管理タスクの分散

この章は、次の項で構成されています。

- 管理タスクの分散について （1 ページ）
- ユーザー ロールの割り当て （1 ページ）
- [ユーザー（Users）] ページ （13 ページ）
- 管理ユーザーの認証について （13 ページ）
- セキュリティ管理アプライアンスへのアクセスに対する追加の制御 （29 ページ）
- メッセージ トラッキングでの機密情報へのアクセスの制御 （33 ページ）
- 管理ユーザー向けメッセージの表示 （34 ページ）
- 管理ユーザー向けメッセージバナーの有効化と無効化 （34 ページ）
- 管理ユーザー アクティビティの表示 （34 ページ）
- 管理ユーザー アクセスのトラブルシューティング （36 ページ）

管理タスクの分散について

ユーザ アカウントに割り当てたユーザ ロールに基づいて、他のユーザに Cisco コンテンツ セキュリティ管理仮想アプライアンスの管理タスクを分散できます。

管理タスクが分散されるように設定するには、事前定義されたユーザ ロールがニーズを満たしているかどうかを判断して、必要なカスタム ユーザ ロールを作成します。次に、セキュリティ アプライアンスでローカルに管理ユーザの認証を行う、および（または）独自の中央集中型の LDAP や RADIUS システムを使用して外部で管理ユーザの認証を行うようにアプライアンスを設定します。

さらに、アプライアンスおよびアプライアンス上の特定の情報へのアクセスに追加の制御を指定できます。

ユーザー ロールの割り当て

- 事前定義済みユーザ ロール （2 ページ）
- カスタム ユーザ ロール （5 ページ）

隔離アクセスには追加設定が必要です。隔離へのアクセス （13 ページ） を参照してください。

事前定義済みユーザ ロール

特記のない限り、次の表で説明されている権限を持つ事前設定ユーザー ロール、またはカスタム ユーザー ロールを各ユーザーに割り当てることができます。

表 *1:* ユーザー ロールの説明

ユーザー ロール名	説明	Web レポーティング/スケジュール設定されたレポート機能
admin	**admin** ユーザーはシステムのデフォルト ユーザーアカウントであり、すべての管理権限を持っています。便宜上、admin ユーザー アカウントをここに記載しましたが、これはユーザー ロールを使用して割り当てることはできず、パスフレーズの変更以外、編集や削除もできません。 **resetconfig** コマンドと **revert** コマンドを発行できるのは、**admin** ユーザだけです。	はい/はい
管理者	Administrator ロールを持つユーザ アカウントはシステムのすべての設定に対する完全なアクセス権を持っています。	はい/はい
オペレータ	Operator ロールを持つユーザ アカウントは次のことができません。 • ユーザー アカウントの作成または編集 • アプライアンスのアップグレード • `resetconfig` コマンドの発行 • システム セットアップ ウィザードの実行 • ユーザ名とパスフレーズ以外の LDAP サーバ プロファイル設定の変更（LDAP が外部認証に対して有効になっている場合）。 • 隔離の設定、編集、削除、または集約。 これら以外は、Administrator ロールと同じ権限を持ちます。	はい/はい

ユーザー ロール名	説明	Web レポーティング/スケジュール設定されたレポート機能
Technician	Technician ロールを持つユーザ アカウントは、アップグレードおよびリブート、アプライアンスからのコンフィギュレーション ファイルの保存、機能キーの管理などのシステム管理アクティビティを開始できます。	[ウェブ（Web）]および[電子メール（Email）]タブのシステム キャパシティ レポートへのアクセス
オペレータ（読み取り専用）	Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために大部分の変更を行って送信できますが、保存できません。または保存を必要としない変更を行うことができます。このロールのユーザは、アクセスが有効の場合、隔離内のメッセージを管理できます。 このロールのユーザは、以下にはアクセスできません。 • ファイル システム、FTP、SCP。 • 隔離を作成、編集、削除、または集中管理するための設定。	はい/いいえ
Guest	Guest ロールを持つユーザ アカウントは、アクセス権限が有効であれば、レポートおよび Web トラッキングを含むステータス情報を表示し、隔離内のメッセージを管理できます。Guest ロールを持つユーザはメッセージ トラッキングにアクセスできません。	はい/いいえ
Web Administrator	Web Administrator ロールを持つユーザ アカウントは、[ウェブ（Web）] タブに表示されるすべての設定に対するアクセス権を持ちます。	はい/はい

ユーザー ロール名	説明	Web レポーティング/スケジュール設定されたレポート機能
Web ポリシー管理者（Web Policy Administrator）	Web Policy Administrator ロールを持つユーザ アカウントは、[Webアプライアンスステータス（Web Appliance Status）] ページと、Configuration Master のすべてのページにアクセスできます。Webポリシー管理者は、ID、アクセス ポリシー、暗号化ポリシー、ルーティング ポリシー、プロキシ バイパス、カスタム URL カテゴリ、および時間範囲を設定できます。Webポリシー管理者は、設定を公開できません。	いいえ/いいえ
メール管理者（Email Administrator）	Email Administrator ロールを持つユーザ アカウントは、隔離など、[メール（Email）] メニューにあるすべての設定へのアクセス権のみを持ちます。	いいえ/いいえ
ヘルプ デスク ユーザー	ヘルプデスク ユーザー ロールを持つユーザーがアクセスできるのは次のものに制限されます。 • メッセージ トラッキング • 隔離内のメッセージ管理 このロールを持つユーザは、CLI を含めたこれ以外のシステムにはアクセスできません。ユーザにこのロールを割り当てた後、このユーザがアクセスできるように隔離を設定する必要があります。	いいえ/いいえ

ユーザー ロール名	説明	Web レポーティング/スケジュール設定されたレポート機能
カスタム ロール	カスタム ユーザー ロールに割り当てられているユーザー アカウントは、ポリシー、機能、またはこのロールに特に与えられた特定のポリシーまたは機能インスタンスに対してのみ、表示および設定を行えます。 これらの機能には、アクセス ログ サブスクリプション、ロギング API、およびログファイルがあります。 新しい Custom Email User ロールまたは新しい Custom Web User ロールは、[ローカルユーザの追加（Add Local User）] ページから作成できます。ただし、ロールを使用できるようにするには、このカスタム ユーザー ロールに権限を割り当てる必要があります。権限を割り当てるには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザロール（User Roles）] に移動して、ユーザ名をクリックします。 （注） Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。 詳細については、カスタムユーザロール （5 ページ） を参照してください。	いいえ/いいえ

カスタムユーザロール

Administration 権限を持つユーザは、セキュリティ管理アプライアンスを使用してカスタム ロールに管理権限を委任できます。カスタム ロールは、事前定義されたユーザ ロールよりも、ユーザのアクセス権に対して柔軟な制御を行えます。

カスタム ユーザー ロールを割り当てたユーザーは、アプライアンス、機能、またはエンドユーザーのサブセットに関して、ポリシーの管理またはレポートへのアクセスを行えます。たとえば、別の国にある組織の支社では、許容可能な使用ポリシーが組織の本社とは異なっている場合に、Web サービスに関して委任を受けた管理者に、支社のポリシーの管理を許可できます。カスタム ユーザー ロールを作成して、それらのロールにアクセス権を割り当てることで、管理を委任します。委任された管理者が表示および編集できるポリシー、機能、レポート、カスタム URL カテゴリなどを決定します。

詳細については、以下を参照してください。

• Custom Email User ロールについて （6 ページ）
• カスタム ユーザ ロールの削除 （12 ページ）

Custom Email User ロールについて

カスタム ロールを割り当てると、委任された管理者がセキュリティ管理アプライアンスにある次の項目にアクセスすることを許可できます。

- すべてのレポート（オプションでレポーティンググループによって制限）
- メールポリシーレポート（オプションでレポーティンググループによって制限）
- DLP レポート（オプションでレポーティンググループによって制限）
- メッセージ トラッキング
- 隔離
- ログ サブスクリプション（Log Subscription）

これらの各項目の詳細については、以下のセクションで説明します。また、これらの権限を付与されたすべてのユーザは、[管理アプライアンス（Management Appliance）] タブ > [集約管理サービス（Centralized Services）] メニューを使用して、[システムステータス（System Status）] を表示できます。Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。

（注） E メール セキュリティ アプライアンスのカスタム ユーザ ロールは、セキュリティ管理アプライアンスのユーザ ロールよりも、より詳細なアクセス権を提供します。たとえば、メールおよび DLP ポリシーと、コンテンツ フィルタへのアクセス権を委任できます。詳細については、お使いの E メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Common Administration」の章の「Managing Custom User Roles for Delegated Administration」の項を参照してください。

