一般（General）] > [アカウント クレデンシャル（Account credentials）] > [サポート リクエスト（Support Request）] 「シスコサポート リクエストのデフォルトの設定」を参照してください。	有線およびワイヤレス デバイス
スマート ライセンスが有効な状態で、Smart Call Home Transport Gateway を使用してインターネット経由で情報を送信するように Transport Gateway のモードを設定します。	[一般（General）] > [アカウント クレデンシャル（Account credentials）] > [スマート ライセンス トランスポート（Smart Licensing Transport）] 「Prime Infrastructure と Cisco Smart Software Manager との間のトランスポート モードの設定」を参照してください。	Prime Infrastructure アプライアンス
特定のデータ タイプ（傾向、デバイス ヘルス、パフォーマンス、ネットワーク監査、システム ヘルス）の保存期間を設定します。	**[一般（General）] > [データ保存（Data Retention）]** 履歴データの保持についてを参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
ゲストアカウント設定値を設定して、有効期限が終了したすべてのゲストアカウントをグローバルに削除します。デフォルトでは、Prime Infrastructure ロビーアンバサダーは作成者に関係なく、すべてのゲストアカウントにアクセスできます。[この Lobby Ambassador が作成したゲストのみを検索して表示（Search and List only guest accounts created by this lobby ambassador）] チェックボックスをオンにした場合、Lobby Ambassador は本人が作成したゲストアカウントのみにアクセスできます。	**[一般（General）] > [ゲスト アカウント（Guest Account）]** ゲスト アカウントの設定を参照してください。	ワイヤレス デバイスのみ
シスコ製品の向上のために、Prime Infrastructure は製品フィードバック データを収集してシスコに送信します。	[一般（General）] > [改善にご協力ください（Help Us Improve）] シスコ製品フィードバックの設定 （54 ページ）を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
ジョブ承認を有効にして、実行する前に管理者の承認を必要とするジョブを指定します。	**[一般（General）] > [ジョブ承認（Job Approval）]** ジョブ承認者を設定してジョブを承認するを参照してください。	有線およびワイヤレス デバイス
すべてのユーザに対してログインページに表示される免責事項テキストを変更します。	**[一般（General）] > [ログインの免責事項（Login Disclaimer）]** ログイン バナー（ログインの免責事項）の作成 （40 ページ）を参照してください。	Prime Infrastructure アプライアンス
定期レポートの保存先パス、およびレポートの保存期間を設定します。	**[一般（General）] > [レポート（Report）]** レポートの保存と保持の制御を参照してください。	有線およびワイヤレス デバイス
• FTP、TFTP、および HTTP/HTTPS サーバープロキシを有効または無効にし、これらのプロキシが通信に使用するポートを指定します。 • Prime Infrastructure に対して現在設定されているローカル タイムゾーンと NTP サーバー名を確認します。	**[一般（General）] > [サーバー（Server）]** サーバー ポートおよびグローバル タイムアウトの設定 （37 ページ）を参照してください。	Prime Infrastructure アプライアンス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
• Prime Infrastructure が Cisco.com でシスコ ソフトウェア イメージ アップデートを確認するときに、cisco.com に保管されているクレデンシャルを使用しないことを指定します。 • 通知を受信する Prime Infrastructure ソフトウェア アップデートの種類（重要な修正、新しいデバイス サポート、Prime Add-On 製品など）を選択します。	**[一般（General）] > [ソフトウェア更新（Software Update）]**	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
インベントリ、サイトグループ、ユーザー定義の CLI や複合テンプレート、関連するサイトマップ、および CMX データを Cisco Prime Infrastructure から Cisco DNA Center に移行します。	**[Mega] メニュー > [Cisco DNA Center coexistence]** Cisco Prime Infrastructure と Cisco Digital Network Architecture Center の共存ガイド [英語] を参照	Prime Infrastructure から Cisco DNA Center への移行
[監査ログのパージ設定（Audit Log Purge Settings）] チェックボックスをオンにして、変更監査 JMS 通知を有効にします。	**[メールおよび通知（Mail and Notification）] > [監査通知の変更（Change Audit Notification）]** 変更監査通知の有効化および syslog レシーバの設定を参照してください。	有線およびワイヤレス デバイス
ユーザージョブごとにジョブ通知メールを送信します。	**[メールと通知（Mail and Notification）] > [ジョブ通知メール（Job Notification Mail）]** 「ユーザージョブ用のジョブ通知メールを設定する」を参照	有線およびワイヤレス デバイス
レポートおよびアラーム通知の電子メール配信を有効にします。	**[メールおよび通知（Mail and Notification）] > [メール サーバー設定（Mail Server Configuration）]** 電子メール サーバー設定の構成を参照してください。	Prime Infrastructure アプライアンス

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
• コントローラおよび自律 AP CLI セッションに使用するプロトコルを設定します。 • 検出時の自律 AP 移行分析を有効にします。	**[ネットワークおよびデバイス（Network and Device）] > [CLI セッション（CLI Session）]** を参照してください。	ワイヤレス デバイスのみ
ワイヤレス コントローラのアップグレード後の自動更新を有効にし、save config トラップを処理します。	**[ネットワークおよびデバイス（Network and Device）] > [コントローダ アップグレード（Controller Upgrade）]** アップグレード後のコントローラの更新を参照してください。	ワイヤレス デバイスのみ
Cisco Prime Infrastructure での Unified AP の ping 機能設定を有効にします。	**[ネットワークとデバイス（Network and Device）] > [Unified AP への Ping 確認（Unified AP Ping Reachability）]**	ワイヤレス デバイスのみ
プラグ アンド プレイの設定を変更します。	**[ネットワークおよびデバイス（Network and Device）] > [プラグ アンド プレイ（Plug & Play）]**	有線デバイスのみ

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
	[ネットワークおよびデバイス（Network and Device）] > [SNMP] グローバル SNMP の設定 （41 ページ）を参照してください。	ワイヤレス デバイスのみ

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
トレース表示値、到達可能性パラメータ、バックオフアルゴリズムを含め、グローバル SNMP ポーリングパラメータを設定します。 バックオフアルゴリズムに [Exponential] を選択した場合は、SNMP 初回試行時には指定したタイムアウト値が使用され、2 回目からは、前回の試行時の 2 倍の待機時間が適用されます。[一定タイムアウト（Constant Timeout）] を選択した場合は、すべての SNMP 試行に対して同じ待機時間（指定したタイムアウト値）が適用されます。到達可能性パラメータを使用することを選択した場合は、Prime Infrastructure はデフォルトで、ユーザーが設定したグローバルな [到達可能性の再試行回数		

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
（Reachability Retries）]および[タイムアウト（Timeout）] を使用します。チェックボックスがオフにされている場合、Prime Infrastructure は常に、指定されたタイムアウトと再試行を使用します。		
不正 AP を設定し、Prime Infrastructure がネットワーク内で不正アクセスポイントの接続先となっているスイッチポートを自動的に追跡できるようにします。	**[ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [自動 SPT（Auto SPT）]** 不正 AP トレース用の SNMP クレデンシャルの設定を参照してください。	ワイヤレス デバイスのみ
不正 AP スイッチ ポートのトレースで使用する SNMP クレデンシャルとトレースパラメータを設定します。	**[ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）]** 不正 AP トレース用の SNMP クレデンシャルの設定を参照してください。	ワイヤレス デバイスのみ
スイッチ ポート トレースの基本パラメータと拡張パラメータを設定します。	**[ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [SPT 設定（SPT Configuration）]** スイッチ ポート トレースを設定するを参照してください。	有線デバイスのみ

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Prime Infrastructure で使用可能なイーサネット MAC アドレスの表示、追加、削除を行います。この一覧に複数のイーサネット MAC アドレスを追加すると、自動スイッチポート トレースで、これらのポートでの不正 AP のスキャンが行われなくなります。	**[ネットワークとデバイス（Network and Device）] > [ポート トレースのスイッチ（SPT）（Switch Port Trace (SPT)）] > [認識済みのイーサネット MAC アドレス（Known Ethernet MAC Address）]**	Prime Infrastructure アプライアンス
デバイス設定の導入時に使用する基本制御パラメータ（実行コンフィギュレーションのバックアップの有効化、ロールバック、キャッシュからの **show** コマンド出力の取得、使用する CLI スレッド プールの数など）を設定します。	**[インベントリ（Inventory）] > [設定（Configuration）]** テンプレート導入前のデバイス設定のアーカイブを参照してください。	有線およびワイヤレス デバイス
設定アーカイブの基本パラメータ（プロトコルや保存する設定バージョン数など）を設定します。	**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** WLC 設定をいつどのようにアーカイブするかの指定を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
IPv4 または IPv6 アドレスの優先設定を指定します。	**[インベントリ（Inventory）] > [Discovery]**	有線およびワイヤレス デバイス
メンバーまたは子が関連付けられていないグループを表示するかどうかを設定します。	**[インベントリ（Inventory）] > [グループ化（Grouping）]**	有線およびワイヤレス デバイス
ソフトウェアイメージのダウンロード、配布、および推奨用のグローバルプリファレンスパラメータを設定します。	**[インベントリ（Inventory）] > [ソフトウェアイメージの管理（Software Image Management）]** ソフトウェアイメージの管理の詳細については、『Cisco Prime Infrastructure User Guide』を参照してください。	有線およびワイヤレス デバイス
インベントリ収集を有効にして、Prime Infrastructure がデバイスに関する syslog イベントを受信した場合にインベントリを収集できるようにします。	**[インベントリ（Inventory）] > [インベントリ（Inventory）]** イベント受信後のインベントリ収集の指定を参照してください。	有線およびワイヤレス デバイス
デバイスに関する追加情報を保存します。	**[インベントリ（Inventory）] > [ユーザー定義フィールド（User Defined Fields）]** ユーザー定義フィールドにデバイス情報を追加する （49 ページ）を参照してください。	有線デバイスのみ

