Cisco Registered Envelope Service 5.3.1 アカウント管理者ガイド

2017 年 10 月 21 日

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスココンタクトセンター
0120-092-255（フリーコール、携帯・PHS 含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number:

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Registered Envelope Service 5.3.1 アカウント管理者ガイド

CONTENTS

CHAPTER 1

概要

Cisco Registered Envelope Service（CRES）は、Cisco 暗号化テクノロジーをサポートするホスト サービスです。CRES は Cisco E メール セキュリティ アプライアンスおよび Cisco 暗号化アプライアンスと併用して、オンプレミス コンテンツ スキャン、ポリシー適用、暗号化を提供します。CRES はメッセージごとに暗号化されたメッセージの暗号キーを保存します。暗号化メッセージの受信者は、復号化キーを受信するサービスを使って自分自身を認証します。

（注） このガイドの最新バージョンと、CRES に関するその他のドキュメントは、この製品ページから入手できます。

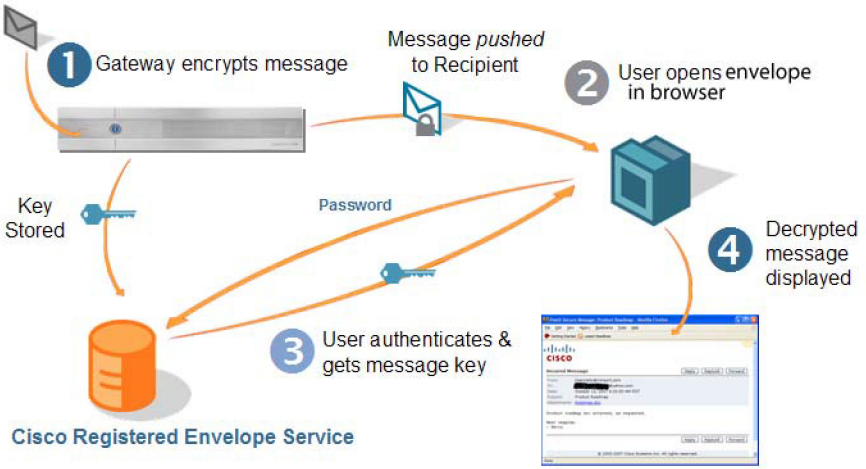
暗号化における Cisco Registered Envelope Service の役割

このサービスは、暗号化の次の要素を管理します。

- **受信者の登録。**登録済みエンベロープ（暗号化されたメッセージ）の受信者は、メッセージが低いセキュリティで送信される場合を除き、エンベロープを開くときにサービスに登録する必要があります。登録は無料です。
- **認証。**登録されたユーザは、シングルサインオン（SSO）を使用するかパスワードを入力して、登録髄エンベロープを開き、暗号化されたメッセージを読みます。
- **暗号化キー。**暗号化キーは、暗号化されたメッセージごとに作成されます。登録された受信者が登録済みエンベロープにパスワードを入力すると、サービスは復号化キーを送信してエンベロープを開封します。

- **メッセージの有効期限とロック。**登録されたユーザは送信する暗号化されたメッセージの有効期限を設定したりメッセージのロックを制御したりできます。企業アカウント管理者は、企業アカウントを使用して送信されるすべての暗号化されたメッセージの有効期限とロックを制御できます。
- **メッセージのセキュリティで保護された転送と返信。**企業アカウントの構成によっては、受信者が暗号化を使用して暗号化されたメッセージを転送および返信できることがあります。CRES は、メッセージのセキュリティで保護された転送と返信のために暗号化を処理します。

この図は、CRES が Cisco E メール セキュリティ アプライアンスと共に動作する方法を示しています。サービスは、暗号化されたメッセージの登録された受信者に復号化キーを指定します。



この図は、次のプロセスを示しています。

手順 1　Cisco E メール セキュリティ アプライアンスは暗号化を使用してメッセージを暗号化し、送信します。

手順 2　受信者は、登録済みエンベロープに自分の CRES パスワードを入力します。

（注）　メッセージが低いセキュリティ向けに設定されている場合、受信者がセキュリティ保護されたエンベロープを開封するためにパスワードを入力する必要はありません。

手順 3　CRES がエンベロープを開封するための復号化キーを指定します。

手順 4　受信者の Web ブラウザに、復号化されたメッセージが表示されます。

企業アカウントの管理

CRES は組織の企業アカウントのための管理機能を提供します。最初の CRES 管理ロールは登録済みの技術担当者に割り当てられています。企業アカウントの管理者は、次のタスクなどを実行できます。

- 登録済みエンベロープに表示されるロゴをカスタマイズします
- サービスから送信されるメッセージを管理します
- アカウント使用状況レポートを生成します
- ユーザを管理します（アカウントのロックやパスワードのリセットなど）
- エンベロープを必要としない暗号化されセキュリティ保護された返信のために TLS 設定を構成します

CHAPTER 2

管理機能

この章では、次の事項について説明します。

管理に関する FAQ

このセクションでは、Cisco Registered Envelope Service（CRES）企業アカウント管理者のロールについてよく寄せられる質問（FAQ）の回答を示します。

Cisco Registered Envelope Service 企業アカウントとは何ですか?

暗号化テクノロジーや CRES を使用する各組織には、サービスを使用するための企業アカウントがあります。このアカウントは、暗号化されたメッセージを送信する 1 つ以上の Cisco E メール セキュリティ アプライアンスと併用することもできます。

通常、組織には単一の企業のアカウントがあり、アカウント管理者はそのアカウントだけを管理します。

アカウント管理者の一般的なタスクとは何ですか?

一般的な管理タスクは次のとおりです。

- 企業アカウントの設定(たとえば、組織のロゴをアップロードして、そのアカウントを使用して送信される登録済みエンベロープで表示するようにします)。
- アカウント使用状況のモニタリング(たとえば、ユーザ登録およびユーザ アカウント アクティベーションの統計情報を表示します)。
- このアカウントを使用して送信されるメッセージの管理(たとえば、特定メッセージへのアクセスを無効にします)。

(注)　アカウント管理者は、Administration Console で管理するユーザ メッセージのコンテンツにアクセスできません。

管理タスクの詳細については、「共通タスク」セクション(2-8 ページ)を参照してください。

このガイドでは、どのような電子メール管理トピックが説明されますか?

Cisco IronPort のセキュア電子メール ソリューションの管理には、2 つの異なる責任領域があります。

- Cisco E メール セキュリティ アプライアンスと Cisco 暗号化アプライアンスの管理
- CRES 企業アカウントの管理

このガイドでは、CRES 企業アカウントの管理について説明します。Cisco E メール セキュリティ アプライアンスの管理については、シスコのカスタマーサポート ポータルで入手可能な製品ドキュメントを参照してください。

受信者の登録とは何ですか?

受信者の登録は、ユーザ*登録*とも呼ばれ、登録済みエンベロープの初回受信者となる CRES ユーザ アカウントを作成するプロセスです。ほとんどのメッセージ受信者は、受信した暗号化されたメッセージを開封する前に、登録プロセスを完了する必要があります。ただし、メッセージが低セキュリティを使用している場合、ユーザは登録せずにメッセージを開くことができます。

登録プロセスでは、受信者はユーザ プロファイル情報を提供し、パスワードを選択し、パスワード確認時の質問と回答を選択します。

Cisco Registered Envelope Service アカウント

ユーザが CRES に登録しても、特定の送信者の企業アカウントに関連付けられることはありません。

送信者にはアカウントがあり、受信者にもアカウントがあります。送信者の CRES アカウントでは、暗号化されたメッセージの送信者がメッセージを期限切れにするか取り消しすることで、セキュアなメッセージを管理できます。

ユーザ

ユーザ アカウントの管理は、CRES でシステム管理者によって処理されます。通常、企業アカウントの管理者は、個々のユーザ アカウントを管理しません。

企業管理者は、パスワードのリセットや既存アカウントのロックのために、内部 CRES ユーザを管理できます。CRES 管理者がユーザ アカウントの管理を希望する場合、管理対象ドメインをアカウントに追加するためにカスタマー サポート チケットを保存する必要があります。

ユーザ グループとロールとは何ですか?

グループとは、登録ユーザのリストです。ロールとは、グループに関連付けることができる権限セットです。たとえば、アカウント管理者を作成するには、アカウントの管理権限を持つ担当者がユーザをアカウント管理者グループに追加する必要があります。ロールはユーザに関連付けられません。

（注）　特定のアカウント管理者グループ内のユーザは、そのアカウントを管理できます。

はじめに

このセクションでは、CRES 企業アカウント用に Administration Console を使用し始める方法について説明します。

企業アカウントの設定プロセスについて

ホステッド キー サービスとして CRES で暗号化を使用するように組織で Cisco E メール セキュリティ アプライアンスを設定すると、企業アカウントが組織に対して作成されます。組織の Cisco E メール セキュリティ アプライアンスは、その企業アカウントに関連付けられます。

（注）　企業アカウント管理者は、最初のアカウント設定プロセスに関与しません。

デフォルトで、新規アカウントのアカウント管理者グループには、組織の最初の企業アカウント管理者が含まれます。企業アカウント管理者は、アカウント管理者グループにユーザを追加することによって追加の管理者を作成できます。詳細については、「企業アカウント管理者の追加」セクション（2-10 ページ）を参照してください。アカウント管理者グループには、組織の Cisco E メール セキュリティ アプライアンスやシステム設定を熟知した Cisco セールス エンジニアを含めることもできます。

ログイン

企業アカウントを管理するには、この URL を使用してログインします。

https://res.cisco.com/admin

複数アカウントの管理者は、ログイン時にアカウントを選択するよう求められます。そこでは、アクションを次の中から選択できます。

- 選択したアカウントをこのコンピュータ上に記憶しておく。
- 次回ログイン時にこの記憶されたアカウントを自動的に選択する。

これらのオプションは、以下の 2 つのチェックボックスで表されます。

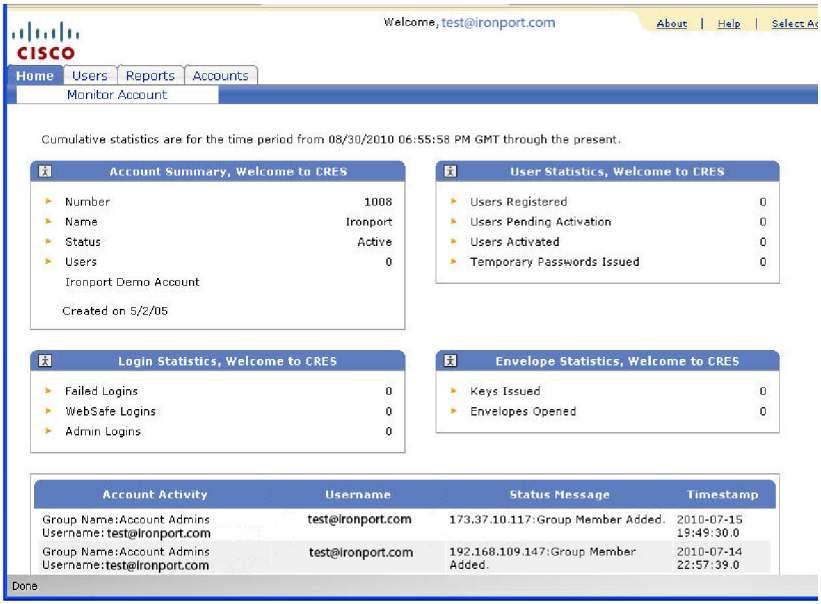
- [Remember account on this computer]：オンにすると、同じブラウザを使用して次回ログインするときに、選択したアカウントもリストで選択されます。アクティブ アカウントだけがリストに表示されます。
- [Automatically select remembered account]：オンにすると、アカウントのリストは表示されず、ログイン時には保存したアカウントの情報が表示されます。

[Remember account on this computer] チェック ボックスがオンでない場合、[Automatically select remembered account] チェックボックスは有効になりません。

ログイン後に別のアカウントを選択するには、Administration Console のホーム ページの下部にある [Select Account] リンクを使用します。このリンクでは、[Automatically select remembered account] チェック ボックスをオフにすることもできます。

企業アカウントにログインすると、Administration Console が表示されます。

図 2-1　　企業アカウントの Administration Console



ホームページは、アカウント アクティビティの要約を表示する [Monitor Account] ページです。

Administration Console には、サイトを移動するための次のタブとリンクがあります。

- **[Home]。**[Monitor Account] ページを表示します。

  [Monitor Account] ページを使用して、システムおよびアカウントのステータスを表示します。[Update] ボタンをクリックすると、最新のステータス情報を取得します。または [Update Interval] フィールドに値を入力して [Update] をクリックすると、ページを定期的に（たとえば 10 秒ごとに）更新します。

- **[Users]。**[User Management] ページを表示します。

  このページは通常、シスコのシステム管理者だけが使用します。企業アカウント管理者は、自分のアカウントに割り当てられているユーザにのみアクセスできます。この場合は、それらのユーザが正しいドメインを追加していることが前提条件となります。

- **[Reports]。**[View Reports] ページを表示します。

  [View Reports] ページは通常、Account Usage レポートを実行するために使用されます。Account Usage レポートの詳細については、第 3 章,「レポート」を参照してください。

  [View Reports] ページには、以下のレポートへのリンクがあります。

  - **User Information レポート。**アカウントに関連付けられたユーザのリストを表示します（シーケンス番号（#）、ユーザ ID、電子メール アドレス、名、姓、ステータス、作成日、最終ログイン日、最終変更日などを含む）。ただし、1 つ以上のドメインがアカウントに関連付けられている場合に限ります。
  - **Users Status レポート。**ドメインに関連付けられたユーザのステータス（[New]、[Active]、[Blocked]）を示します。
  - **Account Usage レポート。**企業アカウントの使用状況の統計情報を表示するには、このレポートを実行します。Account Usage レポートの詳細については、第 3 章,「レポート」を参照してください。

- **[Accounts]。**[Account Management] ページと [Manage Registered Envelopes] ページのタブを表示します。

[Manage Accounts] タブをクリックすると [Account Management] ページが表示され、CRES 企業アカウントを設定できます。詳細については、「登録済みエンベロープのロゴのカスタマイズ」セクション（2-9 ページ）、「企業アカウント管理者の追加」セクション（2-10 ページ）、および「テンプレートのカスタマイズ」セクション（2-11 ページ）を参照してください。

[Manage Registered Envelopes] タブをクリックすると、企業アカウントを使用して送信された登録済みエンベロープを検索および管理できます。詳細については、「メッセージの管理」セクション（2-12 ページ）を参照してください。

Administration Console のアイコンについて

システムを移動したり、アカウントやユーザなどの領域を管理したりするには、Administration Console のアイコンを使用します。各アイコンの意味は、ポップアップされるテキストで示されます。

表 2-1　　アイコンのリスト

アイコン	タイトル	アクション
	Manage Users	[Group Membership] ページにアクセスします。
	Manage Roles	[Group Authorization] ページにアクセスします。
	Save Token	トークンをローカル マシンに保存します。トークンとは、Cisco E メール セキュリティ アプライアンス（ESA）と CRES（またはローカル キー サーバ）との間でデータを暗号化するために使用されるお客様固有のキーです。現在はカスタマー サポートでのみ使用されます。
	Manage Rules	[Rules] ページにアクセスします。
	Close or Delete item	項目を削除します。
	Preview Template	選択した言語でテンプレートをプレビューします。

