Prime Infrastructure のサーバ設定

次の項には、Prime Infrastructure のサーバ設定の設定に関する情報が含まれます。

使用可能なシステム設定

[Administration] > [System Settings] メニューには、Prime Infrastructure 設定を設定または変更するオプションが含まれます。Prime Infrastructure を初めて実装するときにこれらの設定の多くをカスタマイズすることになりますが、実稼働後にはなるべく変更しないでください。

表 2-1 に、[Administration] > [System Settings] メニューから設定または変更できる設定のタイプを示します。

表 2-1　使用可能な Prime Infrastructure 設定

次の手順を実行します。	[Administration] > [System Settings] の順に選択します。	適用可能なデバイス
• 削除するアラーム、イベント、syslog のほか、削除する頻度を変更します。 • 電子メール通知が送信されるアラーム タイプのほか、通知が送信される頻度を設定します。 • [Alarm Summary] ビューに表示するアラーム タイプを設定します。 • 電子メールで送信されるアラーム通知の内容を変更します。	**Alarms and Events** 「[Alarm Clean Up and Display Options] の指定」（P.5-1）を参照してください。	有線および無線のデバイス
監査ログが基本であるか、あるいかテンプレートに基づいているかを選択し、監査するデバイス パラメータを選択します。	**Audit** 「監査設定のセットアップ」（P.5-4）を参照してください。	有線および無線のデバイス
syslog を消去し、消去されたログをトラッシュまたはリモート ディレクトリに送信します。	**Audit Log Purge Settings** 「監査レコードからの syslog の削除」（P.5-5）を参照してください。	N/A
[Enable Change Audit JMS Notification] チェックボックスをオンにすることにより、[Change Audit JMS Notification] を有効にします。	**Change Audit Notification** 「監査通知の変更の有効化」（P.5-6）を参照してください。	有線および無線のデバイス
• 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。 • 検出時に自律 AP 移行分析を有効にします。	**CLI Session** 「CLI セッションのプロトコル設定」（P.7-2）を参照してください。	無線デバイス
• 診断チャネルでの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 サーバからクライアントのホスト名のルックアップを有効にし、キャッシュする時間を設定します。 • 関連付けが解除されたクライアントを保持する時間と、セッション データを設定します。 • トラップまたは syslog を受信したときにのみ、セッションを識別するようにクライアントをポーリングします。 • イベントとしてのクライアント アソシエーション トラップおよびディスアソシエーション トラップおよび 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エラー トラップの保存、保存するエラー トラップ間の時間を有効にします。	**Client** 「クライアント パフォーマンスの設定」（P.3-6）を参照してください。	有線および無線のデバイス
デバイス設定を展開する場合に、実行コンフィギュレーションのバックアップ、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 プールの数などの基本の制御パラメータを設定します。	**Configuration** 「コンフィギュレーションのバックアップおよびロールバック」（P.6-6）を参照してください。	有線および無線のデバイス
プロトコル、タイムアウト値、保存する設定バージョン数などの、コンフィギュレーション アーカイブの基本パラメータを設定します。	**Configuration Archive** 「コンフィギュレーションをアーカイブする日数の指定」（P.6-6）を参照してください。	有線および無線のデバイス

表 2-1　使用可能な Prime Infrastructure 設定 （続き）

次の手順を実行します。	[Administration] > [System Settings] の順に選択します。	適用可能なデバイス
ワイヤレス コントローラのアップグレード後に自動リフレッシュを有効にし、save config トラップを処理します。	**Controller Upgrade Settings** 「アップグレード後のコントローラのリフレッシュ」（P.7-2）を参照してください。	無線デバイス
データの重複排除を有効または無効にします。	**Data Deduplication** 「データの重複排除の有効化」（P.6-4）を参照してください。	N/A
トレンド、デバイス状態、パフォーマンス、ネットワーク監査、システム状態のデータ タイプの保持期間を設定します。	**Data Retention** 「データの保持期間の指定」（P.6-2）を参照してください。	有線および無線のデバイス
デバイス グループの階層を定義します。デフォルトでは、階層は次のとおりです。 • デバイス タイプ/ルータ • デバイス タイプ/スイッチおよびハブ • デバイス タイプ/ルータ/Cisco 1000 音声シリーズ ルータ	**Grouping**	有線および無線のデバイス
期限切れのすべてのゲスト アカウントをグローバルに削除するには、ゲスト アカウント設定を設定します。デフォルトでは、Prime Infrastructure Lobby Ambassador 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。[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。	**Guest Account Settings** 「ゲスト アカウントの設定」（P.9-2）を参照してください。	無線デバイス
ダウンロード、配布、および推奨ソフトウェア イメージのグローバル プリファレンス パラメータを設定します。	**Image Management** Image Management の詳細については、『*Cisco Prime Infrastructure 2.0 User Guide*』を参照してください。	有線および無線のデバイス
デバイスに対しても syslog を受信する場合に、Prime Infrastructure がインベントリを収集できるように、インベントリ収集を有効にします。	**Inventory** 「イベントを受信した後のインベントリ収集の指定」（P.6-5）を参照してください。	有線および無線のデバイス
ジョブが実行される前に、管理者の承認を必要とするジョブを指定するジョブ承認を有効にします。	**Job Approval Settings** 「ジョブに対する管理者の承認の指定」（P.2-12）を参照してください。	有線および無線のデバイス
Prime Infrastructure で使用可能なイーサネット MAC アドレスを表示、追加、または削除します。	**Known Ethernet MAC Address** 「電子メールの設定」（P.2-5）を参照してください。	N/A
すべてのユーザのログイン ページ下部に表示される免責事項テキストを変更します。	**Login disclaimer** 「ログイン ページに表示する免責事項の指定」（P.2-13）を参照してください。	N/A
レポートおよびアラーム通知の電子メールの配信を有効にします。	**Mail server configuration** 「電子メールの設定」（P.2-5）を参照してください。	N/A

