CHAPTER 61

ユーザの管理

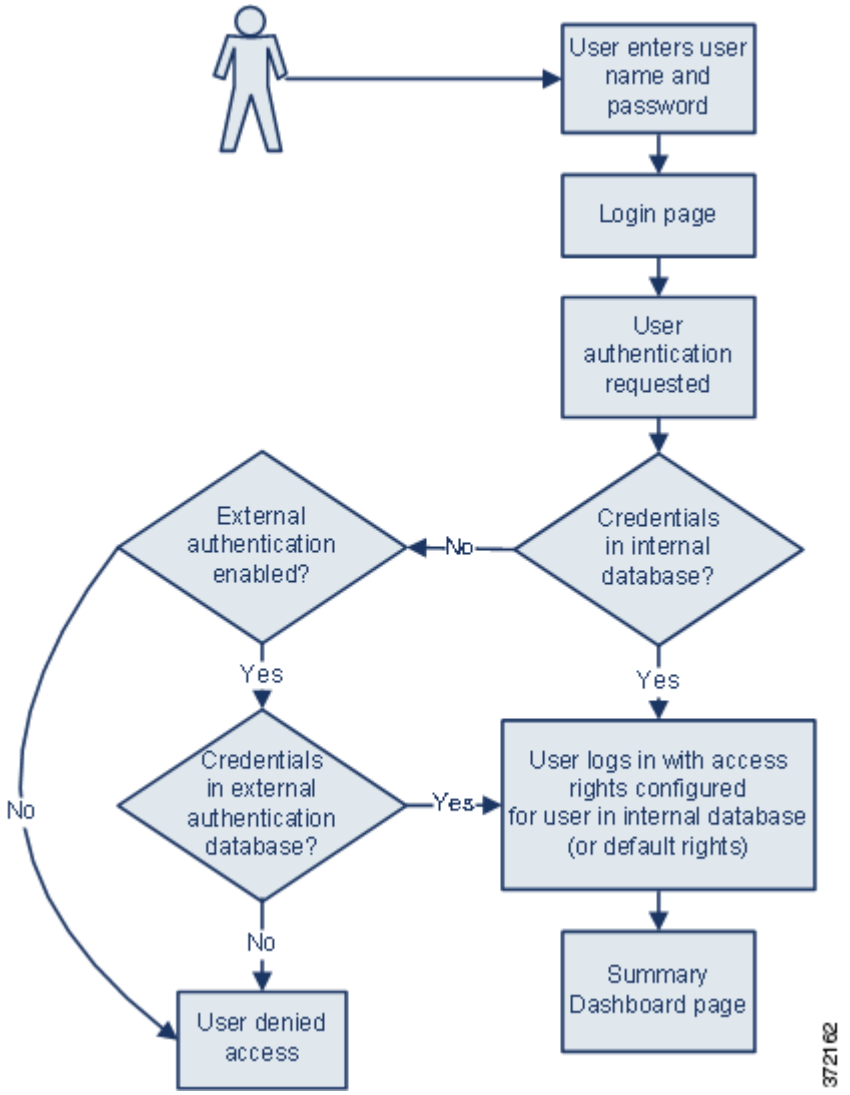
ユーザ アカウントに Administrator アクセスが付与されている場合、防御センターまたは管理対象デバイスの Web インターフェイスにアクセス可能なユーザ アカウントを管理できます。防御センターでは、内部データベースではなく、外部認証サーバを使用したユーザ認証をセットアップすることもできます。

詳細については、次の項を参照してください。

シスコユーザ認証について

ライセンス：任意（Any）

ユーザが Web インターフェイスにログインすると、アプライアンスがローカルのユーザ リストでユーザ名とパスワードに一致するものを検索します。このプロセスは*認証*と呼ばれます。認証には、内部認証と外部認証の 2 種類があります。ユーザ アカウントで内部*認証*が使用される場合、認証プロセスはローカル データベースでこのリストを確認します。アカウントで*外部認証*が使用される場合、プロセスはローカル データベースにユーザが存在するかどうかを調べ、ユーザがローカル データベースに存在しない場合は外部サーバ（Lightweight Directory Access Protocol（LDAP）ディレクトリ サーバ、Remote Authentication Dial In User Service（RADIUS）認証サーバなど）に対してユーザ リストを照会します。



内部認証または外部認証を使用するユーザの場合、ユーザのアクセス許可を制御できます。外部認証を使用するユーザには、ユーザのアクセス許可を手動で変更していない限り、ユーザが属するグループまたはアクセス リストの権限、またはサーバ認証オブジェクトあるいは管理元の防御センターのシステム ポリシーで設定したデフォルト ユーザ アクセス ロールに基づくアクセス許可が付与されます。

詳細については、次の項を参照してください。

- 内部認証について（61-3 ページ）
- 外部認証について（61-3 ページ）
- ユーザ特権について（61-4 ページ）

内部認証について

ライセンス: 任意（Any）

デフォルトでは、FireSIGHT システム が内部認証を使用してユーザのログイン時のユーザ クレデンシャルを確認します。内部認証は、ユーザ名とパスワードが内部 FireSIGHT システム データベースのレコードと照合されるときに発生します。ユーザの作成時に外部認証を有効にしないと、ユーザ クレデンシャルは内部データベースで管理されます。

各内部認証ユーザは手動で作成されるため、ユーザを作成するときにアクセス権を設定します。デフォルト設定は必要ありません。

（注） 外部認証を有効にした場合に、内部認証ユーザと同一のユーザ名が外部サーバに存在し、外部サーバでそのユーザに対して保存されているパスワードを使用してユーザがログインすると、内部認証ユーザが外部認証に変換されることに注意してください。内部認証ユーザを外部認証ユーザに変換した後で、内部認証に戻すことはできません。

外部認証について

ライセンス: 任意（Any）

外部認証は、防御センターまたは管理対象デバイスが LDAP ディレクトリ サーバまたは RADIUS 認証サーバなどの外部リポジトリからユーザ クレデンシャルを取得するときに発生します。外部認証のタイプには、LDAP 認証と RADIUS 認証があります。アプライアンスに対して使用できる外部認証形式は 1 つだけであることに注意してください。

外部認証を使用する場合、ユーザ情報を要求する外部認証サーバごとに、*認証オブジェクト*を設定する必要があります。認証オブジェクトには、そのサーバに接続してユーザ データを取得するための設定が含まれています。管理元の防御センターのシステム ポリシーでそのオブジェクトを有効にし、そのポリシーをアプライアンスに適用して認証を有効にすることができます。外部認証ユーザがログインすると、Web インターフェイスは、システム ポリシーにリストされている順序で各認証サーバを調べ、そのユーザがリストされているかどうかを確認します。

ユーザの作成時に、そのユーザに対し内部認証または外部認証のいずれが実行されるかを指定できます。

（注） シリーズ 3 管理対象デバイスで外部認証を有効にする前に、シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除してください。

管理対象デバイスで外部認証を有効にするために、そのデバイスにシステム ポリシーをプッシュできますが、デバイスの Web インターフェイスから認証オブジェクトを制御することはできません。新規ユーザに対して外部認証を選択すると、デバイスでは外部認証の設定だけが行われます。管理対象デバイスで外部認証を無効にする場合は、管理元の防御センターのシステム ポリシーで外部認証を無効にし、デバイスにポリシーを再適用します。また、デバイス自体に（管理対象デバイスで作成された）ローカル システム ポリシーを適用すると、外部認証も無効になります。

ヒント　システム ポリシーをエクスポートするには、インポート/エクスポート機能を使用できます。外部認証が有効になっているポリシーをエクスポートすると、認証オブジェクトがそのポリシーとともにエクスポートされます。その後、別の防御センターにそのポリシーとオブジェクトをインポートできます。ポリシーと認証オブジェクトを管理対象デバイスにインポート**しないでください**。

各種外部認証の詳細については、次の項を参照してください。

- LDAP 認証（61-6 ページ）
- RADIUS 認証（61-34 ページ）

ユーザ特権について

ライセンス：任意（Any）

FireSIGHT システムでは、ユーザのロールに基づいてユーザ特権を割り当てることができます。たとえばアナリストは通常、モニタ対象ネットワークのセキュリティを分析するためイベント データへのアクセスが必要ですが、FireSIGHT システム自体の管理機能へのアクセス権は必要としません。アナリストに対し、Security Analyst や Discovery Admin などの事前定義ロールを付与し、FireSIGHT システムを管理するネットワーク管理者に対し Administrator ロールを予約することができます。また、組織のニーズに合わせて調整されたアクセス権限を含むカスタム ユーザ ロールを作成できます。

防御センターのシステム ポリシーでは、外部認証されるすべてのユーザのデフォルト アクセス ロールを設定します。外部認証ユーザの初回ログイン後に、[ユーザ管理（User Management）] ページで、そのユーザのアクセス権を追加または削除できます。ユーザの権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。内部認証ユーザは手動で作成されるため、内部認証ユーザの作成時にアクセス権を設定します。

LDAP グループを使用したアクセス権の管理を設定した場合、ユーザのアクセス権は LDAP グループ メンバーシップに基づいています。属しているグループの中で最も高いレベルのアクセスを持つグループのデフォルト アクセス権が付与されます。ユーザがどのグループにも属していない場合にグループ アクセスを設定した場合、ユーザには、LDAP サーバの認証オブジェクトで設定されているデフォルト ユーザ アクセス権が付与されます。グループ アクセスを設定すると、それらの設定によってシステム ポリシーのデフォルト アクセス設定がオーバーライドされます。

同様に、RADIUS 認証オブジェクトの特定のユーザ ロール リストにユーザを割り当てると、1 つ以上のロールが相互に矛盾しない限り、割り当てられたすべてのロールがそのユーザに付与されます。2 つの相互に矛盾するロールのリストにユーザが含まれている場合、最も高いレベルのアクセスを持つロールが付与されます。ユーザがどのリストにも属しておらず、認証オブジェクトでデフォルト アクセス ロールを設定している場合、ユーザにはそのデフォルト アクセス ロールが付与されます。認証オブジェクトでデフォルト アクセスを設定すると、それらの設定によってシステム ポリシーのデフォルト アクセス設定がオーバーライドされます。

FireSIGHT システムでは、ライセンスされている機能に応じて、次に示す事前定義ユーザ ロールがサポートされています。これらのロールは、優先度順にリストされています。

- *Access Admin* はアクセス コントロール ポリシーとファイル ポリシーを表示、変更できますが、ポリシーの変更を適用することはできません。
- *Administrator* は、アプライアンスのネットワーク設定をセットアップし、ユーザ アカウントおよび Collective Security Intelligence クラウド 接続を管理し、システム ポリシーとシステム設定を設定できます。Administrator ロールが割り当てられているユーザは、その他のすべてのロールのすべての権限と特権を持ちます（ただしこれらの特権の制限付きの低いバージョンは除きます）。

- *Discovery Admin* は、ネットワーク検出ポリシーを確認、変更、削除できますが、ポリシー変更を適用することはできません。
- *External Database* ユーザは、JDBC SSL 接続をサポートする外部アプリケーションを使用して FireSIGHT システム データベースに対してクエリを実行できます。Web インターフェイスでは、オンライン ヘルプとユーザ設定にアクセスできます。
- *Intrusion Admin* は、すべての侵入ポリシー、侵入ルール、およびネットワーク解析ポリシーの機能にアクセスできます。Intrusion Admin は、[ポリシー(Policies)] メニューの侵入関連オプションにアクセスできます。Intrusion Admin は、侵入またはネットワーク解析ポリシーをアクセス制御ポリシーの一部として適用できないことに注意してください。
- *Maintenance User* は、モニタ機能(ヘルス モニタ、ホスト統計、パフォーマンス データ、システム ログなど)と保守機能(タスク スケジューリング、システムのバックアップなど)にアクセスできます。