電子メール レポーティングへのアクセス

次のセクションで説明するように、電子メール レポートへのアクセス権をカスタム ユーザー ロールに付与できます。

セキュリティ管理アプライアンスの [電子メール セキュリティ モニター（Email Security Monitor）] ページの詳細については、中央集中型の電子メール セキュリティ レポーティングの使用の該当する章を参照してください。

すべてのレポート

カスタム ロールにすべてのレポートへのアクセス権を付与すると、このロールを割り当てられたユーザーは、すべての E メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [電子メール セキュリティ モニター（Email Security Monitor）] ページを表示できます。

- メール フロー概要
- メール フローの詳細
- [送信先（Outgoing Destinations）]
- ユーザー メールの概要
- DLP インシデント
- コンテンツ フィルタ
- ウイルス フィルタリング
- TLS 暗号化
- スケジュール設定されたレポート（Scheduled Reports）
- アーカイブ レポート（Archived Reports）

メール ポリシー レポート

カスタム ロールにメール ポリシー レポートへのアクセス権を付与すると、このロールを割り当てられたユーザーは、すべての E メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [電子メール セキュリティ モニター（Email Security Monitor）] ページを表示できます。

- メール フロー概要
- メール フローの詳細
- [送信先（Outgoing Destinations）]
- ユーザー メールの概要
- コンテンツ フィルタ
- ウイルス フィルタリング
- アーカイブ レポート（Archived Reports）

DLP レポート

カスタム ロールに DLP レポートへのアクセス権を付与すると、このロールを割り当てられたユーザーは、すべての E メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [電子メール セキュリティ モニター（Email Security Monitor）] ページを表示できます。

- DLP インシデント
- アーカイブ レポート（Archived Reports）

メッセージ トラッキング データへのアクセス

カスタム ロールにメッセージ トラッキングへのアクセス権を付与すると、このロールを割り当てられたユーザーは、セキュリティ管理アプライアンスによってトラッキングされたすべてのメッセージのステータスを表示できます。

DLP ポリシーに違反するメッセージ内の機密情報へのアクセスを制御するには、メッセージ トラッキングでの機密情報へのアクセスの制御 （33 ページ）を参照してください。

セキュリティ管理アプライアンスでメッセージ トラッキングへのアクセスを有効にするためのアプライアンスの設定方法など、メッセージ トラッキングの詳細については、メッセージのトラッキングを参照してください。

カスタム ユーザー ロールの隔離へのアクセス

カスタム ロールに隔離へのアクセス権を付与すると、このロールを割り当てられたユーザは、このセキュリティ管理アプライアンスのすべての隔離メッセージを検索、表示、リリース、または削除できます。

ユーザが隔離にアクセスする前にそのアクセスを有効にする必要があります。隔離へのアクセス （13 ページ） を参照してください。

ログ サブスクリプション（Log Subscription）

ログ サブスクリプション アクセス権限は、カスタムユーザロールに割り当てられた委任管理者がログサブスクリプションまたはロギング API にアクセスしてログファイルを表示またはダウンロードできるかどうかを定義します。

Custom Email User ロールの作成

電子メール レポーティング、メッセージ トラッキング、および隔離へのアクセスに対して、カスタムのメール ユーザ ロールを作成できます。

これらの各オプションに許可されたアクセス権の詳細については、Custom Email User ロールについて （6 ページ）とそのサブセクションを参照してください。

（注） より詳細なアクセス権、または他の機能、レポート、ポリシーへのアクセス権を付与するには、各 E メール セキュリティ アプライアンスで直接カスタム ユーザ ロールを作成してください。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザロール（User Roles）] を選択します。

ステップ 3 [メールユーザ役割の追加（Add Email User Role）] をクリックします。

ヒント　または、既存の Email User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [重複（Duplicate）] アイコンをクリックし、生成されたコピーを編集します。

ステップ 4　ユーザ ロールの一意の名前（たとえば「dlp-auditor」）と説明を入力します。

- Email と Web のカスタム ユーザ ロール名を同じにしないでください。
- 名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュまたは数字にすることはできません。
- このロールのユーザに集約ポリシー隔離へのアクセス権限を許可し、このロールのユーザが E メール セキュリティ アプライアンスのメッセージ フィルタやコンテンツ フィルタおよび DLP メッセージ アクション内にもこれらの集約隔離を指定できるようにする場合、カスタム ロールの名前を両方のアプライアンスで同じにする必要があります。

ステップ 5　このロールに対してイネーブルにするアクセス権限を選択します。

ステップ 6　[送信（Submit）] をクリックして [ユーザ ロール（User Roles）] ページに戻ると、新しいユーザ ロールが表示されます。

ステップ 7　レポーティング グループごとにアクセス権を制限する場合は、該当するユーザ ロールの [メールレポート（Email Reporting）] 列にある [グループが選択されていません（no groups selected）] リンクをクリックして、少なくとも 1 つのレポーティング グループを選択します。

ステップ 8　変更を保存します。

ステップ 9　このロールに隔離へのアクセス権を付与する場合は、このロールに対してアクセス権を有効にします。

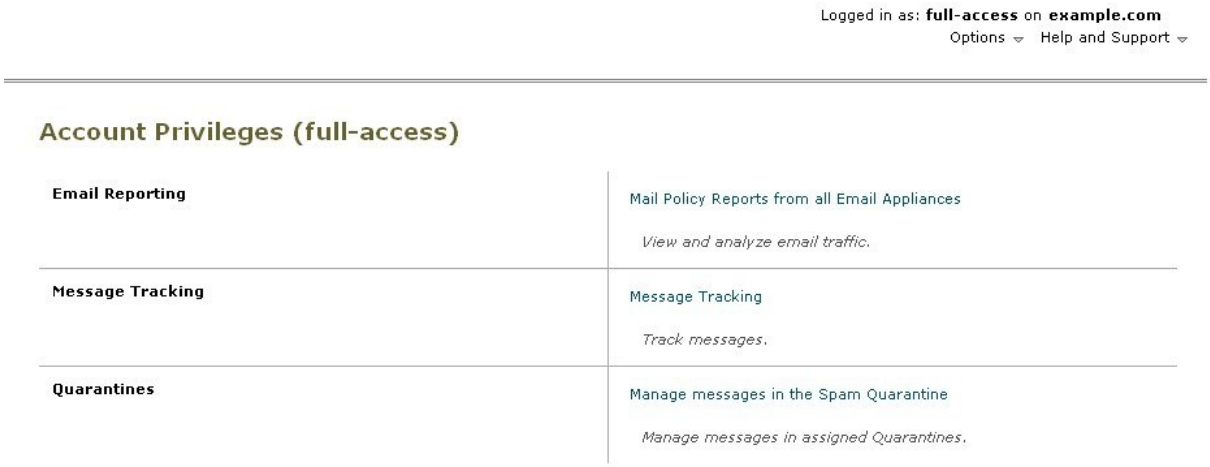
参照先：

- スパム隔離への管理ユーザ アクセスの設定
- ポリシー、ウイルス、およびアウトブレイク隔離の設定

Custom Email User ロールの使用

Custom Email User ロールに割り当てられているユーザーがアプライアンスにログインすると、そのユーザーには、ユーザーがアクセス権を持つセキュリティ機能へのリンクだけが表示されます。そのユーザーは、[オプション（Options）] メニューで [アカウント権限（Account Privileges）] を選択することで、いつでもこのメインページに戻ることができます。これらのユーザーは、Web ページの上部にあるメニューを使用して、アクセス権を持つ機能にアクセスすることもできます。次の例では、ユーザーは Custom Email User ロールによって、セキュリティ管理アプライアンスで使用可能なすべての機能へのアクセス権を持ちます。

図 *1 : Custom Email User* ロールが割り当てられている委任管理者の *[*アカウント権限（*Account Privileges*）*]* ページ



Custom Web User ロールについて

Custom Web User ロールでは、ユーザがポリシーを別の Web セキュリティ アプライアンスに公開することができ、カスタム設定を編集したり、別のアプライアンスに公開できるようになります。

セキュリティ管理アプライアンスの [ウェブ（Web）] > [設定マスター（Configuration Master）] > [カスタムURLカテゴリ（Custom URL Categories）] ページでは、管理および公開できる URL カテゴリとポリシーを表示できます。また、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [今すぐ設定を公開する（Publish Configuration Now）] ページに移動して、可能な設定を表示することもできます。

