



管理タスクの分散

この章は、次の項で構成されています。

- ユーザアカウントを使用する作業, [on page 1](#)
- 委任管理のためのカスタム ユーザ ロールの管理, [on page 7](#)
- パスフレーズ, [on page 18](#)
- 電子メールゲートウェイへのアクセスの設定, [on page 26](#)
- 管理ユーザへのメッセージの表示, [on page 31](#)
- セキュア シェル (SSH) キーの管理, [on page 32](#)
- 管理ユーザ アクセスのモニタリング, [on page 34](#)

ユーザ アカウントを使用する作業

電子メールゲートウェイには、ユーザアカウントを追加する方法が2つあります。電子メールゲートウェイ自体でユーザアカウントを作成する方法と、LDAPまたはRADIUSディレクトリなどの独自の中央認証システムを使用してユーザ認証を有効にする方法です。ユーザと外部認証ソースへの接続を管理するには、GUIで[システム管理 (System Administration)] > [ユーザ (Users)] ページを使用します (または、CLIで **userconfig** コマンドを使用します)。ユーザを認証するために外部ディレクトリを使用することについては、[外部認証, on page 19](#)を参照してください。

必要に応じて、次を使用して、特定のユーザ ロールに二要素認証を有効にできます。

- Web インターフェイスの [システム管理 (System Administration)] > [ユーザ (Users)] ページ。 [二要素認証, on page 25](#)を参照してください。
- CLIでの `userconfig > twofactorauth` コマンド。『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

システムのデフォルトのユーザアカウントである **admin** はすべての管理権限を持っています。**admin** ユーザアカウントは削除できませんが、パスフレーズを変更してアカウントをロックすることはできます。

新しいユーザアカウントを作成する場合は、そのユーザを定義済みのユーザロールまたはカスタムユーザロールに割り当てます。各ロールには、システム内での異なるレベルの権限が含まれます。

電子メールゲートウェイで作成できる各ユーザアカウントの数に制限はありませんが、システムで予約されている名前でユーザアカウントを作成することはできません。たとえば、「operator」や「root」という名前のユーザアカウントは作成できません。

ユーザの役割

Table 1: ユーザロールの一覧

ユーザロール	説明
admin	<p>admin ユーザはシステムのデフォルトユーザアカウントであり、すべての管理権限を持っています。便宜上、admin ユーザアカウントをここに記載しましたが、これはユーザロールを使用して割り当てることはできず、パスワードの変更以外、編集や削除もできません。</p> <p>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。</p>
管理者	<p>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。ただし、resetconfig コマンドと revert コマンドにアクセスできるのは admin ユーザだけです。</p> <p>Note AsyncOS は、GUI から電子メールゲートウェイを同時に設定する複数の管理者をサポートしません。</p>
専門技術者	<p>Technician ロールを持つユーザアカウントは、システムのアップグレード、電子メールゲートウェイの再起動、ライセンスキーの管理を実行できます。また、専門技術者は、電子メールゲートウェイをアップグレードするために以下の処理も実行できます。</p> <ul style="list-style-type: none"> • 電子メールの配信および受信の一時停止。 • ワークキューとリスナーのステータスの表示。 • 設定ファイルの保存および電子メール送信。 • セーフリストとブロックリストのバックアップ。専門技術者はこれらのリストを復元できません。 • クラスタからの電子メールゲートウェイの接続解除。 • Cisco テクニカルサポートへのリモートサービスアクセスの有効化または無効化。 • サポート要求の申請。

ユーザ ロール	説明
オペレータ	<p>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。</p> <ul style="list-style-type: none"> • ユーザ アカウントの作成または編集。 • resetconfig コマンドの発行。 • 電子メールゲートウェイのアップグレード。 • systemsetup コマンドの発行またはシステム設定ウィザードの実行。 • adminaccessconfig コマンドの発行。 • 隔離機能の実行（作成、編集、削除、および隔離の中央集中を含む）。 • 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）。 <p>これら以外は、Administrator ロールと同じ権限を持ちます。</p>
ゲスト	<p>Guest ロールを持つユーザアカウントはステータス情報とレポートだけを参照できます。Guest ロールを持つユーザは、アクセスが隔離でイネーブルの場合、隔離エリア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。</p>
オペレータ（読み取り専用）	<p>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変更を行って送信できますが、保存できません。このロールのユーザは、アクセスが隔離でイネーブルの場合、隔離エリア内のメッセージを管理できます。</p> <p>このロールのユーザは、以下にはアクセスできません。</p> <ul style="list-style-type: none"> • ファイル システム、FTP、SCP。 • 作成、編集、削除、または隔離の中央集中の設定。
ヘルプ デスク ユーザ	<p>ヘルプデスクユーザロールを持つユーザがアクセスできるのは次のものに制限されます。</p> <ul style="list-style-type: none"> • メッセージ トラッキング。 • 隔離エリア内のメッセージの管理。 <p>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。このロールのユーザがそのデバイスを管理する前に、各隔離アクセスをイネーブルにする必要があります。</p>

ユーザ ロール	説明
カスタムユーザ ロール	<p>カスタムユーザ ロールを持つユーザアカウントはそのロールに割り当てられている電子メールセキュリティ機能にのみアクセスできます。アクセスできる機能は、DLP ポリシー、電子メール ポリシー、レポート、検疫、ローカル メッセージ トラッキング、暗号化プロファイル、トレースデバッグツール、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の任意の組み合わせになります。ユーザは、機能のグローバルなイネーブル化を含むシステム設定機能にアクセスできません。カスタムユーザ ロールを定義できるのは管理者だけです。詳細については、委任管理のためのカスタム ユーザ ロールの管理, on page 7を参照してください。</p> <p>Note カスタム ユーザ 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。</p>

上記の表に定義されているロールはすべて GUI と CLI の両方にアクセスできます。ただし、Help Desk User ロールとカスタム ユーザ ロールは GUI にのみアクセスできます。

ユーザを認証するために LDAP ディレクトリを使用する場合は、ユーザ ロールに個々のユーザではなくディレクトリ 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、[外部認証, on page 19](#)を参照してください。

関連項目

- [ユーザの管理, on page 4](#)

ユーザの管理

[ユーザ (Users)] ページには、システムの既存のユーザが一覧 (ユーザ名、氏名、およびユーザ タイプまたはグループを含む) で表示されます。

[ユーザ (Users)] ページからは、次の操作が行えます。

- 新しいユーザの追加。詳細については、[ユーザの追加, on page 5](#)を参照してください。
- ユーザの削除。詳細については、[ユーザの削除, on page 6](#)を参照してください。
- ユーザの編集。ユーザのパスワードの変更、ユーザのアカウントのロックおよびロック解除など。詳細については、[ユーザの編集, on page 5](#)を参照してください。
- ユーザにパスワードの変更を強制します。[ユーザにパスワードの変更を強制, on page 6](#)を参照してください。
- ローカル アカウント用のユーザ アカウントとパスワード設定値の設定。詳細については、[制限的なユーザ アカウントとパスワードの設定値の構成, on page 19](#)を参照してください。

- ユーザを認証するために LDAP または RADIUS ディレクトリを使用するよう 電子メールゲートウェイをイネーブルにする。詳細については、[外部認証, on page 19](#)を参照してください。
- 特定のユーザ ロールに二要素認証を有効にします。詳細については、[二要素認証, on page 25](#)を参照してください。
- メッセージ トラッキング内の DLP Matched Content への管理者以外のアクセスをイネーブルにする。詳細については、[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, on page 6](#)を参照してください。