共通タスク

このセクションでは、以下の管理タスクを実行するために Administration Console を使用する方法について説明します。

- 登録済みエンベロープのロゴのカスタマイズ
- 企業アカウント管理者の追加
- テンプレートのカスタマイズ
- アカウント アクティビティのモニタリング
- メッセージの管理
- パスワード確認時の質問の管理
- パスワード有効期限の設定
- パスワード要件の管理
- ソーシャル ネットワークの資格情報を使用してのエンベロープ開封
- ユーザの管理
- セキュリティ保護されたメッセージをユーザに透過的に暗号化配信するための TLS の使用
- 送信者の登録の有効化
- Java アプレットの有効化
- 認証方法の選択
- BCE プラグインまたはモバイル アプリケーション設定の構成
- BCE Config による署名検証の有効化
- Secure Compose へのアクセスの無効化と有効化
- CRES を含めるような DNS の設定

（注） ユーザはタイムスタンプをローカル タイム ゾーンに設定したり、希望の形式（12 時間または 24 時間）に設定したりできます。タイムスタンプをローカル タイム ゾーンに設定したユーザの場合、ユーザ タイムスタンプが含まれる任意の Administration Console 画面がこの機能の影響を受けます。

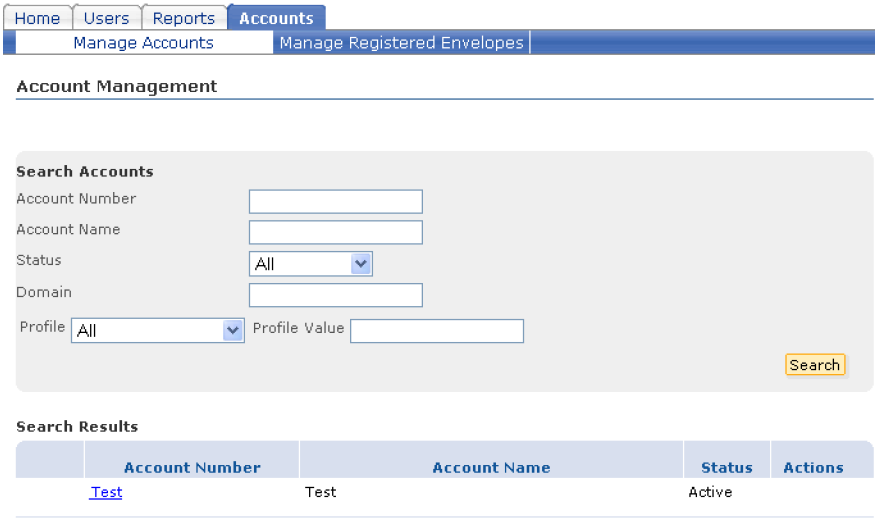
登録済みエンベロープのロゴのカスタマイズ

アカウントを使用して送信するメッセージに表示されるロゴを変更するには、次の手順を実行します。

手順 1　企業アカウントの Administration Console にログインします。

手順 2　[Accounts] タブをクリックします。[Account Management] ページが表示されます。

図 2-2　[Account Management] ページ



手順 3　アカウント番号のリンクをクリックします。

（注）　各組織には、通常、1 つの企業アカウントがあります。

アカウントの [Details] タブが表示されます。

手順 4　アカウントの [Images] タブをクリックします。

図 2-3　　[Images] タブ

手順 5　アップロードするロゴ ファイルを参照して、[Add Image] をクリックします。

（注）　ファイル サイズは 102,400 バイトを超えてはいけません。ロゴ ファイルが 60 x 160 ピクセルを超えないことも推奨します。
ロゴでは任意の種類のファイルを使用できますが、画像コンテンツでは GIF、JPEG、PNG、BMP、または WBM 形式のみ使用できます。ただし、ユーザが通常使用するブラウザでサポートされているファイル タイプのみ使用することを推奨します（例：GIF、JPEG、または PNG）。

企業アカウント管理者の追加

企業アカウント管理者を追加するには、次の手順を実行します。

手順 1　企業アカウントの Administration Console にログインします。

手順 2　[Accounts] タブをクリックします。図 2-2 に示すように、[Account Management] ページが表示されます。

手順 3　アカウント番号のリンクをクリックします。

（注）　組織には、通常、1 つの企業アカウントがあります。

アカウントの [Details] タブが表示されます。

手順 4　アカウントの [Groups] タブをクリックします。

手順 5　[Manage Users] アイコンをクリックします。

詳細については、「Administration Console のアイコンについて」セクション（2-7 ページ）を参照してください。

手順 6　[Group Membership] ページで、企業アカウント管理者として追加する登録済みユーザのユーザ ID を入力します。

手順 7　[Add to Group] をクリックします。

テンプレートのカスタマイズ

通知メッセージのテンプレートをカスタマイズするには、次の手順を実行します。

手順 1　企業アカウントの Administration Console にログインします。

手順 2　[Accounts] タブをクリックします。[Account Management] ページが開きます。

手順 3　アカウント番号のリンクをクリックします。

（注）　各組織には、通常、1 つの企業アカウントがあります。

アカウントの [Details] タブが開きます。

手順 4　アカウントの [Templates] タブをクリックします。

手順 5　[Base Template Set] ドロップダウン リストから、コピーするテンプレートを選択し、新しいテンプレート セットのタイトルを入力します。

手順 6　[Add] をクリックします。

手順 7　追加したテンプレートのリンクをクリックします。

手順 8　テンプレートに必要なロケールをクリックします。[Edit Template] ページが開きます。

手順 9　必要に応じて [HTML] および [Text] フィールドの情報を編集します。

手順 10　[Save（保存）] をクリックします。

手順 11　[Back to Templates List] をクリックします。

手順 12　[Back to Template Set List] をクリックします。

手順 13　[Active Template Set] ドロップダウン リストから、必要なテンプレートを選択します。

手順 14　[Save（保存）] をクリックします。

アカウント アクティビティのモニタリング

IronPort E メール セキュリティ アプライアンスは、暗号化の使用に関する詳細情報を提供します。たとえば、暗号化のメッセージをマーク付けするコンテンツ フィルタに関するレポートを生成するときにアプライアンスを使用できます。

アプライアンスが生成するレポートを補うために、CRES では企業アカウントのアクティビティに関する一般情報を提供します。この情報は Administration Console で確認できます。ホームページの [Monitor Accounts] タブには、アカウントのアクティビティに関する情報が表示されます。たとえば、ユーザ登録やログイン数、開封済みおよび送信済み暗号化メッセージ（登録済みエンベロープ）に関する統計情報などがあります。

また、[Accounts] タブでは Account Usage レポートを表示できます。CRES のレポートの詳細については、第 3 章,「レポート」を参照してください。

メッセージの管理

企業アカウント管理者は、アカウントを使用して送信されるメッセージのステータスを表示および管理できます。

メッセージを管理するには、次の手順を実行します。

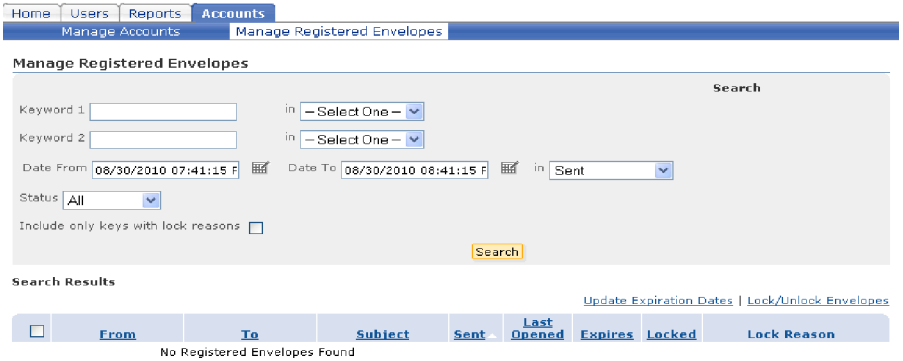
手順 1　企業アカウントの Administration Console にログインします。

手順 2　[Accounts] タブをクリックします。図 2-2 に示すように、[Account Management] ページが表示されます。

手順 3　[Manage Registered Envelopes] タブをクリックします。

[Manage Registered Envelopes] ページが表示されます。

図 2-4　[Manage Registered Envelopes] ページ



手順 4　[Search] をクリックすると、最後の 1 時間に送信されたすべてのメッセージを表示します。または、検索条件を入力して [Search] をクリックすると、特定のメッセージを表示します。

送信時刻、最後に開いた時刻、メッセージの有効期限、メッセージのロック情報など、各メッセージのステータスが検索結果に表示されます。

有効期限を設定するには、1 つ以上のメッセージを選択し、[Update Expiration Dates] リンクをクリックします。

メッセージをロックまたはロック解除するには、1 つ以上のメッセージを選択し、[Lock/Unlock Envelopes] リンクをクリックします。エンベロープをロックするときは、ロックの理由を入力できます。受信者がエンベロープを開こうとするときに、理由がエンベロープに表示されます。

パスワード確認時の質問の管理

[Security] タブでは、ユーザがカスタムのパスワード確認時の質問を定義することを許可または禁止できます。テーブルの [Sort] タブで該当するチェックボックスをオンにすることで、パスワード確認時の質問を変更できます。

[Advanced registration process] チェック ボックスをオンにした場合、ユーザは登録時にパスワード確認時の質問に回答し、個人のセキュリティ フレーズを入力する必要があります。このチェック ボックスをオフにすると、ユーザはセキュリティの質問に答えることなく登録できます。また、[Advanced Settings] フォームに入力してパスワード確認時の質問に回答できます。管理者グループに属していないすべてのユーザは [Edit Profile] ページでパスワード確認時の質問を無効にできます。

図 2-5　　パスワード確認時の質問の管理

パスワード有効期限の設定

[Manage Accounts] ページの [Security] タブでは、ユーザと管理者のパスワードに有効期限を設定できます。

パスワードの有効期限を有効にするには、次の手順を実行します。

手順 1　[Enable password expiration] チェック ボックスをオンにします。

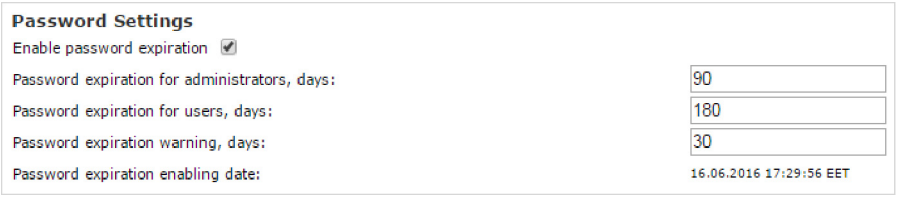
手順 2　次のフィールドに、パスワードが期限切れとなるまでの日数を入力します。

- [Password expiration for users]
- [Password expiration for administrators]

手順 3　[Password expiration warning] フィールドに、ユーザにパスワード変更を求める通知が送信されるまでの日数を入力します。

手順 4　[Save（保存）] をクリックします。

図 2-6　　パスワード有効期限の設定



パスワード要件の管理

パスワードを作成または変更する場合は、パスワードが次の要件を満たすようにしてください。

- パスワードは、英数字である必要があります（必須）。
- パスワードは大文字と小文字が区別される必要があります（必須）。
- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字タイプが含まれる必要があります。

- パスワードには 3 回以上連続して繰り返される文字を含めることはできません。
- パスワードにはユーザ名または反転したユーザ名を含めることはできません。
- パスワードには「Cisco」、「ocsic」の文字列を使用することはできません。また、同様の文字列の小文字を大文字に変更したものや、「i」を「1」、「l」、「!」に置き換えたもの、「o」を「0」に置き換えたもの、「s」を「$」に置き換えたものも使用できません。

2 つのパスワード要件のみデフォルトで設定されています。その他のオプションを選択して、ユーザのパスワード要件を変更できます。

[Manage Accounts] ページの [Security] タブでパスワード要件を管理できます。

図 2-7　　パスワード要件の管理

Check	Rules
☑	Enforce Alphanumeric Password
☐	Enforce Mixed-Case Password
☐	Require at Least One Special Character in Password
☐	Require at Least Three of Lower Case Letters, Upper Case Letters, Digits, Special Characters
☐	Password Must Not Be "Cisco" Or Its Variants
☐	Password Must Not Contain Repeated Characters
☑	Require Case-Sensitive Password
☐	Allow Maximum Password Length

The password rules settings will not apply to all users automatically, only when a user changes a password to a new one.

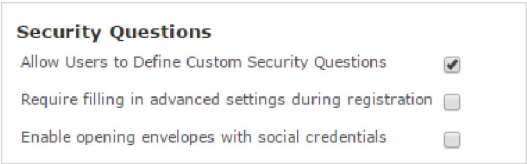
Save　Back to Accounts List

ソーシャル ネットワークの資格情報を使用してのエンベロープ開封

[Manage Accounts] ページの [Security] タブでは、セキュリティで保護されたメッセージをソーシャル ネットワークの資格情報を使用して開くことができるように設定できます。Google 認証でメッセージを開くことができるのは Gmail 受信者のみです。ユーザが CRES に登録されていない Google アカウントを所有している場合、そのユーザはエンベロープの [Sign-up with Google] ボタンをクリックして登録する必要があります。登録すると、Google でサインインしてセキュリティで保護されたメッセージを確認できるようになります。このオプションが有効になっていない場合、[Sign-in with Google] ボタンは表示されません。メッセージを開くには、そのユーザの CRES パスワードを入力する必要があります。

このオプションを有効にするには、[Enable opening envelopes with social credentials] チェック ボックスをオンにします。

図 2-8　　ソーシャル資格情報を使用してのエンベロープ開封の有効化



ユーザの管理

[Users] タブではシステムのユーザを管理できます。このタブではユーザの作成や検索、パスワードのリセット、グループへのユーザ追加、およびユーザの無効化ができます。

アカウントに関連付けられたドメインについてのみユーザを管理できます。ドメインをアカウントに関連付ける必要がある場合は、サポートに連絡してください。

（注） ドメインがアカウントに関連付けられる前にシステムに存在するユーザは、アカウントに移行する必要があります。ドメインの関連付けを要求するときに既存のユーザがあるかどうかをサポートにお知らせください。

