コミュニケーション サービスの設定

この章は、次の内容で構成されています。

HTTP の設定

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

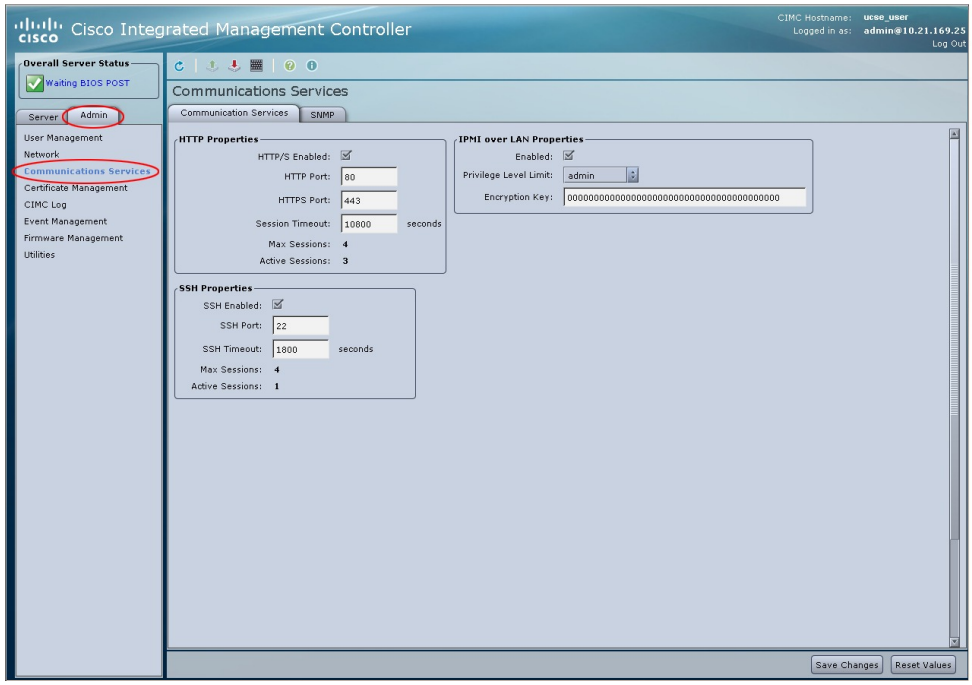
手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

図 *1*：*[Communication Services]* タブ



ステップ 4 [HTTP Properties] 領域で、次のプロパティを更新します。

名前	説明
[HTTP/S Enabled] チェックボックス	HTTP および HTTPS が CIMC でイネーブルかディセーブルか。
[HTTP Port] フィールド	HTTP 通信に使用するポート。 デフォルトは 80 です。
[HTTPS Port] フィールド	HTTPS 通信に使用するポート。 デフォルトは 443 です。
[Session Timeout] フィールド	HTTP 要求の間、CIMC がタイム アウトしてセッションを終了するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 1800 秒です。

名前	説明
[Max Sessions] フィールド	CIMC で許可されている HTTP および HTTPS の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている HTTP および HTTPS セッションの数。