  Maintenance User は、[ポリシー(Policies)] メニューの機能にはアクセスできず、[分析(Analysis)] メニューからダッシュボードへのアクセスだけが可能であることに注意してください。
- *Network Admin* は、デバイス設定を確認、変更、適用し、アクセス制御ポリシーを確認、変更できます。
- *Security Approver* は、設定およびポリシーの変更を確認、適用できますが、作成することはできません。
- *Security Analyst* は、侵入、ディスカバリ、ユーザ アクティビティ、接続、相関、およびネットワーク変更の各イベントを確認、分析、削除できます。ホスト、ホスト属性、サービス、脆弱性、およびクライアント アプリケーションの確認、分析、および(該当する場合は)削除を行うことができます。Security Analyst は、レポートを生成し、ヘルス イベントを確認することもできます(ただしヘルス イベントの削除と変更はできません)。
- *Security Analysts (Read Only)* には、Security Analyst と同じ権限が含まれていますが、イベントの削除はできません。

前述の事前定義ロールの他に、特別なアクセス権限を含むカスタム ユーザ ロールを設定できます。どのロールでも、外部認証ユーザのデフォルト アクセス ロールとして設定できます。

外部認証ユーザ アカウントにユーザ ロール エスカレーション特権を付与できます。また、外部認証ユーザのパスワードをエスカレーション パスワードとして使用できます。詳細については、ユーザ ロール エスカレーションの管理(61-71 ページ)を参照してください。

認証オブジェクトの管理

ライセンス:任意(Any)

認証オブジェクトは、外部認証サーバのサーバ プロファイルであり、これらのサーバの接続設定と認証フィルタ設定が含まれています。防御センターで認証オブジェクトを作成、設定、削除し、また認証オブジェクトを使用して LDAP または RADIUS サーバへの外部認証を管理することができます。詳細については、次の各項を参照してください。

- LDAP 認証(61-6 ページ)
- RADIUS 認証(61-34 ページ)
- 認証オブジェクトの削除(61-45 ページ)

LDAP 認証

ライセンス：任意（Any）

LDAP（Lightweight Directory Access Protocol）により、ユーザ クレデンシャルなどのオブジェクトをまとめるためのディレクトリをネットワーク上の一元化されたロケーションにセットアップできます。その後複数のアプリケーションが、これらのクレデンシャルと、クレデンシャルの記述に使用される情報にアクセスできます。ユーザのクレデンシャルを変更する必要がある場合は、1 か所で変更でき、FireSIGHT システム アプライアンスごとにクレデンシャルを変更する必要はありません。

詳細については、次の各項を参照してください。

LDAP 認証について

ライセンス：任意（Any）

LDAP 認証オブジェクトは防御センターで作成できますが、ほかの FireSIGHT システム アプライアンスでは作成できません。ただし、オブジェクトが有効に設定されているシステム ポリシーをアプライアンスに適用することで、アプライアンスで外部認証オブジェクトを使用できます（仮想デバイスまたは Blue Coat X-Series 向け Cisco NGIPS を除く）。ポリシーを適用すると、オブジェクトがアプライアンスにコピーされます。

（注）　シリーズ 3 管理対象デバイスで外部認証を有効にする前に、シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除してください。

LDAP 命名標準は、アドレスの指定と、認証オブジェクトのフィルタおよび属性の構文に使用できることに注意してください。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』（RFC 3377）に記載されている RFC を参照してください。この手順では構文の例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822（Standard for the Format of ARPA Internet Text Messages）仕様に記載されているアドレス指定構文を使用できることに注意してください。たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Sever を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

（注）　現在 FireSIGHT システムでは、Windows Server 2008 上で Microsoft Active Directory、Windows Server 2008 上で Oracle Directory Server Enterprise Edition 7.0、または Linux 上で OpenLDAP が稼働する LDAP サーバでの LDAP 外部認証がサポートされています。ただし、FireSIGHT システムは、仮想デバイスまたは Blue Coat X-Series 向け Cisco NGIPS の外部認証はサポートしていません。

詳細については、次の項を参照してください。

デフォルトについて

ライセンス：任意（Any）

ユーザが接続する予定のサーバのタイプに基づいて、各種フィールドにデフォルト値を取り込むことができます。サーバのタイプを選択してデフォルトを設定すると、[ユーザ名テンプレート（User Name Template）]、[UI アクセス属性（UI Access Attribute）]、[シェル アクセス属性（Shell Access Attribute）]、[グループ メンバー属性（Group Member Attribute）]、[グループ メンバー URL 属性（Group Member URL Attribute）] の各フィールドにデフォルト値が取り込まれます。

ベース DN について

ライセンス：任意（Any）

ローカル アプライアンスが認証サーバのユーザ情報を取得するため LDAP サーバを検索するときには、検索起点が必要となります。ローカル アプライアンスにより検索されるツリーを指定するには、ベース識別名（*ベース DN*）を指定します。

通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。たとえば、Example 社のセキュリティ（Security）部門のベース DN は、`ou=security,dc=example,dc=com` となります。

プライマリ サーバの指定後に、使用可能なベース DN のリストをプライマリ サーバから自動的に取得し、適切なベース DN を選択できます。

基本フィルタについて

ライセンス：任意（Any）

特定の属性に特定の値を設定する*基本フィルタ*を追加できます（囲み用の括弧を含めて最大 450 文字）。基本フィルタでは、ベース DN でフィルタに設定されている属性値を含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタは括弧で囲みます。たとえば、F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ `(cn=F*)` を使用します。

テスト ユーザ名とパスワードを入力して基本フィルタをより具体的にテストするにはユーザ認証のテスト（61-40 ページ）を参照してください。

偽装アカウントについて

ライセンス：任意（Any）

ローカル アプライアンスがユーザ オブジェクトにアクセスできるようにするには、偽装アカウントのユーザ クレデンシャルを指定する必要があります。*偽装アカウント*とは、ベース DN によって指定されるディレクトリを参照し、必要なユーザ オブジェクトを取得するための適切な権限が付与されているユーザ アカウントです。指定するユーザの識別名は、サーバのツリーで一意である必要があることに注意してください。

LDAP 接続について

ライセンス：任意（Any）

LDAP 接続の暗号化方式を管理できます。暗号化なし、Transport Layer Security（TLS）、または Secure Sockets Layer（SSL）暗号化を選択できます。

TLS または SSL 経由での接続時に認証に証明書を使用する場合、証明書の LDAP サーバ名が、[ホスト名/IP アドレス（Host Name/IP Address）] フィールドで使用する名前と一致している**必要がある**ことに注意してください。たとえば、外部認証設定に `10.10.10.250` と入力し、証明書に `computer1.example.com` と入力すると、接続は失敗します。外部認証設定のサーバ名を `computer1.example.com` に変更すると、接続が正常に行われます。

ユーザ名テンプレートについて

ライセンス：任意（Any）

ユーザ名テンプレートを選択する場合、文字列変換文字（`%s`）をユーザの UI アクセス属性またはシェル アクセス属性の値にマッピングすることで、ログイン時に入力されるユーザ名の形式を指定できます。ユーザ名テンプレートは、認証に使用する識別名の形式です。ユーザがログイン ページにユーザ名を入力すると、文字列変換文字が名前に置き換えられ、その結果生成される識別名がユーザ クレデンシャルの検索に使用されます。

たとえば、Example 社のセキュリティ（Security）部門のユーザ名テンプレートを設定するには、`%s@security.example.com` と入力します。CAC 認証および認可にオブジェクトを使用するには、UI アクセス属性値に対応するユーザ名テンプレートの値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

接続タイムアウトについて

ライセンス：任意（Any）

バックアップ認証サーバを指定する場合は、プライマリ サーバへの接続試行操作のタイムアウトを設定できます。プライマリ認証サーバから応答がない状態でタイムアウト期間が経過すると、アプライアンスはバックアップ サーバに対してクエリを実行します。たとえば、プライマリ サーバで LDAP が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。

ただし LDAP がプライマリ LDAP サーバのポートで実行されており、何らかの理由（誤った設定またはその他の問題など）で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。

属性を使用したアクセスの管理

ライセンス：任意（Any）

LDAP サーバのタイプによって、ユーザ データの保管に使用される属性が異なります。UI およびシェル アクセス属性の詳細については、次の項を参照してください。

UI アクセス属性

LDAP サーバが UI アクセス属性 uid を使用する場合、ローカル アプライアンスは、設定されたベース DN が示すツリー内の各オブジェクトで uid 属性値を調べます。特定の UI アクセス属性を設定しない場合、ローカル アプライアンスは、LDAP サーバの各ユーザ レコードの識別名を調べ、ユーザ名に一致しているかどうかを確認します。いずれかのオブジェクトに一致するユーザ名とパスワードがある場合は、ユーザ ログイン要求が認証されます。

異なる LDAP 属性を使用して、ローカル アプライアンスが、識別名の値ではなく LDAP 属性に対してユーザ名を照合するようにできます。サーバ タイプを選択し、デフォルトを設定すると、そのサーバ タイプに適した UI アクセス属性に値が取り込まれます。いずれかのオブジェクトに、指定した属性の値として一致するユーザ名と、(CAC 以外のオブジェクトの場合に)パスワードあると、ユーザ ログイン要求が認証されます。FireSIGHT システム Web インターフェイスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。有効なユーザ名は一意のユーザ名であり、アンダースコア(_)、ピリオド(.)、ハイフン(-)、英数字を使用できます。CAC 認証および認可にオブジェクトを使用するには、ユーザ名テンプレートの値に対応する UI アクセス属性の値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について(61-10 ページ)を参照してください。

シェル アクセス属性

シェル アクセス属性として LDAP サーバが uid を使用する場合、ローカル アプライアンスはログイン時に入力されたユーザ名を、uid の属性値と照合して調べます。また、uid 以外のカスタム シェル アクセス属性も設定できます。

サーバ タイプを選択し、デフォルトを設定すると、そのサーバ タイプに適したシェル アクセス属性に値が取り込まれることに注意してください。シェル アクセスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。有効なユーザ名は一意のユーザ名であり、アンダースコア(_)、ピリオド(.)、ハイフン(-)、英数字を使用できます。

グループ メンバーシップを使用したアクセスの管理について

ライセンス:任意(Any)

LDAP グループのユーザのメンバーシップに基づいてデフォルト アクセス権を設定する場合は、FireSIGHT システムにより使用される各アクセス ロールに、LDAP サーバの既存のグループの識別名を指定できます。これを行うと、LDAP によって検出された、指定のどのグループにも属さないユーザのデフォルト アクセス設定を設定できます。ユーザがログインすると、FireSIGHT システムは LDAP サーバを動的に検査し、ユーザの現在のグループ メンバーシップに基づいてアクセス権を割り当てます。

LDAP サーバによって認証されたユーザは、ローカル FireSIGHT システム アプライアンスに初めてログインすると、ユーザが属するグループのアクセス権を受け取ります。グループが設定されていない場合は、システム ポリシーで選択されているデフォルト アクセス設定を受け取ります。