ユーザの作成

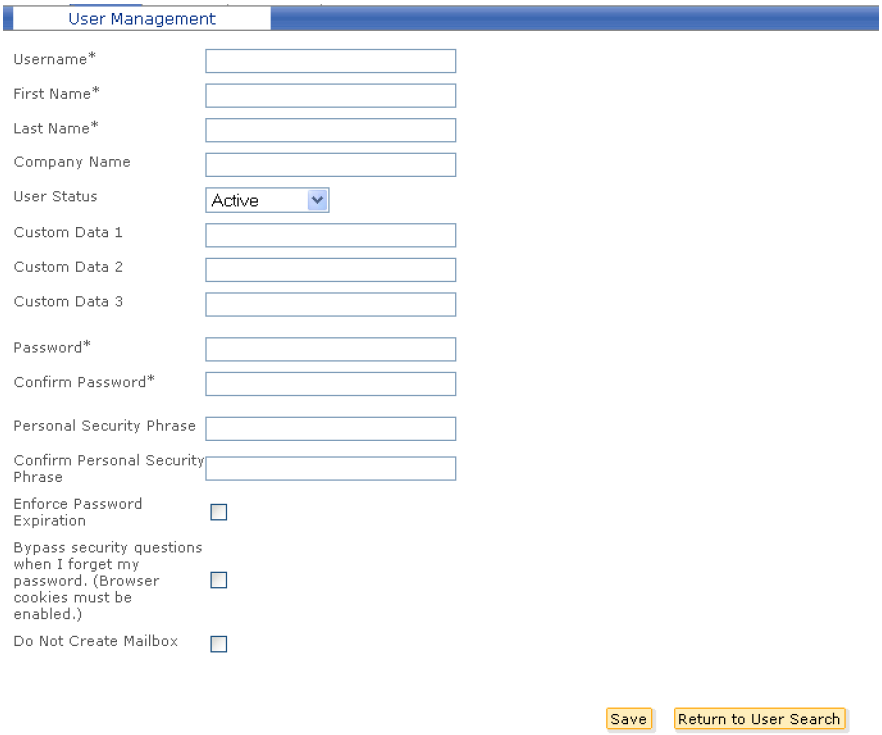
ユーザを作成するには、次の手順に従います。

手順 1　[Manage Users] ページで [Add User] をクリックします。

手順 2　フォームに情報を入力します。

（注）　パスワードは、シスコのパスワード要件に従う必要があります。詳細については、「パスワード確認時の質問の管理」セクション（2-14 ページ）を参照してください。

図 2-9　[Create User] ページ



手順 3　パスワードの有効期限を適用する、パスワード リセット時にパスワード確認時の質問のバイパスをユーザに許可する、特定ユーザのメールボックスの作成を省略するなどのカスタム オプションを設定できます。

手順 4　[Save（保存）] をクリックします。

（注）　作成するユーザは、自分の電子メール ドメインに属する必要があります。

ユーザ パスワードのリセット

ユーザは、次のリンクを使用してパスワードをリセットできます。

https://res.cisco.com/websafe/pswdForgot.action

ユーザは、登録タイプに応じて、パスワード確認時の質問に回答する必要があります。

- **Simple**：パスワード確認時の質問はオプションです。ユーザはパスワードのリセットにあたり、パスワード確認時の質問に回答する必要はありません。
- **Advanced**：パスワード確認時の質問は必須です。ユーザはパスワードを更新する際にパスワード確認時の質問に回答しなくてはなりません。パスワード確認時の質問の答えがわからない場合は、管理者に連絡する必要があります。

（注）　Advanced で登録したユーザに対し、後になってから Simple 登録を有効にした場合、そのユーザは Advanced での登録時に選択選択したパスワード確認時の質問に回答する必要があります。

チャレンジの質問の答えを思い出せない場合は、管理者インターフェイス経由でユーザのパスワードをリセットできます。

ユーザのパスワードをリセットするには、次の手順を実行します。

手順 1　ユーザを選択します（[Manage Users] ページで検索結果のユーザ名をクリックします）。

手順 2　[View Password Challenge Answers] をクリックします。

手順 3　[Reauthenticate] をクリックします。

手順 4　[Next] をクリックします。

手順 5　[Reset Password] をクリックします。

（注）　パスワードをリセットしたら、ユーザは新しいパスワードを作成するためのリンクが記載された電子メールを受信します。

グループへのユーザの追加

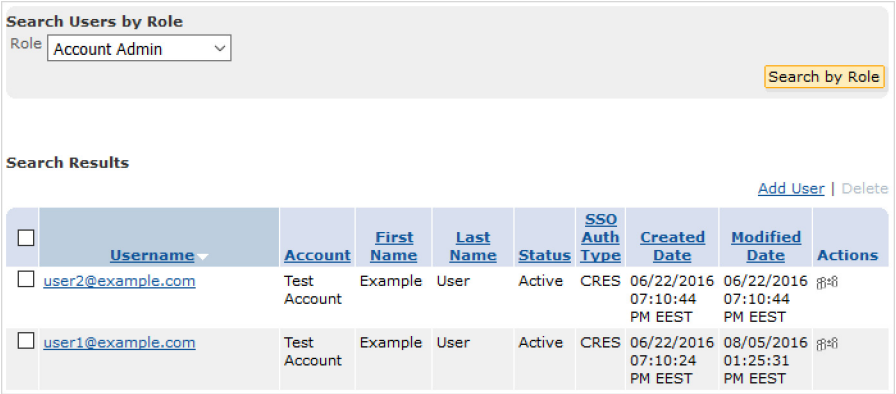
ユーザをグループに追加して（またはユーザをグループから削除して）、そのユーザに追加の権限を与えることができます。

ユーザのグループ メンバーシップを管理するには、次の手順を実行します。

手順 1　ユーザを選択します（[Manage Users] ページで検索結果のユーザ名をクリックします）。

手順 2　ユーザの [Actions] 列で [Groups] アイコンをクリックします。

図 2-10　　ユーザ リストの [Groups] アイコン



手順 3　[Group Membership] ページが表示されます。左のボックスにはユーザがメンバーであるグループが表示されます。右のボックスにはその他の使用可能なグループが表示されます。

手順 4　グループをクリックして選択し、右または左矢印をクリックしてグループを 2 つのボックス間で移動します。

手順 5　[Done] をクリックして変更を保存します。

ユーザの無効化

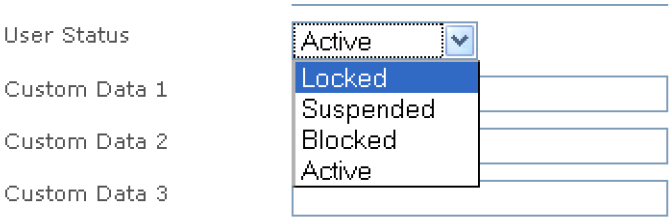
一時的にユーザのアカウントを無効にする必要があることがあります。たとえば、ユーザが退職する場合があります。ユーザを無効にするには、次の手順を実行します。

手順 1　ユーザを選択します（[Manage Users] ページで検索結果のユーザ名をクリックします）。

手順 2　[Modify] をクリックします。

手順 3　[User Status] を [Locked] に設定します。

図 2-11　　ユーザのステータスを [Locked] に設定



手順 4　変更を保存します。

TLS 配信の使用

Transport Layer Security（TLS）配信では、CRES から発信されるメッセージ（セキュリティ保護された返信など）をエンベロープを使用せずに送信元ドメインに暗号化して配信できます。

TLS 配信を使用すれば、電子メールを配信するセキュリティ保護された方法を提供でき、エンド ユーザが電子メールを受信ために CRES にログインしたり暗号化プラグインをインストールしたりする必要はありません。

TLS は、アカウントごとに有効にされます。アカウントごとに TLS ドメインおよびエラー処理の動作を 1 つ以上指定します。

TLS ドメインの追加とテスト

アカウントの TLS を有効にするには、少なくとも 1 つのドメインを追加する必要があります。ドメインを追加すると、TLS サポートのためにドメインがスキャンされるプロセスが開始します。ドメインは、追加する前に TLS ドメイン テストに合格する必要があります。

TLS ドメイン テストでは CRES サーバを使用して情報や接続を確認します。このチェックでは、以下の点を確認します。

- ドメイン エントリと関連する MX レコードが存在すること
- MX レコードは IP アドレスに解決でき、各 MX レコードには関連付けられた動作しているメール サーバがあること

- CRES サーバはポート 25 で上記のメール サーバとの SMTP 接続を確立できること
- 上記の各メール サーバは STARTTLS 拡張をサポートすること
- 最後に、CRES サーバは MX レコードを提供する各メール サーバへの TLS 接続を正常に開始できること

セキュリティ保護された返信に TLS を使用するには、『*Cisco Email Encryption Compatibility Matrix*』の「Supported Certificate Authorities for CRES」セクションにリストされているいずれかの証明書によって署名されている証明書、またはその証明書に接続されている証明書を使用する必要があります。また、期限が切れていない証明書を使用する必要があります。証明書は、TLS 接続が作成されたときの日時が証明書の有効期間内でない場合に、期限が切れています。

ドメインの TLS テストは、合格、未確定（一部合格）、失敗という 3 つの考えられる結果のうち 1 つを生成します。

- 合格：MX レコード内のすべてのサーバでテストが合格した場合、ドメインは TLS テストに合格したと見なされます。TLS テストに合格するドメインは、TLS ドメインとして追加され、カスタマー サポートによる承認の待機中に、[Processing] ステータスを受け取ります。
- 未確定：少なくとも 1 つの関連付けられたメール サーバでテストが合格したものの、合格しなかったメール サーバがある場合、結果は未確定であると見なされます。未確定のドメインは、デフォルトで TLS ドメインとして追加されません。結果に表示される [Request Approval] ボタンをクリックして、未確定のドメインを追加できます。ドメインを追加すべきである理由を入力し、送信します。
- 失敗：ドメインに関連付けられたどのメール サーバも TLS をサポートしない場合、ドメインはテストに失敗しました。TLS テストに失敗したドメインは、TLS ドメインとして追加されません。

合格ドメインごとにカスタマー サポート チケットがオープンし、未確定ドメインの場合は承認要求がオープンします。ドメインが追加されたことを知らせる電子メール、またはドメインに関する詳細情報を要求する電子メールが送信されます。

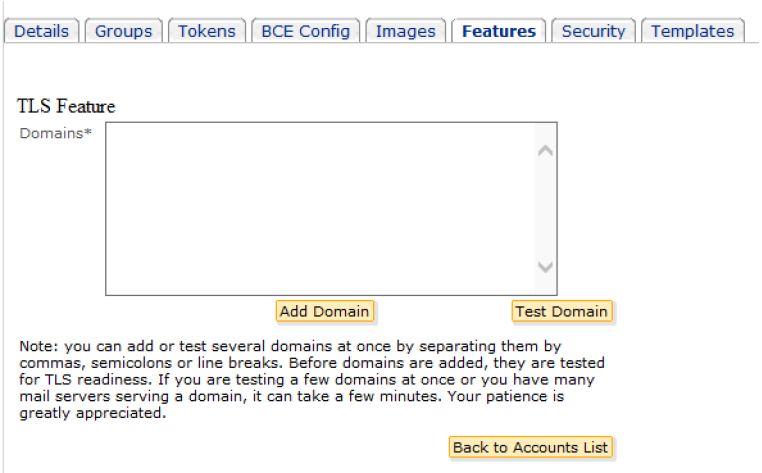
[Add Domain] ボタンではなく [Test Domain] ボタンを使用して、TLS ドメインのリストに追加せずにドメインをテストすることもできます。テストされるドメインに対してサポート要求はオープンしません。

TLS ドメインを追加またはテストするには、次の手順を実行します。

手順 1　[Accounts] タブで、[Manage Accounts] タブを選択します。

手順 2　アカウント番号をクリックして、[Features] タブを選択します。

図 2-12　[Account Management] ページの [Features] タブ



手順 3　ドメインを入力します。

a.　ドメインをテストするには、[Test Domain] をクリックします。

b.　ドメインを追加するには、[Add Domain] をクリックします。

手順 4　結果を示すメッセージが表示されます。

手順 5　追加されたドメインが合格すると、[Domain] リストに [Processing] ステータスで表示されます。

手順 6　ゴミ箱アイコンをクリックして、ドメインを削除します。

（注）　TLS エラー処理の動作の指定を忘れないでください。詳細については、「「TLS エラーの処理」(25 ページ)」を参照してください。

TLS エラーの処理

TLS 配信が動作を停止する場合（たとえば、期限切れの証明書が原因）、TLS エラー処理を設定する必要があります。「Bounce Messages」または「Fallback to Registered Envelope Delivery」を選択できます。

（注）　TLS 障害時の配信設定を「Fallback to Registered Envelope Delivery」に設定する場合は、社内メール サーバで TLS 配信オプションを TLS 優先に変更してください。

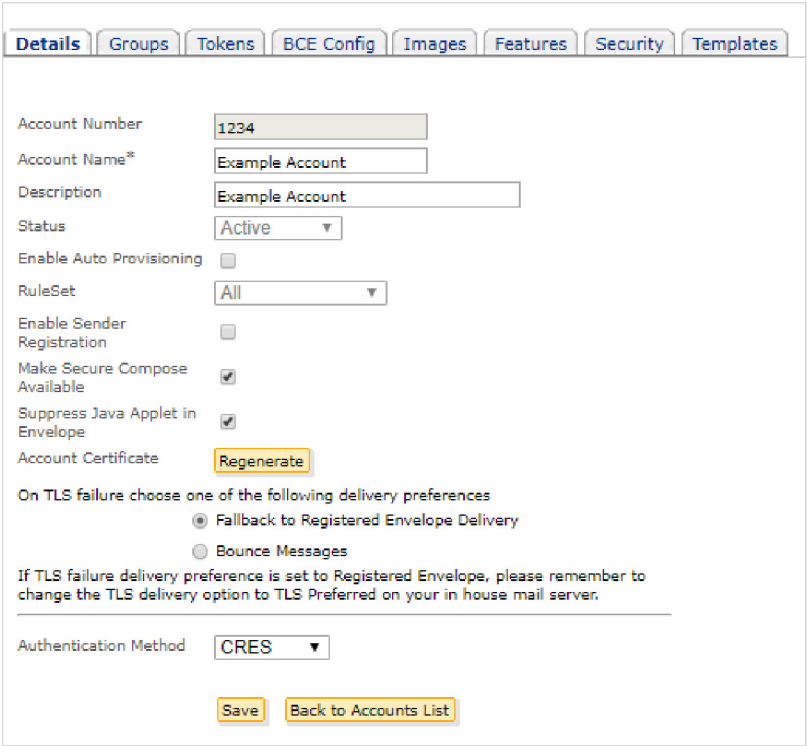
- [Fallback to Registered Envelope Delivery]：TLS 配信が失敗する場合（たとえば、期限切れの証明書が原因）システムは登録済みエンベロープの送信に戻ります。
- [Bounce Messages]：メッセージをバウンスするように設定されたアカウントの場合、TLS 配信が失敗すると、1 時間ごとに再試行され、24 時間後にバウンスが発生します。登録済みエンベロープにフォールバックするように設定されたアカウントの場合、20 分ごとに再試行され、1 時間後にフォールバックが発生します。

アカウントの TLS エラー処理の動作を指定するには、次の手順を実行します。

手順 1　[Accounts] タブで、[Manage Accounts] タブを選択します。

手順 2　アカウント番号をクリックして、[Details] タブを選択します。

図 2-13　[Account Management] ページ



手順 3　TLS 障害時の配信設定を選択します。

手順 4　[Save（保存）] をクリックします。

送信者の登録の有効化

アカウント単位で送信者の登録を自動的に提供するようにシステムを設定できます。これは、暗号化されたメールを送信するために現在 CRES を使用していない電子メール送信者に CRES アカウントを提供する場合にも役立ちます。登録すると、送信者は、暗号化されたメッセージを制御するために使用可能なオプションの詳細を確認できます。