表 2-1　使用可能な Prime Infrastructure 設定 （続き）

次の手順を実行します。	[Administration] > [System Settings] の順に選択します。	適用可能なデバイス
Prime Infrastructure から通知を受信するリモート イベントとアラーム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、設定された通知レシーバに送信されます。通知タイプ UDP の通知受信者を追加する場合、その追加する受信者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、選択したカテゴリについて 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。	**Notification receivers** 「Prime Infrastructure への通知レシーバの追加」（P.2-15）を参照してください。	有線および無線のデバイス
プラグ アンド プレイの設定を変更します。	**Plug & Play**	有線デバイス
Prime Infrastructure サーバとローカル認証サーバのプロキシを設定します。	**Proxy Settings** 「プロキシ設定」（P.2-11）を参照してください。	N/A
スケジュールされたレポートが保存されているパスのほか、レポートの保存期間を設定します。	**Report** 「レポートを保存する場所とその期間の指定」（P.6-4）を参照してください。	有線および無線のデバイス
不正 AP 設定を設定して、不正アクセス ポイントがネットワークに接続されているスイッチ ポートを自動的に追跡できるよう Prime Infrastructure を有効にします。	**Rogue AP Settings** 「不正 AP トレーシングに対する SNMP クレデンシャルの設定」（P.7-1）を参照してください。	無線デバイス
使用される FTP、TFTP、HTTP、HTTPS、NTP サーバ、およびコンプライアンス サービスを設定します。	**Server Settings** 「サーバ設定値の設定」（P.2-11）を参照してください。	N/A
Prime Infrastructure サーバを再起動するときに、サーバのチューニングを有効にします。サーバ チューニングにより、サーバがクライアントの要求を処理するために使用するリソースの数を制限することで、サーバのパフォーマンスを最適化できます。	**Server Tuning** 「クライアント パフォーマンスの設定」（P.3-6）を参照してください。	有線および無線のデバイス
Cisco Prime Infrastructure に Cisco WAAS Central Manager の IP アドレスを設定します。	**Service Container Management** 『Cisco WAAS Central Manager Integration』を参照してください。	有線デバイス
任意の生成されたアラームの重大度を設定します。	**Severity Configuration** 「アラームの重大度の変更」（P.5-3）を参照してください。	有線および無線のデバイス
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。	**SNMP Credentials** 「不正 AP トレーシングに対する SNMP クレデンシャルの設定」（P.7-1）を参照してください。	無線デバイス

表 2-1　使用可能な Prime Infrastructure 設定 （続き）

次の手順を実行します。	[Administration] > [System Settings] の順に選択します。	適用可能なデバイス
到達可能性パラメータやバックオフ アルゴリズムなど、トレース表示値のグローバル SNMP ポーリング パラメータを設定します。 （注）　[Exponential]（デフォルト値）をバックオフ アルゴリズムに選択した場合、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 回めからは、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。到達可能性パラメータを使用することを選択した場合、Prime Infrastructure には、デフォルトで、設定したグローバル到達可能性試行とタイムアウトが適用されます。オフにした場合、Prime Infrastructure は指定されたタイムアウトと試行を必ず使用します。	**SNMP Settings** 「グローバル SNMP の設定」（P.2-6）を参照してください。	無線デバイス
テクニカル サポート リクエストを作成するための設定を設定します。	**Support Request Settings** 「テクニカル サポート リクエストの設定」（P.5-10）を参照してください。	有線および無線のデバイス
基本および高度なスイッチ ポート トレース パラメータを設定します。	**Switch Port Trace** 「スイッチ ポート トレーシングの設定」（P.7-4）を参照してください。	有線デバイス
ベンダーの Organizationally Unique Identifier（OUI）マッピングを追加し、更新されたベンダー OUI マッピングの XML ファイルをアップロードします。	**User Defined OUI** **Upload OUI** 「OUI の管理」（P.2-13）を参照してください。	有線および無線のデバイス
デバイスに関する追加情報を保存します。	**User Defined Field** 「ユーザ定義フィールドへのデバイス情報の追加」（P.2-13）を参照してください。	有線デバイス