ユーザの追加

はじめる前に

- ユーザが使用するユーザ ロールを設定します。
 - 定義済みのユーザ ロールについては、[ユーザの役割, on page 2](#)を参照してください。
 - カスタムロールを作成するには、[委任管理のためのカスタムユーザロールの管理, on page 7](#)を参照してください。
- パスフレーズの要件を指定します。[制限的なユーザアカウントとパスフレーズの設定値の構成, on page 19](#)を参照してください。

Procedure

ステップ 1 [システム管理 (System Administration)] > [ユーザ (Users)] を選択します。

ステップ 2 [ユーザを追加 (Add User)] をクリックします。

ステップ 3 ユーザのログイン名を入力します。一部の単語 (「operator」 や 「root」 など) が予約されています。

ステップ 4 ユーザの氏名を入力します。

ステップ 5 定義済みのユーザ ロールまたはカスタム ユーザ ロール (Custom user role) を選択します。

ステップ 6 パスフレーズを入力します。

Note ログインパスワードを手動で作成することに加えて、電子メールゲートウェイにログインするためのシステム生成パスワードも作成できます。

ステップ 7 変更を送信し、保存します。

ユーザの編集

パスワードなどを変更するには、この手順を使用します。

Procedure

- ステップ1 [システム管理 (System Administration)] > [ユーザ (Users)] を選択します。
 - ステップ2 [ユーザ (Users)] 一覧でユーザの名前をクリックします。
 - ステップ3 ユーザに対して変更を行います。
 - ステップ4 変更を送信し、保存します。
-

ユーザにパスワードの変更を強制

Procedure

- ステップ1 [システム管理 (System Administration)] > [ユーザ (Users)] を選択します。
 - ステップ2 [ユーザ (Users)] 一覧からユーザを選択します。
 - ステップ3 [パスワード変更を適用 (Enforce Passphrase Change)] をクリックします。
 - ステップ4 次のログイン時または指定した期間 (日数) が経過した後にユーザがパスワードを変更する必要があるかどうかを選択します。
 - ステップ5 (任意) 指定した期間が経過した後にパスワードの変更を適用する場合は、パスワードの期限切れ後にパスワードをリセットするまでの猶予期間 (日数) を設定します。
 - ステップ6 [OK] をクリックします。
 - ステップ7 変更を送信し、保存します。
-

ユーザの削除

Procedure

- ステップ1 [ユーザ (Users)] 一覧でユーザ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 変更を保存します。
-

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

機密情報が含まれている可能性のあるメッセージの詳細に対し、管理アクセスを制限することが必要になる場合があります。

- データ損失防止 (DLP) ポリシーに違反するメッセージには、企業の秘密情報、またはクレジットカード番号や医療記録を含む個人情報などの情報が含まれている可能性があります

す。デフォルトでは、この内容は、電子メールゲートウェイへのアクセスを持つすべてのユーザが閲覧可能です。

- アウトブレイク フィルタ、または URL レピュテーションもしくはカテゴリに基づくコンテンツフィルタによって捕捉される URL も、機密性が高いと見なされる場合があります。デフォルトでは、この内容を閲覧できるのは、管理者特権を持つユーザのみです。

この機密性の高い内容は、メッセージトラッキング結果に表示されたメッセージの [メッセージの詳細 (Message Details)] ページにある専用のタブに表示されます。

これらのタブとその内容は、管理ユーザに対し、そのユーザ ロールに基づいて非表示にできません。ただし、管理者ロールを持つユーザに対してこの機密性の高い内容を非表示にするオプションはありますが、管理者ロールを持つユーザは、これらの権限を変更できるため、機密性の高い情報をいつでも閲覧することができます。

はじめる前に

これらの機能の前提条件を満たしていることを確認します。[メッセージトラッキングの URL 詳細の表示](#)を参照してください。

Procedure

- ステップ 1** [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 2** [メッセージトラッキング内の機密情報へのアクセス (Access to Sensitive Information in Message Tracking)] で、[設定の編集 (Edit Settings)] をクリックします。
- ステップ 3** 機密情報のタイプごとに、データ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にアクセスできないカスタム ロールはこの情報を見ることができないため、表示されません。
- ステップ 4** 変更を送信し、保存します。

What to do next

関連項目

- [メッセージトラッキングの詳細](#)
- [メッセージトラッキングでの機密性の高い DLP データの表示](#)
- [メッセージトラッキングの URL 詳細の表示](#)

委任管理のためのカスタム ユーザ ロールの管理

カスタム ユーザ ロールを設計し、組織内でのそれぞれのロールに一致した特定の責任をユーザに委任することができます。委任管理者は、それぞれが責任を負う電子メールセキュリティ機能にのみアクセスでき、それぞれのロールに関連しないシステム設定機能にはアクセスできません。委任管理を行うことで、電子メールゲートウェイの電子メールセキュリティ機能に対

するユーザのアクセスを、定義済みの Administrator、Operator、および Help Desk User ロールより柔軟に制御できるようになります。

たとえば、電子メールゲートウェイの特定ドメインの電子メールポリシーの管理に関与しているユーザがいる場合に、それらのユーザに、定義済みの Administrator および Operator ロールで付与されるシステム管理やセキュリティサービスの設定機能にはアクセスさせたくないことがあります。それぞれのユーザに管理するメールポリシーへのアクセス権限、およびそれらのポリシーで処理されるメッセージを管理するために使用できる他の電子メールセキュリティ機能（メッセージトラッキングやポリシー隔離など）を付与できるメールポリシー管理者用のカスタムユーザロールを作成できます。

GUI で [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページを使用して（または、CLI で `userconfig -> role` コマンドを使用して）、カスタムユーザロールを定義し、それぞれが責任を負う電子メールセキュリティ機能（メールポリシー、DLP ポリシー、電子メールレポート、および隔離など）を管理します。委任管理者が管理できる電子メールセキュリティ機能の一覧については、[アクセス権限の割り当て, on page 9](#)を参照してください。カスタムロールは、[システム管理 (System Administration)] > [ユーザ (Users)] ページを使用して、ローカルユーザアカウントを追加または編集するときにも作成できます。詳細については、[ユーザアカウント追加時のカスタムユーザロールの定義, on page 15](#)を参照してください。

カスタムユーザロールを作成する際には、そのロールの責任が他の委任管理者の責任と重複しすぎないようにする必要があります。たとえば、複数の委任管理者が同じコンテンツフィルタに対する責任を持ち、そのコンテンツフィルタを異なるメールポリシーで使用する場合、1人の委任管理者がそのフィルタに加えた変更により、他の委任管理者が管理しているメールポリシーに意図せぬ悪影響を及ぼすことがあります。

カスタムユーザロールを作成すると、他のユーザロールと同様にローカルユーザと外部認証グループをそのカスタムユーザロールに割り当てることができます。詳細については、[ユーザアカウントを使用する作業, on page 1](#)を参照してください。カスタムロールに割り当てられているユーザは CLI にアクセスできないことに注意してください。

関連項目

- [\[アカウント権限 \(Account Privileges\) \] ページ, on page 8](#)
- [アクセス権限の割り当て, on page 9](#)
- [カスタムユーザロールの定義, on page 15](#)
- [ユーザアカウント追加時のカスタムユーザロールの定義, on page 15](#)
- [カスタムユーザロールの責任のアップデート, on page 16](#)
- [カスタムユーザロールの編集, on page 16](#)
- [カスタムユーザロールの複製, on page 17](#)
- [カスタムユーザロールの削除, on page 17](#)