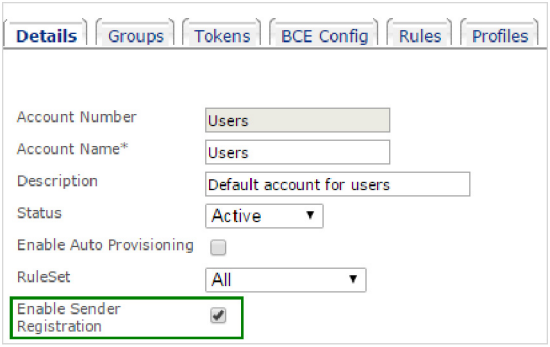
この機能を有効にすると、送信者は CRES サーバでアカウントを作成するために招待する電子メール メッセージを受信します。送信者は、これらの招待を 30 日ごとに受信しますが、招待に記載の手順に従って簡単にオプトアウトできます。招待の頻度は変更できません。

アカウントの送信者の登録を有効にするには、次の手順を実行します。

手順 1　[Accounts] タブで、[Manage Accounts] タブを選択します。

手順 2　アカウント番号をクリックして、[Details] タブを選択します。

図 2-14　　送信者の登録の有効化



手順 3　[Enable Sender Registration] チェック ボックスをオンにします。

手順 4　[Save（保存）] をクリックします。

Java アプレットの有効化

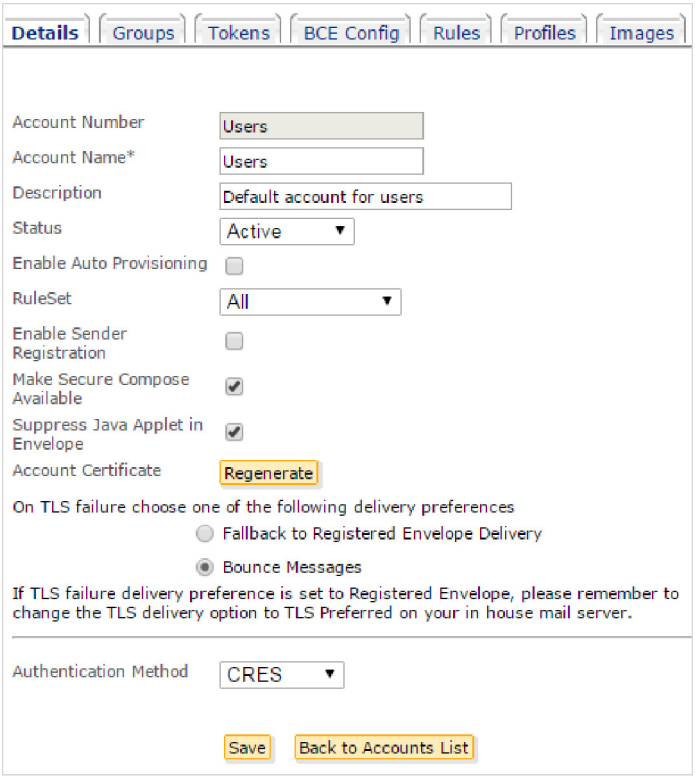
（注）　よく使用されているブラウザでは、セキュリティ上の理由により Java アプレットが無効になっています。

エンベロープ内でも、Java アプレットはデフォルトで無効になっています。Java アプレットを有効にするには、次の手順を実行します。

手順 1　[Accounts] タブで、[Manage Accounts] をクリックします。

手順 2　アカウント番号をクリックして、[Details] タブを選択します。

図 2-15　Java アプレットの有効化



手順 3　[Suppress Java Applet in Envelope] チェック ボックスをオフにします。

手順 4　[Save（保存）] をクリックします。

認証方法の選択

CRES には、3 つの異なるユーザ認証方法が用意されています。

- Google 認証
- CRES 認証
- SAML 認証

CRES に登録されている Google アカウントを持っている場合、[Sign-in with Google] ボタンをクリックすると Google 認証を使用して Websafe にログインできます。また、Google 認証を使用して、セキュリティで保護されたエンベロープを開くこともできます。詳細については、ソーシャル ネットワークの資格情報を使用してのエンベロープ開封（2-17 ページ）を参照してください。

認証プロセスの完全な制御を維持する場合は、CRES 認証を使用できます。

SAML はシングル サインオン（SSO）用の XML アプリケーションです。CRES における SAML 認証の実装方法の詳細については、SAML を使用した認証（2-30 ページ）を参照してください。

Cisco Web セキュリティ アプライアンスまたは PingFederate を SSO の SAML アイデンティティ プロバイダーとしてすでに使用している場合は、SAML ベースの認証を使用することもできます。詳細については、PingFederate ログアウト URL の設定（2-43 ページ）を参照してください。

CRES 認証と SAML 認証の詳細については、以下を参照してください。

- CRES アカウント認証の設定（2-30 ページ）
- SAML アカウント認証の設定（2-33 ページ）

CRES アカウント認証の設定

アカウントの CRES 認証を設定するには、次の手順を実行します。

手順 1　[Accounts] タブで、[Manage Accounts] タブを選択します。

手順 2　アカウント番号をクリックして、[Details] タブを選択します。

手順 3　[Authentication Method] リストで、[CRES] をクリックします。

手順 4　[Save（保存）] をクリックします。

SAML を使用した認証

SAML は、CRES など複数の Web サービスでエンド ユーザを認証するより簡単な方法であるシングル サインオン（SSO）で主に使用される、XML ベースの標準です。現在は、SAML 2.0 のみがサポートされます。

シングル サインオンでは、ユーザは（アイデンティティ プロバイダーに対して）認証を受けるために 1 回ログインします。その後は、再度ログインせずにサービス プロバイダーからのさまざまなサービスを使用します。このプロトコルは、シングル ログアウトもサポートします。

これにより、ユーザ エクスペリエンスが簡素化されます。また、ユーザは複数サービスのログイン詳細を覚えておく必要がなくなるため、セキュリティが向上します。CRES の SAML サポートは、新規および既存の CRES エンベロープで機能します。SAML 認証は、企業アカウントごとに個別に有効にする必要があります。これが完了したら、そのアカウントのすべてのユーザが SAML で認証される必要があります。そのアカウントが所有していないユーザは、引き続き CRES 認証を使用します。

SAML の概要

SAML では、異なるセキュアなネットワーク（セキュリティ ドメインとも呼ばれます）間で認証および許可データを交換できます。通常 SAML は、Web ブラウザを使用してネットワーク（別のドメイン）にアクセスするユーザが 1 つのドメインに存在する場合に使用されます。

シングル サインオンを実行するには、SAML ダイアログが次の用語を使用して各ドメインのエンティティによって組み込まれている必要があります。

- **アイデンティティ プロバイダー（IdP）。**アイデンティティ プロバイダーは SAML アサーションを生成するエンティティです。アイデンティティ プロバイダーは SAML アサーションを生成する前にエンド ユーザを認証します。CRES はほとんどの SAML 2.0 アイデンティティ プロバイダーと連携する必要があります。ただし、Cisco IronPort Web セキュリティ アプライアンス、Active Directory Federation Services（AD FS）、および PingFederate だけと連携することが認定されています。
- **サービス プロバイダー（SP）。**サービス プロバイダーは、SAML アサーションを消費するエンティティです。サービス プロバイダーはアイデンティティ プロバイダーを使用してエンド ユーザを識別し、その識別情報を SAML アサーションで受け取ります。サービス プロバイダーはこのアサーションに基づいてアクセス制御を決定します。SAML 認証が有効な場合、CRES はサービス プロバイダーとして機能します。

SAML アサーションは、アイデンティティ プロバイダーとサービス プロバイダー間の SAML 要求および応答で渡される情報のコンテナです。アサーションにはサービス プロバイダーがアクセス制御の決定に使用するステートメント（認証ステートメントや許可ステートメント）が含まれています。アサーションは <saml:Assertion> タグで始まります。

SAML ダイアログはフローと呼ばれ、フローはどちらのプロバイダーでも開始できます。

- **サービス プロバイダーが開始するフロー。**サービス プロバイダーは、アクセスを要求するエンド ユーザからの問い合わせを受け、アイデンティティ プロバイダーにそのユーザの識別情報を提供するように問い合わせて SAML ダイアログを開始します。サービス プロバイダーが開始するフローの場合、エンド ユーザは http://www.serviceprovider.com/ などのサービス プロバイダーのドメインを含む URL を使用してサービス プロバイダーにアクセスします。
- **アイデンティティ プロバイダーが開始するフロー。**アイデンティティ プロバイダーは、エンド ユーザに代わってサービス プロバイダーに問い合わせてアクセスを要求することで SAML ダイアログを開始します。アイデンティティ プロバイダーが開始したフローの場合、エンド ユーザは http://saas.example.com/ など、ローカル ドメインを含む URL を使用してサービス プロバイダーにアクセスします。

CRES は、サービス プロバイダーが開始するフローのみをサポートします。

（注）　このセクションは、SAML の包括的な説明を提供するものではなく、アイデンティティおよびセキュリティ プロバイダーが相互に通信する方法を示すものではありません。詳細については、http://saml.xml.org/wiki/saml-wiki-knowledgebase を参照してください。アイデンティティ プロバイダーとして Web セキュリティ アプライアンスを使用する詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』（リリース 7.0 以降）の章「Controlling Access to SaaS Applications」を参照してください。

要件

CRES をサービス プロバイダーとして SAML 認証を使用するには、次の要件を満たす必要があります。

- CRES では、Cisco IronPort Web セキュリティ アプライアンス、Active Directory Federation Services（AD FS）、または PingFederate のみを現在アイデンティティ プロバイダーとして使用できます。
- アイデンティティ プロバイダーの SAML ログイン メカニズムは、JavaScript なしで動作できる必要があります。
- アイデンティティ プロバイダーは、SAML 2.0 をサポートする必要があります。
- SAML アサーションでは、SAML NameID または属性に電子メール アドレスが含まれる必要があります。

注意事項

SAML 認証を使用するときの注意事項がいくつかあります。

- SAML は、企業アカウントごとに個別に有効にする必要があります。
- SAML のログイン ページは、CRES ではなく SAML アイデンティティ プロバイダーが提供します。これは、CRES ロギングは SAML のログインに使用できないこと、およびログインの問題は SAML アイデンティティ プロバイダーに報告する必要があることを意味します。
- パスワードを忘れた場合の回復やパスワードの変更など、ユーザ パスワードのメンテナンスは、CRES ではなく SAML 認証されたアカウントのユーザのアイデンティティ プロバイダー経由で実行される必要があります。
- アカウントが誤ってロックされないようにするため、SAML 認証は管理アカウント（管理者設定）に対して有効ではありません。

- CRES 認証されたアカウントとは異なり、SAML 認証されたアカウントを統合できません。
- Cisco IronPort Web セキュリティ アプライアンスがアイデンティティ プロバイダーとして使用される場合、ログイン ページが正しく機能するために JavaScript を有効にする必要があります。
- Cisco IronPort Web セキュリティ アプライアンスがアイデンティティ プロバイダーとして使用される場合、パスワードはキャッシュされず、ユーザはセッションごとに認証される必要があります。
- アイデンティティ プロバイダーに問題がある場合、SAML ユーザはクレデンシャルが有効であっても認証できないことがあります。
- アイデンティティ プロバイダーが完全に使用できなくなった場合は、認証方法を CRES に変更して、ユーザが認証されるようにする必要があります。
- 管理者は、アイデンティティ プロバイダーを使用して、SAML サービスに問題がある場合のアラートを提供します。
- エンド ユーザのクレデンシャルが有効であっても、アイデンティティ プロバイダーに問題がある場合はサービスにアクセスできない可能性があります。

ユーザ エクスペリエンス

SAML 認証のユーザ エクスペリエンスは、JavaScript が有効であるかどうか、1 人以上の受信者がいるかどうか、または受信者が BCC 受信者であるかどうかに関係なく、ほとんど同じです。ユーザはエンベロープ（またはモバイル デバイス サポート（MDS）リンク）を開き、自分のユーザ アイデンティティを選択するか必要に応じて電子メール アドレスを指定し、アイデンティティ プロバイダーを通じて認証されます。または、Web ブラウザで https://res.cisco.com に移動し、電子メール アドレスを入力し、アイデンティティ プロバイダーを使用して認証できます。

SAML アカウント認証の設定

次のうちいずれかのアイデンティティ プロバイダーを使用するように SAML 認証を設定できます。

- Active Directory Federation Services（AD FS）
- Cisco IronPort Web セキュリティ アプライアンス
- PingFederate

これらのアイデンティティ プロバイダーを使用するための設定手順は、次のセクションで説明します。

- AD FS をアイデンティティ プロバイダーとして使用する場合の SAML アカウント認証の設定（2-34 ページ）
- Cisco Ironport Web セキュリティ アプライアンスまたは PingFederate をアイデンティティ プロバイダーとして使用する場合の SAML アカウント認証の設定（2-40 ページ）

AD FS をアイデンティティ プロバイダーとして使用する場合の SAML アカウント認証の設定

SAML 認証を有効にするときは、AD FS アカウントの設定に合わせて CRES アカウントを設定することが重要です。

次の情報（AD FS における同等の情報）が必要です。

- サービス プロバイダーのエンティティ ID（SaaS アプリケーション名または接続 ID）
- カスタマー サービス URL（シングル サインオン URL/ベース URL）
- アイデンティティ プロバイダーの検証証明書
- （オプション）代替の電子メール属性名（SAML 属性または電子メール アドレス）

AD FS をアイデンティティ プロバイダーとして使用する場合の SAML アカウント認証の手順は、次のセクションで説明します。

- AD FS のリレー側の信頼の設定
- 請求ルールの設定
- AD FS の SAML アサーション コンシューマ エンドポイントの追加
- AD FS から署名証明書のエクスポート
- CRES の設定
- AD FS 署名の設定
- SAML ログインの有効化
- LDAP クレデンシャルを使用した Web Safe へのログイン

AD FS のリレー側の信頼の設定

手順 1　AD FS 2.0 Management ツールを起動します。

手順 2　[Add] をクリックします。

手順 3　[Welcome] 画面で、[Start] をクリックします。

手順 4　[Enter data about the relying party manually] を選択し、[Next] をクリックします。

手順 5　CRES SP の表示名を入力し、[Next] をクリックします

手順 6　[AD FS 2.0 profile] を選択し、[Next] をクリックします。

手順 7　[Enable support for the SAML 2.0 Web SSO protocol] を選択します。

手順 8　[Relying party SAML 2.0 SSO service URL] で「https://res.cisco.com/websafe/ssourl」と入力し、[Next] をクリックします。

手順 9　[Relying party trust identifier] で「https://res.cisco.com/」と入力し、[Add] をクリックします。