電子メールの設定

Prime Infrastructure レポート、アラーム通知などから電子メールを送信する際に使用するグローバル電子メール パラメータを設定できます。この [Mail Server] ページでは、1 つの場所に電子メールのパラメータを設定できます。[Mail Server] ページでは、プライマリ SMTP サーバおよびセカンダリ SMTP サーバのホストおよびポート、送信者の電子メール アドレス、および受信者の電子メール アドレスを設定できます。

はじめる前に

グローバル電子メール パラメータを設定する前に、グローバル SMTP サーバを設定する必要があります。

グローバル電子メール パラメータを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] > [Mail Server Configuration] を選択します。[Mail Server Configuration] ページが表示されます。

ステップ 2　プライマリ SMTP サーバのホスト名を入力します。

ステップ 3　SMTP サーバのユーザ名を入力します。

ステップ 4　SMTP サーバにログオンする際のパスワードを入力し、確定します。

（注）　ユーザ名およびパスワードは、両方ともオプションです。

ステップ 5　セカンダリ SMTP サーバに対してと同じ情報を提供します（セカンダリ メール サーバが使用できる場合のみ）。

ステップ 6　ページの [Sender And Receivers] 部分の [From] テキスト ボックスに *PI@Hostname.domainName* が入力されます。これは別の送信者に変更可能です。

ステップ 7　[To] テキスト ボックスに、受信者の電子メール アドレスを入力します。指定した電子メール アドレスは、アラームやレポートなど、その他の機能エリアでデフォルト値として使用されます。複数の電子メール アドレスを追加する場合は、各アドレスをカンマで区切る必要があります。

（注）　ステップ 7 で受信者の電子メール アドレスに加えたグローバルな変更は、電子メール通知が設定されていた場合には無視されます。

プライマリ SMTP メール サーバを指定し、[From] アドレス テキスト ボックスに入力する必要があります。

入力した受信者リストにすべてのアラーム カテゴリを適用させる場合は、[Apply recipient list to all alarm categories] チェックボックスをオンにします。

ステップ 8　電子メールの件名に付加するテキストを入力します。

ステップ 9　（任意）[Configure e-mail notification for individual alarm categories] リンクをクリックすると、有効にするアラーム カテゴリおよびシビリティを指定できます。電子メール通知は、選択した重大度とカテゴリに一致するアラームが発生すると送信されます。

（注）　アラーム カテゴリをクリックし、[Critical]、[Major]、[Minor]、または [Warning] を選択して、電子メール アドレスを入力することで、各アラームのシビリティを設定できます。

ステップ 10　[Test] ボタンをクリックして、設定したパラメータを使用したテスト メールを送信します。テスト操作の結果は同じページに表示されます。このテスト機能では「Prime Infrastructure test e-mail」という件名の電子メールが送信され、プライマリ メール サーバとセカンダリ メール サーバへの接続が確認されます。

満足なテスト結果が得られたら、[Save] をクリックします。

グローバル SNMP の設定

[SNMP Settings] ページでは、Prime Infrastructure からグローバルな SNMP パラメータを設定できます。

このページで行うすべての変更は、Prime Infrastructure にグローバルに影響します。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。

（注） デフォルトのネットワーク アドレスは 0.0.0.0 であり、ネットワーク全体を示します。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。デフォルトのコミュニティ ストリングは、読み取りと書き込みの両方において *private* です。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。

グローバル SNMP を設定するには、次の手順を実行します。

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

ステップ 2　左側のサイドバーのメニューから [SNMP Settings] を選択します。[SNMP Settings] ページが表示されます。

ステップ 3　（任意）[Trace Display Values] チェックボックスをオンにした場合は、SNMP を使用しているコントローラから取得したデータ値がメディエーション トレースレベル ログに表示されます。オフにした場合は、値は表示されません。