（注） 公開権限を持つカスタム ロールを作成した場合、ユーザがログインすると、使用可能なメニューが表示されないことに注意してください。URL やポリシー タブが機能を持たないため、このようなユーザには公開メニューが表示されず、編集不可の固定画面が表示されます。これは、ご使用のユーザでは、カテゴリまたはポリシーの公開および管理ができないということです。この問題の回避策としては、ユーザが公開はできるが、どのカテゴリまたはポリシーも管理できないようにする場合、どのポリシーでも使用されていないカスタム カテゴリを作成し、そのユーザに、そのカスタム カテゴリを管理する権限と公開する権限を付与する必要があります。このようにすると、ユーザがそのカテゴリで URL を追加または削除しても、他に影響が及びません。

カスタム ユーザ ロールを作成および編集して、Web 管理を委任できます。

- Custom Web User ロールの作成 （11 ページ）
- Custom Web User ロールの編集 （12 ページ）
- カスタム ユーザ ロールの削除 （12 ページ）

Custom Web User ロールの作成

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザロール（User Roles）] を選択します。

ステップ 3 [Webユーザ役割の追加（Add Web User Role）] をクリックします。

ヒント または、既存の Web User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [重複（Duplicate）] アイコンをクリックし、生成されたコピーを編集します。

ステップ 4 ユーザ ロールの一意の名前（たとえば「canadian-admins」）と説明を入力します。

（注） 名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュにすることはできません。

ステップ 5 デフォルトで、ポリシーとカスタム URL カテゴリを表示するか、非表示にするかを選択します。

ステップ 6 公開権限をオンにするか、オフにするかを選択します。

この権限を持つユーザは、ユーザがアクセス ポリシーまたは URL カテゴリを編集できるすべての Configuration Master を公開できます。

ステップ 7 新しい（空の）設定で始めるか、既存のカスタムユーザ ロールをコピーするかを選択します。既存のユーザ ロールをコピーする場合は、コピーするロールをリストから選択します。

ステップ 8 [送信（Submit）] をクリックして [ユーザ ロール（User Roles）] ページに戻ると、新しいユーザ ロールが表示されます。

（注） Web レポーティングで匿名機能をイネーブルにしていた場合、Web レポーティングへのアクセス権を持つすべてのユーザ ロールには、インタラクティブなレポート ページで認識できないユーザ名とロールが表示されるようになります。中央集中型 Web レポーティングおよびトラッキングの使用の章のWeb レポートのスケジュール設定のセクションを参照してください。Administrator ロールの場合は例外的に、スケジュール設定されたレポートで実際のユーザ名を確認できます。匿名機能がイネーブルになっている場合、オペレータおよびWeb管理者によって作成されたスケジュール設定されたレポートは匿名になります。

[Web] > [ユーティリティ（Utilities）] > [セキュリティ（Security）] > [サービス表示（Services Display）] > [セキュリティサービス表示の編集（Edit Security Services Display）] ページを使用して設定マスターの 1 つを非表示にしている場合、[ユーザロール（User Roles）] ページでも対応する [設定マスター（Configuration Master）] 列が非表示になりますが、非表示になっている設定マスターに対する権限設定は保持されます。

Custom Web User ロールの編集

ステップ 1 [ユーザロール（User Roles）] ページでロール名をクリックし、[ユーザロールの編集（Edit User Role）] ページを表示します。

ステップ 2 名前、説明、およびポリシーとカスタム URL カテゴリを表示するかどうかなどの設定を編集します。

ステップ 3 [送信（Submit）] をクリックします。

カスタム ユーザ ロールの権限を編集するには、次の手順を実行します。

[ユーザロール（User Roles）] ページに移動します。

- アクセス ポリシー権限を編集するには、[アクセスポリシー（Access policies）] をクリックして、Configuration Master に設定されているアクセス ポリシーのリストを表示します。[含める（Include）] 列で、ユーザ編集アクセス権を付与するポリシーのチェックボックスをオンにします。[送信（Submit）] をクリックして、[ユーザロール（User Roles）] ページに戻ります。

または

- カスタム URL カテゴリ権限を編集するには、カスタム URL カテゴリをクリックして、Configuration Master に定義されているカスタム URL カテゴリのリストを表示します。[含める（Include）] 列で、ユーザ編集アクセス権を付与するカスタム URL カテゴリのチェックボックスをオンにします。[送信（Submit）] をクリックして、[ユーザロール（User Roles）] ページに戻ります。

カスタム ユーザ ロールの削除

1 人以上のユーザに割り当てられているカスタム ユーザ ロールを削除する場合、エラーは受信しません。

CLI へのアクセス権を持つユーザー ロール

一部のロール（Administrator、Operator、Guest、Technician、および Read-Only Operator）は、GUI と CLI の両方にアクセスできます。他のロール（ヘルプデスク ユーザー、メール管理者、Web 管理者、Web ポリシー管理者、URL フィルタリング管理者（Web セキュリティ）、およびカスタム ユーザー）は GUI だけにアクセスできます。

LDAP の使用

ユーザーを認証するために LDAP ディレクトリを使用する場合は、個々のユーザーではなくユーザー ロールにディレクトリ グループを割り当てます。ユーザ ロールにディレクトリ グループを割り当てると、そのグループの各ユーザはそのユーザ ロールで定義された権限を受け取ります。詳細については、外部ユーザ認証 （22 ページ）を参照してください。

隔離へのアクセス

ユーザが隔離にアクセスする前にそのアクセスを有効にする必要があります。次の情報を参照してください。

- スパム隔離への管理ユーザ アクセスの設定
- メッセージ処理タスクの他のユーザへの割り当てについて（ポリシー隔離の場合）、および ポリシー、ウイルス、およびアウトブレイク隔離の設定
- カスタム ユーザー ロールの集約隔離アクセスの設定

[ユーザー（Users）] ページ

次のセクションの詳細について	参照先
Users [パスフレーズのリセット（Reset Passphrases）] ボタン	管理タスクの分散について （1 ページ） ローカルに定義された管理ユーザの管理 （14 ページ） ユーザに対するオンデマンドでのパスフレーズ変更の要求 （21 ページ）
ローカルユーザアカウントとパスフレーズの設定（Local User Account & Passphrase Settings）	パスフレーズの設定およびログインの要件 （17 ページ）
外部認証（External Authentication）	外部ユーザ認証 （22 ページ）
DLPトラッキング権限（DLP Tracking Privileges）	メッセージ トラッキングでの機密情報へのアクセスの制御 （33 ページ）

管理ユーザーの認証について

認可されたユーザーをアプライアンスでローカルに定義したり、外部認証や二要素認証を使用したりすることで、アプライアンスに対するアクセスを制御できます。

- admin ユーザのパスフレーズの変更 （14 ページ）
- 有効期限後のユーザー パスフレーズの変更 （14 ページ）
- ローカルに定義された管理ユーザの管理 （14 ページ）
- 外部ユーザ認証 （22 ページ）
- 二要素認証 （26 ページ）

admin ユーザのパスフレーズの変更

管理者レベルのユーザは、GUI または CLI を使用して「admin」ユーザのパスフレーズを変更できます。

（注） 初めてアプライアンスにログインするか、設定を出荷時の初期設定にリセットする場合、パスフレーズを変更することをお勧めします。

GUI を使用してパスフレーズを変更するには、次の手順を実行します。

- （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで をクリックして、レガシー Web インターフェイスをロードします。
- [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ユーザー（Users）] ページを選択し、管理者ユーザーを選択します。

admin ユーザのパスフレーズを CLI から変更するには、`passphrase` コマンドを使用します。`passphrase` コマンドでは、セキュリティのために古いパスフレーズの入力が必要です。

「admin」ユーザー アカウントのパスフレーズを忘れた場合は、パスフレーズをリセットするためにカスタマー サポート プロバイダーにご連絡ください。

（注） パスフレーズの変更はすぐに有効になり、変更の確定は必要ではありません。

有効期限後のユーザー パスフレーズの変更

アカウントの有効期限が切れると、「お使いのパスフレーズは有効期限が切れています。変更してください、パスフレーズは、ここをクリックしています。」

リンクをクリックして、期限切れのパスフレーズでログインの詳細を入力し、[パスフレーズの変更（Change Passphrase）] ページに進みます。のパスワードの設定の詳細についてはパスフレーズの設定およびログインの要件 （17 ページ）。

（注） パスフレーズの変更はすぐに有効になり、変更の確定は必要ではありません。

ローカルに定義された管理ユーザの管理

- ローカルに定義されたユーザの追加 （15 ページ）
- ローカルに定義されたユーザの編集 （16 ページ）
- ローカルに定義されたユーザの削除 （16 ページ）
- ローカルに定義されたユーザのリストの表示 （16 ページ）