手順 10　[Next] をクリックします。

手順 11　[Permit all users to access this relying party] を選択し、[Next] をクリックします。

手順 12　設定を確認し、[Next] をクリックします。

手順 13　[Open the Edit Claim Rules dialog for this relying party trust when the wizard closes] を選択し、[Close] をクリックします。

請求ルールの設定

手順 1　[Edit Claim Rules for CRES SP] ダイアログが開いたら、[Issuance Transform Rules] タブを選択し、[Add Rule] をクリックします。

手順 2　[Claim rule template] で [Send LDAP Attributes as Claims] を選択し、[Next] をクリックします。

手順 3　[Claim rule name] を入力します。

手順 4　[Attribute store] で、[Active Directory] を選択します。

手順 5　[LDAP Attribute] 列で、[User-Principal-Name] または [E-Mail Addresses] を選択します。

推奨値は [User-Principal-Name] です。これは、Active Directory カタログ内のすべてのユーザに使用できます。SAML 認証中、CRES は Active Directory でのユーザ名とユーザの CRES アカウントとを比較します。

[E-Mail Addresses] 値を使用するには、[User's Properties] 設定の [General] タブにある [E-mail] フィールドに電子メール アドレスを入力する必要があります。CRES では Active Directory 内のユーザのアカウントから電子メール アドレスを取得するので、オプションの [E-mail] フィールドがすべてのユーザに対して正しく設定されていない場合はエラーが発生します。

手順 6　[Outgoing Claim Type] 列で、[E-Mail Addresses] を選択します。

手順 7　[Finish] をクリックし、[Add Rule] をクリックします。

手順 8　[Claim rule template] で [Transform an Incoming Claim] を選択し、[Next] をクリックします。

手順 9　[Claim rule name] を入力します。

手順 10　[Incoming claim type] で [E-mail Address] を選択します。

手順 11　[Outgoing claim type] で [Name ID] を選択します。

手順 12　[Outgoing name ID format] で [Transient Identifier] を選択します。

手順 13　[Pass through all claim values] を選択します。

手順 14　[Finish] をクリックします。

AD FS の SAML アサーション コンシューマ エンドポイントの追加

手順 1　[Relying Party Trusts] で、追加された [Relying Party Trust] を選択します。

手順 2　右ペインで、[Properties] を選択します。

手順 3　[Endpoints] タブで、[Add] をクリックします。

手順 4　[Endpoint Type] で [SAML Assertion Consumer] を選択します。

手順 5　[Binding] で [POST] を選択します。

手順 6　[Index] で [1] を選択します。

手順 7　[URL] で「https://res.cisco.com/keyserver/saml/saml-resp」と入力し、[OK] をクリックします。

手順 8　[OK] をクリックします。

ADFS から署名証明書のエクスポート

手順 1　AD FS 2.0 Management ツールを起動します。

手順 2　左側のペインで、[AD FS 2.0] > [Service] > [Certificates] を選択します。

手順 3　[Token-signing certificate] を選択します。

手順 4　右側のペインで、[View Certificate] をクリックします。

手順 5　[Details] タブで、[Copy to File] をクリックします。

手順 6　[Welcome to the Certificate Export Wizard] 画面で、[Next] をクリックします。

手順 7　エクスポート ファイル形式について [DER excoded binary X .509 (.CER)] を選択し、[Next] をクリックします。

手順 8　エクスポート ファイルの場所とファイル名を入力し、[Next] をクリックします。

手順 9　[Finish] をクリックします。

CRES の設定

手順 1　管理者アカウントのクレデンシャルを使用して CRES にログインします。

手順 2　[Accounts] タブで、[Manage Accounts] タブを選択します。

手順 3　アカウント番号をクリックして、[Details] タブを選択します。

手順 4　[Authentication Method] で、[SAML 2.0] を選択します。

手順 5　[SSO Alternate Email Attribute Name] で、空白のままにします。

手順 6　[SSO Service Provider Entity ID] で「https://res.cisco.com/」と入力します。

手順 7　[SSO Customer Service URL] で、「https://*AD FS*/adfs/ls」と入力します。

手順 8　[SSO Logout URL] で、「https://*AD FS*/adfs/ls」と入力します。

手順 9　[Verification Certificate] で [Browse] をクリックし、AD FS 設定からエクスポートされた署名証明書をアップロードします。

手順 10　[Save] をクリックします。

手順 11　ページを保存したら、[Download] をクリックして CRES 署名証明書をダウンロードします。

AD FS 署名の設定

手順 1　AD FS 2.0 Management ツールを起動します。

手順 2　左側のペインで、[AD FS 2.0] > [Trust Relationships] > [Relying Party Trusts] を選択します。

手順 3　自分のリレー側（CRES SP）を選択し、右側のペインで [Properties] をクリックします。

手順 4　[Signature] タブを選択し、[Add] をクリックし、CRES 管理ページからダウンロードされた CRES 署名証明書を選択します。

手順 5　[Advanced] タブを選択します。

手順 6　[Secure hash algorithm] で [SHA-1] を選択し、[OK] をクリックします。

手順 7　AD FS Management ツールによって、Internet Information Services（IIS）に /adfs/ls Web サイトが作成されます。

手順 8　Server Manager Tool を起動します。

手順 9　左側のペインで、[Server Manager] > [Roles] > [Web Server (IIS)] > [Internet Information Services (IIS) Manager] を選択します。

手順 10　[Connections] ペインで、使用するサーバ > [Sites] > [Default Web Site] > [adfs] > [ls] を選択します。

手順 11　[/adfs/ls Home] ペインで、[IIS] の下にある [Authentication] を選択します。

手順 12　[Anonymous Authentication] を有効にし、その他を無効にします。

手順 13　[Connections] ツリーの [ls] を右クリックし、[Explore] をクリックします。

手順 14　web.config ファイルを右クリックし、[Edit] をクリックします。

手順 15　「localAuthenticationTypes」セクションを検索し、<add name="Forms" page="FormsSignIn.aspx" /> 以外のすべてのエントリを削除します。

これにより、Windows 統合認証の代わりにフォーム認証のみが許可されます。

手順 16　ファイルを保存して、閉じます。

SAML ログインの有効化

手順 1　[Accounts] タブの [Manage Accounts] タブを選択して、[CRES Account] ページに戻ります。

手順 2　アカウント番号をクリックして、[Details] タブを選択します。

手順 3　ページ下部の [Activate SAML] をクリックします。

手順 4　[Continue] をクリックします。

手順 5　ドメイン ユーザ名とパスワードを入力し、[Sign In] をクリックします。

手順 6　[Continue] をクリックして続行します。

手順 7　[Continue] をクリックして、ウィンドウを閉じます。

手順 8　[CRES Account Details] ページの上部にメッセージ「SAML Activated Successfully」が表示されることを確認します。

手順 9　[SSO Enable Date] が現在の時刻に設定されていることを確認します。

手順 10　SAML 2.0 がアカウントの認証方法として選択されていることを確認します。

LDAP クレデンシャルを使用した Web Safe へのログイン

手順 1　Web Safe https://res.cisco.com/websafe/root に移動します。

手順 2　AD FS 認証ページにリダイレクトされることを確認します。

手順 3　Active Directory ユーザおよびパスワードを入力します。

手順 4　[Sign In] をクリックします。

手順 5　Web Safe に正常にログインしたことを確認します。

手順 6　同じドメイン内の任意のユーザにメッセージを送信します。

手順 7　そのユーザが受信した暗号化された電子メールを開きます。

手順 8　Active Directory のクレデンシャルを入力できるように新しいウィンドウが開くことを確認します。

手順 9　Active Directory のクレデンシャルを入力します。

手順 10　エンベロープが復号化されることを確認します。

Cisco Ironport Web セキュリティ アプライアンスまたは PingFederate をアイデンティティ プロバイダーとして使用する場合の SAML アカウント認証の設定

SAML 認証を有効にするときは、アイデンティティ プロバイダー アカウントの設定に合わせて CRES アカウントを設定することが重要です。

次の情報（Cisco Ironport Web セキュリティ アプライアンスまたは PingFederate における同等の情報）が必要です。

- サービス プロバイダーのエンティティ ID（SaaS アプリケーション名または接続 ID）
- カスタマー サービス URL（シングル サインオン URL/ベース URL）
- アイデンティティ プロバイダーの検証証明書
- （オプション）代替の電子メール属性名（SAML 属性または電子メール アドレス）

アイデンティティ プロバイダーとして Cisco Web セキュリティ アプライアンスを使用している場合、この情報は [SaaS Application Authentication Policies] ページで参照できます。証明書は、[Edit Identity Provider Settings for SaaS Single Sign On] ページからダウンロードできます。

アイデンティティ プロバイダーとして PingFederate を使用している場合、この情報は [Summary] 領域で参照できます。

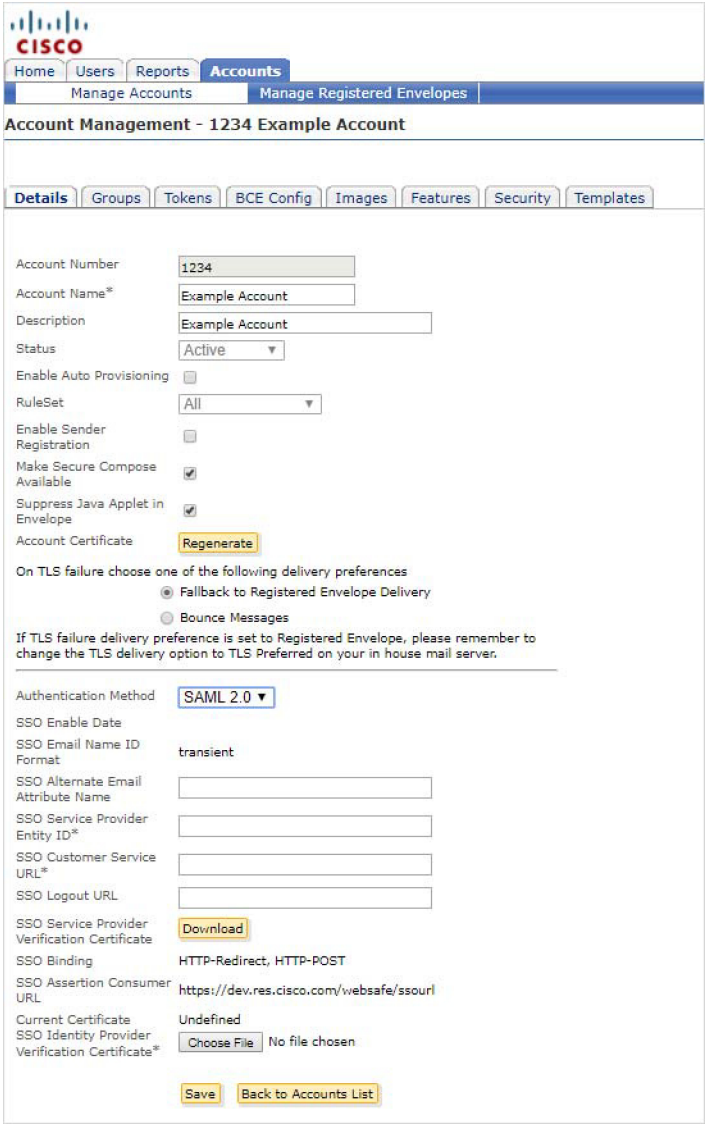
（注） IDP として PingFederate を設定するときは、エンドポイントとして CRES Assertion Consumer Service の URL を指定する必要があります。また、ユーザがログアウトするために SSO ログアウト URL を設定する必要があります。この設定の詳細については、「PingFederate ログアウト URL の設定」（43 ページ）を参照してください。

アカウントの SAML 認証を設定するには、次の手順を実行します。

手順 1　[Accounts] タブで、[Manage Accounts] タブを選択します。

手順 2　アカウント番号をクリックして、[Details] タブを選択します。

図 2-16　　認証方法の選択



手順 3　[Authentication Method] ドロップダウン リストで、[SAML 2.0] を選択します。[SSO Enable Date]（SAML が正常に設定および有効化された最終日）が表示されます。[SSO Email Name ID Format] が表示されます。現在は、一時 SAML 名前形式だけがサポートされます。

手順 4　[SSO Alternate Email Attribute Name] を入力します。これは、名前識別子として使用される代替電子メール アドレスが含まれる属性名です。

手順 5　[SSO Service Provider Entity ID] フィールドで、サービス プロバイダーのエンティティ ID を入力します。

手順 6　[SSO Customer Service URL] を入力します。これは、SAML アイデンティティ プロバイダーのシングル サインオン URL です。

手順 7　[SSO Logout URL] を入力します。これは、SAML アイデンティティ プロバイダーのログアウト URL です。

シングル サインオンのバインディング（通常は [HTTP-Redirect] または [HTTP-POST]）が SSO Assertion Consumer の URL と共に表示されます。

手順 8　（オプション）[Download] をクリックして、SSO サービス プロバイダーの検証証明書のコピーをダウンロードします。これは CRES からの SAML ログアウト要求の署名を検証するためにアイデンティティ プロバイダー（IdP）で必要な公開自己署名証明書です。

手順 9　[Browse] をクリックし、SAML アイデンティティ プロバイダー（Cisco Web セキュリティ アプライアンスまたは PingFederate）から提供される SSO アイデンティティ プロバイダーの検証証明書を選択してアップロードします。現在の証明書が表示されます。

手順 10　[Save（保存）] をクリックします。

手順 11　[Activate] をクリックします。

（注）　詳細を保存したら、SAML ログインを有効化する必要があります。これにより、設定エラーが原因で誤ってユーザをロックアウトすることがなくなります。

PingFederate ログアウト URL の設定

IDP として PingFederate で設定されたエンベロープからログアウトするには、PingFederate でログアウト URL を設定する必要があります。これは、エンド ユーザが CRES から完全にログアウトするにはログアウト ボタンをクリックする必要があるため、非常に重要です。

PingFederate でログアウト URL を設定するには、次の手順を実行します。

手順 1　アカウントの [CRES Account Management] 画面で、公開証明書をダウンロードして保存します。

手順 2　アカウントの PingFederate サーバで、[Signature Verification Certificate] をクリックします。

手順 3　[Manage Certificates] をクリックします。

手順 4　手順 1 で保存した証明書をインポートします。

手順 5　インポートした証明書がプライマリ証明書であることを確認します。

（注）　PingFederate では、SAML ログアウト要求を確認するときに複数の公開証明書を使用できます。その結果、CRES から公開証明書をダウンロードした後、この証明書が PingFederate で 1 番めの、つまりプライマリ証明書であることを確認する必要があります。