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
• 削除するアラーム、イベント、syslog と、削除する頻度を変更します。 • 電子メール通知の送信対象とするアラームのタイプ、および送信する頻度を設定します。 • [Alarm Summary] ビューに表示するアラームのタイプを設定します。 • 電子メールで送信するアラーム通知の内容を変更します。 • 障害の原因の表示方式を変更します。	**[アラームおよびイベント（Alarms and Events）] > [アラームおよびイベント（Alarms and Events）]** アラーム クリーンアップ、表示、および電子メール オプションの指定を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Prime Infrastructure から通知を受信するリモートイベントおよびアラームの受信者を設定します。 アラートおよびイベントは SNMPv2 通知として、設定された通知宛先に送信されます。通知タイプ UDP の通知宛先を追加する場合、その追加する宛先はそれが設定されている同じポート上で UDP をリッスンしている必要があります。デフォルトでは、選択されたカテゴリに対する INFO レベルのイベントのみが処理されます。ノースバウンド通知では、SNMPV2 トラップのみが考慮されます。	**[メールと通知（Mail and Notification）] > [通知宛先（Notification Destination）]** アラーム通知先の設定を参照してください。 **[アラームおよびイベント（Alarms and Events）] > [アラーム通知ポリシー（Alarm Notification Policies）]** アラーム通知ポリシーのカスタマイズを参照してください。	有線およびワイヤレス デバイス
生成される任意のアラームのシビラティ（重大度）を設定します。	**[アラームおよびイベント（Alarms and Events）] > [アラームのシビラティ（重大度）および自動クリア（Alarm Severity and Auto Clear）]** シビラティ（重大度）レベルの変更を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Prime Infrastructure ハードウェアアプライアンスについて生成される SNMP トラップとイベントを設定します。	**[アラームおよびイベント（Alarms and Events）] > [システム イベント設定（System Event Configuration）]** 内部 SNMP トラップの生成を参照してください。	Prime Infrastructure アプライアンス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
	[クライアントおよびユーザー（Client and User）] > [クライアント（Client）] クライアント パフォーマンスの設定を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
• 診断チャネルでクライアントの自動トラブルシューティングを有効にします。 • DNS サーバからのクライアントホスト名のルックアップを有効にし、ホスト名をキャッシュに保持する期間を設定します。 • 関連付けが解除されたクライアントとそのセッションデータを保持する期間を設定します。 • 有線クライアントをポーリングし、トラップまたは syslog を受信した場合にのみセッションを識別します。 （注） これ		

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
は、ワイヤレスクライアントが多数あるネットワークで使用することが推奨されるオプションではあり		

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
ません。 • [拡張クライアント トラップからクライアントを検出する（Discover Clients from enhanced client traps）] を有効にすると、互換性のある Cisco WLC から受信した拡張トラップからのクライアントおよびセッション情報が検出できるようになります。 次の CLI コマンドを使用して、トラップを送信するように WLC を設定する必要があります。		

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
• config trapflags client • config trapflags client • config trapflags client • config trapflags client		

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
• [トランクポート上の有線クライアントを検出（Discover wired clients on trunk ports）] を有効にすると、トランク ポートに接続されている、スイッチとルータ以外の管理対象外エンティティを検出できるようになります。 • イベントとしてのクライアント関連付けおよび関連付け解除のトラップと syslog の保存を無効にします。 • イベントとしてのクライアント認証失敗トラップの保存、および失敗トラップの間でイベントを保		

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
存する期間を有効にします。		
ベンダーの組織固有識別子（OUI）マッピング XML ファイルを追加します。	**[クライアントおよびユーザー（Client and User）] > [ユーザー定義 OUI（User Defined OUI）]** 「新しいベンダー OUI マッピングの追加」を参照してください。	有線およびワイヤレス デバイス
更新されたベンダー OUI マッピング XML ファイルをアップロードします。	**[クライアントおよびユーザー（Client and User）] > [OUI のアップロード（Upload OUI）]** 「更新されたベンダー OUI マッピング ファイルのアップロード」を参照してください。	有線およびワイヤレス デバイス
Cisco Prime Infrastructure に Cisco WAAS Central Manager の IP アドレスを設定します。	**[サービス（Services）] > [サービス コンテナの管理（Service Container Management）]** 『Cisco WAAS Central Manager Integration』（ユーザー ガイド）を参照してください。	有線デバイスのみ

サーバーの接続の保護

データ セキュリティのため、は、標準の公開キー暗号化方式と Public Key Infrastructure（PKI）を使用して送信中のデータを暗号化します。インターネット上で、これらのテクノロジーに関する詳細情報を得ることができます。 は、次の接続間で交換されるデータを暗号化します。

- Web サーバーと Web クライアント間
- CLI クライアントと CLI シェル インターフェイス間（SSH で処理）
- 、AAA のようなシステム、および外部ストレージ間

Web サーバーと Web クライアント間の通信を保護するには、HTTPS メカニズムの一部として組み込まれる公開キー暗号化サービスを使用します。そのためには、Web サーバーの公開キーを生成し、それをサーバーに保存して、Web クライアントと共有する必要があります。これは、標準 PKI 証明書のメカニズムを使用して実現できます。このメカニズムを使用することによって、Web サーバーの公開キーを Web クライアントと共有するだけでなく、アクセスする Web サーバー（URL）に公開キーが必ず属することが保証されます。これにより、第三者が

Web サーバーと見せかけて、Web クライアントが Web サーバーに送信する機密情報を収集することを防ぎます。

以下のトピックでは、Web サーバーを保護するために実行できるその他の手順について説明します。

- シスコでは、 Web サーバーは証明書ベースの認証を使用して、Web クライアントを認証するようお勧めします。
- CLI クライアントと CLI インターフェイスの間の接続を保護するには、のセキュリティを強化する手順を参照してください。
- 、AAA などのシステム、および外部ストレージの間の接続を保護するには、の推奨事項を参照してください。

Prime Infrastructure への HTTPS アクセスをセットアップする

Prime Infrastructure では、セキュア HTTPS クライアント アクセスがサポートされます。HTTPS アクセスを使用するには、秘密キーと対応する証明書ファイルを Prime Infrastructure サーバーに適用し、これらの証明書を信頼するようにユーザーが各自のクライアント ブラウザを更新する必要があります。

このためには、次のいずれかの証明書ファイルを使用できます。

- 自己署名。「関連項目」の「自己署名証明書の生成および適用」の手順に従って、自己署名証明書の生成および適用ができます。
- 認証局（CA）によるデジタル署名。CA とは、識別情報を検証して証明書を発行する組織（Cisco や VeriSign など）です。CA が発行した証明書は、証明書に指定されているエンティティ（サービスやデバイスなど）の名前に公開キーをバインドします。関連項目の「CA 署名付きホスト証明書のインポート」の手順に従って、サードパーティ CA から CA 証明書を取得し、Prime Infrastructure サーバーに適用できます。

（注） インストール時に、秘密キー、およびデフォルトのパラメータを持つ自己署名証明書が生成されます。

関連トピック

自己署名証明書の生成および適用 （25 ページ）
CA 署名付きホスト証明書のインポート （26 ページ）
秘密キーのインポート （29 ページ）
秘密キーのエクスポート （29 ページ）

自己署名証明書の生成および適用

Prime Infrastructure を使用して、自己署名証明書を生成および適用します。

ステップ 1 Prime Infrastructure との CLI セッションを開始します（CLI から接続する方法を参照）。「configure terminal」モードにしないでください。

ステップ 2 ドメイン情報を使用して新しいRSA キーと自己署名証明書を作成するには、次のコマンドを入力してください。

PIServer/admin# **ncs key genkey –newdn**

証明書の [識別名（DN）（Distinguished Name (DN)）] フィールドへの入力が求められます。Prime Infrastructure にアクセスするために使用するドメイン名として、サーバーの完全修飾ドメイン名（FQDN）を指定する必要があります。

ステップ 3 証明書を有効にするため、Prime Infrastructure を再起動します（CLI を使用した Prime Infrastructure の再起動を参照）。

ログインの問題を防ぐため、Prime Infrastructure ログイン ページに次回アクセスするときにブラウザの信頼ストアに自己署名証明書を追加するようにユーザーに指示します。

CA 署名付きホスト証明書のインポート

Prime Infrastructure を使用して、証明書署名要求（CSR）ファイルを生成し、検証のために認証局（CA）に送信します。CA に CSR ファイルを送信する方法は、CA によって異なります。

証明書の CSR ファイルを生成して送信した後は、同じ Prime Infrastructure サーバーで再び新しいキーを生成するために **genkey** コマンドを再度使用しないでください。コマンドを再度使用すると、インポートされる CA 署名付き証明書のキーとサーバー上のファイルのキーが一致しなくなります。

署名付きサーバー証明書はホスト固有であることに注意してください。つまり、Prime Infrastructure バックアップで保持されますが、復元されるのはバックアップ サーバーとリストア サーバーのホスト名が同一である場合だけです。

（注） ハイ アベイラビリティ仮想 IP は、サーバー管理の簡素化を目的として設計されています。署名付きサーバー証明書の設定は、Prime Infrastructure の HA 仮想 IP 展開では機能しません。

ステップ 1 「管理」クレデンシャルを使用して Prime Infrastructure との CLI セッションを開始し、既存の信頼できる証明書を確認します（「CLI 経由の接続方法」を参照）。「configure terminal」モードにしないでください。