[アカウント権限 (Account Privileges)] ページ

委任管理者が電子メールゲートウェイにログインすると、[アカウント権限 (Account Privileges)] ページに委任管理者が責任を持つセキュリティ機能へのリンク、およびそれぞれのアクセス権

限についての簡単な説明が表示されます。委任管理者は、[オプション (Options)]メニューで [アカウント権限 (Account Privileges)]を選択することでこのページに戻ることができます。委任管理者は、Web ページの上部にあるメニューを使用して、管理する機能にアクセスすることもできます。

次の図は、メール ポリシー、電子メール レポート、メッセージ トラッキング、および隔離にアクセスできる委任管理者の [アカウント権限 (Account Privileges)] ページを示しています。

Figure 1: 委任管理者の [アカウント権限 (Account Privileges)] ページ

Account Privileges (bob1)	
Mail Policies	Incoming Mail Policies (1) Incoming Content Filters (1) Outgoing Mail Policies (1) Outgoing Content Filters (None Assigned) <i>Configure Email Policies and Content Filters.</i>
Email Reporting	Policy Reporting and DLP Reporting <i>View and analyze email traffic.</i>
Message Tracking	Message Tracking <i>Track messages.</i>
Quarantine	Manage Message Quarantines (1) <i>Manage messages in assigned Quarantines.</i>

アクセス権限の割り当て

カスタム ユーザ ロールを作成する場合、委任管理者が責任を負うセキュリティ機能へのアクセス レベルを定義します。

委任管理者が管理できるセキュリティ機能は以下のとおりです。

- 送受信のメール ポリシーとコンテンツ フィルタ。
- データ消失防止 (DLP) ポリシー。
- 電子メール レポート。
- メッセージ トラッキング。
- トレース デバッグ ツール。
- スパム、ポリシー、ウイルス、およびアウトブレイク 隔離。
- Cisco Email Encryption プロファイル。
- ログ サブスクリプション (Log Subscription)

カスタム ユーザ ロールのアクセス レベルを定義したら、委任管理者が責任を負うことになる具体的なメールポリシー、コンテンツフィルタ、DLPポリシー、隔離、または暗号化プロファイルを割り当てる必要があります。

たとえば、異なる DLP ポリシーに対して責任を負う 2 つの異なる DLP ポリシー管理者ロールを作成できます。1 つのロールは企業の秘密保持や許容範囲での使用に関する DLP 違反にのみ責任を負い、他のロールはプライバシー保護に関する DLP 違反に責任を負うようにできます。

DLPポリシーへのアクセスに加えて、これらのカスタムユーザロールにはメッセージデータのトラッキング、隔離とレポートの表示に対する権限を割り当てることもできます。これらのロールは、メッセージトラッキングの使用において責任を負うポリシーに関連するDLP違反を検索できます。

カスタムユーザロールに割り当てることのできる責任については、[ユーザの役割 (User Roles)] ページの [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブル内の割り当て済み権限のリンクをクリックして確認できます。[カスタムユーザロールの責任のアップデート](#)、[on page 16](#)を参照してください。

関連項目

- [メールポリシーとコンテンツフィルタ](#), [on page 10](#)
- [DLPポリシー](#), [on page 12](#)
- [電子メールレポート](#), [on page 13](#)
- [メッセージトラッキング](#), [on page 13](#)
- [トレース](#), [on page 14](#)
- [隔離](#), [on page 14](#)
- [暗号化プロファイル](#), [on page 14](#)
- [ログサブスクリプション \(Log Subscription\)](#) , [on page 15](#)

メールポリシーとコンテンツフィルタ

メールポリシーとコンテンツフィルタのアクセス権限では、電子メールゲートウェイ上の送受信メールポリシーとコンテンツフィルタへの委任管理者のアクセスレベルを定義します。特定のメールポリシーとコンテンツフィルタをカスタムユーザロールに割り当て、そのロールに属する委任管理者、および **Operator** と **Administrator** だけがメールポリシーとコンテンツフィルタを管理できるようにすることができます。

このアクセス権限を持つすべての委任管理者は、デフォルトの送受信メールポリシーを表示できますが、すべてのアクセス権限を持っている場合のみそれらのポリシーを編集できます。

アクセス権限を持つすべての委任管理者は、それぞれのメールポリシーで使用する新しいコンテンツフィルタを作成できます。委任管理者が作成したコンテンツフィルタは、そのカスタムユーザロールに割り当てられている他の委任管理者が使用できます。いずれのカスタムユーザロールにも割り当てられていないコンテンツフィルタはパブリックであり、メールポリシーのアクセス権限を持つすべての委任管理者が表示できます。**Operator** や **Administrator** が作成したコンテンツフィルタは、デフォルトでパブリックです。委任管理者は、それぞれのカスタムユーザロールに割り当てられているメールポリシーの既存のコンテンツフィルタはすべてイネーブルまたはディセーブルにできますが、パブリックコンテンツフィルタは変更も削除もできません。

委任管理者が自分のポリシー以外のメールポリシーで使用されているコンテンツフィルタを削除した場合、またはそのコンテンツフィルタが他のカスタムユーザロールに割り当てられている場合、AsyncOS はそのコンテンツフィルタをシステムから削除しません。代わりに、AsyncOS はそのカスタムユーザロールからコンテンツフィルタのリンクを解除し、委任管理

者のメールポリシーから削除します。そのコンテンツフィルタは、他のカスタムユーザロールとメールポリシーでは引き続き使用可能です。

委任管理者は、それぞれのコンテンツフィルタで任意のテキストリソースやディクショナリを使用できますが、GUIで[テキストリソース (Text Resources)] ページや[ディクショナリ (Dictionaries)] ページにアクセスして、それらを表示または変更することはできません。委任管理者は、新しいテキストリソースやディクショナリを作成することもできません。

送信メールポリシーの場合、委任管理者はDLPポリシーをイネーブルまたはディセーブルできますが、DLPポリシーの権限も持っている場合を除き、DLPの設定をカスタマイズすることはできません。

メールポリシーとコンテンツフィルタ用の以下のアクセスレベルのいずれかをカスタムユーザロールに割り当てることができます。

- **アクセスなし (No access)** : 委任管理者は、電子メールゲートウェイのメールポリシーとコンテンツフィルタを表示も編集もできません。
- **割り当てられた隔離を表示、割り当てられた隔離を編集 (View assigned, edit assigned)** : 委任管理者はカスタムユーザロールに割り当てられているメールポリシーとコンテンツフィルタを表示および編集でき、新しいコンテンツフィルタを作成できます。委任管理者は、ポリシーのスパム対策、ウイルス対策、およびアウトブレイクフィルタの設定を編集できます。委任管理者はポリシーに対してそれぞれのコンテンツフィルタをイネーブルにでき、責任があるものかどうかに関係なく、そのポリシーに割り当てられている既存のコンテンツフィルタをディセーブルにできます。委任管理者はメールポリシーの名前、その送信者、受信者、またはグループを変更することはできません。委任管理者は、それぞれのカスタムユーザロールに割り当てられているメールポリシーのコンテンツフィルタの順序を変更できます。
- **すべてを表示、割り当てられた隔離を編集 (View all, edit assigned)** : 委任管理者は、電子メールゲートウェイのすべてのメールポリシーとコンテンツフィルタを表示できますが、そのカスタムユーザロールに割り当てられているもののみ編集できます。