（注） セキュリティ上の理由から、デフォルトではオフになっています。

ステップ 4　[Backoff Algorithm] の場合は、ドロップダウン リストから、[Exponential] または [Constant Timeout] を選択します。[Exponential]（デフォルト値）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 回めからは、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。

（注） 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 5　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、グローバルに設定した [Reachability Retries] と [Timeout] が Prime Infrastructure でデフォルト適用されます。オフにした場合は、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を Prime Infrastructure が常に使用します。デフォルトはオンです。

（注） 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 6　[Reachability Retries] フィールドに、デバイスの到達可能性を判断するためのグローバルな再試行回数を入力します。デフォルトの回数は 2 回です。このフィールドは、[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。

（注） 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 7　[Reachability Timeout] フィールドに、デバイスの到達可能性を判断するためのグローバルなタイムアウト値を入力します。デフォルトの回数は 2 回です。このフィールドは、[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。

ステップ 8　[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。[Maximum VarBinds per Get PDU] フィールドのデフォルトは 30 で、[Maximum VarBinds per Set PDU] フィールドは 50 です。

（注）　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。

表のフィールドあたりの最大行数は設定可能であり、デフォルト値は 200000 行です。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 9　[Save] をクリックして、これらの設定を保存します。

SNMP クレデンシャル詳細の表示

このページに一覧表示される SNMP クレデンシャルは、不正 AP のスイッチ ポートをトレースするためだけに使用されます。

現在の SNMP クレデンシャルの詳細を編集または表示するには、次の手順を実行します。

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

ステップ 2　左側のサイドバーのメニューから [SNMP Credentials] を選択します。

ステップ 3　[Network Address] リンクをクリックすると、[SNMP Credential Details] ページが開きます。[SNMP Credential Details] ページには、次の情報が表示されます。

[General] パラメータ

- [Add Format Type]：表示のみ。[Add Format Type] の詳細については、「新しい SNMP クレデンシャル エントリの追加」（P.2-9）を参照してください。
- Network Address
- Network Mask

[SNMP Parameters]：該当する SNMP パラメータの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。

（注）　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、[Administration] > [Settings] > [SNMP Settings] で設定された SNMP リトライおよびタイムアウト パラメータが使用されます。

- [Retries]：スイッチの検出を試行する回数。
- [Timeout]：秒単位のセッション タイムアウト値。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。
- [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。
  - Username
  - Auth.Type
  - Auth.Password
  - Privacy Type
  - Privacy Password

（注）　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 タイプおよびデフォルト ユーザなしの SNMP v3 が最も安全な SNMP 接続です。

ステップ 4　[OK] をクリックして変更を保存するか、[Cancel] をクリックして SNMP クレデンシャルの詳細を変更せずに [SNMP Credentials] ページに戻ります。

新しい SNMP クレデンシャル エントリの追加

新しい SNMP クレデンシャル エントリを追加する手順は次のとおりです。

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

ステップ 2　左側のサイドバーのメニューから [SNMP Credentials] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから [Add SNMP Entries] を選択し、[Go] をクリックします。

ステップ 4　次のいずれかを選択します。

手動で SNMP クレデンシャル情報を入力するには、[Add Format Type] ドロップダウン リストを [SNMP Credential Info] のままにします。複数のネットワーク アドレスを追加するには、各アドレスの間にカンマを使用します。ステップ 6 に進みます。

CSV ファイルのインポートにより複数のスイッチを追加する場合は、[Add Format Type] ドロップダウン リストから [File] を選択します。CSV ファイルを使用すると、独自のインポート ファイルを生成して必要に応じてデバイスを追加できます。ステップ 5 に進みます。

ステップ 5　[File] を選択した場合は、[Browse] をクリックしてインポートする CSV ファイルの場所を探します。ステップ 10 にスキップします。