PIServer/admin# **ncs key listcacerts**

ここで、**listcacerts** は既存の信頼できる証明書をリストするコマンドです。

ステップ 2 PI サーバーの場所（**/opt/CSCOncs/migrate/restore**）に移動し、「ルート」CLI クレデンシャルを使用してインポートされた証明書を確認します。

ステップ 3 証明書が見つかったら、「管理」CLI クレデンシャルを使用して証明書を削除します（「CA 署名付き証明書の削除」を参照）。証明書が見つからなければ、ステップ 4 に進みます。

PIServer/admin# pi/admin# **ncs key deletecacert** <*certificate name*>

証明書を削除した後、Prime Infrastructure サーバーを再起動します。

ステップ 4 以下のコマンドを入力して、デフォルトのバックアップ リポジトリに CSR ファイルを生成します。

PIServer/admin# **ncs key genkey -newdn -csr <csrfilename> repository <repositoryname>**

-newdn：ドメイン情報を使用して新しい RSA キーと自己署名証明書を生成します。

-csr：新しい CSR 証明書を生成します。

Csrfilename：CSR ファイル名。これは任意の名前です（例：MyCertificate.csr）。

repositoryname：ファイルの場所。ファイルの名前には、最大 80 文字の英数字を使用できます。

例：

PIServer/admin# ncs key genkey -newdn -csr CSRFile.csr repository <*repositoryname*>

The NCS server is running. Changes will take effect on the next server restart

サーバーの完全修飾ドメイン名を入力します：**<FQDN>**

組織単位の名前を入力します：**<organization>**

組織の名前を入力します：**<organization>**

市区町村の名前を入力します：**<city>**

都道府県の名前を入力します：**<state>**

2 文字の国コードを入力します：**<country code>**

サブジェクト代替名を指定します。

指定しない場合は、CN が使用されます。

カンマ区切りのリストを使用します（DNS:<name>,IP:）<address>

DNS:<FQDN>,IP:<IPADDRESS>

公開キー アルゴリズム [rsa/ec] を指定します：**rsa**

RSA キー サイズ [2048/4096/8192] を指定します：**4096**

署名アルゴリズム [sha256/sha512] を指定します：**sha256**

キーと CSR/証明書が以下の詳細で生成されます。

サブジェクト：/C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=DNS:<FQDN>

サブジェクト代替名：DNS:<FQDN>,IP:<IPADDRESS>

公開キー アルゴリズム：4096

署名アルゴリズム：sha256

続行 [yes]：yes

生成しています。

完了しました。変更は次回のサーバーの再起動時に反映されます。

（注） 「サブジェクト代替名」を指定しない場合、このマシンにのみ CA 証明書をインポートできます。

「サブジェクト代替名」を指定した場合、CA から受け取った CA 証明書を、指定の FQDN を持つ任意のサーバーにインポートできます。SAN 指定のサーバーに CA 証明書をインポートするには、CSR を生成したサーバーから秘密キーをエクスポートし、その秘密キーを署名付き証明書とともに他の指定サーバーにインポートする必要があります。

SAN リストに、現在のサーバーの FQDN を追加する必要があります。

ステップ 5 任意の認証局（CA）に CSR ファイルを送信します。

CA は、署名付きサーバー証明書と 1 つ以上の CA 証明書ファイルを送信することで応答します。CA の応答は、ファイルが次のいずれであるかを示します。

- 署名付きサーバー証明書。通常、証明書の適用対象サーバーのホスト名がそのファイル名に反映されています。
- CA 証明書。通常は CA の名前を反映したファイル名が付いています。

すべての証明書を連結して 1 つのファイルにまとめます。ファイルの先頭がホスト証明書で、その後にチェーンと同じ順序で CA 証明書を配置する必要があります。

たとえば Linux の場合、次のコマンドを使用してファイルを結合できます。

cat host.pem subca.pem rootca.pem > servercert.pem

（注） 証明書は PEM 形式である必要があります。

ステップ 6 次のコマンドを入力して、Prime Infrastructure サーバーに署名付きサーバー証明書ファイルをインポートします。

PIServer/admin# **ncs key importcacert tomcat** <*certificate_name*> **repository** <*repositoryname*>

ステップ 7 次のコマンドを入力して、Prime Infrastructure サーバーに署名付き証明書ファイルをインポートします。

PIServer/admin# **ncs key importsignedcert <certificate_name> repository <repositoryname>**

ステップ 8 CA 署名付き証明書を有効にするために、Prime Infrastructure を再起動します（「Prime Infrastructure の再起動」を参照）。

証明書に署名した CA が組織内で信頼される CA ではない場合は、ユーザーに対し、Prime Infrastructure ログイン ページに次回アクセスするときに、CA 署名付き証明書を各自のブラウザの信頼ストアに追加するように指示してください。

（注） CA 証明書をインポートして、PI と外部デバイス/サーバーの間にセキュアな接続を確立するには、以下のコマンドを使用します。

PIServer/admin# **ncs key importcacert truststore {system | devicemgmt}alias <alias_name> <CA_certifcate_name> repository <repository_name>**

詳細については、CLI から接続する方法およびCLI を使用した Prime Infrastructure の再起動を参照してください。

秘密キーのインポート

秘密キーと署名付き証明書を外部で生成できます。外部で生成する場合は、次のコマンドを使用してキーと証明書の両方をインポートできます。

ncs key importkey <private_key_filename> <certificate_filename> repository <repository_name>

秘密キーのエクスポート

秘密キーをエクスポートするコマンドを次に示します。

ncs key exportkey <private_key_filename> <certificate_filename> repository <repository_name>

上記のコマンドを実行すると、秘密キーが生成され、リポジトリの指定されたファイルの場所に配置されます。

証明書の検証設定

TLS/HTTPS 接続のようなセキュアなトランザクション時のユーザー認証（証明書ベースの認証が有効になっている場合）では、Prime Infrastructure は外部エンティティから証明書を受信します。Prime Infrastructure はこれらの証明書を検証して証明書の整合性と証明書の所有者のアイデンティティを確認する必要があります。証明書の検証機能により、ユーザーは他のエンティティから受信した証明書を検証する方法を制御できます。

証明書の検証が適用されると、他のエンティティから受信した証明書は、その証明書が Prime Infrastructure によって信頼されている認証局（CA）が署名している場合にのみ、Prime Infrastructure によって受け入れられます。信頼ストアは、ユーザーが信頼できる CA 証明書を維持できる場所です。署名付き証明書チェーンが信頼ストア内のいずれかの CA 証明書がルートでない場合、検証は失敗します。

信頼ストアの管理

ユーザーは信頼ストア内の信頼できる CA を管理できます。Prime Infrastructure は、さまざまな信頼ストア、つまり、pubnet、system、devicemgmt、および user を提供します。

- pubnet：パブリックネットワーク内のサーバーに接続したときにリモートホストから受信した証明書の検証中に使用されます。
- system：ネットワーク内のシステムに接続したときにリモートシステムから受信した証明書の検証中に使用されます。
- devicemgmt：管理対象デバイスから受信した証明書の検証中に使用されます。
- user：ユーザー証明書の検証に使用されます（証明書ベースの認証が有効になっている場合）。

信頼ストアを管理する *CLI*

次に、信頼ストアを管理するために使用される CLI を示します。

- 信頼ストアへの CA 証明書のインポート （30 ページ）
- 信頼ストアでの CA 証明書の表示 （30 ページ）
- 信頼ストアからの CA 証明書の削除 （30 ページ）

信頼ストアへの CA 証明書のインポート

次に、信頼ストアに CA 証明書をインポートするコマンドを示します。

- ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository <Repository-name> <certificate-file> truststore {devicemgmt | pubnet | system | user}

信頼ストアでの CA 証明書の表示

次に、信頼ストアで CA 証明書を表示するコマンドを示します。

- ncs certvalidation trusted-ca-store listcacerts truststore {devicemgmt | pubnet | system | user}

信頼ストアからの CA 証明書の削除

次に、信頼ストアから CA 証明書を削除するコマンドを示します。

- ncs certvalidation trusted-ca-store deletecacert alias <ALIAS> truststore {devicemgmt | pubnet | system | user}

証明書の検証の設定

ユーザーは、次のカテゴリに対して証明書の検証を設定できます。

- 証明書の検証の有効化
- 証明書の検証の無効化
- TOFU（ゼロトラスト）：信頼ストアは使用されず、リモートホストから受信した証明書が接続が最初に確立された時点で信頼されます。リモートホストが後続の任意の接続に対して別の証明書を送信すると、接続は拒否されます。

証明書の検証の有効化

次に、証明書の検証を有効にするコマンドを示します。

- ncs certvalidation certificate-check trust-on-first-use trustzone {devicemgmt | pubnet | system | user}

証明書検証リストの表示

次に、証明書検証リストを表示するコマンドを示します。

- ncs certvalidation tofu-certs listcerts

証明書の検証の削除

次に、証明書の検証を削除するコマンドを示します。

- ncs certvalidation tofu-certs deletecert host <host>

CA リストの自動更新

シスコは、シスコが推奨する CA 証明書の標準セットを随時リリースしています。これらの信頼ストアは、ソフトウェアアップデート時にシスコの信頼できる CA バンドルを使用して CA リストを更新するように自動的に設定できます。

次に、CA リストの自動更新を設定するコマンドを示します。

- ncs certvalidation trusted-ca-store auto-ca-update enable truststore {devicemgmt | pubnet | system | user}