ステップ 5 [Save Changes] をクリックします。

SSH の設定

はじめる前に

SSH を設定するには、admin 権限を持つユーザとしてログインする必要があります。

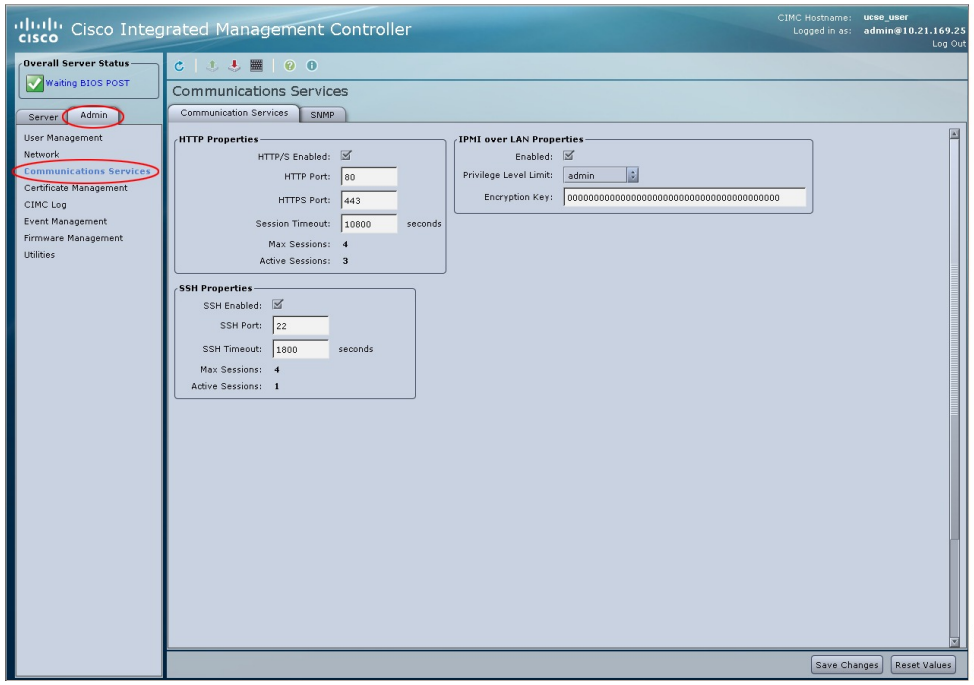
手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

図 2：***[Communication Services]*** タブ



ステップ 4 [SSH Properties] 領域で、次のプロパティを更新します。

名前	説明
[SSH Enabled] チェックボックス	SSH が CIMC でイネーブルかディセーブルか。
[SSH Port] フィールド	セキュア シェル アクセスに使用するポート。 デフォルトは 22 です。
[SSH Timeout] フィールド	SSH 要求がタイムアウトしたものとシステムが判断するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 1,800 秒です。

名前	説明
[Max Sessions] フィールド	CIMC で許可されている SSH の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている SSH セッションの数。

ステップ 5 [Save Changes] をクリックします。

IPMI の設定

IPMI Over LAN

インテリジェント プラットフォーム管理インターフェイス（IPMI）では、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。 このサービス プロセッサはベースボード管理コントローラ（BMC）と呼ばれ、サーバのマザーボードに存在します。 BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。

通常動作の間、IPMI は、サーバのオペレーティング システムがシステム ヘルスについての情報を取得し、システムのハードウェアを制御できるようにします。 たとえば、IPMI を使用すると、温度、ファンの速度、および電圧などのセンサーをモニタして、問題を事前に検出できます。 サーバの温度が指定されているレベルより高くなった場合、サーバのオペレーティング システムは BMC に対して、ファンの速度を上げたり、プロセッサの速度を下げたりして問題に対処するよう指示できます。