CSV ファイルの最初の行は、含まれている列の説明に使用されます。IP アドレス列は必須です。

ファイル例：

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_passw
ord,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
```

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 6　[SNMP Credential Info] を選択した場合は、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には、IP アドレスの文字列の間にカンマを使用します。

ステップ 7　[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 8　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 9　SNMP パラメータの適切な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。
  - Username
  - Auth.Type
  - Auth.Password
  - Privacy Type
  - Privacy Password

（注）　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 タイプおよびデフォルト ユーザなしの SNMP v3 が最も安全な SNMP 接続です。

ステップ 10　[OK] をクリックします。

Prime Infrastructure がリストされている SNMP クレデンシャルを使用して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、[Configure] > [Ethernet Switches] ページに表示されます。

（注）　[Configure] > [Ethernet Switches] ページを使用して手動でスイッチを追加した場合、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 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、[Configure] > [Ethernet] ページからこれらのクレデンシャルを更新する必要があります。

プロキシ設定

[Proxy Settings] ページでは、Prime Infrastructure サーバとローカル認証サーバのプロキシを設定できます。ネットワークとインターネット間のセキュリティ バリアとしてプロキシ サーバを使用する場合、次の手順のようにプロキシ設定を設定する必要があります。

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

ステップ 2　左側のサイドバーのメニューから [Proxy Settings] を選択します。[Proxy Settings] ページが表示されます。

ステップ 3　[Enable Proxy] チェックボックスをオンにして、Prime Infrastructure サーバのプロキシ設定を有効にします。

ステップ 4　必要な情報を入力し、[Save] をクリックします。

サーバ設定値の設定

[Server Settings] ページは、TFTP、FTP、HTTP、HTTPS、またはコンプライアンス サービスを有効または無効にできます。サーバ設定をオンまたはオフにするには、次の手順を実行します。

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

ステップ 2　左側のサイドバーのメニューから、[Server Setting] を選択します。

ステップ 3　インストール時に確立された FTP および TFTP ディレクトリまたは HTTP および HTTPS ポートを変更する場合は、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、[Enable] または [Disable] をクリックします。

変更は再起動後に反映されます。

（注）　コンプライアンス サービスを有効にし、サーバを再起動した後、PSIRT および EOX のレポートを生成するために、インベントリを同期する必要があります。

TFTP サーバまたは FTP サーバの設定

ステップ 1　[Design] > [Management Tools] > [External Management Servers] > [TFTP/FTP Servers] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add TFTP/FTP Server] を選択し、[Go] をクリックします。

ステップ 3　[Server Type] ドロップダウン リストから、[TFTP]、[FTP]、または [Both] を選択します。

ステップ 4　TFTP または FTP サーバのユーザ定義の名前を入力します。

ステップ 5　TFTP または FTP サーバの IP アドレスを入力します。

ステップ 6　[Save] をクリックします。

ジョブに対する管理者の承認の指定

実行される前に、管理者によって承認される必要があるジョブ（たとえば、設定の上書きジョブ）を制御する必要がある場合があります。管理者がジョブの承認要求を拒否すると、ジョブは Prime Infrastructure データベースから削除されます。

デフォルトでは、ジョブの承認がすべてのジョブ タイプで無効です。

ジョブが実行される前に、管理者の承認を必要とするジョブを指定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] > [Job Approval Settings] を選択します。

ステップ 2　[Enable Job Approval] チェックボックスをオンにします。

ステップ 3　ジョブ タイプの一覧から、矢印を使用して、ジョブ承認を有効にするジョブを右側の一覧に移動します。デフォルトでは、ジョブ承認は無効になっているので、すべてのジョブが左側の一覧に表示されます。

ステップ 4　カスタマイズされたジョブ タイプを指定するには、正規表現を使用して [Job Type] フィールドに文字列を入力し、[Add] をクリックします。たとえば、Config で始まるすべてのジョブ タイプのジョブ承認を有効にするには、*Config.** を入力します。

ステップ 5　[Save] をクリックします。

ジョブの承認

ジョブが実行される前に、ジョブが管理者によって承認される必要があることを事前に指定している場合は、管理者はジョブを承認する必要があります（「ジョブに対する管理者の承認の指定」（P.2-12）を参照）。

[Administration] > [Jobs Approval] を選択して、次の内容を実行します。

- 承認を必要とするジョブの一覧を表示します。
- 一覧表示されたジョブを承認する：管理者がジョブを承認したら、ジョブが有効にされ、ジョブで指定したスケジュールごとに実行されます。

- 一覧表示されたジョブの承認要求を拒否する：管理者がジョブを拒否すると、ジョブは Prime Infrastructure データベースから削除されます。

ログイン ページに表示する免責事項の指定

[Login Disclaimer] ページでは、Prime Infrastructure ログイン ページの最上部に表示される免責事項を入力できます。この免責事項はすべてのユーザに対して表示されます。

ログイン ページに表示する免責事項を入力するには、次の手順を実行します。

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

ステップ 2　左側のサイドバーのメニューから、[Login Disclaimer] を選択します。