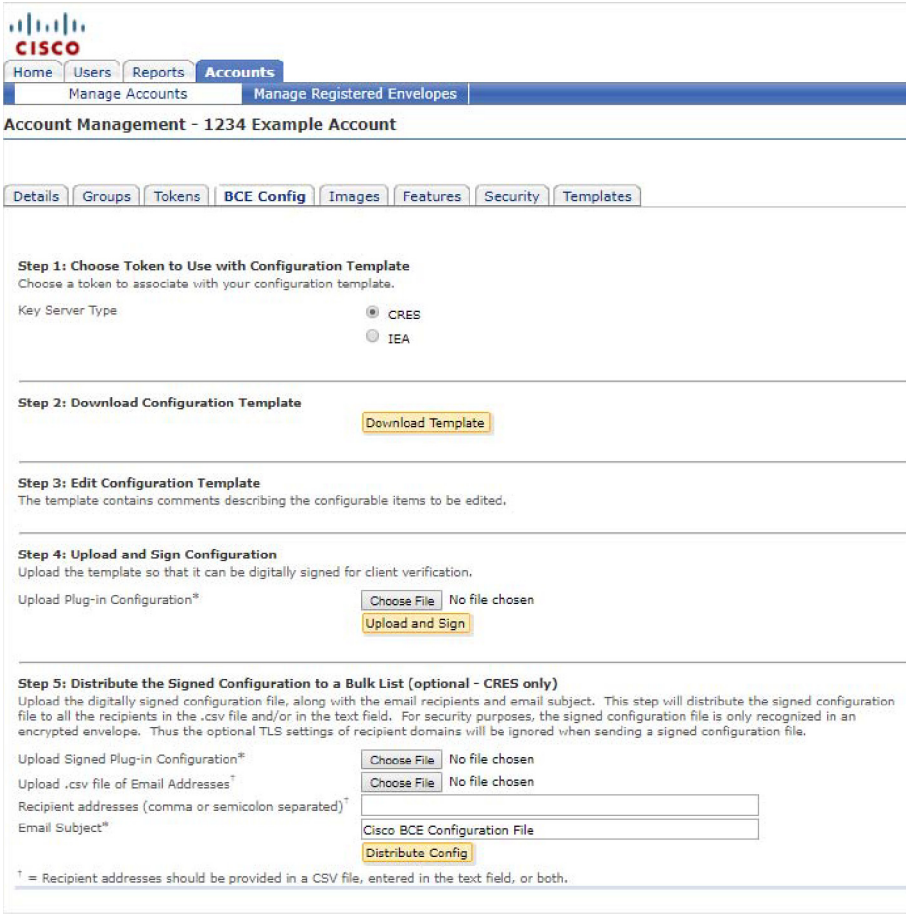
BCE プラグインまたはモバイル アプリケーション設定の構成

ビジネス クラス電子メール（BCE）プラグインまたはモバイル アプリケーションを導入するには、各ユーザに署名済み設定ファイルを送信する必要があります。これらの手順を実行するには、アカウント管理者である必要があります。

BCE 設定ファイルに署名して導入するには、[Accounts] タブに移動し、BCE プラグインを有効にするアカウントを選択します。次に、[BCE Config] タブに移動し、以下の手順に従います。

（注）　キー サーバとして Cisco IronPort アプライアンスを使用する場合は、開始する前に、Cisco IronPort 暗号化アプライアンスからトークンをダウンロードする必要があります。

図 2-17　　[BCE Configuration] タブ



手順 1　設定テンプレートで使用するトークンを選択します。

キー サーバとして CRES を使用する場合は、CRES トークンを選択します。Cisco IronPort アプライアンスを使用する場合は、ローカル マシンにダウンロードした IEA トークンに移動し、アップロードします。

手順 2　テンプレート ファイルを編集するためにダウンロードします。

手順 3　コンフィギュレーション ファイルを編集します。

BCE_Config.xml ファイルには、特定の環境に合わせて編集する必要があるフィールドの詳細が含まれています。テキスト エディタでファイルを開き、コメントに記載されている手順に従って必要な変更を行います。

手順 4　[Browse] をクリックして BCE_Config.xml ファイルを探し、ファイルが見つかったら [Upload and Sign] をクリックします。設定ファイルに署名すると、BCE_Config_signed.xml として表示されます。このファイルをローカル マシンに保存します。

署名済み設定ファイルを個々のエンド ユーザに導入するには、次の手順を実行します。

a. 暗号化された電子メールを作成し、その暗号化された電子メールに BCE_Config_signed.xml ファイルを添付します。

b. 次に、BCE（ビジネス クラス電子メール）を有効にするすべてのエンド ユーザにこの電子メールを送信します。

（注）　電子メールの送信者は、BCE_Config.xml ファイルに署名したアカウント管理者と同じである必要があります。メーリング リスト宛てに BCE_Config_signed.xml ファイルを送らないでください。CRES はメーリング リストに対応していません。

手順 5　（オプション）署名済み設定ファイルを一括リストに送信するには、次の手順を実行します。

（注）　次の一括配布方法は、CRES 管理者のみが利用できます。IEA 管理者が署名済み *BCE_Config_signed.xml* ファイルをユーザに適切に配布するために、IEA 管理者の電子メール アドレスから送信される暗号化された電子メールにこのファイルを添付する必要があります。

a. [Browse] をクリックし、エンド ユーザに送信する *BCE_Config_signed.xml* ファイルに移動します。

b. [Browse] ボタンをクリックして BCE を有効にする電子メール アドレスの .csv ファイルに移動します。または、カンマまたはセミコロンで区切られた電子メール アドレスのリストを手動で入力します。

c. デフォルトで、[Email Subject] は [Cisco BCE Configuration File] です。変更するには、このフィールドに新しいテキストを入力します。

d. [Distribute Config] をクリックして、電子メール アドレスのリストに BCE_Config_signed.xml ファイルを送信します。

（注）　セキュリティ上の理由で、BCE_Config_signed.xml ファイルは暗号化エンベロープでのみ認識されます。そのため、受信者ドメインのオプションの TLS 設定は、BCE_Config_signed.xml ファイルの送信時に無視されます。

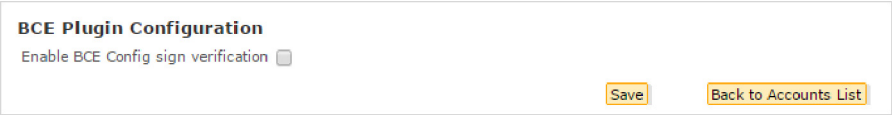
BCE Config による署名検証の有効化

BCE Config による署名検証を有効化して、ユーザが BCE Config ファイルの編集または変更を行った後でも BCE Config ファイルが確実にセキュリティで保護されるようにできます。

BCE Config による署名検証を有効にするには、次の手順を実行します。

手順 1　[Accounts] タブで、[Manage Accounts] タブを選択します。

手順 2　アカウント番号をクリックして、[Security] タブを選択します。



手順 3　[Enable BCE Config sign verification] チェック ボックスを選択します。

手順 4　[Save（保存）] をクリックします。

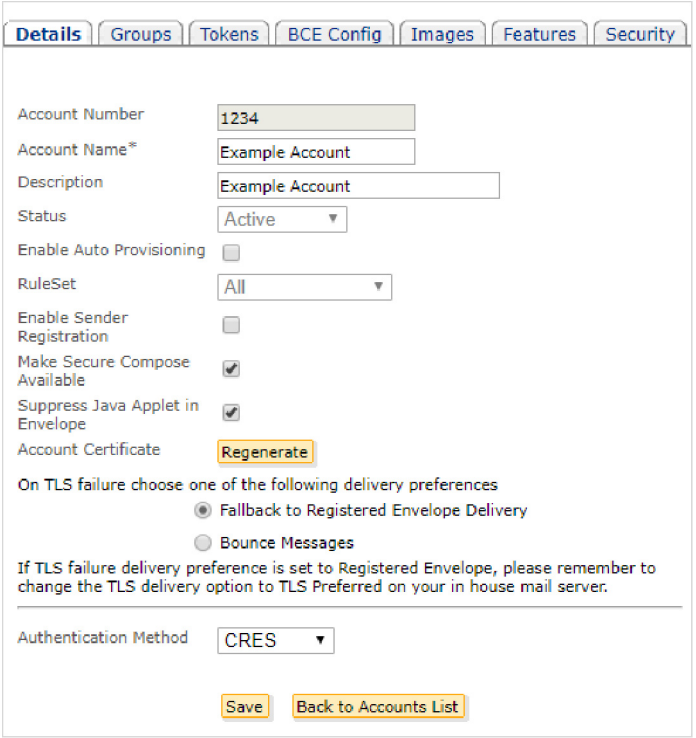
Secure Compose へのアクセスの無効化と有効化

この機能を使用すると、ユーザが Secure Compose を介して電子メールを送信することを制限できます。そのため、スキャンまたはアーカイブできずセキュリティの問題や企業ポリシーの違反が発生する可能性がある Secure Compose からの電子メールを制御できます。

Secure Compose を無効にすると、自分のアカウントのユーザのエンド ユーザ ポータルで、左側のナビゲーション メニューから [Compose Message] リンクが削除されます。

アカウントに関連付けられたドメイン内のユーザについてのみ Secure Compose を無効にできます。ドメインをアカウントに関連付けるには、カスタマー サポートに連絡してください。

図 2-18　　Secure Compose へのアクセスの無効化



手順 1　[Accounts] タブで、[Manage Accounts] タブを選択します。

手順 2　アカウント番号をクリックして、[Details] タブを選択します。

手順 3　Secure Compose へのアクセスを有効にするには、[Make Secure Compose Available] チェック ボックスを選択します。

手順 4　Secure Compose へのアクセスを無効にするには、[Make Secure Compose Available] チェック ボックスを選択解除します。

手順 5　[Save（保存）] をクリックします。

（注）　アカウントの [Tokens] タブに表示される SecureCompose トークンは、内部的に使用され、変更できません。そのトークンを変更または削除しても、Secure Compose は無効に*なりません*。Secure Compose を無効にするには、上記の手順を使用します。

CRES を含めるような DNS の設定

Sender Policy Framework（SPF）検証の失敗を回避するには、mx:res.cisco.com、mxnat1.res.cisco.com、mxnat3.res.csico.com を SPF レコードに追加する必要があります。

CRES を SPF レコードに追加する位置と方法は、ドメイン ネーム システム（DNS）がネットワーク トポロジでどのように実装されているかによって異なります。詳細については、DNS 管理者にお問い合わせください。

CRES を含めるように DNS が設定されていない場合、Secure Compose とセキュリティ保護された返信が生成され、ホステッド キー サーバを介して配信されると、発信 IP アドレスは受信者側でリストされている IP アドレスと一致せず、SPF 検証が失敗します。

CHAPTER 3

レポート

この章では、次の内容について取り上げます。

レポーティングの概要

レポート機能は、検索条件を入力するだけで目的のレポートを生成できる、使いやすいインターフェイスを備えています。選択したレポートは、スプレッドシートまたは PDF 形式でダウンロードできます。レポート機能にアクセスするには、[Reports] タブをクリックします。

利用可能なレポートは次のとおりです。

- **User Information レポート。**アカウントに関連付けられたユーザのリストを表示します(シーケンス番号(#)、ユーザ ID、電子メール アドレス、名、姓、ステータス、作成日、最終ログイン日、最終変更日などを含む)。ただし、1 つ以上のドメインがアカウントに関連付けられている場合に限ります。
- **Users Status レポート。**ドメインに関連付けられたユーザのステータス([New]、[Active]、[Blocked])を示します。
- **Account Usage レポート。**企業アカウントの使用状況の統計情報を表示するには、このレポートを実行します。Account Usage レポートの詳細については、「Account Usage レポート」(2 ページ)を参照してください。

User Information レポートおよび User Status レポートは、通常、システム管理者が使用します。これらのレポートは、ドメイン(およびユーザ)がアカウントに関連付けられている場合だけです。

Account Usage レポート

Account Usage レポートは、特定のアカウントの使用状況情報を表示します。データはトークンでグループ化され、送信メッセージとメッセージ数のリストが含まれます。トークンとは、Cisco E メール セキュリティ アプライアンス（ESA）と CRES（またはローカル キー サーバ）との間でデータを暗号化するために使用されるお客様固有のキーで、カスタマー サポートでのみ使用されます。

（注）　通常、組織のアカウント管理者は、単一の企業アカウントを管理します。

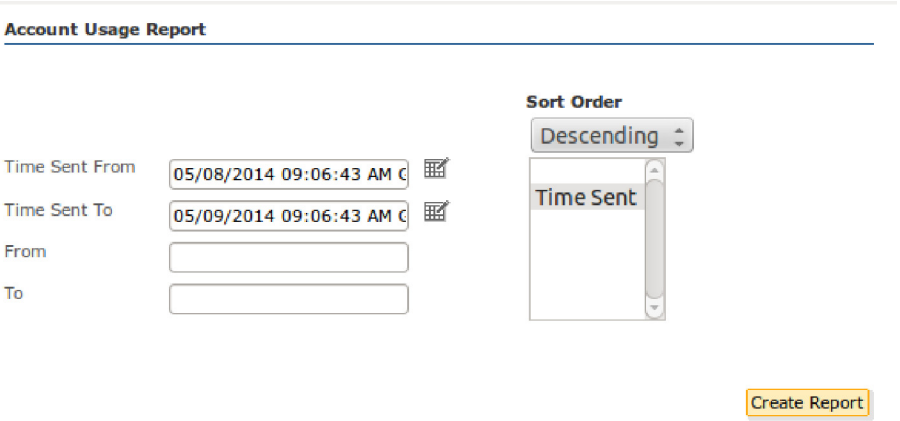
Account Usage レポートを生成するには、次の手順を実行します。

手順 1　[Reports] タブをクリックして、[View Reports] ページにアクセスします。

手順 2　[Account Usage Report] リンクをクリックします。

[Account Usage Report] ページが表示されます。

図 3-1　Account Usage Report



手順 3　レポート データの時間範囲を入力するか選択します。

手順 4　送信者や受信者の電子メール アドレスなど、オプションの検索条件を入力します。

手順 5　レポート データのソート順を選択します。

手順 6　レポートデータに含める列を選択します。値を選択し、列を含める場合は [Add to sort] を、列を除外する場合は [Remove from sort] をクリックします。

手順 7　[Create Report] をクリックします。

レポートの生成後、PDF またはスプレッドシート形式でレポート情報をダウンロードできます。また、レポートの Web ページをブックマークしたり印刷したりできます。

CHAPTER 4

キーの作成に必要なデータの IEA から CRES への移行

この章の内容は、次のとおりです。

キーの作成に必要なデータの IEA から CRES への移行について

Cisco IronPort 暗号化アプライアンス（IEA）の既存のインストールがあり、ローカル キー サーバとして IEA を使用する代わりにキーの作成と管理に Cisco Registered Envelope Service（CRES）を使用する場合は、移行手順を実行する必要があります。

推奨される方法は、エンド ユーザが自分の古いエンベロープを引き続き開封でき、再登録する必要がないように、IEA から CRES にすべての既存のユーザおよびキー データをコピーすることです。これを行うため、CRES では IEA 用にデータ移行クライアント、および CRES 用にデータ インポートサービスを提供します。これらのユーティリティでは既存のハードウェアを使用し、インフラストラクチャに対する変更は必要ないため、ロード バランシングおよびフェールオーバーなどの既存の機能を利用し続けることができます。

デフォルトでは、移行クライアントはデータの移行でパスを 1 回実行します。複数のパスを実行するようにクライアントを設定できます。移行クライアントは、すでに送信済みのレコードを追跡し、CRES によってすでに受信済みのデータは再送信しません。