IPMI over LAN の設定

IPMI over LAN は、CIMC を IPMI メッセージで管理する場合に設定します。

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

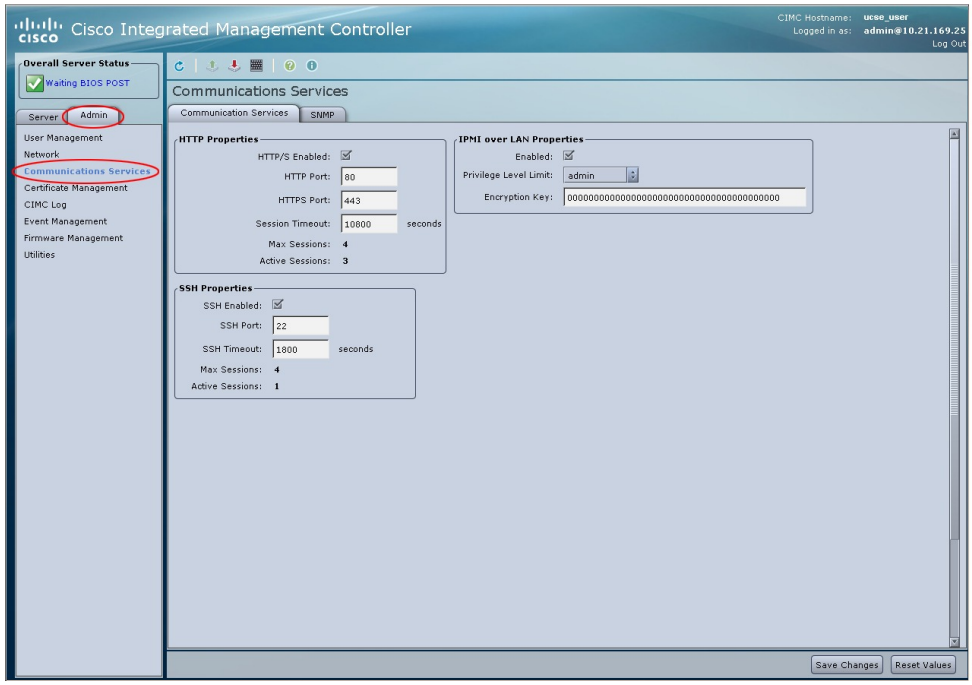
手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

図 *3* : *[Communication Services]* タブ



ステップ 4 [IPMI over LAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	このサーバで IPMI アクセスが許可されているかどうか。

名前	説明
[Privilege Level Limit] ドロップダウン リスト	このサーバで IPMI セッションに割り当て可能な最高特権レベル。 次のいずれかになります。 • [read-only]：IPMI ユーザは情報を表示できますが、変更することはできません。 このオプションを選択した場合、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザが作成できるのは、読み取り専用の IPMI セッションだけです。それ以外に所持している IPMI 特権は関係ありません。 • [user]：IPMI ユーザはいくつかの機能を実行できますが、管理タスクは実行できません。 このオプションを選択した場合、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザ セッションと読み取り専用セッションだけです。 • [admin]：IPMI ユーザは使用可能なすべてのアクションを実行できます。 このオプションを選択した場合、「Administrator」ユーザ ロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
[Encryption Key] フィールド	IPMI 通信に使用する IPMI 暗号キー。

ステップ 5 [Save Changes] をクリックします。

SNMP の設定

SNMP

Cisco UCS E-Series Servers は、サーバの設定およびステータスを表示したり、SNMP トラップによって障害とアラートを送信したりするために、簡易ネットワーク管理プロトコル（SNMP）をサポートしています。

SNMP プロパティの設定

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

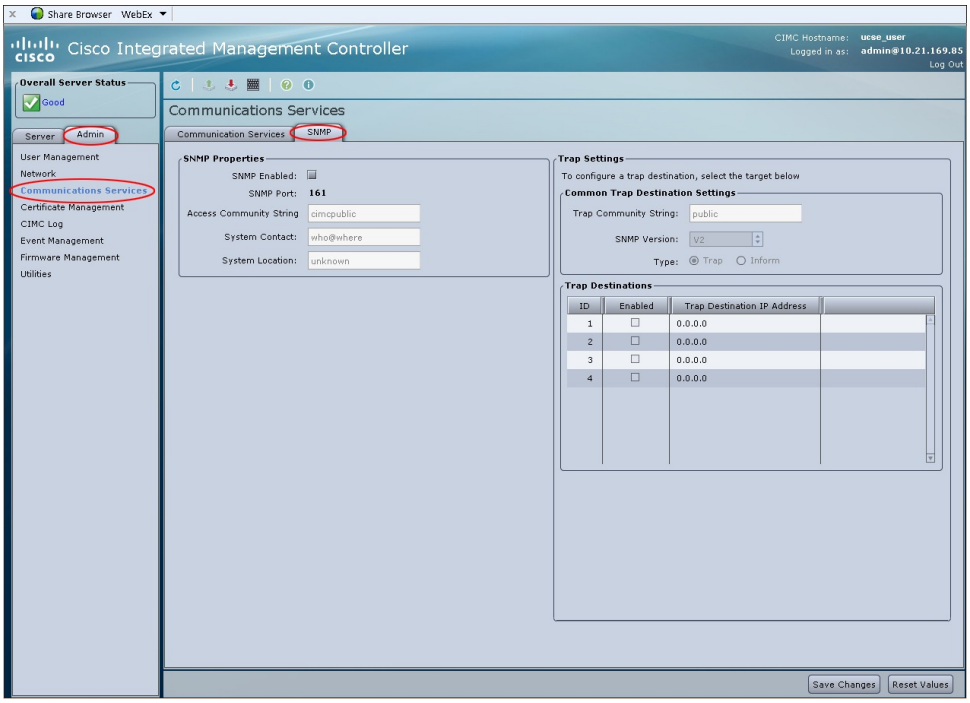
手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