ステップ 3　該当するテキスト ボックスに、ログイン ページに表示する免責事項を入力して、[Save] をクリックします。

ユーザ定義フィールドへのデバイス情報の追加

ユーザ定義フィールド（UDF）は、デバイス位置の属性などのデバイスに関する追加情報を保存するために使用します（たとえば、領域、ファシリティ、フロアなど）。UDF 属性は [Operate] > [Device Work Center] を使用して新しいデバイスが追加、インポートまたはエクスポートされるたびに使用されます。

UDF を追加するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] > [User Defined Field] を選択します。

ステップ 2　[Add Row] をクリックして、UDF を追加します。

ステップ 3　フィールド ラベルと説明をそれぞれのフィールドに入力します。

ステップ 4　[Save] をクリックして、UDF を追加します。

OUI の管理

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 は、vendorMacs.xml という名前の XML ファイルにベンダー OUI マッピングを保存します。このファイルは、Prime Infrastructure のリリースごとに更新されます。OUI の更新により、以下を実行できます。

- 既存の OUI に対するベンダーの表示名を変更します。
- Prime Infrastructure に新しい OUI を追加します。
- 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 にアップロードします。

ここでは、次の内容について説明します。

- 「新しいベンダー OUI マッピングの追加」（P.2-14）

• 「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」（P.2-14）

新しいベンダー OUI マッピングの追加

[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。

新しいベンダー OUI マッピングを追加するには、次の手順に従います。

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

ステップ 2　左側のサイドバーのメニューから、[User Defined OUI] を選択します。[User Defined OUI] ページが表示されます。

ステップ 3　[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 4　[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 5　[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 6　[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 7　[Change Vendor Name] チェックボックスをオンにして、OUI がベンダー OUI マッピングに存在する場合に、ベンダーの表示名を更新して、[OK] をクリックします。

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

更新された vendorMacs.xml ファイルが cisco.com に定期的に掲示されます。このファイルをダウンロードし、同じファイル名の vendorMacs.xml を使用してローカル ディレクトリに保存できます。その後、Prime Infrastructure にファイルをアップロードします。Prime Infrastructure は、既存の vendorMacs.xml ファイルを更新されたファイルに置き換えて、ベンダー OUI マッピングを更新します。ただし、新しいベンダー OUI マッピングまたはユーザが行ったベンダー名の更新は上書きされません。

更新されたベンダー OUI マッピング ファイルをアップロードするには、次の手順に従います。

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

ステップ 2　左側のサイドバーのメニューから、[Upload OUI] を選択します。[Upload OUI From File] ページが表示されます。

ステップ 3　Cisco.com からダウンロードした vendorMacs.xml ファイルを参照し、選択して、[OK] をクリックします。

Prime Infrastructure への通知レシーバの追加

[Notification Receiver] ページには、ゲストのアクセスをサポートする現在の通知レシーバが表示されます。アラートおよびイベントは SNMPv2 通知として、設定された通知レシーバに送信されます。現在の通知レシーバを表示して、追加の通知レシーバを追加できます。

[Notification Receiver] ページにアクセスするには、次の手順を実行します。

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

ステップ 2　左側のサイドバーのメニューから [Notification Receivers] を選択します。現在設定されているすべてのサーバがこのページに表示されます。

ステップ 3　[Select a command] ドロップダウン リストから [Add Notification Receiver] を選択し、[Go] をクリックします。

ステップ 4　サーバの IP アドレスと名前を入力します。

ステップ 5　[North Bound] または [Guest Access] のオプション ボタンをクリックします。

デフォルトでは、[Notification Type] が自動的に UDP に設定されます。

ステップ 6　[Port Number] や [Community] などの UDP パラメータを入力します。設定するレシーバは、設定されたポートと同じポートで UDP を待ち受ける必要があります。

ステップ 7　レシーバ タイプとして [North Bound] を選択した場合は、その条件とシビリティを指定します。選択されたカテゴリのアラームのみが処理されます。選択されたカテゴリと一致する、選択されたシビリティのアラームが処理されます。

ステップ 8　[Save] をクリックして、通知レシーバ情報を確定します。

デフォルトでは、選択したカテゴリについて INFO レベルのイベントのみが処理されます。

SNMPV2 トラップのみが North Bound 通知の対象となります。

通知レシーバの削除

通知レシーバを削除するには、次の手順を実行します。

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

ステップ 2　左側のサイドバーのメニューから [Notification Receivers] を選択します。現在設定されているすべてのサーバがこのページに表示されます。

ステップ 3　削除する通知レシーバのチェックボックスをオンにします。

ステップ 4　[Select a command] ドロップダウン リストから [Remove Notification Receiver] を選択し、[Go] をクリックします。

ステップ 5　[OK] をクリックして、削除を実行します。

North Bound SNMP Receiver からのログ ファイルの例

次に、Prime Infrastructure からのイベント トラップを受信した North Bound SNMP レシーバの出力例を示します。

次の出力例は、Prime Infrastructure で生成されたログ ファイルを示します。このログ ファイルは、Prime Infrastructure サーバのログ ファイル ディレクトリ（/opt/CSCOlumos//webnms/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。