IEA レコードが移行されると、IEA から CRES にトラフィックがリダイレクトされるように、いくつかの手順を実行する必要があります。その手順については次のセクションで詳しく説明しますが、以下のとおりです。

1. エンド ユーザからの HTTP トラフィックを IEA ではなく HTTP プロキシにリダイレクトするように設定します。
2. エンド ユーザが IEA で使用される証明書の代わりにプロキシを使用する HTTP トラフィックで信頼できる既存または新規の SSL 証明書を使用するように HTTP プロキシを設定します。『*Cisco Email Encryption Compatibility Matrix*』の「Supported Certificate Authorities for CRES」セクションにリストされているいずれかの証明書によって署名されている証明書、またはその証明書に接続されている証明書を使用する必要があります。
3. CRES との信頼された HTTP 通信に SSL 証明書を使用するようにプロキシを設定します。
4. IEA へのすべての HTTP トラフィックを代わりに HTTP プロキシにリダイレクトするように DNS サーバおよびファイアウォールのルールを更新します。
5. すべての暗号化アプライアンスとクライアントでトークンを更新します。
6. IEA を無効にします。
7. 電子メール ドメインと CRES のアカウントを関連付けます。

スイッチオーバー プロセスはすぐに実行されないため、一部の IEA クライアントは IEA を使用し続ける可能性があります。そのため、CRES へのミラーリングが必要なデータベースの更新が発生する可能性があります。更新されたデータを定期的に確認し、CRES に更新されたデータを移行するようにデータ移行クライアントを設定できます。

CRES 管理者は、特定のアカウントのキーのインポートを許可し、データをインポートできる期間を指定する単純なポリシーを設定できます。

移行プロセスは IEA から CRES にユーザ データと保留中のユーザ アクティビティをコピーします。ただし、移行データにはユーザ ロールまたは権限データが含まれず、移行プロセスはアカウント管理者またはアカウントに属している他のユーザの CRES 権限を変更しません。このため、ユーザの権限は CRES 上のアカウント管理者の権限にアップグレードされません。ただし、ユーザがすでにアカウント管理者権限を持つ場合、そのアクセス権は IEA でのステータスに関係なく削除されません。移行後、ユーザは通常の方法でアカウント管理者にアップグレードできます。

キーの作成に必要なデータを IEA から CRES に移行する方法

移行の前提条件

CRES に移行する前に、次の前提条件を満たす必要があります。

- CRES に移行後もサポートされない既存の機能を使用する必要がないことを確認します。これらの機能の詳細と例については、「CRES でサポートされない機能」セクション（4-5 ページ）を参照してください。移行プロセスを開始するようにシスコ テクニカル サポートに連絡するときに、状況を説明します。
- 移行担当者がデータベース管理者であるか、またはデータベース管理者にアクセスして支援できることを確認します。
- HTTP プロキシとして使用できるマシン、および HTTP プロキシを実行するために必要なソフトウェアがあることを確認します。
- Cisco IEA ソフトウェアをバージョン 6.5.6.1 にアップグレードする必要があります。

- CRES アカウントがない場合は、stg-cres-provisioning@cisco.com に電子メールを送信し、以下の情報を提供します。
  - アカウントの名前:通常は、会社名です。ホストされたカスタマーの場合、アカウント名は「Company Name ‹ HOSTED」です。
  - アカウント管理者に使用されるカスタマーのメール アドレス
  - 暗号化を行う ESA アプライアンスのシリアル番号
- シスコ カスタマー サポート担当者(iea-migrations@cisco.com)に連絡して以下の情報を提供し、移行プロセスを開始します。
  - CRES のアカウント番号。CRES アカウントがない場合は、前述の前提条件の説明に従って、アカウントを作成するようにシスコに依頼してください。
  - 移行を開始する日付。実際に移行を実行する少なくとも 30 日前にシスコに連絡してください。

  シスコ カスタマー サポート担当者は:
  - 移行を可能にするようにアカウントを設定します。
  - 移行の開始日時と終了日時を設定します。
  - アカウントの詳細と移行ソフトウェアへのリンクが記載された電子メールを送信します。
  - セキュリティで保護されたエンベロープでセキュリティ キーを使用して電子メールを送信します。
- シスコ カスタマー サポート担当者から送信される電子メールの指示に従って、次のインストール スクリプトをダウンロードします。
  - cres-dbmigrate_install-4.5.1.xxx.sh
- 次のコマンドを実行して、コンソールに出力された SHA1 ダイジェストとダウンロード サイトに示されている SHA1 ダイジェストとを比較することにより、インストール スクリプトが正常にダウンロードされたことを検証します。

  openssl dgst -SHA1 cres-dbmigrate_install-4.5.1.xxx.sh
- 後述する手順の最初の 2 つのステップに従って、以下の項目を取得します。
  - token.jar
  - セキュリティ キー(移行のスケジュール後にセキュリティ保護されたエンベロープで電子メール送信)

- PostgreSQL を使用してデータベースを管理している場合、後述する手順 4 でデータベース変更スクリプトを実行するために、PL/pgSQL がインストールされている必要があります。

CRES でサポートされない機能

CRES に移行した場合、Cisco Ironport 暗号化アプライアンス（IEA）の代わりに Cisco E メール セキュリティ アプライアンスを使用する必要があります。CRES はホステッド サービスであるため、IEA などのローカル キーサーバが提供する一部の機能をサポートできません。したがって、CRES に移行する前に、CRES でサポートされていない IEA の機能が必要ないことを確認する必要があります。

CRES に移行できるかどうかを確認できるように、IEA で広く使用されている機能のうち CRES で現在利用できないものの例を次のリストに示します。

- Oracle データベース：Oracle を使用する IEA は、現在移行の対象ではありません。今後のリリースでサポートされる予定です。
- セキュリティ保護されたメールボックス
- LFS（容量の大きいファイルのサポート）
- ステートメントの配信
- 一部の認証方法：CRES のローカル データベースおよび SAML（カスタマー所有の電子メール ドメインの場合のみ）で登録されたユーザは、CRES で使用可能な唯一の認証方法です。LDAP や Kerberos などその他の IEA 認証方法はサポートされません。また、複数ソースの認証ルックアップ（チェーン化ルックアップ）はサポートされません。

IEA 機能の詳細については、『*Cisco Ironport Encryption Appliance 6.5 Configuration Manual*』を参照してください。

移行手順

IEA から CRES に移行するには：

手順 1　token.jar ファイルをローカル ドライブに保存します。

a. CRES に管理者としてログインし、[Accounts] タブを選択します。

b. [Manage Accounts] タブを選択します。

c. カスタマー アカウント マネージャのアカウントを選択します。

d. [Tokens] タブを選択します。

e. トークンの表で SecureCompose トークンの [Actions] 列の下にあるダウンロード アイコンをクリックします。

手順 2 セキュリティ キーは、移行のスケジュール後にセキュリティ保護されたエンベロープでシスコ テクニカル サポートから電子メール送信されます。

手順 3 IEA に移行クライアントをインストールします。

a. 次のコマンドを入力して、SCP を使用して IEA に移行クライアント ファイルをコピーします。

scp cres-dbmigrate_install-4.5.1.xxx.sh admin@<IEA IP Address>:

scp token.jar admin@<IEA IP Address>:

b. SSH を使用して IEA に接続します。例を示します。

ssh admin@<IEA IP Address>

c. メイン メニューで、オプション x を入力して UNIX コマンド プロンプトに戻ります。

（注） x オプションは隠しコマンドであるため、メニュー オプションのリストに表示されません。

d. 次のコマンドを使用して、移行クライアントをインストールします。

sh ./cres-dbmigrate_install-4.5.1.xxx.sh

手順 4 データベース変更スクリプトを実行します。

- PostgreSQL の場合は、次のように入力します。

  cd dbmigrate/scripts/postgres

  psql -p 5432 -h localhost -d *database-name* -U *db-admin-name* -f ~/dbmigrate/scripts/postgresql/migration_table.sql

（注） この手順を完了するには、PL/pgSQL がインストールされている必要があります。

- MSSQL の場合は、SQL Server 管理者ツールがインストールされている Windows マシンにスクリプトをコピーし、次のいずれかの方法でスクリプトを実行します。
  - SQL Server Management Studio GUI の使用
  - 次の CLI コマンドの実行

    sqlcmd -H *hostname* -S *sqlserver-instance-name* -d *database-name* -U *db-admin-name* -P *db-admin-password* -i migration_table.sql

手順 5　シスコ テクニカル サポートに確認して、dbmigrate.properties ファイルのパラメータを設定します。このパラメータは、移行クライアントの機能を設定するために使用されます。これらのパラメータについては、以下の表で説明します。

以下の表に示す基本設定パラメータに加えて、付録 B で説明される拡張パラメータを使用することもできます。

設定可能な機能の 1 つは、移行完了時に自分とシスコ テクニカル サポートに通知電子メールを送信することです。この通知ではパラメータ *mailserver*、*mailserverport*、*notifyComplete*、*notificationRecipient*、および *notifyCompleteForm* を設定します。

データの移行完了時にエンド ユーザに通知電子メールを送信する機能も設定できます。エンド ユーザ向け通知を設定する場合は、電子メール通知を受け取ったときに混乱を避けるため、移行プロセスをエンド ユーザに説明することを推奨します。そのため、この機能は拡張機能と見なされます。エンド ユーザ通知用のオプションの拡張パラメータについては、付録 B を参照してください。

dbmigrate.properties ファイルまたは CLI を使用して、次の表に示す移行クライアント パラメータを設定できます。dbmigrate.properties ファイルは、移行クライアント インストーラを含むフォルダの *conf* サブディレクトリにあります。

パラメータ	必須または オプション	定義
url	必須	データベースの JDBC 接続 URL。推奨される値については、以下の注記を参照してください。
driver	必須	JDBC ドライバ名。以下の注記を参照してください。
user	必須	データベース ユーザ名。

パラメータ	必須または オプション	定義
password	必須	データベース パスワード。
token	必須	CRES アカウントのトークン JAR ファイルの名前。
securitykey	必須	認証の追加セキュリティ キー。
importserver	オプション	CRES 移行インポート サービスの URL。
passcount	オプション	終了する前に実行されるユーザとキーテーブルのパス数。(デフォルト:1。最大:なし)。
passdelay	オプション	移行の実行間隔(秒)。値 0 は遅延が無限になります。(デフォルト:12 時間。最小:1 時間)。
mailserver	オプション	メール サーバの IP アドレス。
mailserverport	オプション	メール サーバのポート番号。
notifyComplete	オプション	移行完了時の通知電子メール送信を有効または無効にします。有効な値は *true* または *false* です。
notificationRecipient	オプション	移行完了時の通知電子メールの受信者の電子メール アドレス。
notifyCompleteFrom	オプション	移行完了時の通知電子メールの送信者の電子メール アドレス。
notifyComplete Subject	オプション	移行が完了したことを通知するために送信する電子メールの件名行。

(注) IEA に使用するものとは異なる JDBC ドライバを使用する場合は、そのドライバの JAR ファイルを lib フォルダにコピーする必要があります。

MSSQL を使用している場合は、次のパラメータを設定します。

- driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
- url=jdbc:sqlserver://*database_server*;instanceName=*instance_name*;databaseName=postx;*other_options*

dbmigrate.properties ファイルで設定できるすべてのパラメータは、コマンドラインを使用して設定することもできます。ただし、コマンドラインには 2 つの追加オプション パラメータがあります。次の表に示すように、コマンドラインで必要なパラメータは 4 つのみです。

パラメータ	必須または オプション	定義
url	必須	データベースの JDBC 接続 URL。
driver	必須	JDBC ドライバ名。
user	必須	データベース ユーザ名。
password	必須	データベース パスワード。
help	オプション	構成パラメータの説明を出力します。
config	オプション	構成プロパティ ファイルの名前。

手順 6　次のコマンドを入力して、dbmigrate_check スクリプトを実行します。

```
./dbmigrate_check
```

dbmigrate_check スクリプトは、移行クライアントが正しく設定されていること（移行に必要なテーブルが作成されること、適切なトークンとセキュリティ キーがあること）を検証します。スクリプトは、ユーザ、キー、連絡先、uuid 数、年別のキー数に関する情報も提供し、非 PostxAuth キーについてデータベースを確認します。

データベースから次の情報がコンソールに出力されます。

- T_KEYSTORE テーブル内のキーの数
- T_USER テーブル内のユーザの数
- T_CONTACT テーブル内のユーザの数
- T_UUID テーブル内のユーザの数
- T_KEYSTORE テーブル内の年で分割したキーの数
- T_EXPORT_KEYSTORE テーブル内のキーの数
- T_EXPORT_USER テーブル内のユーザの数
- データベースが非 PostxAuth キー（T_KEYSTORE テーブル）を使用する場合は、警告

手順 7　ダウンロードしたファイルに含まれるスクリプトを実行して移行クライアントを開始するには、次のコマンドを入力します。

```
./dbmigrate_client --password=db_password
```

手順 5 の説明に従ってメール サーバと通知パラメータを設定した場合は、移行が完了したときに移行クライアントから自分とシスコ テクニカル サポートに通知電子メールが送信されます。シスコ テクニカル サポートは、移行の結果を確認し、移行が成功したかどうかを通知します。

（注）　ユーザ アカウントおよびドメイン メンバーシップは移行プロセスによって処理されません。既存のユーザ レコードは異なるアカウントに移動されず、すべての新規ユーザ レコードはデフォルト ユーザ アカウント（ID 1）に追加されます。シスコ テクニカル サポートは、移行後にログインし、ユーザを手動で正しいアカウントに移動する必要があります。

IEA ユーザが CRES にすでに存在する場合、そのユーザの CRES データは保持され、エラー メッセージは生成されません。

IEA メッセージの送信者が CRES で見つからない場合（たとえばメッセージが現在存在しないユーザまたは削除されたユーザから送信された場合）、このキーは移行されず、エラー メッセージが表示されます。このようなキーを移行するには、CRES で適切なユーザを手動で作成し、移行を再実行する必要があります。

移行が完了し、プロキシが設定されると、ユーザはエンベロープを開封するために IEA クレデンシャルの代わりに CRES クレデンシャルを使用する必要があります。このような状況が発生することをエンド ユーザに通知するのは管理者の責任です。

手順 8　移行が完了した後、エンド ユーザからの HTTP トラフィックを IEA ではなく HTTP プロキシにリダイレクトするように設定する必要があります。リダイレクトが必要なトラフィックには次のものがあります。

- エンベロープの新しいキーを作成したり既存のエンベロープのキーを取得したりするキー サーバ要求
- WebSafe への接続
- Secure Compose への接続
- オンライン エンベロープ オープナーへの接続
- その他の Web アプリケーションへの接続

このトラフィックをリダイレクトするには、IEA の代わりに動作するように HTTP/HTTPS プロキシを設定する必要があります。このプロキシの実装方法は、既存のネットワークに依存します。HTTP プロキシを実行する既存の Web サーバまたはプロキシ サーバがない場合は、HTTP プロキシを実行するために新しいマシンを設定する必要があります。設定例については、「HTTP プロキシの設定例」セクション（4-14 ページ）を参照してください。