[Certificate Validation] ページへのアクセス

証明書は、UI で利用可能な [Certificate Validation] ページから生成可能になったため、管理 CLI コマンドを使用せずに CSR を直接生成して、インポートまたはエクスポートできます。

[Certificate Validation] ページにアクセスするには、次のメニューに移動します。

[Administration] > [Settings] > [Certificate] メニューには、Cisco Prime Infrastructure で証明書を作成、インポート、およびエクスポートするためのオプションがあります。

信頼できる CA と設定：

インポートされた証明書とカテゴリがここにリストされます。

- [System]：システムレベルで PI と他のサーバーとの間で発生する通信を有効にできます。
- [Pubnet]：pubnet レベルで PI と他のサーバーとの間で発生する通信を有効にできます。
- [Device management]：PI と他のサーバー間のデバイス管理通信を有効にできます。
- [User]：PI と他のサーバー間のユーザー通信を有効にできます。

[Certificate Validation]：証明書をインポートまたはエクスポートするときに使用される検証の詳細を選択できます。

ピン留めされた *TOFU* 証明書

PI サーバーと通信する他のサーバーの全 TOFU 証明書が一覧表示されます。

カスタム OCSP レスポンダ

発行日や有効期限などの検証の詳細が提供されます。

MIB と Prime Infrastructure アラート/イベントのマッピング

次の表に、CISCO_WIRELESS_NOTIFICATION_MIB フィールドおよび OID から Prime Infrastructure アラート/イベントへのマッピングの要約を示します。

表 *2 : CISCO_WIRELESS_NOTIFICATION_MIB* から *Prime Infrastructure* アラート/イベントへのマッピング

フィールド名およびオブジェクト ID	データ タイプ	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationTimestamp	DateAndTime	createTime：NmsAlert eventTime：NmsEvent	アラーム/イベントの作成時刻。
cWNotificationUpdatedTimestamp	DateAndTime	modTime：NmsAlert	アラームの修正時刻。 イベントには修正時刻がありません。
cWNotificationKey	SnmpAdminString	objectId：NmsEvent entityString：NmsAlert	文字列形式の一意のアラーム/イベント ID。

フィールド名およびオブジェクト ID	データ タイプ	Prime Infrastructure イベント/アラート フィールド	説明
cwNotificationCategory	CWirelessNotificationCategory	該当なし	イベント/アラームのカテゴリ。値は次のとおりです。 unknown accessPoints adhocRogue clients controllers coverageHole interference contextAwareNotifications meshLinks mobilityService performance rogueAP rrm security wcs switch ncs
cWNotificationSubCategory	OCTET STRING	アラートの Type フィールドおよびイベントの eventType。	このオブジェクトはアラートのサブカテゴリを表します。
cWNotificationServerAddress	InetAddress	該当なし	Prime Infrastructure の IP アドレス。

フィールド名およびオブジェクト ID	データ タイプ	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationManagedObjectAddressType	InetAddressType	該当なし	管理対象オブジェクトに到達可能なインターネットアドレスの種類。有効値： 0：不明 1：IPv4 2：IPv6 3：IPv4z 4：IPv6z 16：DNS Prime Infrastructure は IPv4 アドレスのみをサポートしているため、常に「1」に設定されます。
cWNotificationManagedObjectAddress	InetAddress	getNode() 値を使用（存在する場合）	getNode はイベントおよび一部のアラートに対して設定されます。ヌルでない場合は、このフィールドに使用されます。
cWNotificationSourceDisplayName	オクテット文字列	アラート/イベントの sourceDisplayName フィールド。	このオブジェクトは、通知の送信元の表示名を表します。
cWNotificationDescription	OCTET STRING	Text：NmsEvent Message：NmsAlert	アラームの説明を示す文字列。
cWNotificationSeverity	INTEGER	severity：NmsEvent、NmsAlert	アラート/イベントのシビラティ（重大度）は以下のとおりです。 cleared(1) critical(3) major(4) minor(5) warning(6) info(7)

フィールド名およびオブジェクト ID	データ タイプ	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationSpecialAttributes	OCTET STRING	基本アラート/イベント クラス以外のすべてのアラート/イベントの属性。	このオブジェクトは、アラート専用の属性（APAssociated、APDisassociated、RogueAPAlert、CoverageHoleAlert など）を表します。文字列は CSV 形式で「プロパティ=値」のペアで表されます。
cWNotificationVirtualDomains	OCTET STRING	該当なし	アラームを発生させたオブジェクトの仮想ドメイン。現行リリースの場合、このフィールドは空です。

サーバーとの SSH セッションの確立

サーバーに接続するときには、admin ユーザーとして SSH を使用してログインします。（詳細については、ユーザー インターフェイス、ユーザー タイプ、およびそれらの間の遷移を参照してください）。

ステップ 1 SSH セッションを開き、 admin ユーザーとしてログインします。

- コマンド ラインから次のように入力します。*server-ip* は です。

```
ssh admin server-ip
```

- SSH クライアントを開き、**admin** としてログインします。

（注） ユーザーは、SSH または PuTTY に接続する新しいアルゴリズムを作成してカスタマイズできるようになりました。

ステップ 2 admin パスワードを入力します。プロンプトが次のように変化します。

```
(admin)
```

管理ユーザーが実行できる操作のリストを表示するには、プロンプトで **?** と入力します。

admin コンフィギュレーション モードを開始するには、次のコマンドを入力します（プロンプトの変化に注意してください）。

```
(admin) configure terminal
(config)
```

サーバーでの NTP の設定

Network Time Protocol（NTP）は、ネットワーク内のすべてのデバイスと サーバーで正しく同期される必要があります。ネットワーク全体の NTP 同期の管理で障害が発生した場合、 で異常な結果が発生する可能性があります。これには、 バックアップに使用する任意のリモート FTP サーバー、セカンダリ 高可用性サーバーなど、すべての 関連サーバーが含まれます。

サーバーのインストール時にデフォルトおよびセカンダリの NTP サーバーを指定します。また、 の **ntp server** コマンドを使用して、インストール後に NTP サーバーのリストを追加または変更することもできます。

（注） は NTP サーバーとして設定できません。NTP クライアントとしてだけ機能します。最大で 3 台までの NTP サーバーが使用できます。

ステップ 1 サーバーに管理者ユーザーとしてログインし、コンフィギュレーションモードを開始します。サーバーとの SSH セッションの確立 （35 ページ）を参照してください。

ステップ 2 次の方法のいずれかのコマンドを使用して、NTP サーバーを設定します。

認証されていない NTP サーバーのセットアップの場合：

ntp server *ntp-server-IP*

認証済み NTP サーバーのセットアップの場合：

ntp server *ntp-server-IP ntp-key-id ntp-type password*

ここで、

- *ntp server IP* は、 サーバーにクロック同期を提供するサーバーの IP アドレスまたはホスト名です
- *ntp-key-id* は、認証済み NTP サーバーの MD5 キー ID MD5 キーです。
- *ntp-type* は、プレーンまたはハッシュのいずれかにすることができます。
- *password* は NTPv4 サーバーの MD5 プレーン テキスト パスワードです。

プロキシ サーバーの設定

サーバーのプロキシと、そのローカル認証サーバー（設定されている場合）のプロキシを設定するには、次の手順に従います。ネットワークとインターネットの間のセキュリティ バリアとしてプロキシ サーバーを使用する場合、次の手順に従ってプロキシを設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [プロキシ（Proxy）] タブをクリックします。

ステップ 3 [プロキシの有効化（Enable Proxy）] チェックボックスをオンにし、Cisco.com に接続してプロキシとして機能するサーバーに関する必須情報を入力します。

ステップ 4 [認証プロキシ（Authentication Proxy）] チェックボックスをオンにし、プロキシ サーバーのユーザー名とパスワードを入力します。

ステップ 5 [接続のテスト（Test Connectivity）] をクリックして、プロキシ サーバーに接続できることを確認します。

ステップ 6 [Save] をクリックします。

サーバー ポートおよびグローバル タイムアウトの設定

[サーバー（Server）] ページでは、Prime Infrastructure の FTP、TFT、HTTP/HTTPS の各サービスの有効化または無効化ができます。

通常、FTP および TFTP サービスはデフォルトで有効です。HTTP サービスはデフォルトで無効になっています。プラグ アンド プレイ機能を使用し、デバイスが HTTP を使用してブートストラップ設定の初期設定を取得するように設定されている場合は、HTTP サービスを有効にする必要があります。

詳細については、最新の『Prime Infrastructure Quick Start Guide』を参照してください。

ステップ 1 [管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[一般（General）]>[サーバー（Server）] の順に選択します。

ステップ 2 インストール時に確立された FTP、TFTP、または HTTP サービスのステータスとポートを変更するには、変更するポート番号（または必要に応じてポート番号およびルート）を入力し、[有効（Enable）] または [無効（Disable）] をクリックします。

[グローバル アイドル タイムアウト（Global Idle Timeout）] はデフォルトで有効になっており、10 分に設定されています。[グローバル アイドル タイムアウト（Global Idle Timeout）] 設定は、[自分の環境設定（My Preferences）] ページの [ユーザー アイドル タイムアウト（User Idle Timeout）] 設定より優先されます。管理者権限を持つユーザーのみが [グローバル アイドル タイムアウト（Global Idle Timeout）] の値を無効化したり、そのタイムリミットを変更できます。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 変更を適用するにはサーバーを再起動する必要があります（CLI を使用した Prime Infrastructure の再起動を参照）。