```
06/04/10 08:30:58.559 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]Adding into queue
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrTotalNotifications2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrHandledInNotification2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrNonCongestedIn2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService][addNBAlert]Added into queue
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][getNbAlarm]incrHandledOutNotification2
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.services] :
[NBNotificationService][startNotifier]Processing the
alertNoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.notification] :
[NbAlertToNmsAlertCorrelator][formVarBindList]Generating the varbind list for NB
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.2.1.1.3.0 variable value: 10 days, 20:22:17.26
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.6.3.1.1.4.1.0 variable value:
1.3.6.1.4.1.9.9.199991.0.1
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.2 variable value:
07:da:05:18:0c:30:0d:09:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.3 variable value:
07:da:06:04:08:1e:3a:04:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.4 variable value:
NoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.5 variable value: 2
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.6 variable value: Radio
load threshold violation
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.7 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.8 variable value:
172.19.29.112
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.9 variable value: AP
1250-LWAP-ANGN-170-CMR, Interface 802.11b/g/n
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.10 variable value:
Noise changed to acceptable level on '802.11b/g/n' interface of AP
'1250-LWAP-ANGN-170-CMR', connected to Controller '172.19.29.112'.
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.11 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.12 variable value:
06/04/10 08:30:58.565 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.14 variable value:
06/04/10 08:30:58.573 INFO[com.cisco.ncslogger.notification] : [NBUtil][sendTrap]OSS list
size with reachability status as up1
06/04/10 08:30:58.573 INFO[com.cisco.ncslogger.notification] : [NBUtil][sendTrap]Sending
UDP Notification for receiver:172.19.27.85 on port:162
```

Prime Infrastructure サーバへの HTTPS アクセスの設定

Prime Infrastructure サーバは、セキュアな HTTPS クライアント アクセスをサポートできます。証明書は自己署名するか、認証局（CA）のデジタル署名で証明することができます。認証局（CA）は ID を検証し、証明書を発行するエンティティです。CA によって発行された証明書により、その証明書を識別するエンティティ名（サーバ名またはデバイス名など）に特定の公開キーがバインドされます。証明書で認証する公開キーだけが、証明書で識別するエンティティが所有する対応した秘密キーと連動します。

Prime Infrastructure サーバの既存の SSL 証明書を表示するには、次の手順を実行する必要があります。

ステップ 1　root ユーザとして Prime Infrastructure サーバの CLI にログインします。

ステップ 2　/opt/CSCOlumos ディレクトリに変更して、次のコマンドを入力します。

jre/bin/keytool -list -alias tomcat -keystore conf/keystore -storepass changeit –v

既存の SSL 証明書の詳細が表示されます。

ステップ 3　Prime Infrastructure 信頼ストアにある CA 証明書の一覧を表示するには、Prime Infrastructure admin モードで次のコマンドを入力します。

ncs key listcacerts

Prime Infrastructure の自己署名証明書の生成

Prime Infrastructure の自己署名証明書を生成するには、次の手順を実行します。

ステップ 1　admin モードで Prime Infrastructure サーバの CLI にログインします。

ステップ 2　admin プロンプト（admin #）で、次のコマンドを入力します。

ncs key genkey –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が生成されます。証明書の [Distinguished Name] フィールドを入力するよう求められます。Prime Infrastructure にアクセスするのに使用されるドメイン名としてサーバの完全修飾ドメイン名（FQDN）を指定することが重要です。

ステップ 3　証明書を有効にするには、この順序で次のコマンドを発行することにより、Prime Infrastructure プロセスを再起動します。

- ncs stop

- ncs start

証明書署名要求（CSR）ファイルの生成

SSL 証明書は、サード パーティからも取得できます。このサポートを設定するには、次の手順を実行する必要があります。

1. 証明書署名要求ファイルを生成します。