その後、これらの設定がグループ メンバーシップを介して付与されていない場合には、設定を変更できます。

シェル アクセスについて

ライセンス:任意(Any)

LDAP サーバを使用して、管理対象デバイスまたは防御センターでシェル アクセス用のアカウントを認証できます。シェル アクセスを付与するユーザの項目を取得する検索フィルタを指定します。シェル アクセスは、システム ポリシーの最初の認証オブジェクトでのみ設定できることに注意してください。認証オブジェクトの順序の管理については、外部認証の有効化(63-13 ページ)を参照してください。

admin アカウントを除き、シェル アクセスは設定したシェル アクセス属性によって完全に制御されます。シェル ユーザはアプライアンスのローカル ユーザとして設定されます。ここで設定するフィルタにより、シェルにログインできる LDAP サーバのユーザが決定されます。

ログイン時に各シェル ユーザのホーム ディレクトリが作成されること、および（LDAP 接続を無効にすることで）LDAP シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは `/etc/password` 内の `/bin/false` に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

ベース DN で限定されるすべてのユーザがシェル アクセス権限でも限定される場合は、[基本フィルタと同一にする（Same as Base Filter）] を選択してシェル アクセス フィルタを設定することで、より効率的に検索できます。通常、ユーザを取得する LDAP クエリは、基本フィルタとシェル アクセス フィルタを組み合わせます。同じシェル アクセス フィルタを基本フィルタとして入力すると、同じクエリが 2 回実行されることになり、不必要に時間を消費することになります。

シェル ユーザは、小文字で構成されたユーザ名を使用してログインすることができます。シェルのログイン認証では、大文字と小文字が区別されます。

注意　シリーズ 3 防御センターでは、すべてのシェル ユーザに `sudoers` 特権が付与されます。シェル アクセスが付与されるユーザのリストを適切に制限してください。シリーズ 3 と仮想デバイスでは、外部認証ユーザに付与されるシェル アクセスのデフォルトは、**Configuration** レベルのコマンド ライン アクセスになります。このアクセスでも `sudoers` 特権が付与されます。

CAC を使用した LDAP 認証について

ライセンス：任意（Any）

組織で Common Access Card（CAC）が使用される場合は、Web インターフェイスにログインするユーザを認証し、グループ メンバーシップまたはデフォルト アクセス権に基づいて特定機能へのアクセスを許可するように、LDAP 認証を設定できます。CAC 認証および認可が設定されている場合、ユーザは、アプライアンスに個別のユーザ名とパスワードを指定せずに直接ログインすることができます。

（注）　CAC 設定プロセスの一部としてユーザ証明書を有効にするには、ブラウザに有効なユーザ証明書（この場合は CAC を介してユーザのブラウザに渡されるサーバ証明書）が存在している**必要があります**。CAC 認証および認可の設定後に、ネットワーク上のユーザはブラウズ セッション期間にわたって CAC 接続を維持する**必要があります**。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

CAC 認証および認可を設定および管理する方法の詳細については、次の項を参照してください。

- CAC 認証および認可の設定（61-11 ページ）
- CAC 認証および認可の管理（61-12 ページ）

CAC 認証および認可の設定

ライセンス: 任意（Any）

サポートされるデバイス: 仮想または X-シリーズ を除くすべて

サポートされる防御センター: 仮想または X-シリーズ を除くすべて

ネットワークのユーザが各自の CAC クレデンシャルを使用してログインする前に、適切なアクセス許可を持つユーザが、CAC 認証および認可のマルチステップ設定プロセスを完了しておく必要があります。

CAC 認証および認可を設定して有効にする方法:

アクセス: Admin/Network Admin

手順 1　組織の指示に従い CAC を挿入します。

手順 2　ブラウザで `https://hostname/` を開きます（*hostname* はご使用の防御センターのホスト名に対応しています）。

手順 3　プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

PIN が受け入れられます。

手順 4　プロンプトが表示されたら、ドロップダウン リストから適切な証明書を選択します。

ブラウザが選択内容を受け入れ、[ログイン（Login）] ページが表示されます。

手順 5　[ユーザ名（Username）] フィールドと [パスワード（Password）] フィールドに、Administrator 特権を持つユーザとしてログインします。ユーザ名では、大文字と小文字が区別されます。

ヒント　CAC 認証および認可の設定が完了するまで、CAC 証明書を使用したログインは**できません**。

デフォルトの開始ページが表示されます。

手順 6　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] に移動し、[外部認証（External Authentication）] タブをクリックします。LDAP 認証オブジェクトの作成の準備（61-13 ページ）および拡張 LDAP 認証オブジェクトの作成（61-18 ページ）で説明する手順に従い、CAC 認証および認可専用の LDAP 認証オブジェクトを作成します。次の設定を行う必要があります。

- [LDAP 固有のパラメータ（LDAP-Specific Parameters）] セクションの詳細設定オプションの [ユーザ名テンプレート（User Name Template）]。詳細については、ユーザ名テンプレートについて（61-8 ページ）を参照してください。
- [属性マッピング（Attribute Mapping）] セクションの [UI アクセス属性（UI Access Attribute）]。詳細については、属性を使用したアクセスの管理（61-8 ページ）を参照してください。
- [グループ制御アクセス ロール（Group Controlled Access Roles）] セクションの既存の LDAP グループの識別名（LDP グループ メンバーシップによってアクセス権を事前に設定する場合）。詳細については、グループ メンバーシップを使用したアクセスの管理について（61-9 ページ）を参照してください。

ヒント　同一認証オブジェクトで CAC 認証とシェル アクセスの両方を設定**できない**ことに注意してください。シェル アクセスのユーザを認証する場合は、別の認証オブジェクトを作成し、システム ポリシーで個別に有効にします。

手順 7　[保存(Save)] をクリックします。

[外部認証(External Authentication)] ページが表示され、このページに新しいオブジェクトが示されます。

手順 8　[システム(System)] > [ローカル(Local)] > [システム ポリシー(System Policy)] に移動します。外部認証の有効化(63-13 ページ)の手順に従って外部認証を有効にし、続いてシステム ポリシーで CAC 認証を有効にします。

注意　変更は、システム ポリシーを防御センターとその管理対象デバイスに適用するまでは反映**されません**。詳細については、システム ポリシーの適用(63-4 ページ)を参照してください。

手順 9　[システム(System)] > [ローカル(Local)] > [設定(Configuration)] に移動し、[HTTPS 証明書(HTTPS Certificate)] をクリックします。HTTPS サーバ証明書をインポートし、必要に応じてサーバ証明書のアップロード(64-6 ページ)で説明する手順に従います。

(注)　認証および認可に使用する予定の CAC で、HTTPS サーバ証明書とユーザ証明書が同じ認証局(CA)により発行される**必要があります**。

[現行 HTTPS 証明書(Current HTTPS Certificate)] ページが更新され、新しい証明書が反映されます。

手順 10　[HTTPS ユーザ証明書の設定(HTTPS User Certificate Settings)] の [ユーザ証明書の有効化(Enable User Certificates)] を選択します。詳細については、ユーザ証明書の要求(64-6 ページ)を参照してください。

手順 11　オプションで、ユーザが初めてログインした後で [システム(System)] > [ローカル(Local)] > [ユーザ管理(User Management)] に移動し、そのユーザのアクセス権を手動で追加または削除します。ユーザの権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。詳細については、ユーザ特権について(61-4 ページ)およびユーザ特権とオプションの変更(61-59 ページ)を参照してください。

CAC ユーザの初回ログイン後の CAC ユーザのロールの変更の詳細については、CAC 認証および認可の管理(61-12 ページ)を参照してください。

CAC 認証および認可の管理

CAC 認証および認可を設定して有効にすると、ネットワークのユーザは各自の CAC クレデンシャルを使用してアプライアンスの Web インターフェイスにログインできます。詳細については、アプライアンスへのログイン(2-1 ページ)を参照してください。

システムでは、CAC 認証ユーザは Electronic Data Interchange Personal Identifier(EDIPI)番号により識別されます。ユーザが CAC クレデンシャルを使用して初めてログインした後で、[ユーザ管理(User Management)] ページでのこれらのユーザのアクセス権限を手動で追加または削除できます。グループ制御アクセス ロールを使用してユーザの権限を事前に設定していない場合、ユーザには、システム ポリシーでデフォルトで付与される権限だけが与えられています。詳細については、ユーザ特権について(61-4 ページ)、グループ メンバーシップを使用したアクセスの管理について(61-9 ページ)、およびユーザ特権とオプションの変更(61-59 ページ)を参照してください。

操作が行われない状態で 24 時間が経過すると、システムによって [ユーザ(User Management)] ページから CAC 認証ユーザが消去されるときに、手動で設定されたアクセス権限が削除されることに注意してください。その後ユーザがログインするたびに、ユーザがページに復元されますが、ユーザのアクセス権限に対する手動での変更はすべて再設定する必要があります。

LDAP 認証オブジェクトの作成の準備

ライセンス：任意（Any）

LDAP サーバへの接続を設定する前に、LDAP 認証オブジェクトの作成に必要な情報を収集する必要があります。設定の特定の側面については、LDAP 認証について（61-6 ページ）を参照してください。

すべての認証オブジェクトに必要な情報は次のとおりです。

- 接続するサーバのサーバ名または IP アドレス
- 接続するサーバのサーバ タイプ
- LDAP ツリーを参照するための十分な権限が付与されているユーザ アカウントのユーザ名とパスワード
- アプライアンスと LDAP サーバの間にファイアウォールがある場合、発信接続を許可するファイアウォールの項目
- ユーザ名が存在するサーバ ディレクトリのベース識別名（可能な場合）

サードパーティの LDAP クライアントを使用して、LDAP ツリーを参照し、ベース DN と属性の説明を確認できることに注意してください。またそのクライアントを使用して、選択したユーザが、選択した DN を参照できることを確認することもできます。LDAP 管理者に連絡し、ご使用の LDAP サーバ向けの推奨される認定 LDAP クライアントを確認してください。

LDAP 認証オブジェクト設定をどのようにカスタマイズするかによって、次の表に示す情報が必要となることがあります。

表 61-1　追加の LDAP 設定情報

目的	必要な情報
389 以外のポートを介した接続	ポート番号
暗号化接続を使用した接続	接続の証明書
属性値に基づいてアプライアンスにアクセスできるユーザをフィルタにより絞り込む	フィルタの条件となる属性と値のペア
ユーザ識別名を検査するのではなく、特定の属性を UI アクセス属性として使用する	属性の名前
ユーザ識別名を検査するのではなく、特定の属性をシェル ログイン属性として使用する	属性の名前
属性値に基づいてシェルを介してアプライアンスにアクセスできるユーザをフィルタにより絞り込む	フィルタの条件となる属性と値のペア
特定のユーザ ロールへのグループの関連付け	各グループの識別名、およびグループがスタティック グループの場合はグループ メンバー属性、グループがダイナミック グループの場合はグループ メンバーの URL 属性
認証および認可での CAC の使用	CAC、CAC を発行した CA により署名されたサーバ証明書、および両方の証明書の証明書チェーン

基本 LDAP 認証オブジェクトの作成

ライセンス: 任意（Any）

LDAP 認証オブジェクトをセットアップできます。LDAP 認証オブジェクトでは多くの値をカスタマイズします。ただし、特定ディレクトリ内のすべてのユーザを認証するだけの場合は、そのディレクトリのベース DN を使用して基本認証オブジェクトを作成できます。ご使用のサーバ タイプでベース DN のデフォルトを設定し、サーバからユーザ データを取得するために使用するアカウントの認証クレデンシャルを指定すれば、認証オブジェクトを簡単に作成できます。このためには、次の手順に従います。