- パスフレーズの設定と変更 （16 ページ）
- パスフレーズの設定およびログインの要件 （17 ページ）
- ユーザに対するオンデマンドでのパスフレーズ変更の要求 （21 ページ）
- ローカル ユーザー アカウントのロックおよびロック解除 （21 ページ）

ローカルに定義されたユーザの追加

外部認証を使用していない場合は、次の手順に従って、ユーザをセキュリティ管理アプライアンスに直接追加します。または、CLI で **userconfig** コマンドを使用します。

（注） 外部認証もイネーブルである場合は、ローカル ユーザ名が外部認証されたユーザ名と重複しないことを確認してください。

アプライアンスに作成できるユーザ アカウントの数に制限はありません。

ステップ 1 カスタムユーザ ロールを割り当てる場合は、そのロールを先に定義しておくことを推奨します。カスタムユーザロール （5 ページ）を参照してください。

ステップ 2 （新しいWebインターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 3 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 4 [ユーザの追加（Add User）] をクリックします。

ステップ 5 ユーザの一意の名前を入力します。システムで予約されている語（「`operator`」や「`root`」など）を入力することはできません。

外部認証も使用する場合は、ユーザ名を外部認証されたユーザ名と重複させることはできません。

ステップ 6 ユーザの氏名を入力します。

ステップ 7 事前定義されたロールまたはカスタム ロールを選択します。ユーザ ロールの詳細については、事前定義済みユーザ ロール （2 ページ）セクションの表「ユーザ ロールの説明」を参照してください。

新しい Email ロールまたは Web ロールをここに追加する場合は、ロールの名前を入力します。命名上の制限については、Custom Email User ロールの作成 （8 ページ）またはCustom Web User ロールの作成 （11 ページ）を参照してください。

ステップ 8 セキュリティ検証のために現在のパスフレーズを確認します。

ステップ 9 パスフレーズを生成または入力して、確認のためにパスフレーズをもう一度入力します。

ステップ 10 変更を送信し、保存します。

ステップ 11 このページにカスタムユーザ ロールを追加する場合は、この時点でそのロールに権限を割り当てます。カスタムユーザロール （5 ページ） を参照してください。

ローカルに定義されたユーザの編集

たとえば、パスフレーズを変更するには、この手順を実行します。

ステップ 1 [ユーザー（Users）] 一覧でユーザーの名前をクリックします。
ステップ 2 ユーザに対して変更を行います。
ステップ 3 セキュリティ検証のために現在のパスフレーズを確認します。
ステップ 4 変更を送信し、保存します。

ローカルに定義されたユーザの削除

ステップ 1 [ユーザー（Users）] 一覧でユーザーの名前に対応するゴミ箱アイコンをクリックします。
ステップ 2 表示される警告ダイアログで [削除（Delete）] をクリックして削除を確認します。
ステップ 3 [確定する（Commit）] をクリックして変更を保存します。

ローカルに定義されたユーザのリストの表示

ローカルで定義されたユーザの一覧を表示するには、次の手順を実行します。

- [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

（注） アスタリスクは、委任された管理に応じてユーザに割り当てられたカスタム ユーザ ロールを示します。ユーザのカスタム ロールが削除されている場合は、[未定義（Unassigned）] と赤く表示されます。カスタム ユーザ ロールの詳細については、カスタムユーザロール（5 ページ）を参照してください。

パスフレーズの設定と変更

- ユーザを追加する場合は、そのユーザに初期パスフレーズを指定します。
- システムに設定されたユーザのパスフレーズを変更するには、GUI の [ユーザの編集（Edit User）] ページを使用します（詳細は、ローカルに定義されたユーザの編集 （16 ページ）を参照してください）。

（注） 初めてアプライアンスにログインする場合や、システムセットアップ ウィザードを完了した後は、パスフレーズを変更することをお勧めします。

- システムのデフォルト管理ユーザアカウントのパスフレーズを変更するには、admin ユーザのパスフレーズの変更 （14 ページ）を参照してください。
- ユーザにパスフレーズの変更を強制するには、ユーザに対するオンデマンドでのパスフレーズ変更の要求 （21 ページ）を参照してください。
- GUI 右側上部の [オプション（Options）] メニューをクリックして、[パスフレーズの変更（Change Passphrase）] オプションを選択することで、ユーザは自分のパスフレーズを変更できます。

パスフレーズの設定およびログインの要件

ユーザ アカウントとパスフレーズの制限を定義して、組織全体にパスフレーズ ポリシーを強制的に適用することができます。ユーザアカウントとパスフレーズの制限は、セキュリティ管理アプライアンスで定義されているローカルユーザに適用されます。次の設定値を設定できます。

- **ユーザアカウントのロック。**ユーザのアカウントがロックアウトされる失敗ログインの試行回数を定義できます。
- **パスフレーズ存続期間のルール。**ログイン後にユーザがパスフレーズの変更を要求されるまでの、パスフレーズの存続期間を定義できます。
- **パスフレーズルール。**任意指定の文字や必須の文字など、ユーザが選択できるパスフレーズの種類を定義できます。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ユーザ（Users）] を選択します。

ステップ 3 [ローカルユーザアカウントとパスワードの設定（Local Account and **Passphrase** Settings）] セクションまで下にスクロールします。

ステップ 4 [設定の編集（Edit Settings）] をクリックします。

ステップ 5 設定を次のように構成します。

設定	説明
[ユーザ アカウントのロック（User Account Lock）]	ユーザが正常にログインできない場合に、ユーザアカウントをロックするかどうかを決定します。アカウントをロックすることになる失敗ログイン試行の回数を指定します。1 から 60 までの任意の数を入力できます。デフォルトは 5 です。 アカウントのロックを設定する場合は、ログインを試みているユーザに表示するメッセージを入力します。テキストは 7 ビット ASCII 文字を使用して入力します。このメッセージは、ユーザがロックされているアカウントの正しいパスフレーズを入力した場合のみ表示されます。 ユーザ アカウントがロックされた場合、管理者は GUI で [ユーザの編集（Edit User）] ページを使用するか、`userconfig` CLI コマンドを使用してロックを解除できます。 失敗したログインの試行は、ユーザが接続しているマシンや、接続のタイプ（SSH または HTTP など）に関係なく、ユーザ別に追跡されます。ユーザがログインに成功すると、失敗ログイン試行の回数は 0 にリセットされます。 失敗ログイン試行の最大回数に達したためにユーザアカウントがロックアウトされると、管理者にアラートが送信されます。このアラートは「Info」重大度レベルに設定されます。 （注） 個々のユーザアカウントを手動でロックすることもできます。手動によるユーザ アカウントのロック （21 ページ）を参照してください。
パスフレーズのリセット	管理者がユーザのパスフレーズを変更した後で、ユーザにパスフレーズを強制的に変更させるかどうかを選択します。 パスワードが期限切れになった後で、ユーザにパスフレーズを強制的に変更させるかどうかを選択することもできます。ユーザによるパスフレーズの変更が必要になるまでの、パスフレーズの有効日数を入力します。1 から 366 までの任意の数を入力できます。デフォルトは 90 です。スケジュール外の時間に、ユーザにパスフレーズの変更を強制するには、ユーザに対するオンデマンドでのパスフレーズ変更の要求 （21 ページ）を参照してください。 期限切れ後にユーザにパスフレーズを強制的に変更させる場合は、次回のパスフレーズ期限に関する通知を表示できます。期限切れの何日前にユーザに通知するかを選択します。 （注） ユーザ アカウントがパスフレーズ チャレンジの代わりに SSH キーを使用している場合でも、パスフレーズ リセット ルールが適用されます。SSH キーを使用しているユーザ アカウントが期限切れになった場合、ユーザは古いパスフレーズを入力するか、アカウントに関連付けられているキーを変更するためにパスフレーズを手動で変更するよう管理者に依頼する必要があります。