2. 選択した認証局（CA）に署名要求を送信します。
3. 署名付きセキュリティ証明書ファイルをサーバに適用します。

ステップ 1　Prime Infrastructure サーバに対して証明書署名要求（CSR）ファイルを生成するには、次の手順を実行します。

a. Prime Infrastructure アプライアンスで、コマンドラインを終了します。

b. コマンドラインで、管理者 ID とパスワードを使ってログインし、Prime Infrastructure をインストールします。

c. 次のコマンドを入力して、デフォルトのバックアップ リポジトリの CSR ファイルを生成します。

- ncs key genkey -newdn -csr *CertName*.**csr repository** *RepoName*

値は次のとおりです。

- *CertName* は、選択の任意の名前です（例、**`MyCertificate.csr`**）。
- *RepoName* は、以前に設定されたバックアップ リポジトリです（例、**`defaultRepo`**）。

ステップ 2　アクセスできる場所に CSR ファイルをコピーします。次に例を示します。

copy disk:/*RepoName*/*CertName*.**csr ftp://your.ftp.server.**

ステップ 3　選択した認証局（CA）に CSR ファイルを送信します。

（注）　証明書のに対して CSR ファイルを生成し、送信した場合、同じ Prime Infrastructure サーバに新しいキーを生成するために、**genkey** コマンドを使用「しない」でください。指定すると、署名付き証明書ファイルをインポートした場合に、ファイル内およびサーバ上のキー間で不一致が発生します。

ステップ 4　CA から同じファイル名で、ファイル拡張子 CER の署名付き証明書ファイルを受信します。続行する前に、次の内容を確認します。

- CER ファイルは 1 つしかありません。場合によっては、個々のファイルとしてチェーン証明書を受信することもできます。その場合、単一の CER ファイルにこれらのファイルを連結します。
- CER ファイルの空白行が削除されます。

ステップ 5　コマンド ラインで、バックアップ レポジトリに CER ファイルをコピーします。次に例を示します。

- copy ftp://your.ftp.server/*CertName*.**cer disk:***RepoName*

ステップ 6　次のコマンドを使用して Prime Infrastructure サーバに CER ファイルをインポートします。

- ncs key importsignedcert *CertName*.**cer repository** *RepoName*

ステップ 7　この順序で次のコマンドを発行することにより、Prime Infrastructure サーバを再起動します。

- ncs stop

- ncs start

ステップ 8　証明書に署名した認証局（CA）がすでに信頼できる CA ではない場合、Prime Infrastructure ログインページにアクセスする際に、ブラウザの信頼ストアに証明書を追加するようにユーザに指示します。

認証局（CA）証明書とキーのインポート

Prime Infrastructure の信頼ストアに CA 証明書をインポートするには、次の手順を実行します。

ステップ 1　コマンドラインで、管理者 ID とパスワードを使ってログインし、次のコマンドを入力します。

ncs key importcacert *aliasname ca-cert-filename* **repository** *repositoryname*

ここで、

- *aliasname* は、この CA 証明書に指定された短い名前です。
- *ca-cert-filename* は、CA 証明書ファイル名です。
- *repositoryname* は、ca-cert-filename がホストされている Prime Infrastructure で設定されたリポジトリ名です。

ステップ 2　Prime Infrastructure に RSA キーおよび署名付き証明書をインポートするには、admin モードで次のコマンドを入力します。

ncs key importkey *key-filename cert-filename* repository *repositoryname*

ここで、

- *key-filename* は、RSA 秘密キーのファイル名です。
- *cert-filename* は、証明書ファイル名です。
- *repositoryname* は、キー ファイルと証明書ファイルがホストされている Prime Infrastructure で設定されたリポジトリ名です。

ステップ 3　この順序で次のコマンドを発行することにより、Prime Infrastructure サーバを再起動します。

- ncs stop

- ncs start

CA 証明書の削除

Prime Infrastructure から CA 証明書を削除するには、コマンドラインで、管理者 ID とパスワードを使ってログインし、次のコマンドを入力します。

ncs key deletecacert <*aliasname*>

[*aliasname*] は CA 証明書の短い名前です。この名前は、**ncs key listcacert** コマンドを発行することにより取得できます。

MIB - Prime InfrastructureAlert/Event マッピング

表 2-2 に、Cisco-Prime Infrastructure-Notification-MIB から Prime Infrastructure へのアラート / イベント マッピングをまとめています。

表 2-2　Cisco-Prime Infrastructure-Notification-MIB - Prime InfrastructureAlert/Event マッピング

フィールド名およびオブジェクト ID	データ型	Prime Infrastructure の [Event/Alert] 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。
cwNotificationCategory	CWirelessNotificationCategory	N/A	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	N/A	Prime Infrastructure の IP アドレス。

表 2-2　Cisco-Prime Infrastructure-Notification-MIB - Prime InfrastructureAlert/Event マッピング （続き）

フィールド名およびオブジェクト ID	データ型	Prime Infrastructure の [Event/Alert] フィールド	説明
cWNotificationManagedObject AddressType	InetAddressType	N/A	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。
cWNotificationManagedObject Address	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。
cWNotificationSourceDisplay Name	OCTET STRING	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/イベントのシビリティ： critical(1) major(2) minor(3) warning(4) clear(5) info(6) unknown(7)
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＝値の組で表されます。
cWNotificationVirtualDomains	OCTET STRING	N/A	アラームを発生させたオブジェクトの仮想ドメイン。このフィールドは現在のリリースでは空白になります。