（注） （CAC 認証および認可の設定などのために）認証オブジェクトを作成するときに、各認証設定を検討してカスタマイズする場合は、拡張 LDAP 認証オブジェクトの作成（61-18 ページ）の手順に従ってオブジェクトを作成します。サーバへの接続の暗号化、ユーザ タイムアウトの設定、ユーザ名テンプレートのカスタマイズ、または LDAP グループ メンバーシップに基づく FireSIGHT システム ユーザ ロールの割り当てを行う場合にも、この高度な手順を使用してください。

LDAP サーバへの接続を設定する前に、LDAP 認証オブジェクトの作成に必要な情報を収集する必要があります。設定の特定の側面については、LDAP 認証について（61-6 ページ）を参照してください。

基本認証オブジェクトを作成するには、次の情報が必要です。

- 接続するサーバのサーバ名または IP アドレス
- 接続するサーバのサーバ タイプ
- LDAP ツリーを参照できる十分な権限が付与されているユーザ アカウントのユーザ名とパスワード。シスコはこの目的でドメイン管理ユーザのアカウントを使用することを推奨します。

オプションで、ユーザ検索をさらに絞り込む場合には、特定の属性に特定の値を設定する基本フィルタを追加できます。基本フィルタでは、ベース DN でフィルタに設定されている属性値を含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタは括弧で囲みます。たとえば、F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ `(cn=F*)` を使用します。認証オブジェクトを保存すると、ローカル アプライアンスは、基本フィルタを使用してクエリを実行し、基本フィルタをテストして、このフィルタが正しいかどうかを示します。

LDAP 認証オブジェクトを作成する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[外部認証（External Authentication）] タブをクリックします。

[外部認証（External Authentication）] ページが表示されます。

手順 3　[外部認証オブジェクトの作成（Create External Authentication Object）] をクリックします。

手順 4　[認証方式（Authentication Method）] ドロップダウン リストから [LDAP] を選択します。

LDAP 設定オプションが表示されます。

手順 5　[名前（Name）] フィールドと [説明（Description）] フィールドに、認証サーバの名前と説明を入力します。

手順 6　[サーバ タイプ(Server Type)] ドロップダウン リストからサーバ タイプを選択し、[デフォルトの設定(Set Defaults)] ボタンをクリックして、そのタイプのデフォルト設定を設定します。次の選択肢があります。

- Microsoft Active Directory Server に接続する場合は、[MS Active Directory] を選択し、次に [デフォルトの設定(Set Defaults)] をクリックします。
- Sun Java System Directory Server または Oracle Directory Server に接続する場合は、[Oracle Directory] を選択し、次に [デフォルトの設定(Set Defaults)] をクリックします。
- OpenLDAP サーバに接続する場合は、[OpenLDAP] を選択し、次に [デフォルトの設定(Set Defaults)] をクリックします。
- 上記のサーバ以外のサーバに接続し、デフォルト設定をクリアする場合は、[その他(Other)] を選択し、次に [デフォルトの設定(Set Defaults)] をクリックします。

手順 7　認証データを取得するプライマリ サーバの IP アドレスまたはホスト名を [プライマリ サーバのホスト名/IP アドレス(Primary Server Host Name/IP Address)] フィールドに入力します。

(注)　証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要があります。また、暗号化接続では IPv6 アドレスはサポートされていません。

手順 8　すべてのベース DN のリストを取得するには、[DN を取得(Fetch DNs)] をクリックして、ドロップダウン リストから適切なベース DN を選択します。

たとえば、Example 社のセキュリティ(Security)部門の名前を認証するには、`ou=security,dc=example,dc=com` を選択します。

手順 9　オプションで、ベース DN として指定したディレクトリ内の特定のオブジェクトだけを取得するフィルタを設定するには、[基本フィルタ(Base Filter)] フィールドに、属性タイプ、比較演算子、フィルタとして使用する属性値を括弧で囲んで入力します(囲み用の括弧を含めて最大 450 文字)。

たとえば、ツリー内のユーザ オブジェクトに physicalDeliveryOfficeName 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

手順 10　[ユーザ名(User Name)] フィールドと [パスワード(Password)] フィールドに、LDAP サーバを参照できる十分なクレデンシャルを持つユーザの識別名とパスワードを入力します。

たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ(Security)部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

注意　Microsoft Active Directory Server に接続する場合は、末尾の文字が `$` のサーバ ユーザ名は指定できません。

手順 11　[パスワードの確認(Confirm Password)] フィールドにパスワードを再入力します。

手順 12　オプションで、シェル アクセスのユーザを取得するには、フィルタ条件とする属性タイプを [シェル アクセス属性(Shell Access Attribute)] フィールドに入力します。

たとえば、Microsoft Active Directory Server で `sAMAccountName` シェル アクセス属性を使用してシェル アクセス ユーザを取得するには、[シェル アクセス属性(Shell Access Attribute)] フィールドに `sAMAccountName` と入力します。

(注)　シェル認証では IPv6 アドレスはサポートされていません。

手順 13　[ユーザ名（User Name）] フィールドと [パスワード（Password）] フィールドに、LDAP サーバへのアクセスの検証にクレデンシャルが使用されるユーザの `uid` 値またはシェル アクセス属性値と、パスワードを入力します。この場合も、Microsoft Active Directory Server に関連付けられたサーバ ユーザ名の末尾の文字が `$` であってはならないことに注意してください。

たとえば、Example 社のユーザ `JSmith` のクレデンシャルを取得できるかどうかをテストするには、`JSmith` と入力します。

手順 14　[テスト（Test）] をクリックして接続をテストします。

テストの成功を示すメッセージ、または欠落しているか訂正する必要がある設定を詳しく示すメッセージが表示されます。テストが成功した場合、テストの出力はページ下部に表示されます。この出力には、接続によって取得されたユーザのリストが含まれています。テストの出力に示されるユーザ数が、LDAP サーバから返されるユーザ レコードの数により制限される場合、テスト出力にこの制限が示されます。

手順 15　以下の 2 つの対処法があります。

- テストが成功した場合は [保存（Save）] をクリックします。

  [外部認証（External Authentication）] ページが表示され、このページに新しいオブジェクトが示されます。

  アプライアンスでオブジェクトを使用して LDAP 認証を有効にするには、そのオブジェクトが有効になっているシステム ポリシーをアプライアンスに適用する必要があります。詳細については、外部認証の有効化（63-13 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

- テストが失敗した場合、または取得したユーザのリストをさらに絞り込む場合は、次の項の基本 LDAP 認証接続の調整（61-16 ページ）に進みます。

基本 LDAP 認証接続の調整

ライセンス：任意（Any）

LDAP 認証オブジェクトを作成したが、選択したサーバへの接続が失敗したか、または必要なユーザのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- 画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザ名とパスワードが有効であることを確認します。
- サードパーティの LDAP ブラウザを使用して LDAP サーバに接続し、ベース識別名に示されているディレクトリを参照する権限がユーザにあることを確認します。
- ユーザ名が、LDAP サーバのディレクトリ情報ツリーで一意であることを確認します。
- ユーザ名に、アンダースコア、ピリオド、ハイフン、英数字だけが使用されていることを確認します。
- テスト出力に LDAP バインド エラー 49 が示される場合は、ユーザのユーザ バインディングが失敗しています。サードパーティ アプリケーションを使用してサーバ認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
- サーバを正しく指定していることを確認します。
- サーバの IP アドレスまたはホスト名が正しいことを確認します。

- ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。
- サーバへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。
- 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、サーバに使用されているホスト名と一致している必要があります。
- シェル アクセスを認証する場合は、サーバ接続に IPv6 アドレスを使用していないことを確認します。
- サーバ タイプのデフォルトを使用している場合は、正しいサーバ タイプであることを確認し、[デフォルトの設定（Set Default）] をもう一度クリックしてデフォルト値をリセットします。

  詳細については、LDAP 認証サーバの指定（61-19 ページ）を参照してください。
- ベース識別名を入力した場合は、[DN を取得（Fetch DNs）] をクリックし、サーバで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたはシェル アクセス フィルタを使用している場合は、フィルタが括弧で囲まれており、有効な比較演算子を使用していることを確認します。詳細については、基本フィルタについて（61-7 ページ）およびシェル アクセスについて（61-9 ページ）を参照してください。
- より制限された基本フィルタをテストするには、特定のユーザだけを取得するため、フィルタにそのユーザのベース識別名を設定します。
- 暗号化接続を使用する場合：
- 証明書の LDAP サーバの名前が、接続に使用するホスト名と一致していることを確認します。
- 暗号化されたサーバ接続で IPv6 アドレスを使用していないことを確認します。
- テスト ユーザを使用する場合、ユーザ名とパスワードが正しく入力されていることを確認します。
- テスト ユーザを使用する場合、ユーザ クレデンシャルを削除してオブジェクトをテストします。
- 次の構文を使用して、接続するアプライアンスでコマンド ラインから LDAP サーバに接続し、使用するクエリをテストします。

  ```
  ldapsearch -x -b 'base_distinguished_name'
  -h LDAPserver_ip_address -p port -v -D
  'user_distinguished_name' -W 'base_filter'
  ```

  たとえば、domainadmin@myrtle.example.com ユーザと基本フィルタ (cn=*) を使用して myrtle.example.com のセキュリティ ドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

  ```
  ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
  -h myrtle.example.com -p 389 -v -D
  'domainadmin@myrtle.example.com' -W '(cn=*)'
  ```

接続のテストが正常に完了したが、システム ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、アプライアンスに適用されるシステム ポリシーで有効になっていることを確認します。

正常に接続したが、接続で取得されたユーザ リストを調整する必要がある場合は、基本フィルタまたはシェル アクセス フィルタを追加または変更するか、ベース DN をさらに制限するかまたは制限を緩めて使用することができます。詳細は、次のトピックを参照してください。

- ベース DN について（61-7 ページ）
- 基本フィルタについて（61-7 ページ）
- LDAP 固有パラメータの設定（61-20 ページ）

拡張 LDAP 認証オブジェクトの作成

ライセンス：任意（Any）

アプライアンスにユーザ認証サービスを提供するため、LDAP 認証オブジェクトを作成できます。

認証オブジェクトの作成時に、認証サーバに接続できるようにするための設定を定義します。また、サーバからユーザ データを取得するために使用するディレクトリ コンテキストと検索条件も選択します。オプションで、シェル アクセス認証を設定できます。

ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。

ご使用のサーバ タイプのデフォルト設定を使用して基本 LDAP 設定を迅速にセットアップできますが、詳細設定をカスタマイズして、アプライアンスから LDAP サーバに暗号化接続するかどうか、接続のタイムアウト、およびサーバがユーザ情報を検査する属性を制御することもできます。

LDAP 固有のパラメータの場合、LDAP 命名基準とフィルタおよび属性の構文を使用できます。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』（RFC 3377）に記載されている RFC を参照してください。この手順では構文の例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822（Standard for the Format of ARPA Internet Text Messages）仕様に記載されているアドレス指定構文を使用できることに注意してください。たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Sever を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

（注） CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を**取り外さないでください**。ユーザ証明書を有効にした後では、CAC が常に挿入された状態にしておく**必要があります**。詳細については、ユーザ証明書の要求（64-6 ページ）および CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