図 *4* : *[SNMP]* タブ



ステップ 4 [SNMP Properties] 領域で、次のプロパティを更新します。

名前	説明
[SNMP Enabled] チェックボックス	このサーバが指定のホストに SNMP トラップを送信するかどうか。
[SNMP Port] フィールド	サーバが SNMP ホストとの通信に使用するポート。 この値は変更できません。

名前	説明
[Access Community String] フィールド	デフォルトの SNMP v1 または v2c コミュニティ名。 最大 18 文字の文字列を入力します。
[System Contact] フィールド	SNMP の実装を担当するシステムの連絡先。 電子メール アドレスや名前、電話番号など、最大 254 文字の文字列を入力します。
[System Location] フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 254 文字の文字列を入力します。

ステップ 5 [Save Changes] をクリックします。

次の作業

「SNMP トラップ設定の指定」の説明に従って SNMP トラップ設定を設定します。

SNMP トラップ設定の指定

はじめる前に

プラットフォーム イベント アラートをディセーブルにするには、admin 権限を持つユーザとしてログインする必要があります。

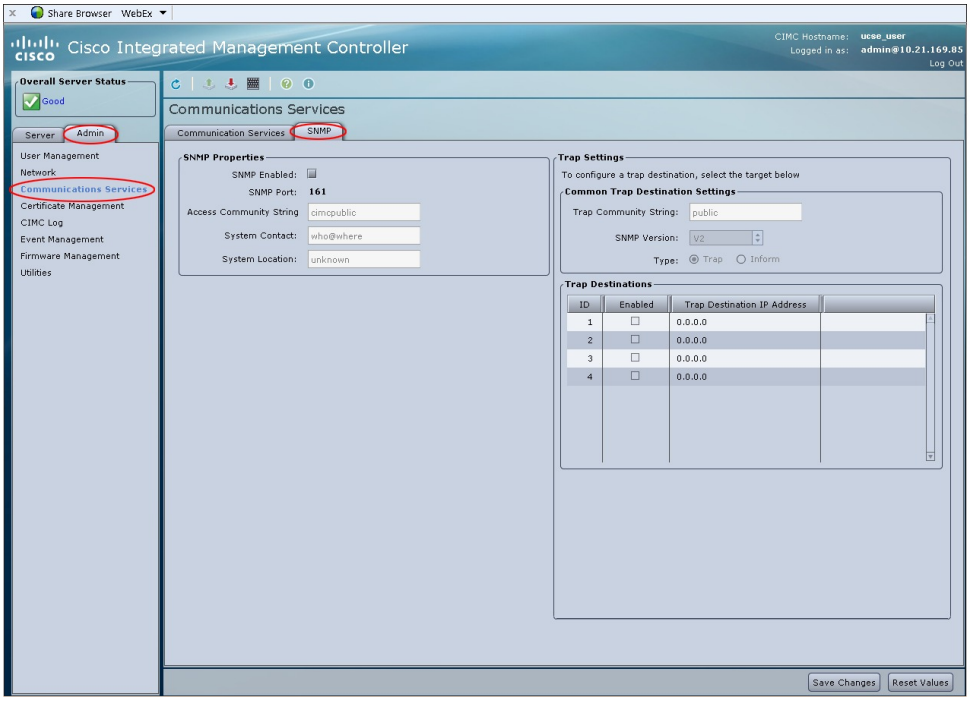
手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