設定	説明
パスフレーズ ルール： <number> 文字以上にする必要があります。	パスフレーズに含める最小文字数を入力します。 1 ～ 128 の範囲内の任意の数を入力してください。 デフォルトは 8 です。 パスフレーズには、ここで指定した数より多い文字を使用できます。
パスフレーズ ルール： 数字(0～9)が1文字以上必要です。	パスフレーズに数字を少なくとも 1 文字含める必要があるかどうかを選択します。
パスフレーズ ルール： 特殊文字が1文字以上必要です。	パスフレーズに 1 文字以上の特殊文字を含める必要があるかどうかを決定します。パスフレーズには、次の特殊文字を使用できます。 ~ ? ! @ # $ % ^ and * - _+ = \ | / [ ] ( ) < > { } ` ' " ; : , 。
パスフレーズ ルール： ユーザ名とその変化形をパスフレーズとして使用することはできません。	対応するユーザ名またはユーザ名の変化形と同じものを、パスフレーズに使用できるかどうかを決定します。ユーザ名の変化形の使用を禁止する場合、次のルールがパスフレーズに適用されます。 • 大文字か小文字かに関係なく、パスフレーズはユーザ名と同じであってはならない。 • 大文字か小文字かに関係なく、パスフレーズはユーザ名を逆にしたものと同じであってはならない。 • パスフレーズは、次の文字置換が行われたユーザ名、またはユーザ名を逆にしたものと同じであってはならない。 • 「a」の代わりに「@」または「4」 • 「e」を「3」に置換 • 「i」を「|」、「!」、または「1」に置換 • 「o」を「0」に置換 • 「s」を「$」または「5」に置換 • 「t」を「+」または「7」に置換
パスフレーズ ルール： 直近 <number> 個のパスフレーズを再使用することはできません。	ユーザにパスフレーズの変更を強制する場合に、最近使用したパスフレーズを選択できるかどうかを決定します。最近のパスフレーズの再使用を禁止する場合、再使用を禁止する最近のパスフレーズの個数を入力します。 1 から 15 までの任意の数を入力できます。デフォルトは 3 です。

設定	説明
パスフレーズルール: パスフレーズで許可しない単語の一覧	パスフレーズでの使用を禁止する単語のリストを作成できます。 このファイルは、許可しない単語ごとに行を分けたテキストファイルにします。forbidden_passphrase_words.txt という名前でファイルを保存し、SCP や FTP を使用してアプライアンスにファイルをアップロードします。 この制限を選択しても単語のリストをアップロードしないと、この制限は無視されます。
パスフレーズの強度	管理者またはユーザが新しいパスフレーズを入力するときに、パスフレーズ強度インジケータを表示できます。 この設定によって強固なパスフレーズが作成されるわけではありません。この設定は、入力したパスフレーズの推測されやすさを示すだけです。 インジケータを表示する対象ロールを選択します。次に、選択したロールごとにゼロより大きい数字を入力します。数字が大きいほど、強力であるとして登録されるパスフレーズは推測されにくいことを意味します。この設定に最大値はありません。 例： • 30 と入力した場合は、少なくとも 1 つの大文字と小文字、数字、特殊文字を含む 8 文字のパスフレーズが強力なパスフレーズとして登録されます。 • 18 と入力した場合は、すべて小文字で数字と特殊文字を含まない 8 文字のパスフレーズが強固なパスフレーズとして登録されます。 パスフレーズの強度は対数目盛で測定されます。評価は、NIST SP 800-63 付則 A の定義に準拠する、米国国立標準技術研究所のエントロピールールに基づいています。 一般的に、強固なパスフレーズは次のような特徴を備えています。 • 長い。 • 大文字、小文字、数字、および特殊文字を含む。 • あらゆる言語の辞書にある語を含まない。 これらの特徴を備えたパスフレーズを適用するには、このページの他の設定を使用します。

ステップ 6 変更を送信し、保存します。

次のタスク

ユーザにパスフレーズを新しい要件を満たす新しいパスフレーズに変更するよう要求します。ユーザに対するオンデマンドでのパスフレーズ変更の要求 （21 ページ）を参照してください

ユーザに対するオンデマンドでのパスフレーズ変更の要求

すべての、または選択したユーザに、アドホック ベースでパスフレーズを変更するように要求するには、次の手順を実行します。これは 1 回限りのアクションです。

パスフレーズを変更するための定期的な要求を自動化するには、パスフレーズの設定およびログインの要件 （17 ページ）で説明されている [パスワードのリセット（Passphrase Reset）] オプションを使用します。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ユーザ（Users）] を選択します。

ステップ 3 [ユーザ（Users）]セクションで、パスフレーズの変更が必要なユーザの横のチェック ボックスをオンにします。

ステップ 4 [パスワードの変更を実施（**Enforce PassphraseChanges**）]を選択します。

ステップ 5 オプションを選択します。

猶予期間のグローバル設定は[ローカルユーザアカウントとパスワードの設定（Local User Account & Passphrase Settings）] で設定します。

ステップ 6 [OK] をクリックします。

ローカル ユーザー アカウントのロックおよびロック解除

ユーザー アカウントのロックは、ローカル ユーザーがアプライアンスにログインするのを防止します。ユーザー アカウントは、次のいずれかの場合にロックされることがあります。

- すべてのローカル ユーザー アカウントを、設定した試行回数の後にユーザーが正常なログインに失敗するとロックするように、設定することができます。パスフレーズの設定およびログインの要件 （17 ページ）を参照してください。
- 管理者はユーザアカウントを手動でロックできます。手動によるユーザアカウントのロック （21 ページ）を参照してください。

[ユーザの編集（Edit User）]ページでユーザ アカウントを表示すると、AsyncOS によりユーザ アカウントがロックされた理由が表示されます。

手動によるユーザ アカウントのロック

ステップ 1 初回のみ：アプライアンスを設定して、ユーザー アカウントのロックをイネーブルにします。

ステップ 2 次の手順を実行します。

a) （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。
b) [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザー（Users）] に移動します。
c) [ローカルユーザアカウントとパスワードの設定（Local User Account & **Passphrase** Settings）] セクションで、[設定の編集（Edit Settings）] をクリックします。
d) [管理者が手動でユーザアカウントをロックした場合、ロックされたアカウントメッセージを表示します。（Display Locked Account Message if Administrator has manually locked a user account）] に対するチェックボックスを選択して、メッセージを入力します。
e) 変更を送信します。

ステップ 3 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザー（Users）] に移動して、ユーザー名をクリックします。

（注） admin アカウントをロックする前に、ロック解除できることを確認してください。ユーザー アカウントのロック解除 （22 ページ）の（注）を参照してください。

ステップ 4 [アカウントのロック（Lock Account）] をクリックします。

AsyncOS は、ユーザがアプライアンスにログインできなくなるというメッセージを表示し、継続するかどうかを問い合わせてきます。

ユーザー アカウントのロック解除

ユーザー アカウントをロック解除するには、[ユーザー（Users）] 一覧でユーザー名をクリックしてユーザー アカウントを開き、[アカウントのロック解除（Unlock Account）] をクリックします。

（注） admin アカウントをロックした場合は、シリアル コンソール ポートへのシリアル通信接続経由で admin としてログインしてロック解除するしかありません。admin ユーザは、admin アカウントがロックされた場合でも、シリアル コンソール ポートを使用して常にアプライアンスにアクセスできます。シリアル コンソール ポートを使用してアプライアンスにアクセスする方法の詳細については、お使いの E メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Setup and Installation」の章を参照してください。

外部ユーザ認証

ネットワークの LDAP または RADIUS ディレクトリにユーザ情報を保存する場合は、外部ディレクトリを使用してアプライアンスにログインするユーザを認証するようセキュリティ管理アプライアンスを設定できます。

（注） ビューのカスタマイズで説明されている一部の機能は、外部認証ユーザには使用できません。

- 展開でローカル認証と外部認証の両方を使用している場合、ローカルユーザ名と外部認証ユーザ名を同じにしないでください。
- アプライアンスが外部ディレクトリと通信できない場合、外部アカウントとローカルアカウントの両方を持つユーザーは、ローカル ユーザー アカウントを使用してアプライアンスにログインできます。

参照先：

- LDAP を使用した管理ユーザの外部認証の設定
- RADIUS 認証の有効化 （23 ページ）

LDAP 認証の設定

LDAP 認証を設定するには、LDAP を使用した管理ユーザの外部認証の設定を参照してください。

RADIUS 認証の有効化

ユーザを認証し、アプライアンスを管理しているユーザ ロールにユーザ グループを割り当てるために RADIUS ディレクトリを使用できます。RADIUS サーバは CLASS 属性をサポートする必要があります（AsyncOS は RADIUS ディレクトリのユーザをユーザ ロールに割り当てるために CLASS 属性を使用します）。

（注） 外部ユーザが RADIUS グループのユーザ ロールを変更する場合は、アプライアンスからログアウトして再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

始める前に

RADIUS サーバへの共有シークレット キーの長さは 48 文字以下でなければなりません。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページを選択して、[有効化（Enable）] をクリックします。

ステップ 3 [外部認証を有効にする（Enable External Authentication）] チェックボックスをオンにします。

ステップ 4 認証タイプとして RADIUS を選択します。

ステップ 5 RADIUS サーバのホスト名を入力します。

ステップ 6 RADIUS サーバのポート番号を入力します。デフォルト ポート番号は、1812 です。

ステップ 7 RADIUS サーバの共有シークレット キーを入力します。

（注） E メール セキュリティ アプライアンスのクラスタに対して外部認証を有効にするには、クラスタ内のすべてのアプライアンスで同じ共有シークレット キーを入力します。