拡張認証オブジェクトを作成する方法：

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[外部認証（External Authentication）] タブをクリックします。

[外部認証（External Authentication）] ページが表示されます。

手順 3　[外部認証オブジェクトの作成（Create External Authentication Object）] をクリックします。

[外部認証オブジェクトの作成（Create External Authentication Object）] ページが表示されます。

手順 4　外部認証のためのユーザ データを取得する認証サーバを指定します。詳細については、LDAP 認証サーバの指定（61-19 ページ）を参照してください。

手順 5　認証対象ユーザを取得する検索要求を作成するための認証設定を設定します。ユーザがログイン時に入力するユーザ名の形式を規定するユーザ名テンプレートを指定します。詳細については、LDAP 固有パラメータの設定（61-20 ページ）を参照してください。

手順 6　オプションで、デフォルト アクセス ロール割り当ての基準として使用する LDAP グループを設定します。詳細については、グループによるアクセス権の設定（61-25 ページ）を参照してください。

ヒント　CAC 認証および認可にこのオブジェクトを使用する予定の場合、シスコは、アクセス ロール割り当ての管理のために LDAP グループを設定することを推奨します。詳細については、CAC 認証および認可の管理（61-12 ページ）を参照してください。

手順 7　オプションで、シェル アクセスの認証設定を設定します。詳細については、シェル アクセスの設定（61-26 ページ）を参照してください。

手順 8　正常に認証を実行できるユーザの名前とパスワードを入力して、設定をテストします。詳細については、ユーザ認証のテスト（61-28 ページ）を参照してください。

変更が保存されます。認証の変更がアプライアンスで行われる前に、オブジェクトが有効に設定されているシステム ポリシーをそのアプライアンスに適用する必要があることに注意してください。詳細については、外部認証の有効化（63-13 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

LDAP 認証サーバの指定

ライセンス：任意（Any）

認証オブジェクトの作成時には、管理対象デバイスまたは防御センターが認証のために接続する、プライマリおよびバックアップ サーバとサーバ ポートを最初に指定します。

LDAP 認証サーバを指定する方法：

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[外部認証（External Authentication）] タブをクリックします。

[外部認証（External Authentication）] ページが表示されます。

手順 3　[外部認証オブジェクトの作成（Create External Authentication Object）] をクリックします。

[外部認証オブジェクトの作成（Create External Authentication Object）] ページが表示されます。

手順 4　[認証方式（Authentication Method）] ドロップダウン リストから [LDAP] を選択します。

LDAP 設定オプションが表示されます。

手順 5　オプションで、CAC 認証および認可にこの認証オブジェクトを使用する予定の場合は、[CAC] チェックボックスをオンにします。

CAC 認証および認可の設定の概要については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

手順 6　[名前(Name)] フィールドと [説明(Description)] フィールドに、認証サーバの名前と説明を入力します。

手順 7　オプションで、[サーバ タイプ(Server Type)] フィールドで接続先 LDAP サーバのタイプを選択し、[デフォルトの設定(Set Defaults)] をクリックして、[ユーザ名テンプレート(User Name Template)]、[UI アクセス属性(UI Access Attribute)]、[シェル アクセス属性(Shell Access Attribute)]、[グループ メンバー 属性(Group Member Attribute)]、および [グループ メンバー URL 属性(Group Member URL Attribute)] の各フィールドにデフォルト値を取り込みます。次の選択肢があります。

- Microsoft Active Directory Server に接続する場合は、[MS Active Directory] を選択し、[デフォルトの設定(Set Defaults)] をクリックします。
- Sun Java System Directory Server または Oracle Directory Server に接続する場合は、[Oracle Directory] を選択し、次に [デフォルトの設定(Set Defaults)] をクリックします。
- OpenLDAP サーバに接続する場合は、[OpenLDAP] を選択し、次に [デフォルトの設定(Set Defaults)] をクリックします。
- 上記のサーバ以外の LDAP サーバに接続し、デフォルト設定をクリアする場合は、[その他(Other)] を選択し、次に [デフォルトの設定(Set Defaults)] をクリックします。

手順 8　認証データを取得するプライマリ サーバの IP アドレスまたはホスト名を [プライマリ サーバのホスト名/IP アドレス(Primary Server Host Name/IP Address)] フィールドに入力します。

(注)　証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要があります。また、暗号化接続では IPv6 アドレスはサポートされていません。

手順 9　オプションで、[プライマリ サーバ ポート(Primary Server Port)] フィールドでプライマリ認証サーバが使用するポートを変更します。

手順 10　オプションで、認証データを取得するバックアップ サーバの IP アドレスまたはホスト名を [バックアップ サーバのホスト名/IP アドレス(Backup Server Host Name/IP Address)] フィールドに入力します。

手順 11　オプションで、[バックアップ サーバ ポート(Backup Server Port)] フィールドでプライマリ認証サーバが使用するポートを変更します。

LDAP 固有パラメータの設定(61-20 ページ)に進みます。

LDAP 固有パラメータの設定

ライセンス: 任意(Any)

LDAP 固有パラメータ セクションの設定により、アプライアンスがユーザ名を検索する LDAP ディレクトリの領域が決定され、アプライアンスから LDAP サーバへの接続の詳細が制御されます。

これらの設定を行う場合、有効なユーザ名は一意のユーザ名であり、アンダースコア(_)、ピリオド(.)、ハイフン(-)、英数字を使用できることに注意してください。

ほとんどの LDAP 固有設定の他に、LDAP 命名基準とフィルタおよび属性の構文を使用できます。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』（RFC 3377）に記載されている RFC を参照してください。この手順では構文の例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822（Standard for the Format of ARPA Internet Text Messages）仕様に記載されているアドレス指定構文を使用できることに注意してください。たとえばユーザ オブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Sever を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security, dc=example,dc=com` は使用しません。

次の表で、各 LDAP 固有パラメータについて説明します。

表 61-2　LDAP 固有パラメータ

設定	説明	例
ベース DN（Base DN）	アプライアンスがユーザ情報を検索する LDAP サーバのディレクトリのベース識別名を指定します。 通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。 プライマリ サーバを特定したら、そのサーバから使用可能なベース DN のリストが自動的に取得され、該当するベース DN を選択できることに注意してください。	Example 社のセキュリティ（Security）部門のベース DN は、`ou=security,dc=example,dc=com` となります。
基本フィルタ（Base Filter）	ベース DN でフィルタに設定されている特定の属性と値のペアを含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタは括弧で囲む必要があることに注意してください。 テスト ユーザ名とパスワードを入力して基本フィルタをより具体的にテストするにはユーザ認証のテスト（61-28 ページ）を参照してください。	F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ `(cn=F*)` を使用します。
[ユーザ名/ パスワード（User Name/ Password）]	ローカル アプライアンスがユーザ オブジェクトにアクセスできるようにします。取得する認証オブジェクトに対する適切な権限を持つユーザのユーザ クレデンシャルを指定します。指定するユーザの識別名は、LDAP サーバのディレクトリ情報ツリーで一意である必要があります。Microsoft Active Directory Server に関連付けられたサーバ ユーザ名の末尾の文字が `$` であってはならないことに注意してください。	Example 社のセキュリティ（Security）部門の `admin` ユーザのユーザ名は、`cn=admin, ou=security, dc=example,dc=com` です。
暗号化（Encryption）	通信が暗号化されるかどうかと、暗号化方法を示します。暗号化なし、Transport Layer Security（TLS）、または Secure Sockets Layer（SSL）暗号化を選択できます。TLS または SSL 経由で接続するときに認証に証明書を使用する場合、証明書の LDAP サーバ名が、接続時に使用する名前と一致している**必要がある**ことに注意してください。 ポートを指定した後で暗号化方式を変更すると、ポートが、選択されているサーバ タイプのデフォルト値にリセットされます。	外部認証設定に `10.10.10.250` と入力し、証明書に `computer1.example.com` と入力すると、`computer1.example.com` の IP アドレスが `10.10.10.250` の場合でも、接続は失敗します。外部認証設定のサーバ名を `computer1.example.com` に変更することで、接続が正常に行われます。
[SSL 証明書アップロード パス（SSL Certificate Upload Path）]	ローカル コンピュータで、暗号化に使用する証明書のパスを指定します。	`c:/server.crt`

表 61-2　LDAP 固有パラメータ（続き）

設定	説明	例
[ユーザ名テンプレート（User Name Template）]	文字列変換文字（%s）をユーザのシェル アクセス属性の値にマッピングすることで、ログイン時に入力されるユーザ名の形式を指定します。ユーザ名テンプレートは、認証に使用する識別名の形式です。ユーザがログイン ページにユーザ名を入力すると、アプライアンスにより文字列変換文字が名前に置き換えられ、その結果生成される識別名がユーザ クレデンシャルの検索に使用されます。 CAC 認証および許可にこのオブジェクトを使用するには、[UI アクセス属性（UI Access Attribute）] の値に対応する値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。	%s@security.example.com, %s@mail.com, %s@mil, %s@smil.mil,
Timeout	プライマリ サーバへの接続試行のタイムアウトを設定します。これにより、接続がバックアップ サーバにロールオーバーされます。プライマリ認証サーバからの応答がない状態でこのフィールドに示されている秒数（または LDAP サーバのタイムアウト）が経過すると、アプライアンスはバックアップ サーバに対してクエリを実行します。 ただし LDAP がプライマリ LDAP サーバのポートで実行されており、何らかの理由で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。	プライマリ サーバで LDAP が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。
[UI アクセス属性（UI Access Attribute）]	ローカル アプライアンスに対し、ユーザ識別名の値ではなく、特定の属性の値の照合を行うように指示します。FireSIGHT システム Web インターフェイスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。いずれかのオブジェクトに一致するユーザ名とパスワードがある場合は、ユーザ ログイン要求が認証されます。 サーバ タイプを選択し、デフォルトを設定すると、[UI アクセス属性（UI Access Attribute）] に、そのサーバ タイプに適した値が取り込まれます。 このフィールドを空白のままにすると、ローカル アプライアンスは、LDAP サーバの各ユーザ レコードのユーザ識別名値を調べ、ユーザ名に一致しているかどうかを確認します。 CAC 認証および許可にこのオブジェクトを使用するには、[ユーザ名テンプレート（User Name Template）] の値に対応する値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。	sAMAccountName, userPrincipalName, メール アドレス
[シェル アクセス属性（Shell Access Attribute）]	シェル アクセス クレデンシャルの特定の属性を調べる場合は、その属性に一致するようにこのフィールドを明示的に設定する必要があります。シェル アクセスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。 このフィールドを空白のままにした場合、シェル アクセス認証にはユーザ識別名が使用されます。 サーバ タイプを選択し、デフォルトを設定すると、そのサーバ タイプに適した属性がこのフィールドに事前に取り込まれることに注意してください。	sAMAccountName

サーバに LDAP 固有のパラメータを設定する方法:

アクセス: 管理

手順 1　[外部認証オブジェクトの作成（Create External Authentication Object）] ページの [LDAP 固有のパラメータ（LDAP-Specific Parameters）] セクションには、ベース DN を設定する 2 つのオプションがあります。

- 使用可能なすべてのドメインのリストを取得するには、[DN を取得（Fetch DNs）] をクリックして、ドロップダウン リストから適切なベース ドメイン名を選択します。
- アクセスする LDAP ディレクトリのベース識別名を [ベース DN（Base DN）] フィールドに入力します。

たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` を入力または選択します。

手順 2　オプションで、ベース DN として指定したディレクトリ内の特定のオブジェクトだけを取得するフィルタを設定するには、[基本（Base Filter）] フィールドに、属性タイプ、比較演算子、フィルタとして使用する属性値を括弧で囲んで入力します。

たとえば、ディレクトリ ツリー内のユーザ オブジェクトに physicalDeliveryOfficeName 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

手順 3　[ユーザ名（User Name）] および [パスワード（Password）] フィールドに、LDAP ディレクトリへのアクセスの検証にクレデンシャルが使用されるユーザの識別名とパスワードを入力します。

たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

注意　Microsoft Active Directory Server に接続する場合は、末尾の文字が `$` のサーバ ユーザ名は指定できません。

手順 4　[パスワードの確認（Confirm Password）] フィールドにパスワードを再入力します。

手順 5　基本的な LDAP 固有パラメータの設定後に行う手順には、いくつかの選択肢があります。

- 詳細オプションにアクセスするには、[詳細オプションの表示（Show Advanced Options）] の横の矢印をクリックし、次のステップに進みます。
- LDAP グループ メンバーシップに基づいてユーザ デフォルト ロールを設定する場合は、グループによるアクセス権の設定（61-25 ページ）に進みます。
- 認証に LDAP グループを使用しない場合は、シェル アクセスの設定（61-26 ページ）に進みます。

手順 6　オプションで、次のいずれかの暗号化モードを選択できます。

- セキュア ソケット レイヤ（SSL）を使用して接続するには、[SSL] を選択します。
- Transport Layer Security（TLS）を使用して接続するには、[TLS] を選択します。
- 暗号化なしで接続するには、[なし（None）] を選択します。

（注）　ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされることに注意してください。[なし（None）] または [TLS] の場合、ポートはデフォルト値 389 を使用します。SSL 暗号化を選択した場合は、ポートはデフォルト値 636 を使用します。

手順 7　TLS または SSL 暗号化を選択しており、認証に証明書を使用する場合は、[参照（Browse）] をクリックして有効な TLS または SSL 証明書のロケーションを参照するか、または [SSL 証明書アップロード パス（SSL Certificate Upload Path）] フィールドに証明書のパスを入力します。

証明書のアップロードが正常に完了したことを示すメッセージが表示されます。

（注）　以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、システム ポリシーをアプライアンスに再適用して、新しい証明書を上書きコピーします。

手順 8　オプションで、[ユーザ名テンプレート（User Name Template）] フィールドに、[UI アクセス属性（UI Access Attribute）] の値からユーザ名を判別するときに使用する文字列変換文字（`%s`）を入力します。

たとえば、シェル アクセス属性が `uid` である OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門で働くすべてのユーザを認証するには、[User Name Template] フィールドに `uid=%s,ou=security,dc=example,dc=com` と入力します。Microsoft Active Directory Server の場合は `%s@security.example.com` と入力します。

認証および認可に CAC クレデンシャルを使用するには、[ユーザ名テンプレート（User Name Template）] フィールドに値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

手順 9　オプションで、バックアップ接続にロールオーバーするまでの経過秒数を [タイムアウト（Timeout）] フィールドに入力します。

手順 10　オプションで、ベース DN および基本フィルタの代わりに属性に基づいてユーザを取得する場合、2 つのオプションがあります。

- [属性の取得（Fetch Attrs）] をクリックして使用可能な属性のリストを取得し、適切な属性を選択します。
- 属性を [UI アクセス属性（UI Access Attribute）] フィールドに入力します。

たとえば Microsoft Active Directory Server では、Active Directory Server ユーザ オブジェクトに `uid` 属性がないため、[UI アクセス属性（UI Access Attribute）] を使用してユーザを取得することがあります。代わりに [UI アクセス属性（UI Access Attribute）] フィールドに `userPrincipalName` と入力して、`userPrincipalName` 属性を検索できます。

認証および認可に CAC クレデンシャルを使用するには、[UI アクセス属性（UI Access Attribute）] フィールドに値を入力する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

手順 11　オプションで、シェル アクセスのユーザを取得するには、フィルタ条件とする属性を [シェル アクセス属性（Shell Access Attribute）] フィールドに入力します。

たとえば、Microsoft Active Directory Server で `sAMAccountName` シェル アクセス属性を使用してシェル アクセス ユーザを取得するには、[シェル アクセス属性（Shell Access Attribute）] フィールドに `sAMAccountName` と入力します。

（注）　同一認証オブジェクトで CAC 認証および認可とシェル アクセスの両方を設定することは**できません**。[CAC] チェックボックスをオンにすると、そのページのシェル アクセス設定のオプションが無効になります。代わりに、別の認証オブジェクトを作成し、システム ポリシーで個別に有効にします。詳細については、外部認証の有効化（63-13 ページ）を参照してください。

手順 12　次のステップでは、3 つの選択肢があります。

- LDAP グループ メンバーシップに基づいてユーザ デフォルト ロールを設定する場合は、グループによるアクセス権の設定（61-25 ページ）に進みます。
- 認証に LDAP グループを使用**しない**が、シェル アクセスを設定する場合は、シェル アクセスの設定（61-26 ページ）に進みます。
- 認証に LDAP グループを使用**せず**、シェル アクセスを設定**しない**場合は、ユーザ認証のテスト（61-28 ページ）に進みます。

グループによるアクセス権の設定

ライセンス：任意（Any）

LDAP グループのユーザのメンバーシップに基づいてデフォルト アクセス権を設定する場合は、FireSIGHT システムにより使用される各アクセス ロールに、LDAP サーバの既存のグループの識別名を指定できます。これを行うと、LDAP によって検出された、指定のどのグループにも属さないユーザのデフォルト アクセス設定を設定できます。ユーザがログインすると、FireSIGHT システムは LDAP サーバを動的に検査し、ユーザの現在のグループ メンバーシップに基づいてデフォルト アクセス権を割り当てます。

CAC 認証および認可にオブジェクトを使用する予定の場合、シスコは、CAC 認証ユーザへのアクセス ロール割り当ての管理のために LDAP グループを設定することを推奨します。詳細については、CAC 認証および認可の管理（61-12 ページ）を参照してください。

参照するグループはすべて LDAP サーバに存在している必要があります。スタティック LDAP グループまたはダイナミック LDAP グループを参照できます。スタティック LDAP グループとは、特定のユーザを指し示すグループ オブジェクト属性によってメンバーシップが決定されるグループであり、ダイナミック LDAP グループとは、ユーザ オブジェクト属性に基づいてグループ ユーザを取得する LDAP 検索を作成することでメンバーシップが決定されるグループです。ロールのグループ アクセス権は、グループのメンバーであるユーザにのみ影響します。

ユーザが FireSIGHT システムにログインするときに付与されるアクセス権は、LDAP 構成によって異なります。

- LDAP サーバでグループ アクセス権が設定されていない場合、新しいユーザがログインすると、FireSIGHT システムはそのユーザを LDAP サーバに対して認証し、システム ポリシーに設定されているデフォルトの最小アクセス ロールに基づいてユーザ権限を付与します。
- グループ設定を設定すると、指定されたグループに属している新しいユーザは、メンバーとなっているグループの最小アクセス設定を継承します。
- 新しいユーザが指定のどのグループにも属していない場合は、認証オブジェクトの [グループ制御アクセス ロール（Group Controlled Access Roles）] セクションに指定されているデフォルトの最小アクセス ロールが割り当てられます。
- 設定されている複数のグループにユーザが属している場合、ユーザは最も高いアクセスを持つグループのアクセス ロールを最小アクセス ロールとして受け取ります。

FireSIGHT システム ユーザ管理ページでは、LDAP グループ メンバーシップによってアクセス ロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理（User Management）] ページの [認証方式（Authentication Method）] 列に、[外部 - ローカル変更（External - Locally Modified）] というステータスが表示されます。

(注)　ダイナミック グループを使用する場合、LDAP クエリは、LDAP サーバで設定されているとおりに使用されます。この理由から、検索構文エラーが原因で無限ループが発生することを防ぐため、FireSIGHT システムでは検索の再帰回数が 4 回に制限されています。この再帰回数内でユーザのグループ メンバーシップが確立されない場合、[グループ制御アクセス ロール(Group Controlled Access Roles)] セクションで定義されているデフォルト アクセス ロールがユーザに付与されます。

グループ メンバーシップに基づいてデフォルトのロールを設定する方法:

アクセス:管理

手順 1　[外部認証オブジェクトの作成(Create External Authentication Object)] ページで、[グループ制御アクセス ロール(Group Controlled Access Roles)] の横の下矢印をクリックします。

セクションが展開されます。

手順 2　オプションで、グループ メンバーシップ別のアクセス デフォルトを設定します。

FireSIGHT システム ユーザ ロールに対応する [DN] フィールドに、これらのロールに割り当てる必要があるユーザを含む LDAP グループの識別名を入力します。

たとえば、`Example` 社の情報テクノロジー(Information Technology)部門の名前を認証するには、[Administrator] フィールドに次のように入力します。

```
cn=itgroup,ou=groups, dc=example,dc=com
```

ユーザ アクセス ロールの詳細については、新しいユーザ アカウントの追加(61-47 ページ)を参照してください。

手順 3　[デフォルト ユーザ ロール(Default User Role)] から、指定のどのグループにも属さないユーザのデフォルト最小アクセス ロールを選択します。

ヒント　複数のロールを選択するには、Ctrl キーを押しながらロール名をクリックします。

手順 4　スタティック グループを使用していた場合は、スタティック グループのメンバーシップを指定する LDAP 属性を [グループ メンバー属性(Group Member Attribute)] フィールドに入力します。

たとえば、デフォルトの Security Analyst アクセスのために参照するスタティック グループのメンバーシップを示すために `member` 属性を使用する場合は、`member` と入力します。

手順 5　ダイナミック グループを使用していた場合は、ダイナミック グループのメンバーシップの決定に使用される LDAP 検索文字列を含む LDAP 属性を [グループ メンバー URL 属性(Group Member URL Attribute)] フィールドに入力します。

たとえば、デフォルトの Admin アクセスに対して指定したダイナミック グループのメンバーを取得する LDAP 検索が `memberURL` 属性に含まれている場合は、`memberURL` と入力します。

手順 6　シェル アクセスの設定(61-26 ページ)に進みます。

シェル アクセスの設定

ライセンス:任意(Any)

LDAP サーバを使用して、管理対象デバイスまたは防御センターでシェル アクセス用アカウントを認証することもできます。シェル アクセスを付与するユーザの項目を取得する検索フィルタを指定します。

同一認証オブジェクトで CAC 認証および認可とシェル アクセスの両方を設定することは**できません**。代わりに、別の認証オブジェクトを作成し、システム ポリシーで個別に有効にします。シェル アクセスの認証オブジェクトは、システム ポリシーの最初の認証オブジェクトである必要があります。認証オブジェクトの順序の管理については、外部認証の有効化（63-13 ページ）を参照してください。

（注） シスコは、仮想デバイスまたは Blue Coat X-Series 向け Cisco NGIPS の外部認証をサポートしていません。さらに、シェル アクセス認証では IPv6 がサポートされていません。

admin アカウントを除き、シェル アクセスは設定したシェル アクセス属性によって完全に制御されます。設定するシェル アクセス フィルタにより、シェルにログインできる LDAP サーバのユーザが決定します。