図 5 : *[SNMP]* タブ



ステップ 4 [Common Trap Destination Settings] 領域の [Trap Community String] テキスト ボックスに、トラップ情報の送信先となる SNMP コミュニティの名前を入力します。

ステップ 5 [Trap Destinations] 領域で、目的の SNMP トラップ宛先の行をクリックします。
[Traps Details] ダイアログボックスが開きます。

ステップ 6 [Trap Details] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ID] カラム	トラップの宛先 ID。 この値は変更できません。
[Enabled] カラム	使用する SNMP トラップの宛先ごとに、このカラムの対応するチェックボックスをオンにします。
[Trap Destination IP Address] カラム	SNMP トラップ情報の送信先の IP アドレス。

ステップ 7 [Save Changes] をクリックします。

テスト SNMP トラップ メッセージの送信

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

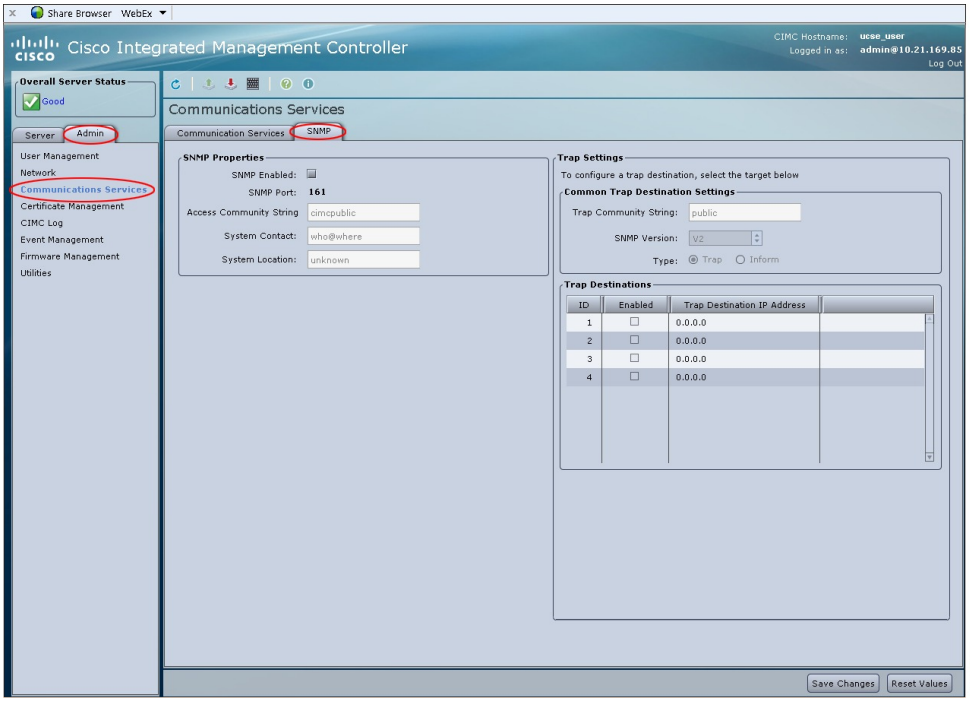
手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

図 *6* : *[SNMP]* タブ



ステップ 4 [Trap Destinations] 領域で、目的の SNMP トラップ宛先の行をクリックします。
[Traps Details] ダイアログボックスが開きます。

ステップ 5 [Send SNMP trap] をクリックします。

SNMPv1 テスト トラップ メッセージがトラップ宛先に送信されます。

（注） テスト メッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。