SMTP 電子メール サーバーの設定

で（アラーム、ジョブ、レポートなどの）電子メール通知の送信を可能にするには、システム管理者はプライマリ SMTP 電子メールサーバーを（また、できればセカンダリ電子メール サーバーも）設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、次に **[メールと通知（Mail and Notification）] > [メール サーバー設定（Mail Server Configuration）]** を選択します。

ステップ 2 [プライマリ SMTP サーバー（Primary SMTP Server）] で、 が使用する電子メール サーバーに合わせて、[ホスト名/IP（Hostname/IP）]、[ユーザー名（User Name）]、[パスワード（Password）]、および [パスワードの確認（Confirm Password）] フィールドに入力します。物理サーバーの IP アドレスを入力し、プライマリ SMTP サーバーのホスト名を入力します。

（注） 仮想 IP アドレスを [ホスト名/IP（Hostname/IP）] フィールドに入力することはできません。また、IP アドレスをロード バランサの後に配置することはできません。

ステップ 3 （オプション）[セカンダリ SMTP サーバー（Secondary SMTP Server）] で同じ各フィールドに入力します。SMTP サーバーのユーザー名とパスワード。

ステップ 4 [送信者および受信者（Sender and Receivers）] で、 の正当なメール アドレスを入力します。

ステップ 5 完了したら、[保存（Save）] をクリックします。

サーバーでの FTP/TFTP/SFTP サービスの有効化

FTP/TFTP/SFTP は、デバイス設定およびソフトウェアイメージファイルの管理のために、サーバーとデバイスの間でファイルを転送する目的で使用されます。また、これらのプロトコルは、高可用性導入環境において、セカンダリ サーバーにファイルを転送するためにも使用されます。これらのサービスは、通常はデフォルトで有効になっています。FIPS モードで をインストールした場合、これらはデフォルトで無効になります。このページを使用してこれらのサービスを有効にすると、 は FIPS に準拠しなくなります。

SFTP は、セキュリティで保護されたバージョンのファイル転送サービスです。デフォルトでこれが使用されます。FTP は、セキュリティで保護されていないファイル転送サービス バージョンです。TFTP は、セキュリティで保護されていない、単純なサービス バージョンです。FTP または TFTP のいずれかを使用するには、サーバーの追加後にサービスを有効化する必要があります。

ステップ 1 FTP、TFTP、または SFTP サーバーを使用するように を設定します。

a) **[管理（Administration）] > [サーバー（Servers）] > [TFTP/FTP/SFTP サーバー（TFTP/FTP/SFTP Servers）]** を選択します。

b) [コマンドの選択（Select a command）] ドロップダウン リストから、[TFTP/FTP/SFTP サーバーの追加（Add TFTP/FTP/SFTP Server）] を選択し、[移動（Go）] をクリックします。

- **[サーバータイプ（Server Type）]** ドロップダウンリストから、**[FTP]**、**[TFTP]**、**[SFTP]**、または **[すべて（All）]** を選択します。
- サーバーのユーザー定義名を入力します。
- サーバーの IP アドレスを入力します。

c) [保存（Save）] をクリックします。

ステップ 2 FTP または TFTP を使用する場合には、 サーバーでそれを有効化します。

a) **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバー（Server）]** を選択します。

b) [FTP] または [TFTP] エリアに移動します。

c) [有効（Enable）] をクリックします。

d) **[保存（Save）]** をクリックします。

ステップ 3 を再起動し、変更を適用します。 の停止と再起動 （40 ページ）を参照してください。

保存されている Cisco.com クレデンシャルの設定

では、次のタスクの実行時に Cisco.com にログインするためのユーザー名のみが保存され、パスワードは保存されません。

- 製品ソフトウェア アップデートの有無の確認
- デバイス ソフトウェア イメージ アップデートの有無の確認

アップデートをダウンロードし、サポート ケースを開いたり確認したりするには、パスワードを入力する必要があります。

これらが設定されていない場合、ではユーザーがこれらのタスクを行うと、ユーザーに対してクレデンシャルの入力を求めます。グローバル Cisco.com ユーザー名とパスワードを設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [Cisco.com クレデンシャル（Cisco.com Credentials）] タブでユーザー名とパスワードを入力し、[保存（Save）] をクリックします。

ログイン バナー（ログインの免責事項）の作成

すべてのユーザーに対してログイン前に表示するメッセージがある場合は、ログインの免責事項を作成します。テキストは GUI クライアント ログイン ページのログイン フィールドとパスワード フィールドの下に表示されます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [ログインの免責事項（Login Disclaimer）]** を選択します。

ステップ 2 ログインの免責事項テキストを入力（または編集）します。

（注） 改行文字は無視されます。

変更はすぐに反映されます。

の停止と再起動

製品ソフトウェアのアップグレード、ログファイルの設定変更、セキュアポート設定のハンギング、レポートファイルの圧縮、サービス検出設定の変更、LDAP 設定の構成の後などに、再起動が必要です。 サーバーを停止すると、すべてのユーザー セッションが終了します。

サーバーを停止するには、サーバーとの CLI セッションを開いて、以下を入力します。

```
ncs stop
```

サーバーを再起動するには、サーバーとの CLI セッションを開いて、以下を入力します。

```
ncs start
```

ネットワーク要素との通信に適用するグローバル SNMP の設定

[SNMP の設定（SNMP Settings）] ページは、サーバーが SNMP を使用してデバイスにアクセスおよびモニターする方法を制御します。これらの設定によって、デバイスが到達不能であると判断される条件が決まります。このページで行う変更はグローバルに適用され、再起動されても、バックアップと復旧が行われても保存された状態に維持されます。

（注） デフォルトのネットワーク アドレスは0.0.0.0です。これは、ネットワーク全体を意味します。SNMPクレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。0.0.0.0はSNMPクレデンシャルのデフォルトであり、SNMPクレデンシャルが定義されていないときに使用されます。事前に設定されたSNMPクレデンシャルを独自のSNMP情報で更新する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[ネットワークとデバイス（Network and Device）] > [SNMP]** を選択します。

ステップ 2 （任意）SNMPを使用して取得されたメディエーショントレース レベル ログのデータ値を表示するには、[トレース表示値（Trace Display Values）] チェックボックスをオンにします。

ステップ 3 [バックオフ アルゴリズム（Backoff Algorithm）] ドロップダウン リストからアルゴリズムを選択します。

- [指数（Exponential）]：SNMP の初回試行時には指定したタイムアウト値が使用され、2 回目からは、前回の試行時の 2 倍の待機時間が適用されます。
- [一定（Constant）]：SNMP の試行時に、毎回同じ待機時間（タイムアウト）が適用されます。このオプションは、必要な再試行回数が多い、不安定なネットワークで役立ちます。再試行のたびにタイムアウト時間が倍加しないので、再試行回数が増えた場合でもそれほど時間がかかりません。

ステップ 4 デバイスで指定されているタイムアウトと再試行を使用しない場合は、次のパラメータを設定します。

（注） スイッチ ポート トレースが完了するまでに長い時間がかかる場合は、[到達可能性再試行回数（Reachability Retries）] の値を小さくします。

- [到達可能性再試行回数（Reachability Retries）]：グローバルに適用する再試行回数を入力します。
- [到達可能性タイムアウト（Reachability Timeout）]：グローバルに適用するタイムアウト値を入力します。

ステップ 5 [PDU取得ごとの最大変数バインド（Maximum VarBinds per Get PDU）] フィールドおよび [PDU設定ごとの最大変数バインド（Maximum VarBinds per Set PDU）] フィールドに、要求 PDU または応答 PDU で使用する SNMP 変数バインドの最大数を入力します。これらのフィールドを使用することで、SNMP に関連した障害が発生したときに、必要な変更を加えることができます。ネットワークでのPDUフラグメンテーションに問題がある場合は、この数を 50 に減らすと、通常はフラグメンテーションが解消されます。

ステップ 6 必要に応じて [テーブルごとの最大行数（Maximum Rows per Table）] の値を調整します。

ステップ 7 [Save] をクリックします。

グローバル SNMP の設定

[SNMP の設定（SNMP Settings）] ページでは、グローバル SNMP 設定を Prime Infrastructure 用に構成することができます。

このページで行った変更は Prime Infrastructure 全体に影響します。変更は、再起動をまたがって有効であり、バックアップと復元をまたがって有効です。

デフォルトのネットワーク アドレスは 0.0.0.0 です。これは、ネットワーク全体を意味します。SNMP クレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。0.0.0.0 は SNMP クレデンシャルのデフォルトであり、SNMP クレデンシャルが定義されていないときに使用されます。事前に設定された SNMP クレデンシャルを独自の SNMP 情報で更新する必要があります。

ステップ 1 [Administration] > [Settings]> [System Settings] > [Network and Device] > [SNMP] の順に選択します。

ステップ 2 （オプション）SNMP を使用しているコントローラから取得したメディエーション トレース レベル ログのデータ値を表示するには、[Trace Display Values] チェック ボックスをオンにします。オフにした場合は、これらの値は表示されません。

ステップ 3 [Backoff Algorithm] から、[Exponential] または [Constant Timeout] を選択します。[指数（Exponential）] を選択した場合、SNMP の初回試行時には指定したタイムアウト値が使用され、2 回目からは、前回の試行時の 2 倍の待機時間が適用されます。[Constant Timeout] を選択した場合は、すべての SNMP 試行に対して同じ待機時間（指定したタイムアウト値）が適用されます。

ネットワークの信頼性が低く、再試行回数が多くなる可能性がある場合（衛星ネットワークなど）は、通常 [Constant Timeout] を使用します。再試行のたびにタイムアウト時間が倍加しないので、再試行回数が増えた場合でもそれほど時間がかかりません。