すべてを表示、すべてを編集 (フルアクセス) (View all, edit all (full access)) : 委任管理者は、電子メールゲートウェイのすべてのメールポリシーとコンテンツフィルタ (デフォルトのメールポリシーを含む) に対するすべてのアクセス権限を持ち、新しいメールポリシーを作成できます。委任管理者は、すべてのメールポリシーの送信者、受信者、およびグループを変更できます。メールポリシーの順序を変更することもできます。

[ユーザの役割 (User Roles)] ページの [電子メールセキュリティ マネージャ (Email Security Manager)] または [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルを使用して、個々のメールポリシーとコンテンツフィルタをカスタムユーザロールに割り当てることができます。

[代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルを使用したメールポリシーとコンテンツフィルタの割り当ての詳細については、[カスタムユーザロールの責任のアップデート](#), on page 16を参照してください。

DLP ポリシー

DLP ポリシーのアクセス権限では、電子メールゲートウェイの DLP Policy Manager を介した DLP ポリシーへの委任管理者のアクセスレベルを定義します。DLP ポリシーを特定のカスタム ユーザ ロールに割り当て、オペレータと管理者に加えて、委任管理者にそれらのポリシーを管理させることができます。DLP アクセス権を持つ委任管理者は、データ消失防止の Global Settings ページから DLP 設定ファイルをエクスポートできます。

委任管理者がメール ポリシー権限も保持している場合は、DLP ポリシーをカスタマイズできます。委任管理者は、それぞれの DLP ポリシーの任意のカスタム DLP デictionary を使用できますが、カスタム DLP デictionary は表示も変更もできません。

DLP ポリシー用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- **アクセスなし (No access)** : 委任管理者は 電子メールゲートウェイの DLP ポリシーを表示も編集もできません。
- **割り当てられた隔離を表示 (View assigned)**、**割り当てられた隔離を編集 (edit assigned)** : 委任管理者は DLP Policy Manager を使用して、カスタム ユーザ ロールに割り当てられている DLP ポリシーを表示および編集できます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの名前変更も順序変更もできません。委任管理者は DLP 設定をエクスポートできます。
- **すべてを表示 (View all)**、**割り当てられた隔離を編集 (edit assigned)** : 委任管理者はカスタム ユーザ ロールに割り当てられている DLP ポリシーを表示および編集できます。委任管理者は DLP 設定をエクスポートできます。委任管理者は、そのカスタム ユーザ ロールに割り当てられていない DLP ポリシーをすべて表示できますが、編集することはできません。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序変更やポリシー名の変更はできません。
- **すべてを表示、すべてを編集 (フルアクセス) (View all, edit all (full access))** : 委任管理者は、電子メールゲートウェイのすべての DLP ポリシーに対するすべてのフルアクセス権限を持ち、新しいポリシーを作成することもできます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序を変更できます。電子メールゲートウェイで使用する DLP モードは変更できません。

[ユーザーの役割 (User Roles)] ページの [DLPポリシーマネージャ (DLP Policy Manager)] または [代表管理者用のカスタムのユーザー役割 (Custom User Roles for Delegated Administration)] テーブルを使用して、個々の DLP ポリシーをカスタム ユーザ ロールに割り当てることができます。

DLP ポリシーや DLP Policy Manager の詳細については、[データ損失の防止](#)を参照してください。

[代表管理者用のカスタムのユーザー役割 (Custom User Roles for Delegated Administration)] の一覧を使用して DLP ポリシーを割り当てる方法の詳細については、[カスタム ユーザ ロールの責任のアップデート](#) , on page 16を参照してください。

電子メール レポーティング

電子メール レポーティングのアクセス権限では、カスタム ユーザ ロールのメール ポリシー、コンテンツ フィルタ、および DLP ポリシーへのアクセス権限に従い、委任管理者が表示できるレポートと [電子メール セキュリティ モニタ (Email Security Monitor)] ページを定義します。それらのレポートは割り当てられているポリシーに対してフィルタリングされていません。委任管理者は、自分が責任を負っていないメールと DLP ポリシーのレポートを表示できます。

電子メール レポーティング用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- **アクセスなし (No access)** : 委任管理者は、電子メールゲートウェイのレポートを表示できません。
- **関連するレポートを表示 (View relevant reports)** : 委任管理者は、[電子メール セキュリティ モニタ (Email Security Monitor)] ページにあるそれぞれのメール ポリシー、コンテンツ フィルタ、および DLP ポリシーのアクセス権限に関連するレポートを表示できます。メール ポリシーとコンテンツ フィルタのアクセス権限がある委任管理者は、以下の [電子メール セキュリティ モニタ (Email Security Monitor)] ページを表示できます。
 - 概要
 - 受信メール
 - [送信先 (Outgoing Destinations)]
 - [送信者 (Outgoing Senders)]
 - [内部ユーザ (Internal Users)]
 - コンテンツ フィルタ
 - ウイルス アウトブレイク (Virus Outbreaks)
 - ウイルスの種類
 - アーカイブ レポート (Archived Reports)

DLP ポリシーのアクセス権限がある委任管理者は、以下の [電子メール セキュリティ モニタ (Email Security Monitor)] ページを表示できます。

- 概要
- DLP インシデント (DLP Incidents)
- アーカイブ レポート (Archived Reports)
- **すべてのレポートを表示 (View all reports)** : 委任管理者は、電子メールゲートウェイのすべてのレポートと [電子メール セキュリティ モニタ (Email Security Monitor)] ページを表示できます。

電子メール レポーティングと [電子メール セキュリティ モニタ (Email Security Monitor)] の詳細については、[電子メール セキュリティ モニタの使用方法](#)の章を参照してください。

メッセージ トラッキング

メッセージ トラッキングのアクセス権限では、カスタム ユーザ ロールに割り当てられている委任管理者がメッセージ トラッキングへのアクセス権限を持つかどうかを定義します。メッ

メッセージトラッキングには、[システム管理 (System Administration)] > [ユーザ (Users)] ページで [DLP トラッキング ポリシー (DLP Tracking Policies)] オプションがイネーブルになっている、カスタム ユーザ ロールに DLP ポリシーのアクセス権限もある場合に、組織の DLP ポリシー違反となる可能性があるメッセージの内容も含まれます。

委任管理者はそれぞれに割り当てられている DLP ポリシーに対する DLP 違反のみ検索できません。

メッセージトラッキングの詳細については、[メッセージトラッキング](#)を参照してください。

委任管理者に、メッセージトラッキング内の一致した DLP の内容を表示するためのアクセスを許可する方法の詳細については、[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](#), on page 6を参照してください。

トレース

トレースのアクセス権限では、カスタム ユーザ ロールに割り当てられている委任管理者がトレースを使用して、システムを介したメッセージフローをデバッグできるかどうかを定義します。アクセス権限がある委任管理者は、トレースを実行して、生成されるすべての出力を表示できます。トレース結果は、委任管理者のメールまたは DLP ポリシー権限に基づきフィルタリングはされません。

トレースの使用法の詳細については、[テストメッセージを使用したメールフローのデバッグ：トレース](#)を参照してください。

隔離

隔離のアクセス権限では、委任管理者が割り当てられた隔離を管理できるかどうかを定義します。委任管理者は、割り当てられた隔離内の任意のメッセージを表示して、メッセージの解放や削除などのアクションを実行できますが、隔離の設定（サイズ、保存期間など）の変更、隔離の作成や削除はできません。

[モニタ (Monitor)] > [隔離 (Quarantines)] ページまたは [ユーザの役割 (User Roles)] ページの [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルを使用して、任意の隔離をカスタム ユーザ ロールに割り当てることができます。