（注） 移行プロセスの後、IEA のセキュリティ保護されたエンベロープのカスタム ロゴの代わりにデフォルトの CRES ロゴが表示されます。カスタム ロゴを設定するには、IEA のカスタム ロゴの要求を CRES のカスタム ロゴの要求に変更するようにプロキシを設定します。
IEA のロゴの要求の例は、次にあります。
https://customer_domain/websafe/branding/customer-logo.gif
CRES のカスタム ロゴの要求の例は、次にあります。
https://res.cisco.com/websafe/logo/your_CRES_account_ID/branding/customer-logo.gif
CRES アカウントにカスタム ロゴを追加するには、「登録済みエンベロープのロゴのカスタマイズ」セクション（2-9 ページ）を参照してください。

手順 9　エンド ユーザが IEA で使用される証明書の代わりにプロキシを使用する HTTP トラフィックで信頼できる既存または新規の SSL 証明書を使用するように HTTP プロキシを設定します。

（注） 『*Cisco Email Encryption Compatibility Matrix*』の「Supported Certificate Authorities for CRES」セクションにリストされているいずれかの証明書によって署名されている証明書、またはその証明書に接続されている証明書を使用する必要があります。

SSL バージョン 3 は、今後のリリースでサポートされません。そのため、Transport Layer Security（TLS）を利用するソフトウェアを使用する必要があります。

サポートされる認証局によって署名されている場合は IEA に使用したものと同じ証明書を使用でき、新しい証明書を使用することもできます。可能であれば、既存の証明書を使用することを推奨します。

手順 10　CRES との信頼された HTTP 通信に SSL 証明書を使用するように HTTP プロキシを設定します。

この場合の最善の方法は、CA 証明書の信頼ストアを参照するようにプロキシを設定します。管理可能性が低い別の方法としては、CRES 証明書を明示的に信頼するようにプロキシを設定することです。ただしこのアプローチでは CRES 証明書が更新されるたびに明示的な信頼関係を更新する必要があります。

手順 11 HTTP を設定したら、IEA のために代わりに HTTP プロキシにすべての HTTP トラフィックをリダイレクトするように DNS サーバおよびファイアウォールのルールを更新する必要があります。

手順 12 すべての暗号化アプライアンスとクライアントでトークンを更新します。これは keyserver パラメータの暗号化と復号化が動作するために必要です。

Cisco E メール セキュリティ アプライアンス上のトークンを更新するには、CRES 暗号化プロファイルがプロビジョニングされる必要があります。Outlook プラグイン、Cisco BCE Mobile App for Android、Cisco BCE Mobile App for iOS などクライアント上のトークンを更新するには、CRES プロファイルで作成された新しい BCE コンフィギュレーション ファイルをダウンロードし、CRES アカウントの管理者からの暗号化された電子メールとして当該ユーザに送信します。

手順 13 IEA 暗号化サーバを停止します。ただし、IEA を物理的に切断しないでください。

手順 14 移行クライアントを再実行して、最初の実行以降の更新を反映します。または、複数パス モードで移行クライアントを実行させることもできます。

2 回目の実行が正常に完了した場合、シスコ テクニカル サポートはそれ以降のアカウント移行を無効にします。

手順 15 シスコ テクニカル サポートに連絡し、電子メール ドメインを CRES アカウントに関連付けます。このプロセスの一環として、シスコ テクニカル サポートはその電子メール ドメイン内に既存の CRES ユーザをアカウントに移動します。自分が所有する電子メール ドメインだけを自分の CRES アカウントに関連付けることができます。

移行完了後の機能の違い

CRES には IEA とは異なる機能セットがあるため、この違いがユーザの混乱を招く可能性があります。これら 2 つの機能セット間の機能の違いについてユーザに説明することを推奨します。

IEA 機能の詳細については、『*Cisco Ironport Encryption Appliance 6.5 Configuration Manual*』を参照してください。

また、前述の手順 15 のとおり、電子メール アカウントを自分が所有していない場合は、それを自分の CRES アカウントと関連付けることはできません。そのため、これらのアカウントから送信される電子メールは、電子メール エイリアスで別のドメイン名を持ちます。混乱を避けるために、この違いについてもユーザに説明することを推奨します。

移行エラー メッセージ

以下のエラー メッセージは、移行プロセス中に生成される最も一般的なメッセージです。その他のエラー メッセージが表示された場合は、問題を解決する方法についてシスコ カスタマー サポートにお問い合わせください。

エラー メッセージ

```
This IEA database uses a non-standard authentication system for
keys, you may continue with this migration, but when these keys
are moved to CRES they will be modified to use CRES
authentication.
```

説明　IEA データベースは PostXAuth 以外のキー サーバ認証タイプを使用しています。

推奨処置　回避策として、Yes と応答して移行を続行し、CRES 認証を使用することができます。ただし、その判断の前にシスコ カスタマー サポートに連絡することを推奨します。

エラー メッセージ

```
This IEA database uses non-standard key authentication, i.e.,
C_LOOKUPNAME <> 'PostXDatabase' and the Keystore checker failed
to prompt the user for resolution (console not available).
```

説明　IEA データベースは PostXAuth 以外のキー サーバ認証タイプを使用しています。また、precondition.keychecker.actionOnFail パラメータが *fail* に設定されています。

推奨処置　シスコ カスタマー サポートに連絡してください。

エラー メッセージ

```
ERROR: language "‘plpgsql’" does not exist.
```

説明　前提条件として、PostgreSQL を使用してデータベースを管理している場合は、データベース変更スクリプトを実行するために PL/pgSQL がインストールされている必要があります。しかし、この前提条件を満たしていません。

推奨処置　PostgreSQL を使用する場合は、PL/pgSQL がインストールされていることを確認します。

HTTP プロキシの設定例

この例では、HTTP/HTTPS プロキシを設定する場合に最もよく使用される製品の 1 つである Apache HTTP サーバを設定する方法を示します。これは決して可能な唯一の例ではなく、最も推奨される製品というわけではありません。インフラストラクチャによって、HTTP/HTTPS プロキシとして使用するのに最適な製品を判断します。

次の手順でこのシナリオを設定します。

手順 1　Apache httpd.conf ファイルまたは同等のファイルで次のコマンドを入力して、プロキシと SSL を有効にします。

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule ssl_module modules/mod_ssl.so
```

手順 2　CA 証明書が適切なフォルダ（例：/etc/ssl/certs）にあることを確認し、次のコマンドを入力して、そのフォルダにある CA 証明書を検索するように Apache サーバを設定します。

```
SSLCACertificatePath /etc/ssl/certs/
```

手順 3　証明書（例：/etc/ssl/your-host-certificate.pem）用に Apache インストールで使用するディレクトリに証明書ファイルをコピーして、IEA 証明書をインストールします。

手順 4　次のコマンドを入力して、HTTP ポート 80 のプロキシ処理を有効にします。

```
<VirtualHost www.your-hostname.com:80>
    ServerName www.your-hostname.com
```

```
    ProxyPreserveHost On
     ProxyRequests off
     ProxyPass / http://res.cisco.com:80/
    ProxyPassReverse / http://res.cisco.com:80/
</VirtualHost>
```

手順 5　次のコマンドを入力して、HTTPS ポート 443 のプロキシ処理を有効にします。

```
<VirtualHost www.your-hostname.com:443>
    ServerName www.your-hostname.com

    ProxyPreserveHost On
    ProxyRequests off

    ProxyPass / https://res.cisco.com:443/
    ProxyPassReverse / https://res.cisco.com:443/

    SSLEngine on
    SSLProxyEngine on
    SSLCertificateFile    /etc/ssl/your-host-certificate.pem
</VirtualHost>
```

シスコ コンテンツ セキュリティにコメントをお寄せください

Cisco Content Security テクニカル マニュアル チームは、製品ドキュメントの向上に努めています。お客様からのご意見をお待ちしています。次の電子メール アドレス宛にお送りください。

contentsecuritydocs@cisco.com

APPENDIX **A**

カスタマー サポートへの問い合わせ

Cisco Registered Envelope Service（CRES）のカスタマー サポートにお問い合わせの際は、次のアドレスまでメールをお送りください。

support@res.cisco.com

カスタマー サポートの詳細については、次の URL を参照してください。

https://res.cisco.com/websafe/help?topic=ContactSupport

（注） 次の URL からインスタント メッセージによるチャット サポートにアクセスできます。

サポートは、電話またはオンライン（24 時間年中無休）で依頼することもできます。次のいずれかの方法で Cisco カスタマーサポートにお問い合わせください。

- Cisco サポート ポータル：http://www.cisco.com/support
- 電話サポート：Cisco Technical Assistance Center（TAC）にお問い合わせください。米国およびカナダ内では 800-553-2447 へ、それ以外は Worldwide Phone Numbers を参照してください。

再販業者または別のサプライヤからサポートを購入した場合は、製品のサポートの問題について直接そのサプライヤに連絡してください。

注　利用可能なサポートのレベルは、お客様のサービス レベル契約によって異なります。Cisco IronPort カスタマー サポートのサービス レベル契約の詳細については、サポート ポータルをご覧ください。サポート レベルの詳細については、このページで確認してください。

サポートに連絡する理由は次のとおりです。

- 問題の報告
- アカウントへのドメインの追加
- ドメインへのユーザの追加
- CRES を介してユーザを直接管理しない場合のユーザの管理(パスワードのリセットやユーザのロックなど)。

Cisco Content Security にコメントをお寄せください

Cisco Content Security テクニカル マニュアル チームは、製品ドキュメントの向上に努めています。お客様からのご意見をお待ちしています。次の電子メール アドレス宛にお送りください。

contentsecuritydocs@cisco.com

APPENDIX **B**

キーの作成に必要なデータを IEA から CRES に移行するための追加パラメータ

移行クライアントの dbmigrate.properties ファイルまたは第 2 章で説明するコマンドラインで使用されるパラメータに加えて、次の表のパラメータを使用できます。

シスコ テクニカル サポートによる支援なしで、dbmigrate.properties ファイルまたはコマンドラインを使用してこれらのパラメータのデフォルト値を変更しないでください。

max-Errors パラメータは,移行クライアントが現在の実行を放棄する前に発生する可能性があるエラーの最大数を示します。max-Errors パラメータの値が 0 の場合、発生する可能性があるエラーの数に制限がないことを示します。

一部のパラメータは、移行の実行前に満たす必要がある前提条件をキー チェッカー プロセスが指定するために使用されます。キー チェッカー プロセスは PostXAuth 以外のキー サーバ認証タイプが存在するかどうかデータベースをスキャンします。指定の前提条件が満たされていない場合にキー チェッカー プロセスが特定のアクションを実行するようにパラメータを設定できます。

移行プロセスで発生する可能性のあるエラーについては、「移行エラー メッセージ」セクション（4-13 ページ）を参照してください。

パラメータ	コマンドライン/プロパティ ファイルで使用	定義
maxUserErrors	両方	ユーザ テーブルの移行を停止するまでに、移行中に発生する可能性があるエラーの最大数。
maxUuidErrors	両方	UUID テーブルの移行を停止するまでに、移行中に発生する可能性があるエラーの最大数。
maxKeyErrors	両方	キー テーブルの移行を停止するまでに、移行中に発生する可能性があるエラーの最大数。
maxContactErrors	両方	連絡先テーブルの移行を停止するまでに、移行中に発生する可能性があるエラーの最大数。
precondition.keychecker.databaseName=*dbname*	両方	移行が実行される前に、キー チェッカー プロセスによって使用されるルール ファイルで設定する必要があるデータベースを指定します。
precondition.keychecker.class=*class*	両方	移行が実行される前に、キー チェッカー プロセスによって満たされる必要のある前提条件として呼び出す必要があるクラスを指定します。
precondition.keychecker.actionOnFail=*action*	両方	キー チェッカー プロセスの前提条件が満たされていない場合に実行するアクションを設定します。 *action* に使用可能な値は、prompt、pass、および fail です。
autoNotifyUser	オプション	移行完了時のユーザごとの通知電子メール送信を有効または無効にします。有効な値は、true または false です。
notifyUserFrom	オプション	移行完了時のユーザ通知電子メールの送信者の電子メール アドレス。

パラメータ	コマンドライン/プロパティ ファイルで使用	定義
notifyUserSubject	オプション	移行が完了したことをユーザに通知するために送信する電子メールの件名行。
notifyUser.params.company	オプション	移行が完了したことを示す通知を受信するユーザの会社名。
notifyUser.params.cres.login	オプション	移行が完了したことを示す通知を受信するユーザの会社の CRES ログイン URL。
level	両方	ロギング レベル。使用可能な値は、ERROR、WARN、INFO（デフォルト）、DEBUG です。
logfile	両方	ログ ファイル名（デフォルト：dbmigrate.log）。
tableset	両方	エクスポートする一連のテーブルのカンマ区切りリスト。値は次のとおりです。 • users：すべてのユーザ、ユーザ マップ、およびユーザ プロファイルのテーブルをエクスポートするのに使用されます。 • contacts：すべてのアドレス帳のテーブルをエクスポートするのに使用されます。 • keys：すべてのキーをエクスポートするのに使用されます。 • uuids：UUID をエクスポートするのに使用されます。

パラメータ	コマンドライン/プロパティ ファイルで使用	定義
reportProcessors	両方	レポートを生成する一連のテーブルのカンマ区切りリスト。値は次のとおりです。 • users-report：すべてのユーザ、ユーザマップ、およびユーザ プロファイルのテーブルのレポート。 • keys-report：キーのレポート。
maxsize	両方	IEA から送信される HTTP メッセージ本文の最大サイズ（バイト数）（デフォルト：2 MB。最大：10 MB）。
batchsize	両方	要求ごとに送信されるレコードの最大数（デフォルト：200。最大：10000）。
batchdelay	両方	バッチ間で一時停止する時間（デフォルト：0.6 秒。最小：0.2 秒）。
retrycount	両方	各バッチを中止するまでに再試行する回数（デフォルト：5。最大：30）。
retrydelay	両方	再試行間で一時停止する時間（デフォルト：20 秒。最小：1 秒）。
ルール	両方	ルール ファイルの名前。
help	コマンド ライン	構成パラメータの説明を出力します。
config	コマンド ライン	構成プロパティ ファイルの名前。
connectTimeout	両方	HTTP 接続のタイムアウト。
socketTimeout	両方	HTTP ソケットのタイムアウト。
sendBufferSize	両方	HTTP 送信バッファのサイズ。
receiveBufferSize	両方	HTTP 受信バッファのサイズ。
acceptSelfSigned	両方	自己署名 SSL 証明書を使用できないため、このパラメータはデフォルト設定の false のままにする必要があります。

パラメータ	コマンドライン/プロパティ ファイルで使用	定義
acceptUntrusted	両方	信頼できない SSL 証明書を使用できないため、このパラメータはデフォルト設定の false のままにする必要があります。
acceptExpired	両方	期限切れの SSL 証明書を使用できないため、このパラメータはデフォルト設定の false のままにする必要があります。
requireServerTLS	両方	TLS サーバの使用が必要です。有効な値は、true または false です。