ステップ 4 到達可能性に関するパラメータを使用するかどうかを決定します。オンにした場合は、Prime Infrastructure がデフォルトで、構成されたグローバルな [到達可能性の再試行回数（Reachability Retries）] および [到達可能性のタイムアウト（Reachability Timeout）] に設定されます。オフにした場合は、Prime Infrastructure ではコントローラごと、または IOS アクセス ポイントごとに指定したタイムアウトと再試行が常に使用されます。

スイッチ ポート トレーシングの完了まで長時間かかる場合は、この設定を調整して小さくしてください。

ステップ 5 [到達可能性の再試行回数（Reachability Retries）] に、デバイスの到達可能性を判別するためのグローバルな再試行回数を入力します。このフィールドは、[到達可能性パラメータの使用（Use Reachability Parameters）] チェック ボックスをオンにした場合だけ使用できます。

スイッチ ポート トレーシングの完了まで長時間かかる場合は、この設定を調整して小さくしてください。

（注） [到達可能性のタイムアウト（Reachability Timeout）] の値は編集できません。デフォルト値は 2 秒です。

ステップ 6 [PDU あたりの最大変数バインド数（Maximum VarBinds per PDU）] フィールドに、要求 PDU または応答 PDU で使用する SNMP 変数バインドの最大数を入力します。

この [Maximum VarBinds per PDU] フィールドを使用することで、関連した障害が発生したときに、必要な SNMP の変更を実施できます。

ネットワークでの PDU フラグメンテーションに問題がある場合は、この数を 50 に減らすとフラグメンテーションが解消されます。

テーブルのフィールドごとの最大行数を設定できます。設定した値は、Prime Infrastructure を新しいバージョンにアップグレードしても保持されます。

ステップ 7 [保存（Save）] をクリックして、これらの設定を保存します。

関連トピック

SNMP クレデンシャルの詳細表示 （43 ページ）
SNMP クレデンシャルの追加 （44 ページ）
SNMP クレデンシャルのインポート （45 ページ）

SNMP クレデンシャルの詳細表示

このページに表示される SNMP クレデンシャルは、不正 AP スイッチ ポート トレースにのみ使用されます。

ステップ 1 [Administration] > [Settings]> [System Settings] > [Network and Device] > [Switch Port Trace (SPT)] > [Manual SPT] の順に選択します。

ステップ 2 [Network Address] リンクをクリックすると、[SNMP Credential Details] ページが表示されます。このページには、次の情報が表示されます。

- General Parameters
  - [フォーマット タイプの追加（Add Format Type）]：表示のみ。詳細については、「関連項目」の「SNMP クレデンシャルの追加」を参照してください。
  - ネットワーク アドレス（Network Address）
  - Network Mask
- [SNMP Parameters]：SNMP パラメータの該当するバージョンを選択します。SNMP クレデンシャルは、選択されている SNMP バージョンに応じて検証されます。
- 書き込みアクセスに対応する SNMP パラメータ（存在する場合）を入力します。表示専用のアクセス パラメータでは、スイッチが追加されますが、その設定を Prime Infrastructure では変更できません。デバイス接続テストでは、SNMP 再試行およびタイムアウト パラメータが使用されます。
- [再試行（Retries）]：スイッチの検出を試行する回数。
- [Timeout]：セッション タイムアウト値（秒数）。これは、クライアントに再認証を強制するまでの最大許容時間を指定します。
- [SNMP v1 Parameters or v2 Parameters]：選択した場合は、入力可能なテキスト ボックスに該当するコミュニティを入力します。
- [SNMP v3 Parameters]：選択した場合は、次のパラメータを設定します。
  - ユーザ名
  - Auth. タイプ
  - Auth. パスワード
  - Privacy タイプ

- プライバシー パスワード（Privacy Password）

デフォルト コミュニティの SNMP v1 または v2 が設定されている場合、デフォルト コミュニティはよく知られているため、ネットワークが攻撃しやすくなります。デフォルトでないコミュニティの SNMP v1 または v2 はデフォルト コミュニティよりも安全性が高くなりますが、Auth および Privacy タイプを使用する、デフォルト ユーザーなしの SNMP v3 が最も安全な SNMP 接続です。

ステップ 3 [OK] をクリックして変更を保存します。

関連トピック

グローバル SNMP の設定 （41 ページ）
SNMP クレデンシャルの追加 （44 ページ）
SNMP クレデンシャルのインポート （45 ページ）

SNMP クレデンシャルの追加

Prime Infrastructure がネットワーク デバイスのポーリングやそれらの構成のバックアップおよび変更を実行するには、デバイスの SNMP クレデンシャルが必要です。SNMP クレデンシャルは手動で追加できます。また、それらを一括してインポートすることもできます（詳細については、「関連項目」の「SNMP クレデンシャルのインポート」を参照）。

ステップ 1 [管理（Administration）] > [設定（Settings）]> [システム設定（System Settings）] > [ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）] の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] > [SNMP エントリの追加（Add SNMP Entries）] > [実行（Go）] の順に選択します。

ステップ 3 [フォーマット タイプの追加（Add Format Type）] ドロップダウン リストで、[SNMP クレデンシャル情報（SNMP Credential Info）] を選択します。

ステップ 4 追加するスイッチの IP アドレスを入力します。複数のスイッチを追加する場合は、各 IP アドレスの間にカンマを使用します。

ステップ 5 [再試行（Retries）] フィールドに、スイッチの検出を試行する回数を入力します。

ステップ 6 セッション タイムアウト値を秒単位で入力します。この値により、クライアントの再認証が強制されるまでの最大時間が決定されます。

ステップ 7 SNMP パラメータの該当するバージョンを選択します。SNMP クレデンシャルは、選択されている SNMP バージョンに応じて検証されます。

- [SNMP v1 Parameters or v2 Parameters] が選択されている場合は、入力可能なテキスト ボックスに該当するコミュニティを入力します。
- [SNMP v3 Parameters] が選択されている場合は、次のパラメータを設定します。
- ユーザ名
- Auth. タイプ
- Auth. パスワード

- Privacy タイプ
- プライバシー パスワード（Privacy Password）

デフォルト コミュニティの SNMP v1 または v2 が設定されている場合、デフォルト コミュニティはよく知られているため、ネットワークが攻撃しやすくなります。デフォルトでないコミュニティの SNMP v1 または v2 はデフォルト コミュニティよりも安全性が高くなりますが、Auth および Privacy タイプを使用する、デフォルト ユーザーなしの SNMP v3 が最も安全な SNMP 接続です。

ステップ 8 [OK] をクリックします。

リストされている SNMP クレデンシャルを使用して Prime Infrastructure がスイッチにアクセスできる場合は、今後使用できるようにスイッチが追加され、[ネットワーク デバイス（Network Devices）] ページに表示されます。このページは、[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] からアクセスできます。[ネットワーク デバイス（Network Devices）] ページから手動でスイッチを追加する場合、スイッチ ポートのトレースではこのページのクレデンシャルが使用され、[SNMP クレデンシャル（SNMP Credentials）] ページにリストされているクレデンシャルは使用されません。手動で追加したスイッチ クレデンシャルが変更されている場合は、[ネットワーク デバイス（Network Devices）] ページを使用してこれらのクレデンシャルを更新する必要があります。

関連トピック

グローバル SNMP の設定 （41 ページ）
SNMP クレデンシャルの詳細表示 （43 ページ）
SNMP クレデンシャルのインポート （45 ページ）

SNMP クレデンシャルのインポート

Prime Infrastructure がネットワーク デバイスのポーリングやそれらの構成のバックアップおよび変更を実行するには、デバイスの SNMP クレデンシャルが必要です。SNMP クレデンシャルは、CSV ファイルからインポートすることで、一括インポートができます。また、それらを手動で追加することもできます（「関連項目」の「SNMP クレデンシャルの追加」を参照）。

CSV ファイルが適切なフォーマットで作成されており、Prime Infrastructure のアクセスに使用するクライアント マシン上のフォルダからアップロード可能であることを確認してください。以下に、インポート用の SNMP クレデンシャル CSV ファイル例を示します。