管理ユーザに隔離管理タスクを割り当てる方法については、[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とスパム隔離への管理ユーザアクセスの設定](#)を参照してください。

[代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] 一覧を使用して隔離を割り当てる方法の詳細については、[カスタム ユーザ ロールの責任のアップデート](#), on page 16を参照してください。

暗号化プロファイル

暗号化プロファイルのアクセス権限では、委任管理者がコンテンツ フィルタまたは DLP ポリシーの編集時に、それぞれのカスタム ユーザ ロールに割り当てられている暗号化プロファイルを使用できるかどうかを定義します。暗号化プロファイルは、メールまたは DLP ポリシーのアクセス権限があるカスタム ユーザ ロールにのみ割り当てることができます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべて

の委任管理者が使用できます。委任管理者はいずれの暗号化プロファイルも表示または変更できません。

暗号化プロファイルは、[セキュリティ サービス (Security Services)] > [IronPort メール暗号化 (IronPort Email Encryption)] ページを使用して暗号化プロファイルを作成または編集するとき割り当てることができます。

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、カスタムユーザー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。

カスタムユーザーロールの定義

GUI で [ユーザの役割 (User Roles)] ページを使用して (または CLI で `userconfig -> role` コマンドを使用して)、新しいユーザーロールを定義し、そのロールのアクセス権限を割り当てます。[ユーザの役割 (User Roles)] ページには、電子メールゲートウェイの既存のすべてのカスタムユーザーロールと各ロールのアクセス権限が表示されます。

Procedure

- ステップ 1 [システム管理 (System Administration)] > [User Roles (ユーザの役割)] を選択します。
- ステップ 2 [ユーザ役割の追加 (Add User Role)] をクリックします。
- ステップ 3 ユーザーロールの名前を入力します。
- ステップ 4 ユーザーロールの説明とその権限を入力します。
- ステップ 5 ユーザーロールのアクセス権限を選択します。(各タイプのアクセス権限の詳細については、[アクセス権限の割り当て](#), on page 9 を参照してください)。
- ステップ 6 変更を送信し、保存します。

ユーザーアカウント追加時のカスタムユーザーロールの定義

電子メールゲートウェイに対してローカルユーザーアカウントの追加または編集を行う際に、新しいカスタムユーザーロールを作成できます。

ユーザーアカウントの追加の詳細については、[ユーザの管理](#), on page 4 を参照してください。

Procedure

- ステップ 1 [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 2 [ユーザの追加 (Add User)] をクリックします。

- ステップ 3** ユーザ アカウント作成時には、[カスタム役割 (Custom Roles)] を選択します。
- ステップ 4** [役割を追加 (Add Role)] を選択します。
- ステップ 5** 新しいロールの名前を入力します。
- ステップ 6** 新しいユーザ アカウントを送信します。
- AsyncOS により、新しいユーザ アカウントとカスタム ユーザ ロールが追加されたという通知が表示されます。
- ステップ 7** [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。
- ステップ 8** [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルでカスタム ユーザ ロールの名前をクリックします。
- ステップ 9** ユーザ ロールの説明とその権限を入力します。
- ステップ 10** ユーザ ロールのアクセス権限を選択します。(各タイプのアクセス権限の詳細については、[アクセス権限の割り当て](#), on page 9を参照してください)。
- ステップ 11** 変更を送信し、保存します。

カスタム ユーザ ロールの責任のアップデート

Procedure

- ステップ 1** [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。
- ステップ 2** アップデートするカスタム ユーザ ロールのアクセス権限の名前をクリックします。
- AsyncOS により、電子メールゲートウェイで使用可能なすべてのメールポリシー、コンテンツフィルタ、DLP ポリシー、または隔離の一覧、およびその他すべての割り当て済みカスタム ユーザ ロールの名前が表示されます。
- ステップ 3** 委任管理者に責任を割り当てるメール ポリシー、コンテンツ フィルタ、DLP ポリシー、または隔離を選択します。
- ステップ 4** 変更を送信し、保存します。

カスタム ユーザ ロールの編集

Procedure

- ステップ 1** [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。
- ステップ 2** [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] 一覧でユーザ ロールの名前をクリックします。

ステップ3 ユーザ ロールに変更を加えます。

ステップ4 変更を送信し、保存します。

カスタム ユーザ ロールの複製

同様のアクセス権限がある複数のカスタム ユーザ ロールを作成し、異なるユーザのセットに異なる責任を割り当てたいことがあります。たとえば、電子メールゲートウェイが複数ドメインのメッセージを処理する場合、同様のアクセス権限だが、ドメインに基づく異なるメールポリシーに対する権限であるカスタムユーザロールを作成することができます。こうすることで、委任管理者は、他の委任管理者の責任を妨げることなくそれぞれのドメインのメールポリシーを管理できます。

Procedure

ステップ1 [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。

ステップ2 [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] 一覧で、複製するユーザ ロールに対応する複製アイコンをクリックします。

ステップ3 カスタム ユーザ ロールの名前を変更します。

ステップ4 新しいカスタム ユーザ ロールに必要なすべてのアクセス権限の変更を行います。

ステップ5 変更を送信し、保存します。

カスタム ユーザ ロールの削除

カスタムロールが削除されると、ユーザは未割り当て状態になり、電子メールゲートウェイにアクセスできなくなります。複数の個人に割り当てられたカスタム ユーザ ロールを削除すると、警告メッセージを受信しません。削除したカスタム ユーザ ロールに割り当てられていたすべてのユーザを再割り当てする必要があります。

Procedure

ステップ1 [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。

ステップ2 [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] 一覧で、削除するユーザ ロールに対応するゴミ箱のアイコンをクリックします。

ステップ3 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4 変更を保存します。

パスワード

- [パスワードの変更, on page 18](#)
- [ユーザアカウントのロックおよびロック解除, on page 18](#)
- [制限的なユーザアカウントとパスワードの設定値の構成, on page 19](#)
- [外部認証, on page 19](#)
- [二要素認証, on page 25](#)

パスワードの変更

管理ユーザは GUI の最上部にある [オプション (Options)]>[パスワードの変更 (Change Passphrase)] リンクを使用して自分のパスワードを変更できます。

新しいパスワードを送信するとすぐにログアウトされ、ログイン画面が表示されます。

CLI で、`passphrase` コマンドまたは `passwd` コマンドを使用してパスワードを変更します。
「admin」ユーザアカウントのパスワードを忘れた場合は、パスワード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。



Note ログインパスワードを手動で作成することに加えて、電子メールゲートウェイにログインするためのシステム生成パスワードも作成できます。

`passphrase` コマンドでは、セキュリティのために古いパスワードの入力が必要です。



Note パスワード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。

ユーザアカウントのロックおよびロック解除

ユーザアカウントのロックは、ローカルユーザが電子メールゲートウェイにログインするのを防止します。ユーザアカウントは、次のいずれかの場合にロックされることがあります。

- AsyncOS は、ユーザが [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)] セクションで定義されている失敗ログイン試行の最大回数を超えた場合にユーザアカウントをロックします。
- 管理者は、[システム管理 (System Administration)]>[ユーザ (Users)] ページを使用して、セキュリティ目的でユーザアカウントを手動でロックできます。

[ユーザ役割の編集 (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。

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

ローカルユーザアカウントを手動でロックするには、[ユーザ (Users)] 一覧でユーザ名をクリックしてユーザアカウントを開き、[アカウントのロック (Lock Account)] をクリックします。AsyncOSは、ユーザが電子メールゲートウェイ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。