ログイン時に各シェル ユーザのホーム ディレクトリが作成されること、および（LDAP 接続を無効にすることで）LDAP シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは `/etc/password` 内の `/bin/false` に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

[基本フィルタと同一にする（Same as Base Filter）] チェックボックスを使用すると、ベース DN で限定されるすべてのユーザが、シェル アクセス権限でも限定される場合に、より効率的に検索できます。通常、ユーザを取得する LDAP クエリは、基本フィルタとシェル アクセス フィルタを組み合わせます。シェル アクセス フィルタが基本フィルタと同一である場合は、同じクエリが 2 回実行されることになり、不必要に時間を消費することになります。[基本フィルタと同一にする（Same as Base Filter）] オプションを使用すると、この両方の目的でクエリを 1 回だけ実行することができます。

シェル ユーザは、小文字で構成されたユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

注意 シリーズ 3 防御センターでは、すべてのシェル ユーザに `sudoers` 特権が付与されます。シェル アクセスが付与されるユーザのリストを適切に制限してください。シリーズ 3 と仮想デバイスでは、外部認証ユーザに付与されるシェル アクセスのデフォルトは、**Configuration** レベルのコマンド ライン アクセスになります。このアクセスでも `sudoers` 特権が付与されます。

シェル アカウント認証を設定する方法:

アクセス: 管理

手順 1 オプションで、[外部認証オブジェクトの作成（Create External Authentication Object）] ページでシェル アクセス アカウント フィルタを設定します。次の複数のオプションがあります。

- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、括弧で囲んで [シェル アクセス フィルタ（Shell Access Filter）] フィールドに入力します。
- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同一にする（Same as Base Filter）] を選択します。
- シェル アクセスの LDAP 認証を防止するには、このフィールドを空白にします。シェル アクセス フィルタを指定しないことを選択すると、認証オブジェクトの保存時に、フィルタを空白のままにすることを確認する警告が表示されます。

たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

手順 2 ユーザ認証のテスト（61-28 ページ）に進みます。

ユーザ認証のテスト

ライセンス：任意（Any）

LDAP サーバを設定し、認証設定を行ったら、これらの設定をテストするため、認証できる必要があるユーザのユーザ クレデンシャルを指定できます。

ユーザ名として、テストに使用するユーザの uid 属性の値を入力できます。Microsoft Active Directory Server に接続して uid の代わりにシェル アクセス属性を指定する場合は、ユーザ名としてこの属性の値を使用します。ユーザの完全修飾識別名も指定できます。

テスト出力には、有効なユーザ名と無効なユーザ名が示されます。有効なユーザ名は一意のユーザ名であり、英数字と、アンダースコア（_）、ピリオド（.）、ハイフン（-）のみを使用できます。無効なユーザ名は、その他の英数字以外の文字（スペースなど）が含まれているユーザ名です。

Web インターフェイスのページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。

ヒント　テスト ユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。最初に、追加のテスト パラメータを使用せずにサーバ設定をテストします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

ユーザ認証をテストする方法：

アクセス：管理

手順 1　[ユーザ名（User Name）] フィールドと [パスワード（Password）] フィールドに、LDAP サーバへのアクセスの検証にクレデンシャルが使用されるユーザの uid 値またはシェル アクセス属性値と、パスワードを入力します。

たとえば、Example 社のユーザ JSmith のクレデンシャルを取得できるかどうかをテストするには、JSmith と入力します。

手順 2　[テスト（Test）] をクリックします。

テストの成功を示すメッセージ、または欠落しているか訂正する必要がある設定を詳しく示すメッセージが表示されます。以下の 2 つの対処法があります。

- テストが成功した場合、テストの出力がページ下部に表示されます。[保存（Save）] をクリックします。[外部認証（External Authentication）] ページが表示され、このページに新しいオブジェクトが示されます。

  アプライアンスでオブジェクトを使用して LDAP 認証を有効にするには、そのオブジェクトが有効になっているシステム ポリシーをアプライアンスに適用する必要があります。詳細については、外部認証の有効化（63-13 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

- テストが失敗した場合は、接続のトラブルシューティングの提案事項につて基本 LDAP 認証接続の調整（61-16 ページ）を参照してください。表示されるエラー メッセージに、接続失敗の原因が示されていることに注意してください。

LDAP 認証オブジェクトの例

ライセンス：任意（Any）

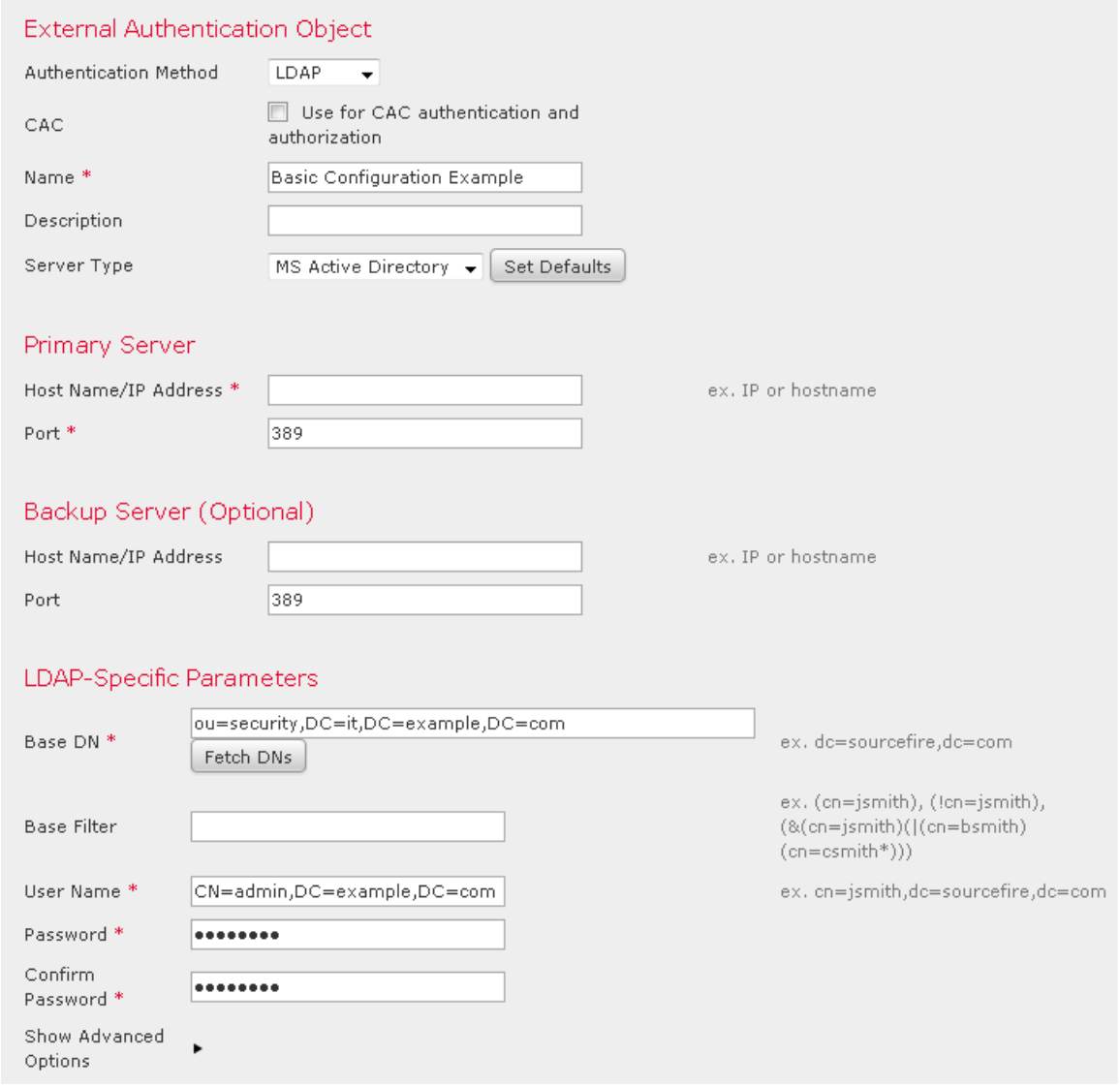
ここでは、基本設定を使用する LDAP 設定の例と、詳細な設定オプションを使用する例を示します。

- 例：LDAP の基本設定（61-29 ページ）
- 例：詳細な LDAP 設定（61-30 ページ）

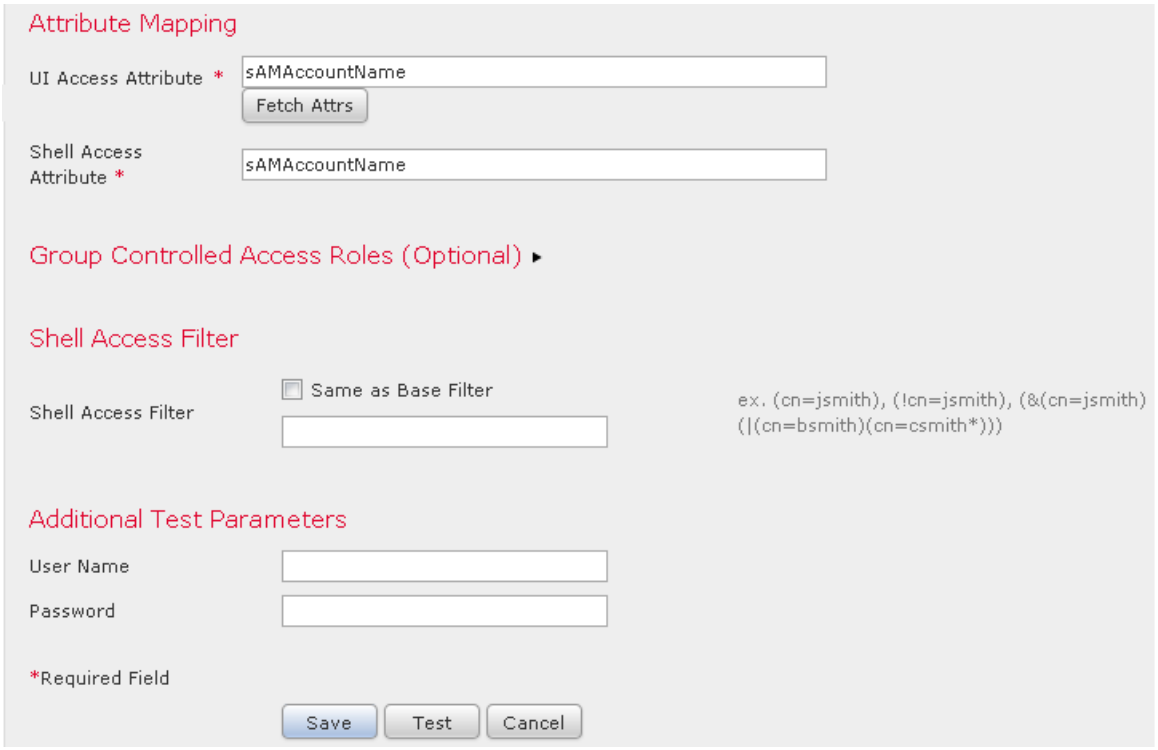
例：LDAP の基本設定

ライセンス：任意（Any）

次の図は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの基本設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 389 が使用されます。



この例では、Example 社の情報テクノロジー ドメインのセキュリティ（Security）部門のベース識別名として OU=security,DC=it,DC=example,DC=com が使用されています。