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_password,
snmpv3_privacy_type,snmpv3_privacy_password,network_mask 1.1.1.0,v2,private,user1,HMAC-MD5,
12345,DES,12345,255.255.255.0 2.2.2.0,v2,private,user1,HMAC-MD5,password3,DES,password4,
255.255.255.0 10.77.246.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
```

ファイルの最初の行は、列配置を説明するための必須行です。IP アドレス列も必須です。CSV ファイルには、次のフィールドを含めることができます。

- ip_address：IP アドレス
- snmp_version：SNMP バージョン
- network_mask：ネットワーク マスク
- snmp_community：SNMP V1/V2 コミュニティ

- snmpv3_user_name：SNMP V3 ユーザ名
- snmpv3_auth_type：SNMP V3 認証タイプ。None または HMAC-MD5 または HMAC-SHA を選択できます
- snmpv3_auth_password：SNMP V3 認証パスワード
- snmpv3_privacy_type：SNMP V3 プライバシー タイプ。None または DES または CFB-AES-128 を選択できます
- snmpv3_privacy_password：SNMP V3 プライバシー パスワード
- snmp_retries：SNMP リトライ
- snmp_timeout：SNMP タイムアウト

ステップ 1 [管理（Administration）] > [設定（Settings）]> [システム設定（System Settings）] > [ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）] の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] > [SNMP エントリの追加（Add SNMP Entries）] > [実行（Go）] の順に選択します。

ステップ 3 [フォーマット タイプの追加（Add Format Type）] ドロップダウン リストで、[ファイル（File）] を選択します。

ステップ 4 [参照（Browse）] をクリックして、インポートする CSV ファイルに移動し、それを選択します。

ステップ 5 [OK] をクリックしてファイルをインポートします。

リストされている SNMP クレデンシャルを使用して Prime Infrastructure がスイッチにアクセスできる場合は、今後使用できるようにスイッチが追加され、[ネットワーク デバイス（Network Devices）] ページに表示されます。このページは、[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] からアクセスできます。[ネットワーク デバイス（Network Devices）] ページから手動でスイッチを追加する場合、スイッチ ポートのトレースではこのページのクレデンシャルが使用され、[SNMP クレデンシャル（SNMP Credentials）] ページにリストされているクレデンシャルは使用されません。手動で追加したスイッチ クレデンシャルが変更されている場合は、[ネットワーク デバイス（Network Devices）] ページを使用してこれらのクレデンシャルを更新する必要があります。

関連トピック

グローバル SNMP の設定 （41 ページ）
SNMP クレデンシャルの詳細表示 （43 ページ）
SNMP クレデンシャルの追加 （44 ページ）

コンプライアンス サービスの有効化

コンプライアンス サービスにより、Prime Infrastructure ユーザーが Cisco PSIRT セキュリティ レポートおよび EOX 廃止デバイス コンプライアンス レポートを実行できるようになります。

また、この機能により、ベースラインデバイス設定標準の確立、これらの標準に照らした監査領域の設定、非準拠のデバイスおよびそれらの設定の標準からの逸脱状況の特定もユーザが実施可能になります。

コンプライアンス サービスは、デフォルトで無効化されています。これらを使用するには、Prime Infrastructure 管理者が機能を有効化する必要があります。また、サーバーのデバイス インベントリの再同期も必要になります。また、[設定（Configuration）] > [コンプライアンス（Compliance）] メニュー オプションを表示する場合、すべてのユーザーは、ログアウトした後にログインし直す必要があります。

コンプライアンス サービスは、次の Prime Infrastructure サーバー オプションのみで使用可能です。

- Professional 仮想アプライアンス。詳細については、最新の『Cisco Prime Infrastructure Quick Start Guide』の「Virtual Appliance Options」および「Understanding System Requirements」のセクションを参照してください。
- Cisco Unified Computing System（UCS）Gen 2 物理アプライアンス。詳細については、最新の『Cisco Prime Infrastructure Quick Start Guide』の「Virtual Appliance Options」および「Understand System Requirements」のセクションを参照してください。
- 標準 Prime Infrastructure 仮想アプライアンス詳細については、最新の『Cisco Prime Infrastructure Quick Start Guide』の「Prime Infrastructure Minimum Server Requirements」のセクションを参照してください。

Express、Express-Plus 上でコンプライアンス サービスを有効化しないでください。その場合、機能そのものが動作しません。また、有効化した後、新規にインストールした Professional や Gen 2 UCS アプライアンスにデータを移行すると、元の Express または Express-Plus から移行したデータの設定により、ターゲットのアプライアンス上でコンプライアンス サービスが動作しません。この問題は、Express または Express-Plus 上ではコンプライアンス サービス機能を無効化したままにして、Professional または Gen2 UCS アプライアンスにデータを移行するだけで回避できます。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [サーバー（Server）] の順に選択します。

ステップ 2 [Compliance Services] の横にある [Enable] をクリックします。

ステップ 3 [Save] をクリックします。

ステップ 4 Prime Infrastructure のデバイス インベントリを再同期します。手順としては、[Inventory] > [Network Devices] の順に選択し、[All Devices] を選択した後、[Sync] アイコンをクリックします。

ステップ 5 現在 Prime Infrastructure にログインしているユーザにログアウトするよう求めます。再度ログインすると、[設定（Configuration）] > [コンプライアンス（Compliance）] の新しいメニュー オプションが表示されます。

詳細については、「Virtual Appliance Options」と「Physical Appliance Options」を参照してください。

ISE サーバーの設定

ステップ 1 [管理（Administration）] > [サーバー（Servers）] > [ISE サーバー（ISE Servers）] を選択します。

ステップ 2 [Select a command] > [Add ISE Server] を選択し、[Go] をクリックします。

ステップ 3 ISE サーバの IP アドレス、ユーザ名、およびパスワードを設定します。

ステップ 4 ISE サーバのパスワードを確認入力します。

ステップ 5 [Save] をクリックします。

ソフトウェア イメージ管理サーバーを設定する

イメージの配布のため、最大 3 台のソフトウェア イメージ管理サーバーを追加できます。

ステップ 1 [管理（Administration）] > [サーバー（Servers）] > [ソフトウェア イメージ（Software Image）] をクリックします。

ステップ 2 [追加（Add）] アイコンをクリックし、次のフィールドに値を入力します。

- サーバー名（Server Name）
- [IPアドレス（IP Address）]
- 対象サイト（Sites Served）
- 説明

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [プロトコルの管理（Manage Protocols）] をクリックしてプロトコルを追加します。

ステップ 5 [追加（Add）] アイコンをクリックし、次のフィールドに値を入力します。

- プロトコル
- [ユーザ名（Username）]
- パスワード
- プロトコル ディレクトリ（Protocol Directory）

（注） TFTP プロトコルを選択した場合は、[プロトコル ディレクトリ（Protocol Directory）] フィールドに、先頭にスラッシュを付けずに相対パスを入力します。[プロトコルディレクトリ（Protocol Directory）] フィールドを空にした場合は、イメージ転送で外部サーバーのデフォルトのホームディレクトリが使用されます。

ステップ 6 [Save] をクリックします。

ユーザー定義フィールドにデバイス情報を追加する

ユーザー定義フィールド（UDF）は、デバイスのロケーション属性（たとえば、エリア、施設、フロア）など、デバイスに関する追加情報を格納するために使用されます。新しいデバイスの追加、インポート、またはエクスポートが行われるたびに、UDF 属性が使用されます。

ステップ 1 [Administration] > [System Settings] > [Inventory] > [User Defined Field] の順に選択します。

ステップ 2 UDF を追加するには、[行の追加（Add Row）] をクリックします。

ステップ 3 フィールド ラベルおよび説明を対応するフィールドに入力します。

ステップ 4 [保存（Save）] をクリックして UDF を追加します。

OUI を管理する

Prime Infrastructure では、IEEE 組織固有識別子（OUI）データベースを使用してクライアントベンダー名マッピングが識別されます。Prime Infrastructure では、ベンダー OUI マッピングは、vendorMacs.xml という名前の XML ファイルに保存されます。このファイルは、Prime Infrastructure のリリースごとに更新されます。OUI 更新を使用すると、既存の OUI のベンダー表示名を変更したり、新しい OUI を Prime Infrastructure に追加したり、新しいベンダー OUI マッピングで vendorMacs.xml ファイルを更新し、Prime Infrastructure にアップロードしたりできます。

関連トピック

新しいベンダー OUI マッピングの追加 （49 ページ）
更新されたベンダー OUI マッピング ファイルのアップロード （50 ページ）

新しいベンダー OUI マッピングの追加

[ユーザー定義 OUI リスト（User Defined OUI List）] ページに、作成したベンダー OUI マッピングのリストが表示されます。このページで、新しいベンダー OUI マッピングの追加、OUI エントリの削除、および vendorMacs.xml ファイルに存在する OUI のベンダー名の更新を実行できます。

OUI を追加すると、Prime Infrastructure は vendorMacs.xml ファイルを調べて OUI があるかどうかを確認します。OUI がある場合、Prime Infrastructure は OUI のベンダー名を更新します。OUI がない場合、Prime Infrastructure はベンダー OUI マッピングに新しい OUI エントリを追加します。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [クライアントおよびユーザー（Client and User）] > [ユーザー定義 OUI（User Defined OUI）] の順に選択します。[ユーザー定義 OUI（User Defined OUI）] ページが表示されます。

ステップ 2 [Select a Command] ドロップダウン リストから [Add OUI Entries] を選択し、[Go] をクリックします。

ステップ 3 [OUI] フィールドに有効な OUI を入力します。形式は aa:bb:cc です。

ステップ 4 [Check] をクリックして、OUI がベンダー OUI マッピングに存在するかどうかを確認します。

ステップ 5 [Name] フィールドに、OUI のベンダーの表示名を入力します。

ステップ 6 [ベンダー名の変更（Change Vendor Name）] チェックボックスをオンにしてから [OK] をクリックし、OUI がベンダー OUI マッピングに存在する場合にはベンダーの表示名が更新されるようにします。

更新されたベンダー OUI マッピング ファイルのアップロード

Prime Infrastructure を使用すると、IEEE 登録局データベースからオンラインで OUI アップデートを取得できます（「関連項目」の RA データベースのリンク参照）。Prime Infrastructure が IEEE データベースに到達できない場合、メッセージが表示され、ファイルを保存して Prime Infrastructure サーバーにアップロードするよう指示されます。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [クライアントおよびユーザー（Client and User）] > [OUI のアップロード（Upload OUI）] の順に選択します。[Upload OUI From File] ページが表示されます。

ステップ 2 [IEEE からオンラインでアップロード（Update online from IEEE）] をクリックして、IEEE 登録局データベースから OUI アップデートを取得します（「関連項目」の RA データベースのリンク参照）。Prime Infrastructure が IEEE データベースに到達できない場合、メッセージが表示され、ファイルを保存してアップロードするよう指示されます。

ステップ 3 アップデートが正常に終了したら、[OK] をクリックします。

[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [OUI のアップロード（Upload OUI）] ページで vendorMacs.xml ファイルをアップロードした後、[一意のクライアントとユーザーの概要（Unique Clients and Users Summary）] レポートで既存の不明ベンダー クライアントにベンダー名が反映されていない場合は、*updateUnknownClient.sh* スクリプトを実行します。このスクリプトは、/opt/CSCOlumos/bin フォルダにあります。

詳細については、「IEEE Registration Authority database」を参照してください。

ノースバウンド SNMP レシーバのログ ファイル例

以下の出力例に、Prime Infrastructure によって生成された *ncs_nb.log* ファイルを示します。このログ ファイルは、Prime Infrastructure サーバーのログ ファイル ディレクトリ（/opt/CSCOlumos/logs）にあります。ログ出力は、アラームを North Bound SNMP レシーバで受信していない場合のトラブルシューティングに役立ちます。