ステップ 8 タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 9 認証プロトコルとして、パスフレーズ認証プロトコル（PAP）を使用するか、またはチャレンジ ハンドシェイク認証プロトコル（CHAP）を使用するか選択します。

ステップ 10 （任意）[行の追加（Add Row）] をクリックして別の RADIUS サーバを追加します。認証のためにアプライアンスで使用する各 RADIUS サーバに対してステップ 6 とステップ 7 を繰り返します。

複数の外部サーバを定義する場合、アプライアンスは、アプライアンスに定義されている順序でサーバに接続します。1 つのサーバが一時的に使用できない場合、フェールオーバーを実行できるように、複数の外部サーバを定義する場合があります。

ステップ 11 Web ユーザ インターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

（注） RADIUS サーバがワンタイム パスフレーズ（たとえば、トークンから作成されるパスフレーズ）を使用する場合、ゼロ（0）を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバに再アクセスしません。

ステップ 12 グループ マッピングの設定

設定	説明
[外部認証されたユーザを複数のローカルロールに割り当てます（推奨）（Map externally authenticated users to multiple local roles（Recommended））]	AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザをアプライアンス ロールに割り当てます。CLASS 属性の要件： • 3 文字以上 • 253 文字以下 • コロン、カンマ、または改行文字なし • 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性（この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します）。 複数の CLASS 属性のある RADIUS ユーザの場合、AsyncOS は最も制限されたロールを割り当てます。たとえば、Operator ロールにマッピングされている CLASS 属性と、Read-Only Operator ロールにマッピングされている CLASS 属性の 2 つが RADIUS ユーザにある場合、AsyncOS は、Operator ロールよりも制限された Read-Only Operator ロールに RADIUS ユーザを割り当てます。 次のアプライアンス ロールは、制限の少ないものから順番に並べられています。 • 管理者（Administrator） • Email Administrator • Web Administrator • Web Policy Administrator • URL Filtering Administrator（Web セキュリティ） • カスタム ユーザ ロール（電子メールまたは Web） ユーザにカスタムユーザ ロールにマッピングされた複数のクラス属性が割り当てられている場合、RADIUS サーバのリストの最後のクラス属性が使用されます。 • 専門技術者 • 演算子 • Read-Only Operator • ヘルプ デスク ユーザ • ゲスト

設定	説明
[外部認証されたすべてのユーザを管理者ロールに割り当てます（Map all externally authenticated users to the Administrator role）]	AsyncOS は RADIUS ユーザを Administrator ロールに割り当てます。

ステップ 13 （任意）[行の追加（Add Row）] をクリックして別のグループを追加します。アプライアンスが認証するユーザの各グループに対してステップ 11 を繰り返します。

ステップ 14 変更を送信し、保存します。

二要素認証

RADIUSディレクトリを使用して、特定のユーザ ロールの二要素認証を設定できます。アプライアンスは、RADIUS サーバーとの通信用の次の認証プロトコルをサポートします。

- パスフレーズ認証プロトコル（PAP）
- Challenge Handshake Authentication Protocol（CHAP）

次のユーザ ロールに対して二要素認証を有効にできます。

- 定義済み
- カスタム

機能は次によりテストされています。

- RSA 認証マネージャ v8.2
- FreeRADIUS v1.1.7 以上
- ISE v1.4 以降

関連トピック：

- 二要素認証の有効化 （26 ページ）
- 二要素認証の無効化 （27 ページ）
- 事前共有キーによる SSH を介した E メールまたは Web セキュリティ アプライアンスの追加 （27 ページ）

二要素認証の有効化

IT 管理者から二要素認証に必要な RADIUS サーバーの詳細を得ていることを確認してください。

ステップ 1 （新しいWebインターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [システム管理（System Administration）]>[ユーザー（Users）] ページを選択し、[二要素認証（Two-Factor Authentication）] の下の [有効化（Enable）] をクリックします

ステップ 3 RADIUS サーバのホスト名または IP アドレスを入力します。

ステップ 4 RADIUS サーバのポート番号を入力します。

ステップ 5 RADIUS サーバーの共有秘密パスフレーズを入力します。

ステップ 6 タイムアウトまでにサーバからの応答を待つ時間を秒単位で入力します。

ステップ 7 適切な認証プロトコルを選択します。

ステップ 8 （任意）[行の追加（Add Row）] をクリックして別の RADIUS サーバを追加します。各 RADIUS サーバについて、2 ～ 6 のステップを繰り返します。

（注） 最大 10 個の RADIUS サーバを追加できます。

ステップ 9 二要素認証を有効にする必須ユーザ ロールを選択します。

ステップ 10 変更を送信し、保存します。

二要素認証を有効にすると、ユーザーはアプライアンスにログインするために、ユーザー名とパスフレーズを入力した後にパスコードを入力することが求められます。

二要素認証の無効化

始める前に

お使いのアプライアンスで二要素認証を有効にしていることを確認します。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [システム管理（System Administration）] > [ユーザー（Users）] ページを選択し、[二要素認証（Two-Factor Authentication）] の下の [グローバル設定を編集（Edit Global Settings）] をクリックします

ステップ 3 [二要素認証を有効にする（Enable Two-Factor Authentication）] の選択を解除します。

ステップ 4 変更を送信し、保存します。

事前共有キーによる SSH を介した E メールまたは Web セキュリティ アプライアンスの追加

次の例は、事前共有キーを使用し、SSH を介して、セキュリティ管理アプライアンス (testsma.example.com) に E メール セキュリティ アプライアンス (testesa.example.com) を追加する方法を示しています。

Web セキュリティ アプライアンスを追加するには、シスコのアプライアンスのタイプが求められたときに、**WSA** を選択します。

```
testsma.example.com> applianceconfig

Choose the operation you want to perform.

ADD - Add SMA Connection Parameters and Keys.
EDIT - Edit an appliance.
DELETE - Remove an appliance.
TEST - Test that an appliance is properly configured.
SERVICES - Configure the centralized services for an appliance.
STATUS - Display the status of centralized services.
PORT - Configure which port is used to communicate with remote appliances.

[]> add

Please enter the type of Cisco appliance that this device is
1. ESA
2. WSA

[1]> 1

Enter the IP address or hostname of an appliance to transfer data with.
(A hostname may be entered in this field, however it will be immediately
resolved to an IP address when the form is submitted.)
[]> IP address entered

Enter a name to identify this appliance

[]> name of appliance

File transfer access via SSH is required to transfer reporting data, message logs,
and quarantine safelist/blocklist data from appliances

Would you like to configure file transfer access for this appliance? [Y]>

Would you like to use a custom ssh port to connect to this appliance? [N]>

Would you like to connect an Email Security appliance using pre-shared keys?
Use this option if you have enabled two-factor authentication on the Email
Security appliance. [N]> yes

To add an Email Security appliance to the Content Security Management appliance
using pre-shared keys, log in to the Email Security appliance,
run the smaconfig > add command, enter the following details.

Host: vm10sma0006.qa

User Key:
AAAAB3NzaC1yc2EAAAADAQABAAABAQDgm3kG9RHc4gVZxRe0orh5DW5Yje5UB9BpJqcTRQJoxUIAv2Xig
8q5geyaWHZcFoUxH61YQbPX3R8CVMYgJ8/QB/iunjkr3jowV/SCuBBikEFgj1zuxlsFhL0L487epEgbylgH0rfJ
gwSa2/6dhfyUayst6pT87CZGOQltgx7s51wc+ve770X3SqlQD5bdYC4x9+gCX0wdwfhTH1+4/82jwYjK1lAEXc
O4k4TuZJEJnyBQ3YyCyVwXuDkXpI6xJDemxcc36e7Wwtpn3mn2VLaTG2/I38XwSvlYB6TcqmWnO10gL+aD
wkKAKcuhYpz4NFr9myej1mhMk7ZAFXmRNxvT
```

（注） 次の手順に進む前に、**ホスト**と**ユーザー キー**の詳細が E メールまたは Web セキュリティ アプライアンスに追加されていることを確認します。E メールまたは Web セキュリティ アプライアンスで変更を確定してから、セキュリティ管理アプライアンスで接続パラメータを追加するプロセスを続行します。

```
Do you want to continue connecting using pre-shared keys? [Y]> yes
```