ユーザが設定した試行回数を超えた後でログインに失敗した場合、すべてのローカルユーザアカウントをロックするように設定することもできます。詳細については、[制限的なユーザアカウントとパスワードの設定値の構成](#), on page 19を参照してください。

**Note**

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電子メールゲートウェイ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電子メールゲートウェイにアクセスする方法の詳細については、[電子メールゲートウェイへの接続](#)を参照してください。

制限的なユーザアカウントとパスワードの設定値の構成

ユーザアカウントとパスワードの制限を定義して、組織全体にパスワード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ワードの制限は、電子メールゲートウェイに定義された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。
- **パスワード存続期間のルール。**ログイン後にユーザがパスワードの変更を要求されるまでの、パスワードの存続期間を定義できます。
- **パスワードのルール。**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ワードの種類を定義できます。

ユーザアカウントとパスワードの制限は、[システム管理 (System Administration)] > [ユーザ (Users)] ページの [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)] セクションで定義します。

外部認証

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電子メールゲートウェイにログインするユーザを認証するよう電子メールゲートウェイを設定できます。認証のために外部ディレクトリを使用するよう電子メールゲートウェイを設定するには、GUIで[システム管理 (System Administration)] > [ユーザ (Users)] ページを使用するか、CLIでuserconfig コマンドと external サブコマンドを使用します。

外部認証がイネーブルの状態ではユーザが電子メールゲートウェイにログインすると、電子メールゲートウェイは最初に、ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。ユーザがシステム定義の「admin」アカウントでない場合、電子メールゲートウェイは最初に設定された外部サーバをチェックして、ユーザがそこで定義されたかどうかを確認します。電子メールゲートウェイが最初の外部サーバに接続できなければ、電子メールゲートウェイは一覧の次の外部サーバをチェックします。

LDAPサーバの場合は、ユーザが外部サーバで認証に失敗すると、電子メールゲートウェイはここで定義されたローカルユーザとしてユーザを認証しようとします。そのユーザが外部サーバまたは電子メールゲートウェイに存在しない場合、またはユーザが間違えたパスワードを入力した場合は、電子メールゲートウェイへのアクセスが拒否されます。

外部RADIUSサーバに接続できなければ、一覧の次のサーバが試行されます。すべてのサーバに接続できない場合、電子メールゲートウェイはここで定義されたローカルユーザとしてユーザを認証しようとします。ただし、外部RADIUSサーバが何らかの理由（パスワード間違いやユーザ未登録など）でユーザを拒否すると、電子メールゲートウェイへのアクセスは拒否されます。

関連項目

- [LDAP 認証のイネーブル化, on page 20](#)
- [RADIUS 認証の有効化, on page 21](#)
- [SAML 認証の有効化, on page 24](#)

LDAP 認証のイネーブル化

ユーザを認証するために LDAP ディレクトリを使用する以外に、LDAP グループを Cisco ユーザ ロールに割り当てることができます。たとえば、IT グループのユーザを管理者ユーザ ロールに割り当てたり、Support グループのユーザをヘルプデスク ユーザ ロールに割り当てたりできます。1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。



Note

外部ユーザが自分の LDAP グループのユーザロールを変更する場合は、電子メールゲートウェイからログアウトして再度ログインする必要があります。これにより、そのユーザに新しいロールの権限が付与されます。

はじめる前に

LDAPサーバの LDAP サーバプロファイルおよび外部認証クエリを定義します。詳細については、[LDAP クエリ](#)を参照してください。

Procedure

- ステップ 1 [システム管理 (System Administration)] > [ユーザ (Users)] を選択します。
- ステップ 2 [Web 認証 (Web Authentication)] セクションまでスクロールします。
- ステップ 3 [有効 (Enable)] をクリックします。
- ステップ 4 [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 5 認証タイプとして [LDAP] を選択します。
- ステップ 6 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。
- ステップ 7 ユーザを認証する LDAP 外部認証クエリーを選択します。
- ステップ 8 タイムアウトするまで電子メールゲートウェイ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 電子メールゲートウェイで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。
- ステップ 10 また、[行の追加 (Add Row)] をクリックして別のディレクトリ グループを追加することもできます。電子メールゲートウェイが認証する各ディレクトリグループに対してステップ 9 とステップ 10 を繰り返します。
- ステップ 11 変更を送信し、保存します。

RADIUS 認証の有効化

ユーザの認証に RADIUS ディレクトリを使用し、ユーザのグループを Cisco ロールに割り当てることもできます。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 Cisco ユーザ ロールに割り当てるために CLASS 属性を使用します)。AsyncOS は、RADIUS サーバと通信するために Password Authentication Protocol (PAP; パスワード認証プロトコル) と Challenge Handshake Authentication Protocol (CHAP; チャレンジ ハンドシェイク認証プロトコル) の 2 つの認証プロトコルをサポートします。

RADIUS ユーザを Cisco ユーザ ロールに割り当てるには、最初に RADIUS サーバで <radius-group> という文字列値を使用して CLASS 属性を設定します (これは Cisco ユーザ ロールにマップされます)。CLASS 属性には文字、数字、およびダッシュを含めることができますが、先頭にダッシュを使用することはできません。AsyncOS は CLASS 属性で複数の値をサポートしません。CLASS 属性またはマップされていない CLASS 属性がないグループに属する RADIUS ユーザは、電子メールゲートウェイにログインできません。

電子メールゲートウェイが RADIUS サーバと通信できない場合、ユーザは電子メールゲートウェイのローカルユーザアカウントでログインできます。



Note 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。

Procedure

- ステップ 1** [システム管理 (System Administration)]>[ユーザ (Users)] ページで、[有効 (Enable)] をクリックします。
- ステップ 2** すでに有効になっていない場合は、[外部認証を有効にする (Enable External Authentication)] オプションをオンにします。
- ステップ 3** RADIUS サーバのホスト名を入力します。
- ステップ 4** RADIUS サーバのポート番号を入力します。デフォルトのポート番号は 1812 です。
- ステップ 5** RADIUS サーバの共有秘密パスワードを入力します。
- ステップ 6** タイムアウトするまで電子メールゲートウェイ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 7** (任意) [行を追加 (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、3 ~ 6 のステップを繰り返します。
- Note** 最大 10 個の RADIUS サーバを追加できます。
- ステップ 8** RADIUS サーバに再度問い合わせ、「External Authentication Cache Timeout」フィールドで再認証するまで、AsyncOS が外部認証クレデンシャルを保存する秒数を入力します。デフォルトはゼロ (0) です。
- Note** RADIUS サーバがワンタイム パスワード (たとえば、トークンから作成されるパスワード) 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 9** 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 ロールにマッピング。	<p>AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザを電子メールゲートウェイロールに割り当てます。</p> <p>CLASS 属性の要件：</p> <ul style="list-style-type: none"> • 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）。 <p>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。</p> <p>次の 電子メールゲートウェイロールは、制限の少ないものから順番に並べられています。</p> <ul style="list-style-type: none"> • admin • 管理者 (Administrator) • 専門技術者 • Operator cloudadmin • Read-only Operator • ヘルプ デスク ユーザ • ゲスト
外部認証されたすべてのユーザを管理ロールにマップします。	<p>AsyncOS は RADIUS ユーザを Administrator ロールに割り当てます。</p>

ステップ 10 Administrator ロールまたは異なる 電子メールゲートウェイ ユーザ ロール タイプにすべての外部認証されたユーザをマッピングするかを選択します。