```
2013-12-02 17:11:53,868 [main] INFO  services - Queue type is order
2013-12-02 17:11:53,870 [main] INFO  services - Starting the notification thread..
2013-12-02 17:11:53,871 [NBNotifier] INFO  services - Fetching the head of the queue
```

```
2013-12-02 17:11:53,871 [NBNotifier] INFO  services - The Queue is empty
2013-12-02 17:11:53,871 [main] INFO  notification - Setting the NB process flag
2013-12-02 17:41:50,839 [Task Scheduler Worker-10] ERROR notification - Unable to get
OSS list
2013-12-03 08:22:39,227 [main] INFO  services - Queue type is order
2013-12-03 08:22:39,229 [main] INFO  services - Starting the notification thread..
2013-12-03 08:22:39,231 [NBNotifier] INFO  services - Fetching the head of the queue
2013-12-03 08:22:39,231 [NBNotifier] INFO  services - The Queue is empty
2013-12-03 08:22:39,231 [main] INFO  notification - Setting the NB process flag
2013-12-03 08:44:40,287 [main] INFO  services - Queue type is order
2013-12-03 08:44:40,289 [main] INFO  services - Starting the notification thread..
2013-12-03 08:44:40,290 [NBNotifier] INFO  services - Fetching the head of the queue
2013-12-03 08:44:40,290 [NBNotifier] INFO  services - The Queue is empty
2013-12-03 08:44:40,290 [main] INFO  notification - Setting the NB process flag
2013-12-03 08:56:18,864 [Task Scheduler Worker-8] ERROR notification - Unable to get OSS
 list
```

システムの問題を示すサーバー内部 SNMP トラップの使用

は、システム コンポーネントに関する潜在的な問題を示す内部 SNMP トラップを生成します。これには、ハードウェア コンポーネントの障害、ハイ アベイラビリティ状態の変化、バックアップ ステータスなどが含まれます。障害トラップは、障害または状態の変化が検出されるとすぐに生成され、クリアリング トラップは、障害が修正されると生成されます。TCA（CPU、メモリ、ディスクの高い使用率に関するトラップなど）では、しきい値を超えるとトラップが生成されます。

サーバーの内部 SNMP トラップの完全なリストについては、『』に記載されています。 は通知宛先のポート 162 にトラップを送信します。このポートは現時点ではカスタマイズできません。

以下のトピックの説明に従って、これらのトラップをカスタマイズしたり、管理したりできます。

- サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送 （51 ページ）
- サーバー内部 SNMP トラップをトラブルシュートする （52 ページ）

サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送

トラップのシビラティ（重大度）または（TCA の場合）しきい値を調整することで、サーバの内部 SNMP トラップをカスタマイズできます。また、トラップを無効化/有効化することもできます。サーバーの内部 SNMP トラップは、「*Cisco Evolved Programmable Network* でサポートされているアラーム」で確認できます。

（注） は SNMPv2 通知も SNMPv3 通知も送信しません。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[アラームおよびイベント（Alarms and Events）] > [システム イベントの設定（System Event Configuration）]** を選択します。

ステップ 2 設定する各 SNMP イベントに対して、次の手順を実行します。

a) そのイベントの行をクリックします。

b) 必要に応じて、[イベントのシビラティ（重大度）（Event Severity）] を [重大（Critical）]、[メジャー（Major）]、または [マイナー（Minor）] に設定します。

c) CPU、ディスク、およびメモリの使用率や、その他のハードウェアのトラップに対しては、[しきい値値（Threshold）] にパーセンテージ（1 ～ 99）を入力します。これらのイベントは、使用率がしきい値限度を超えたときに、関連の SNMP トラップを送信します。（しきい値設定が NA と表示されるイベントのしきい値は設定できません）。これらのイベントは、関連付けられた障害が検出されるたびにトラップを送信します。

d) バックアップしきい値と証明書の有効期日（重要）に対しては、[しきい値値（Threshold）] に日数（*x* ～ *y*）を入力します。ここで、*x* は最小の日数、*y* は最大の日数です。

e) トラップを生成するかどうかを制御するには、[イベントステータス（Event Status）] を設定します。

ステップ 3 **[その他の設定（Other Settings）]** で、**[アラーム反復の作成とクリア（Create and Clear Alarm Iteration）]** に必要な値を入力します。

ステップ 4 トラップの変更内容を保存するには、（テーブルの下にある）[保存（Save）] をクリックします。

ステップ 5 サーバーの内部 SNMP トラップの受信者を設定するには、情報を電子メールで送信するか、トラップ通知として送信するかに応じて、以下のトピックで説明している手順を参照してください）。

サーバー内部 SNMP トラップをトラブルシュートする

「」では、サーバーの内部 SNMP トラップの完全なリスト、その推定原因、および問題を解決するための推奨処置が提供されています。必要な情報がこのドキュメントに記載されていない場合は、次の手順に従って、サーバーの問題をトラブルシュートし、詳細情報を入手してください。

ステップ 1 サーバーから通知に ping を実行し、 と管理アプリケーション間の接続を確認します。

ステップ 2 ファイアウォールの ACL 設定がポート 162 をブロックしていないかを確認し、必要に応じてそのポートの通信を開きます。

ステップ 3 管理者権限を持つユーザー ID を使用して にログインします。**Administration > Logging** を選択してログ ファイルをダウンロードします。次に、これらのログ ファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

- ncs_nbi.log：これは が送信したすべてのノースバウンド SNMP トラップ メッセージのログです。受信していないメッセージの有無をチェックします。
- ncs-#-#.log：これはその他の最新の アクティビティのログです。受信していないハードウェア トラップ メッセージの有無をチェックします。

- hm-#-#.log：これはすべてのヘルス モニター アクティビティのログです。未受信のハイ アベイラビリティ状態の変更およびアプリケーション プロセス障害に関する、最近のメッセージをチェックします。

これらのログに表示されるメッセージは、管理アプリケーションに表示されるアクティビティと一致する必要があります。大きな違いがある場合は、Cisco Technical Assistance Center（TAC）でサポート ケースを開き、疑わしいログ ファイルをケースに添付してください。シスコ サポート ケースの登録を参照してください。

シスコサポート リクエストのデフォルトの設定

デフォルトでは、 GUI のさまざまな部分からシスコサポート リクエストを作成できます。必要に応じて、送信者の電子メールアドレスやその他の電子メールの特性を設定できます。これらを設定しない場合、ユーザーがケースを登録するときに情報を入力できます。

ユーザーが GUI クライアントからリクエストを作成できないようにするには、その機能を無効にします。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[一般（General）]** > **[アカウント設定（Account Settings）]** を選択します。

ステップ 2 [サポート リクエスト（Supporte Request）] タブをクリックします。

ステップ 3 必要なインタラクション タイプを選択します。

- [サーバーから直接インタラクションを有効にしてください（Enable interactions directly from the server）]：サーバーから直接サポート ケースを作成する場合は、このオプションを指定します。サポート プロバイダーへの電子メールは、 サーバーに関連付けられているメール アドレス、または指定したメール アドレスから送信されます。
- [クライアントシステムを介したインタラクションのみ（Interactions via client system only）]：サポート ケースに必要な情報をクライアント マシンにダウンロードする場合は、このオプションを指定します。この場合、ダウンロードしたサポート ケースの詳細および情報をサポート プロバイダーに電子メールで送信する必要があります。

ステップ 4 テクニカル サポート プロバイダーを選択します。

- [Cisco] をクリックし、シスコ テクニカル サポートにサポート ケースを登録し、各自の Cisco.com クレデンシャルを入力し、[接続のテスト（Test Connectivity）] をクリックして次のサーバーへの接続を確認します。
  - メール サーバー
  - シスコ サポート サーバー
  - フォーラム サーバー

- [サードパーティ サポート プロバイダー（Third-party Support Provider）] をクリックして、サードパーティ サポート プロバイダーへのサービス要求を作成します。プロバイダーの電子メールアドレス、件名、Web サイト URL を入力します。

シスコ製品フィードバックの設定

シスコ製品の向上のために、 は以下のデータを収集してシスコに送信します。

- 製品情報：製品タイプ、ソフトウェア バージョン、インストール済みライセンス。
- システム情報：サーバーのオペレーティング システムおよび利用可能なメモリ。
- ネットワーク情報：ネットワーク上のデバイスの数とタイプ。

この機能はデフォルトでイネーブルになっています。データは日単位、週単位、または月単位で収集され、HTTPS を使用してシスコ クラウドの REST URL に送信されます。**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[一般（General）] > [改善にご協力ください（Help Us Improve）]** を選択します。

- シスコが収集するデータの種類を確認するには、[シスコが収集するデータについて（What data is Cisco collecting?）] をクリックします。
- この機能を無効にするには、[今回は協力しない（Not at this time, thank you）] を選択し、[保存（Save）] をクリックします。

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。