セキュリティ管理アプライアンスへのアクセスに対する追加の制御

- IP ベースのネットワーク アクセスの設定 （29 ページ）
- Web UI セッション タイムアウトの設定 （32 ページ）

IP ベースのネットワーク アクセスの設定

組織がリモート ユーザーに逆プロキシを使用する場合、アプライアンスに直接接続するユーザー、および逆プロキシを介して接続するユーザーのためのアクセス リストを作成することで、ユーザーがどの IP アドレスからセキュリティ管理アプライアンスにアクセスするのかを制御できます。

- 直接接続 （29 ページ）
- プロキシ経由の接続 （29 ページ）
- アクセス リストの作成 （30 ページ）

直接接続

セキュリティ管理アプライアンスに接続できるマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザーは、アクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。リストに含まれていないアドレスからアプライアンスに接続しようとするユーザーのアクセスは拒否されます。

プロキシ経由の接続

リモート ユーザーのマシンとセキュリティ管理アプライアンスの間で逆プロキシ サーバーが使用される組織のネットワークの場合、AsyncOS ではアプライアンスに接続可能なプロキシの IP アドレスを含むアクセス リストを作成できます。

逆プロキシを使用している場合でも、AsyncOS は、ユーザー接続が許可されている IP アドレスのリストと照合して、リモート ユーザーのマシンの IP アドレスを検証します。リモート ユーザーの IP アドレスを E メール セキュリティ アプライアンスに送信するには、プロキシで x-forwarded-for HTTP ヘッダーをアプライアンスへの接続要求に含める必要があります。

x-forwarded-for ヘッダーは RFC 非準拠の HTTP ヘッダーであり、次の形式になります。

x-forwarded-for: client-ip, proxy1, proxy2,... CRLF .

このヘッダーの値はカンマ区切りの IP アドレスのリストです。左端のアドレスがリモートユーザマシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます（ヘッダー名は設定可能です）。セキュリティ管理アプライアンスは、ヘッダーのリモートユーザーの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リストで許可されたユーザー IP アドレスやプロキシ IP アドレスと照合します。

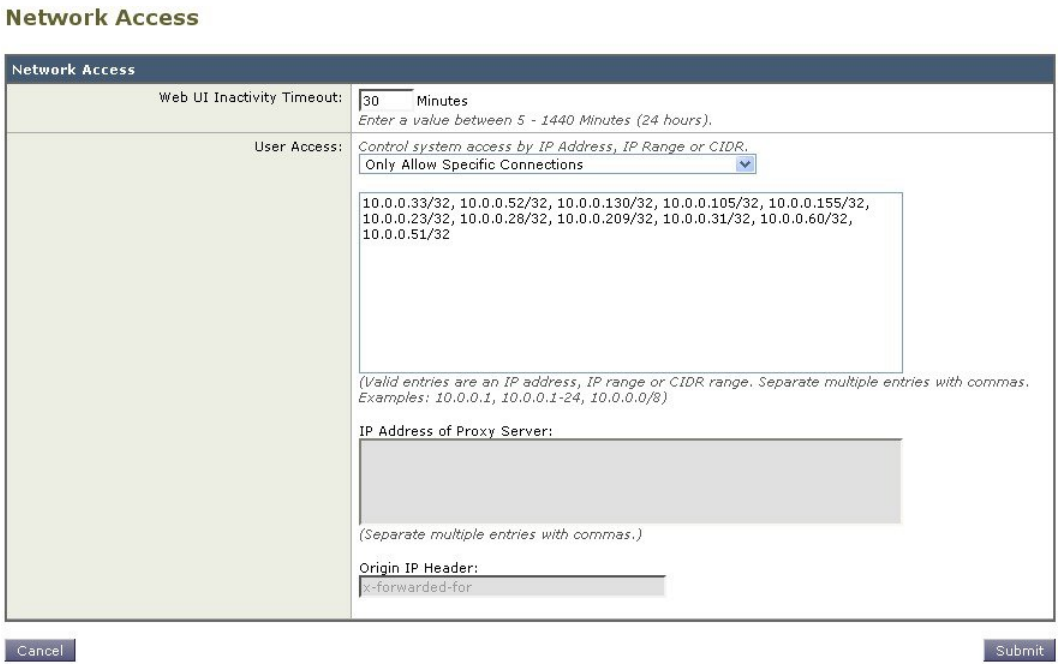
（注） AsyncOS は x-forwarded-for ヘッダーでは IPv4 アドレスだけをサポートします。

アクセス リストの作成

GUI の [ネットワークアクセス（Network Access）] ページまたは CLI の **adminaccessconfig > ipaccess** コマンドを介して、ネットワーク アクセス リストを作成できます。次の図は、セキュリティ管理アプライアンスへの直接的な接続が許可されているユーザー IP アドレスのリストが表示された [ネットワークアクセス（Network Access）] ページを示しています。

次の設定は、アプライアンスのレガシー Web インターフェイスおよび新しい Web インターフェイスに適用できます。

図 *2:* ネットワーク アクセス設定の例



AsyncOS はアクセス リストの制御で 4 種類のモードを用意しています。

- **[すべて許可（Allow All）]。**このモードはアプライアンスへの接続をすべて許可します。これが操作のデフォルト モードです。

- **[特定の接続のみを許可（Only Allow Specific Connections）]。**このモードは、ユーザーの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザーのアプライアンスへの接続を許可します。
- **[特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）]。**このモードは、次の条件を満たせば、逆プロキシ経由でアプライアンスへの接続を許可します。
  - 接続プロキシの IP アドレスが、アクセス リストの [プロキシサーバのIPアドレス（IP Address of Proxy Server）] フィールドに含まれている。
  - プロキシの接続要求に x-forwarded-header HTTP ヘッダーが記載されている。
  - x-forwarded-header の値が空ではない。
  - リモート ユーザの IP アドレスが x-forwarded-header に含まれ、それがアクセス リスト内のユーザに対して定義された IP アドレス、IP 範囲、または CIDR 範囲と一致する。
- **[特定の直接接続またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）]。**このモードは、アクセス リストに含まれる IP アドレス、IP 範囲、CIDR 範囲のいずれかにユーザーの IP アドレスが一致すれば、アプライアンスへの逆プロキシ経由接続または直接接続を許可します。プロキシ経由接続の条件は、[特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] モードと同じです。

次のいずれかの条件がtrueの場合、変更を送信して確定した後、アプライアンスにアクセスできなくなることがありますので注意してください。

- [特定の接続のみを許可（Only Allow Specific Connections）] を選択し、現在のマシンの IP アドレスがリストに含まれていない場合。
- [特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] を選択し、現在アプライアンスに接続されているプロキシの IP アドレスがプロキシ リストに存在せず、許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合。
- [特定の直接接続またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）] を選択し、
  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合

    または

  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在せず、アプライアンスに接続されたプロキシの IP アドレスが許可されているプロキシのリストに存在しない場合。

アクセス リストを修正せずに続行した場合、ユーザーが変更を確定すると、AsyncOS はアプライアンスからユーザーのマシンまたはプロキシを切断します。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [システム管理（System Administration）] > [ネットワークアクセス（Network Access）] を選択します。

ステップ 3 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 4 アクセス リストの制御モードを選択します。

ステップ 5 アプライアンスへの接続を許可するユーザーの IP アドレスを入力します。

IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを指定する場合は、カンマで区切ります。

ステップ 6 プロキシ経由接続が許可されている場合は、次の情報を入力します。

- アプライアンスへの接続を許可するプロキシの IP アドレス。複数のエントリを指定する場合は、カンマで区切ります。
- プロキシがアプライアンスに送信する発信元の IP ヘッダーの名前。これには、リモート ユーザー マシンの IP アドレスと、要求を転送したプロキシ サーバーの IP アドレスが含まれます。デフォルトのヘッダー名は x-forwarded-for です。

ステップ 7 変更を送信し、保存します。

Web UI セッション タイムアウトの設定

セキュリティ管理アプライアンスの Web UI から AsyncOS が、非アクティブなユーザーをログアウトするまでの時間を指定できます。この Web UI セッション タイムアウトは、admin を含むユーザー全員に適用されます。また、HTTP セッションと HTTPS セッションのいずれにも使用されます。

AsyncOS によってユーザーがログアウトされると、アプライアンスはユーザーの Web ブラウザをログイン ページにリダイレクトします。

（注） Web UI セッション タイムアウトはスパム隔離セッションには適用されません。このセッションには 30 分のタイムアウトが設定されており、変更できません。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [システム管理（System Administration）] > [ネットワークアクセス（Network Access）] ページを使用します。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 ログアウトまでにユーザを非アクティブにできる分数を [Web UI 非アクティブ タイムアウト（Web UI Inactivity Timeout）] フィールドに入力します。5 ～ 1440 分のタイムアウト期間を定義できます。