ステップ 11 異なるロールタイプにユーザをマッピングする場合、[グループ名 (Group Name)] または [ディレクトリ (Directory)] フィールドの RADIUS CLASS 属性に定義されているようにグループ名を入力し、[ロール (Role)] フィールドから 電子メールゲートウェイ ロール タイプを選択します。[行を追加 (Add Row)] をクリックして、さらにロールマッピングを追加できます。

ユーザ ロール タイプの詳細については、[ユーザ アカウントを使用する作業, on page 1](#) を参照してください。

ステップ 12 変更を送信し、保存します。

SAML 認証の有効化

SAML を使用したシングル サインオンを有効化し、ユーザを認証してユーザのグループをシスコのルールに割り当てることができます。

始める前に

サービスプロバイダーおよび ID プロバイダーの設定を含む SAML プロファイルが設定済みである必要があります。「[電子メールゲートウェイでの SSO の設定方法](#)」を参照してください。

手順

ステップ 1 [システム管理 (System Administration)] > [ユーザ (Users)] に移動します。

ステップ 2 [Web 認証 (Web Authentication)] セクションまでスクロールします。

ステップ 3 [有効 (Enable)] をクリックします。

ステップ 4 [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 5 ドロップダウンリストから、認証タイプとして [SAML] を選択します。

ステップ 6 (任意) [外部認証属性名マップ (External Authentication Attribute Name Map)] フィールドに、グループ マッピングから検索する属性名を入力します。

属性名は、SAML 応答をリレーするために ID プロバイダーに対して設定する属性によって異なります。電子メールゲートウェイは、[グループマッピング (Group Mapping)] フィールドに設定した属性に照らし、SAML 応答からの属性名の一一致するエントリを検索します。これは省略可能であり、設定しない場合、電子メールゲートウェイは、SAML 応答内に存在するすべての属性の一一致するエントリを、[グループマッピング (Group Mapping)] フィールドに設定された値と照らして検索します。

ステップ 7 [グループマッピング (Group Mapping)] フィールドに、事前定義済みまたはカスタムのユーザ ロールに基づいて SAML ディレクトリで定義されているグループ名属性を入力します。[行の追加 (Add Row)] をクリックして複数のロール マッピングを追加できます。

グループ マッピングには、グループ属性を含める必要があります。「未指定のグループ (Unspecified Groups) 」属性を追加して、SAML アサーションまたは応答を認証できます。

ユーザ ロール タイプの詳細については、[ユーザ アカウントを使用する作業 \(1 ページ\)](#) を参照してください。

(注) [グループマッピング (Group Mapping)] の属性は、大文字と小文字が区別されます。正しい結果が返されるようにするには、正確に一一致している必要があります。

ステップ 8 変更を送信し、保存します。

次のタスク

SAML 外部認証を有効にした後は、電子メールゲートウェイのログインページにある [シングルサインオンを使用 (Use Single Sign On)] リンクを使用し、ユーザ名を入力して電子メールゲートウェイにログインできます。

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。電子メールゲートウェイは、RADIUS サーバとの通信に使用する次の認証プロトコルをサポートします。

- Password Authentication Protocol (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

関連項目

- [二要素認証の有効化 \(25 ページ\)](#)
- [二要素認証の無効化 \(26 ページ\)](#)

二要素認証の有効化

はじめる前に

IT 管理者から二要素認証に必要な RADIUS サーバの詳細を入手していることを確認します。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [ユーザ (Users)] ページで、[二要素認証 (Two-Factor Authentication)] の下の [有効にする (Enable)] をクリックします。
 - ステップ 2** 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 3** RADIUS サーバのポート番号を入力します。
 - ステップ 4** RADIUS サーバの共有秘密パスワードを入力します。

ステップ5 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6 適切な認証プロトコルを選択します。

ステップ7 (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8 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9 変更を送信し、保存します。

二要素認証を有効にすると、ユーザは電子メールゲートウェイにログインするために、ユーザ名とパスワードを入力した後にパスワ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

はじめる前に

お使いの電子メールゲートウェイで二要素認証を有効にしていることを確認します。

手順

ステップ1 [システム管理 (System Administration)] > [ユーザ (Users)] ページで、[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2 [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3 変更を送信し、保存します。

電子メールゲートウェイへのアクセスの設定

AsyncOS では、電子メールゲートウェイへのユーザのアクセス権管理を、管理者が制御できます。これを使用して、Web UI セッションのタイムアウトや、ユーザと組織のプロキシサーバから電子メールゲートウェイへのアクセス元となる IP アドレスを指定する、アクセスリストなどを管理できます。

関連項目

- [IP ベースのネットワーク アクセスの設定, on page 27](#)
- [セッションタイムアウトの設定, on page 29](#)

IP ベースのネットワーク アクセスの設定

アプライアンスに直接接続するユーザおよび逆プロキシで接続するユーザ（リモートユーザに逆プロキシを使用する組織の場合）のアクセスリストを作成して、電子メールゲートウェイにアクセスするユーザの IP アドレスを制御できます。

関連項目

- [直接接続, on page 27](#)
- [プロキシ経由の接続, on page 27](#)
- [ネットワーク アクセスを制限する際の重要な注意事項, on page 27](#)
- [アクセス リストの作成, on page 28](#)

直接接続

電子メールゲートウェイに接続可能なマシンの 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、電子メールゲートウェイ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電子メールゲートウェイに接続しようとするユーザのアクセスは拒否されます。

プロキシ経由の接続

リモートユーザのマシンと電子メールゲートウェイの間で逆プロキシサーバが使用される組織のネットワークの場合、AsyncOS では電子メールゲートウェイ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、リモートユーザのマシンの IP アドレスを検証します。リモートユーザの IP アドレスを電子メールゲートウェイに送信するには、プロキシで `x-forwarded-for` HTTP ヘッダーを電子メールゲートウェイ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、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）。電子メールゲートウェイは、ヘッダーのリモートユーザの 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 IP アドレスやプロキシ IP アドレスと照合します。



Note 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。

ネットワーク アクセスを制限する際の重要な注意事項

注意： 次のいずれかの条件が `true` の場合、ネットワークアクセスの変更を送信して確定した後、電子メールゲートウェイにアクセスできなくなることがあります。

- [特定の接続のみを許可 (Only Allow Specific Connections)] を選択し、現在のマシン (クラスタ化環境内の PC、電子メールゲートウェイ、または Cisco Secure Manager Email and Web Gateway など) の IP アドレスがリストに含まれない場合。
- [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、現在電子メールゲートウェイ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、電子メールゲートウェイ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。

アクセスリストの作成

ネットワーク アクセス リストは、GUI または `adminaccessconfig > ipaccess` CLI コマンドを使用して作成できます。

はじめる前に

ネットワークアクセスの設定を変更後、電子メールゲートウェイからロックアウトされないようにします。[ネットワークアクセスを制限する際の重要な注意事項, on page 27](#)を参照してください。

Procedure

ステップ 1 [システム管理 (System Administration)] > [Network Access (ネットワーク アクセス)] を選択します。

ステップ 2 [設定の編集 (Edit Settings)] をクリックします。

ステップ 3 アクセスリストの制御モードを選択します。

オプション	説明
すべてを許可 (Allow All)	このモードでは、電子メールゲートウェイへのすべての接続が許可されます。 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、ユーザの電子メールゲートウェイへの接続を許可します。

オプション	説明
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、逆プロキシ経由で電子メールゲートウェイへの接続を許可します。 <ul style="list-style-type: none"> • 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の IP アドレスが一致すれば、電子メールゲートウェイ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。

ステップ 4 電子メールゲートウェイへの接続を許可するユーザの 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 5 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。

- a. 電子メールゲートウェイ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。
- b. プロキシが電子メールゲートウェイに送信する発信元の IP ヘッダーの名前。これには、リモートユーザマシンの IP アドレスと、要求を転送したプロキシサーバの 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 6 変更を送信および確定後に電子メールゲートウェイからロックアウトされる変更が構成されていないことを確認します。

ステップ 7 変更を送信し、保存します。

セッションタイムアウトの設定

- [Web UI セッションタイムアウトの設定, on page 30](#)

- [CLI セッションタイムアウトの設定, on page 30](#)

Web UI セッションタイムアウトの設定

AsyncOS が、電子メールゲートウェイの Web UI から非アクティブなユーザ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以下に適用されます。

- すべてのユーザ（管理者を含む）
- HTTP セッションおよび HTTPS セッション
- Cisco スпам隔離

AsyncOS によってユーザがログアウトされると、電子メールゲートウェイはユーザの Web ブラウザをログインページにリダイレクトします。

Procedure

-
- ステップ 1** [システム管理 (System Administration)] > [Network Access (ネットワーク アクセス)] を選択します。
 - ステップ 2** [設定の編集 (Edit Settings)] をクリックします。
 - ステップ 3** 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 4** 変更を送信し、保存します。
-

What to do next

また、CLI で `adminaccessconfig` コマンドを使用して Web UI 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 Secure Email Gateway*』を参照してください。

CLI セッションタイムアウトの設定

AsyncOS が、電子メールゲートウェイの CLI から非アクティブなユーザ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



Note 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。

Procedure

- ステップ 1 [システム管理 (System Administration)] > [Network Access (ネットワーク アクセス)] を選択します。
- ステップ 2 [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3 [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 4 変更を送信し、保存します。

What to do next

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 Secure Email Gateway*』を参照してください。

管理ユーザへのメッセージの表示

- [ログイン前のメッセージの表示 , on page 31](#)
- [ログイン後のメッセージの表示 , on page 31](#)

ログイン前のメッセージの表示

ユーザが SSH、FTP、または Web UI から電子メールゲートウェイにログインしようとする前にメッセージを表示するように電子メールゲートウェイを設定できます。ログインバナーは、ログインプロンプトの上に表示されるカスタマイズ可能なテキストです。ログインバナーを使用して、内部のセキュリティ情報または電子メールゲートウェイのベストプラクティスに関する説明を表示できます。たとえば、許可しない電子メールゲートウェイの使用を禁止する簡単な注意文言を作成したり、ユーザが電子メールゲートウェイに対して行った変更を確認する企業の権利に関する詳細な警告を作成したりできます。

CLI の `adminaccessconfig> banner` コマンドを使用して、ログインバナーを作成します。ログインバナーは、80 x 25 のコンソールに収まるように最大 2000 文字になっています。ログインバナーは、電子メールゲートウェイの `/data/pub/configuration` ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更内容を確定します。

ログイン後のメッセージの表示

ユーザが SSH、FTP、または Web UI を使用して電子メールゲートウェイに正常にログインした後に、ウェルカムバナーを表示するように AsyncOS を設定できます。ウェルカムバナーを使用して、内部のセキュリティ情報または電子メールゲートウェイのベストプラクティスに関する説明を表示できます。

CLI で `adminaccessconfig > welcome` コマンドを使用して、ウェルカム バナーを作成します。ウェルカム バナーの最大長は 1600 文字です。

ウェルカムバナーは、電子メールゲートウェイの `/data/pub/configuration` ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更内容を確定します。

詳細については、『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

セキュアシェル (SSH) キーの管理

`sshconfig` コマンドを使用して、次の操作を実行します。

- システムで設定されたユーザアカウント (admin アカウントを含む) の `authorized_keys` ファイルにセキュアシェル (SSH) 公開ユーザ キーを追加したり、それらのキーを削除したりできます。これにより、パスフレーズチャレンジではなく SSH キーを使用してユーザアカウントを認証できるようになります。
- 次の SSH サーバの設定を編集できます。
 - 公開キー認証アルゴリズム
 - 暗号アルゴリズム
 - KEX アルゴリズム
 - MAC メソッド
 - 最小サーバキー サイズ



Note 電子メールゲートウェイから他のホストマシンへのログファイルの SCP プッシュを実行する場合に使用されるホストキーを設定するには、`logconfig -> hostkeyconfig` を使用します。詳細については、[ログ](#)を参照してください。

`hostkeyconfig` を使用すると、リモートホストのキーをスキャンし、電子メールゲートウェイに追加できます。

関連項目

- [例：新しい公開キーのインストール, on page 32](#)
- [例：SSH サーバ設定の編集, on page 33](#)

例：新しい公開キーのインストール

次の例では、管理者アカウントの新規公開キーをインストールします。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
```



```
[ ]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[ ]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[ ]>
```

例：SSH サーバ設定の編集

次に、SSH サーバ設定を編集する方法の例を示します。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[ ]> sshd
ssh server config settings:
Public Key Authentication Algorithms:
    rsa1
    ssh-dss
    ssh-rsa
Cipher Algorithms:
    aes128-ctr
    aes192-ctr
    aes256-ctr
    arcfour256
    arcfour128
    aes128-cbc
    3des-cbc
    blowfish-cbc
    cast128-cbc
    aes192-cbc
    aes256-cbc
    arcfour
    rijndael-cbc@lysator.liu.se
MAC Methods:
    hmac-md5
    hmac-sha1
    umac-64@openssh.com
    hmac-ripemd160
    hmac-ripemd160@openssh.com
    hmac-sha1-96
    hmac-md5-96
Minimum Server Key Size:
    1024
KEX Algorithms:
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group-exchange-sha1
    diffie-hellman-group14-sha1
    diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[ ]> setup
Enter the Public Key Authentication Algorithms do you want to use
```

```
[rsal,ssh-dss,ssh-rsa]> rsal
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,
cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se]> aes192-ctr
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96]> hmac-sha1
Enter the Minimum Server Key Size do you want to use
[1024]> 2048
Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1]> diffie-hellman-group-exchange-sha1
ssh server config settings:
Public Key Authentication Algorithms:
    rsal
Cipher Algorithms:
    aes192-ctr
MAC Methods:
    hmac-sha1
Minimum Server Key Size:
    2048
KEX Algorithms:
    diffie-hellman-group-exchange-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
```

リモート SSH コマンド実行

CLI では、リモート SSH コマンド実行を使用してコマンドを実行できます。たとえば、電子メールゲートウェイで `admin` アカウントに対して SSH 公開キーが設定されている場合は、チャレンジされないリモートホストから次のコマンドを実行できます。

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003

System status: online

[rest of command deleted]
```

管理ユーザ アクセスのモニタリング

目的	操作手順
電子メールゲートウェイについて、アクティブユーザすべてのセッション詳細を表示する	<p>ページ右上で[オプション (Options)]>[アクティブなセッション (Active Sessions)]をクリックします</p> <p>コマンドラインインターフェイスで、<code>w</code>、<code>whoami</code> および <code>who</code> コマンドを使用します。</p>

目的	操作手順
<p>電子メールゲートウェイに最近ログインしたユーザを表示します。</p> <p>また、リモートホストのIPアドレス、ログイン時間、ログアウト時間、および合計時間も表示する</p>	<p>コマンドラインインターフェイスで last コマンドを使用します。</p>