ステップ 5 変更を送信し、保存します。

CLI セッション タイムアウトの設定

セキュリティ管理アプライアンスの CLI から AsyncOS が、非アクティブなユーザーをログアウトするまでの時間を指定できます。以下に CLI セッション タイムアウトが適用されます。

- すべてのユーザ（管理者を含む）
- セキュア シェル（SSH）、SCP、および直接シリアル接続を使用している接続のみ

（注） CLI セッション タイムアウト時に未確定の設定変更は失われます。設定を変更したらすぐに確定してください。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [システム管理（System Administration）] > [ネットワークアクセス（Network Access）] ページを使用します。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 [CLI 非アクティブ タイムアウト（CLI Inactivity Timeout）] フィールドに、ログアウトされるまでにユーザを非アクティブにできる分数を入力します。5 ～ 1440 分のタイムアウト期間を定義できます。

ステップ 5 変更を送信し、保存します。

次のタスク

また、CLI で `adminaccessconfig` コマンドを使用して CLI セッション タイムアウトを設定することもできます。『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

メッセージ トラッキングでの機密情報へのアクセスの制御

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ユーザ（Users）] ページに移動します。

ステップ 3 [トラッキング権限（Tracking Privileges）] セクションで、[設定の編集（Edit Settings）] をクリックします。

ステップ 4 メッセージ トラッキングで機密情報へのアクセス権を付与するロールを選択します。

メッセージ トラッキングへのアクセス権を持つカスタム ロールだけが一覧表示されます。

ステップ 5 変更を送信し、保存します。

この設定を有効にするには、[管理アプライアンス（Management Appliance）]>[集約管理サービス（Centralized Services）] で中央集中型電子メール メッセージ トラッキング機能をイネーブルにする必要があります。

管理ユーザー向けメッセージの表示

管理ユーザーがアプライアンスにサインインするときにメッセージを表示できます。

メッセージを設定またはクリアするには、次の手順を実行します。

ステップ 1 テキストファイルの使用使用を計画している場合は、アプライアンスの `/data/pub/configuration` ディレクトリにアップロードします。

ステップ 2 コマンドライン インターフェイス（CLI）にアクセスします。

ステップ 3 adminaccessconfig > BANNER コマンドを実行します。

ステップ 4 バナーメッセージをロードします。

ステップ 5 変更を確定します。

管理ユーザー向けメッセージバナーの有効化と無効化

アプライアンスのレガシー Web インターフェイスからアプライアンスの新しい Web インターフェイスに移動するためのリンクを含むバナーを有効または無効にできます。

ステップ 1 コマンドライン インターフェイス（CLI）にアクセスします。

ステップ 2 adminaccessconfig > NGUIBANNER コマンドを実行します。

ステップ 3 バナーメッセージを有効または無効にします。

ステップ 4 変更を確定します。

管理ユーザー アクティビティの表示

• Web を使用したアクティブなセッションの表示 （35 ページ）

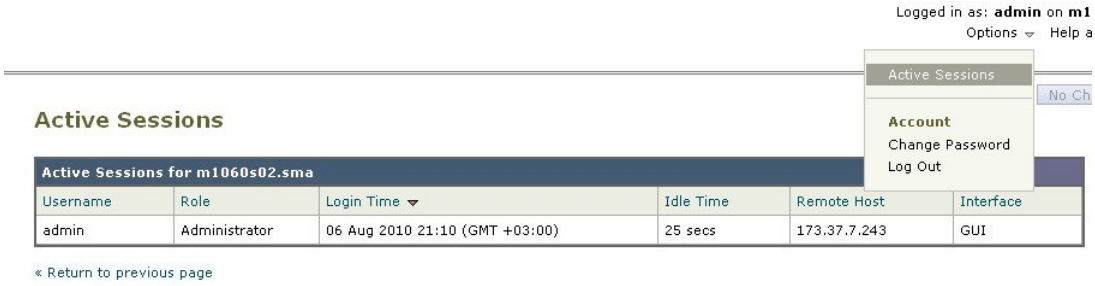
• 最近のログイン試行の表示 （35 ページ）
• コマンドライン インターフェイスを介した管理ユーザー アクティビティの表示 （35 ページ）

Web を使用したアクティブなセッションの表示

セキュリティ管理アプライアンスでは、すべてのアクティブなセッションと、アプライアンスにログインしているユーザーを表示できます。

ウィンドウの右上から、[オプション（Options）] > [アクティブなセッション（Active Sessions）] を選択します。

図 3 : [アクティブなセッション（*Active Sessions*）] メニュー



[アクティブなセッション（Active Sessions）] ページから、ユーザー名、ユーザーが持っているロール、ユーザーのログイン時間、アイドル時間、およびユーザーがコマンドラインと GUI のどちらからログインしたかを表示できます。

最近のログイン試行の表示

Web インターフェイス、SSH、または FTP 経由で直近のいくつかのログイン試行（失敗または成功）を表示するには、次を実行します。

ステップ 1 ログインします。

ステップ 2 画面の右上部付近にある [次のユーザーとしてログイン（Logged in as）] の横の [図アイコン（Figure-icon）] アイコンをクリックします。

コマンドライン インターフェイスを介した管理ユーザー アクティビティの表示

次に、アプライアンスへの複数ユーザー アクセスをサポートするコマンドを示します。

- **who** コマンドは、CLI または Web ユーザー インターフェイスを介してシステムにログインしたすべてのユーザー、ユーザーのロール、ログイン時刻、アイドル時間、およびユーザーがログインしたリモート ホストを一覧表示します。
- whoami コマンドは、現在ログインしているユーザーのユーザー名および氏名と、ユーザーが属しているグループを表示します。

```
mail3.example.com>
whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- last コマンドは、アプライアンスに最近ログインしたユーザーを表示します。リモート ホストの IP アドレス、ログイン、ログアウト、および合計時間も表示されます。

```
mail3.example.com> last
Username  Remote Host  Login Time        Logout Time       Total Time
========  ===========  ================  ================  ==========
admin     10.1.3.67    Sat May 15 23:42  still logged in   15m
admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m
admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown                                 Fri May 14 16:22
shutdown                                 Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m
admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m
admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m
admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m
admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```

管理ユーザー アクセスのトラブルシューティング

- エラー：ユーザーにアクセス権限が割り当てられていません（User Has No Access Privileges Assigned） （36 ページ）
- アクティブメニューがありません（User Has No Active Menus） （37 ページ）
- 外部認証されたユーザーに設定オプションが表示されます（Externally-Authenticated Users See Preferences Option） （37 ページ）

エラー：ユーザーにアクセス権限が割り当てられていません（User Has No Access Privileges Assigned）

問題

管理を委任されたユーザーはセキュリティ管理アプライアンスにログインできますが、アクセス権限が割り当てられていないというメッセージが表示されます。

ソリューション

このユーザーに割り当てられたカスタム ユーザー ロールに権限を割り当てたことを確認します。[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]

> [ユーザー（Users）] を表示して、割り当てられているユーザー ロールを特定してから、[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ユーザーロール（User Roles）]に移動し、ユーザー ロールの名前をクリックしてロールに権限を割り当てます。

レポーティング グループに基づいてアクセスを割り当てた場合は、[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ユーザーロール（User Roles）]ページで、そのユーザーのレポーティング グループが選択されていることを確認します。グループを割り当てるには、[委任管理用のユーザー役割（User Roles for Delegated Administration）] テーブルの [メールレポート（Email Reporting）] 列で [グループが選択されていません（No groups selected）] リンクをクリックします。

アクティブメニューがありません（User Has No Active Menus）

問題

公開権限を付与されたユーザーのログイン時に、アクティブ メニューがありません。

ソリューション

少なくとも 1 つのアクセス ポリシーまたはカスタム URL カテゴリへのアクセス権があることを確認します。いずれかを編集できるこのユーザー権限を付与しない場合は、どのポリシーでも使用されていないカスタム URL カテゴリを作成し、[カスタムユーザー役割（Custom User Role）] ページでこのカテゴリにこのユーザー ロール権限を付与します。

外部認証されたユーザーに設定オプションが表示されます（Externally-Authenticated Users See Preferences Option）

問題

外部認証されたユーザーに設定オプションが表示されます。

ソリューション

セキュリティ管理アプライアンスで直接追加するユーザーのユーザー名が、外部認証データベースで使用されていない一意のユーザー名であることを確認します。

外部認証されたユーザーに設定オプションが表示されます（**Externally-Authenticated Users See Preferences Option**）

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。