ただし、このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に uid 属性ではなく sAMAccountName 属性が使用されます。サーバのタイプとして MS Active Directory を選択し、[デフォルトの設定（Set Defaults）] をクリックすると、[UI アクセス属性（UI Access Attribute）] が sAMAccountName に設定されます。その結果、ユーザが FireSIGHT システムへのログインを試行すると、FireSIGHT システムは各オブジェクトの sAMAccountName 属性を検査し、一致するユーザ名を検索します。

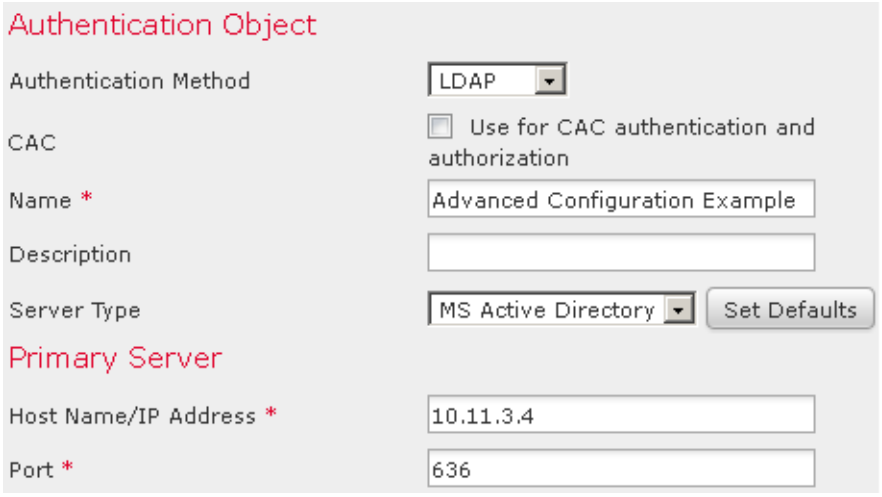
また、[シェル アクセス属性（Shell Access Attribute）] が sAMAccountName の場合、ユーザがアプライアンスでシェル アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 sAMAccountName 属性が検査され、一致が検索されます。

基本フィルタはこのサーバに適用されないため、FireSIGHT システムはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバへの接続は、デフォルトの期間（または LDAP サーバで設定されたタイムアウト期間）の経過後にタイムアウトします。

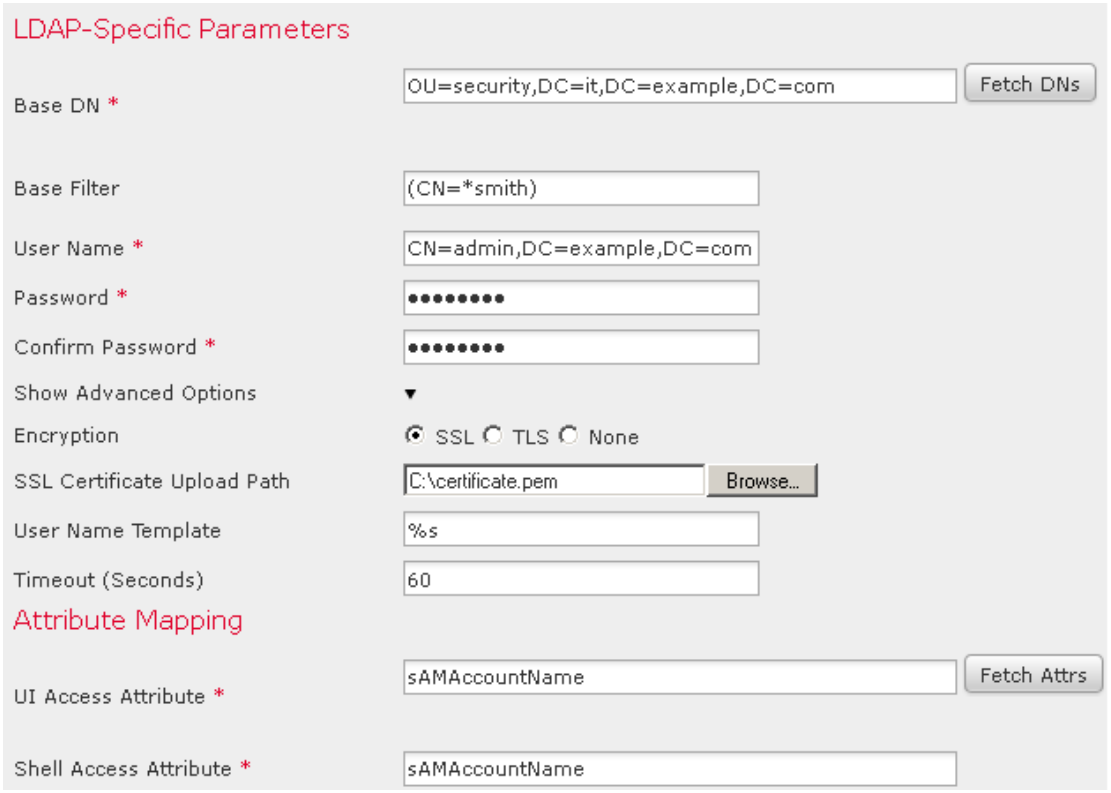
例：詳細な LDAP 設定

ライセンス：任意（Any）

次の例は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの詳細設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 636 が使用されます。



この例では、Example 社の情報テクノロジー ドメインのセキュリティ（Security）部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` が使用されています。ただし、このサーバに基本フィルタ（`(cn=*smith)`）が設定されていることに注意してください。このフィルタは、サーバから取得するユーザを、一般名が `smith` で終わるユーザに限定します。

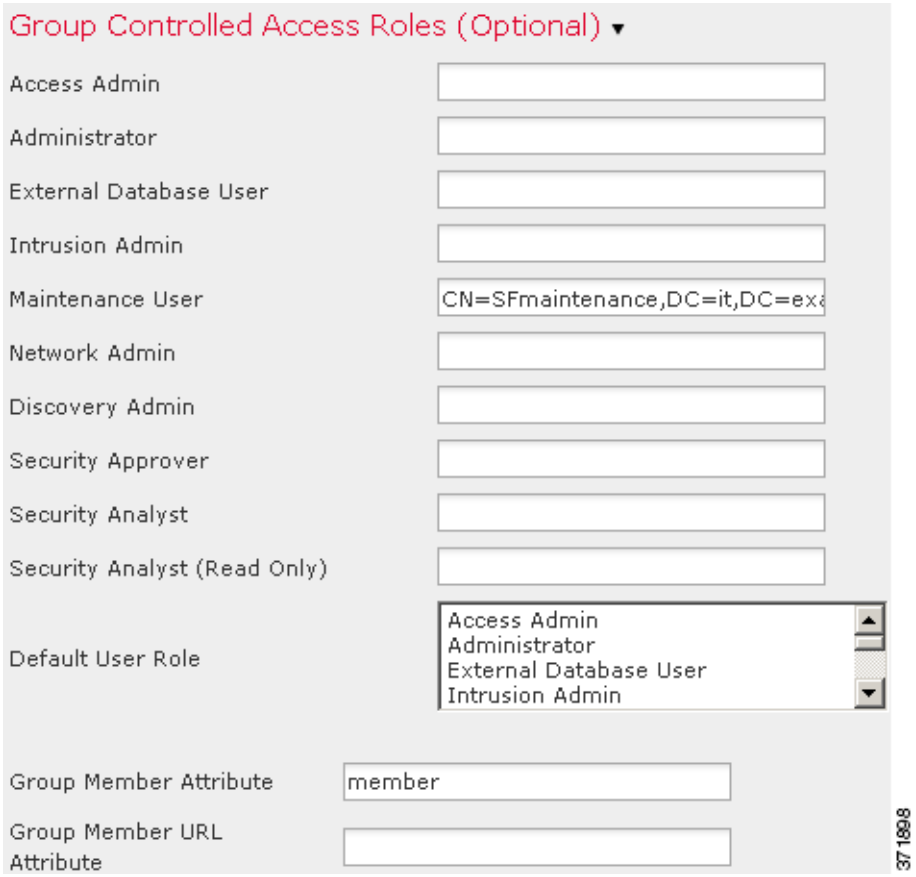


サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[タイムアウト（Timeout）] の設定により、60 秒経過後にサーバへの接続がタイムアウトします。

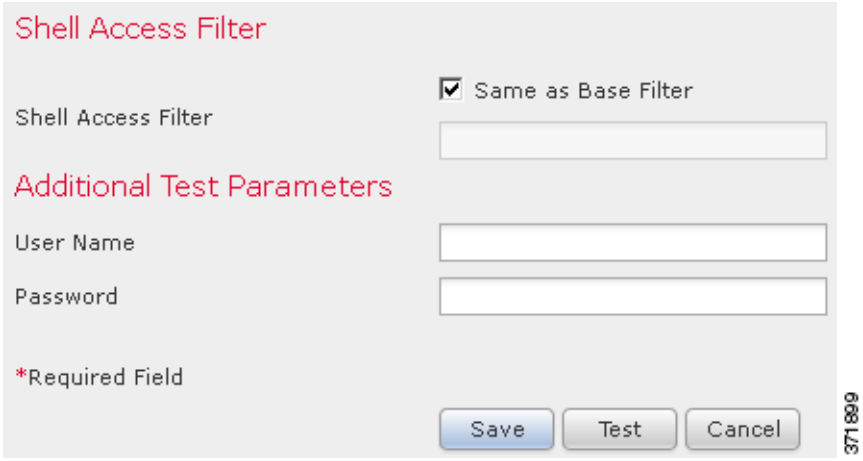
このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に uid 属性ではなく sAMAccountName 属性が使用されます。設定では、[UI アクセス属性（UI Access Attribute）] が sAMAccountName であることに注意してください。その結果、ユーザが FireSIGHT システムへのログインを試行すると、FireSIGHT システムは各オブジェクトの sAMAccountName 属性を検査し、一致するユーザ名を検索します。

また、[シェル アクセス属性（Shell Access Attribute）] が sAMAccountName の場合、ユーザがアプライアンスでシェル アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 sAMAccountName 属性が検査され、一致が検索されます。

この例では、グループ設定も行われます。Maintenance User ロールが、member グループ属性を持ち、ベース ドメイン名が CN=SFmaintenance,DC=it,DC=example,DC=com であるグループのすべてのメンバーに自動的に割り当てられます。



シェル アクセス フィルタは、基本フィルタと同一に設定されます。このため、同じユーザが Web インターフェイスを使用する場合と同様に、シェルを介してアプライアンスにアクセスできます。



LDAP 認証オブジェクトの編集

ライセンス:任意（Any）

既存の認証オブジェクトを編集できます。ポリシーを再適用するまでは、変更内容は反映されません。

認証オブジェクトを編集する方法:

アクセス:管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[外部認証（External Authentication）] タブをクリックします。

[外部認証（External Authentication）] ページが表示されます。

手順 3　編集するオブジェクトの横にある編集アイコン（ ）をクリックします。

[外部認証オブジェクトの作成（Create External Authentication Object）] ページが表示されます。

手順 4　必要に応じてオブジェクト設定を変更します。

手順 5　[テスト（Test）] をクリックします。

テストの成功を示すメッセージ、または欠落しているか訂正する必要がある設定を詳しく示すメッセージが表示されます。テストが成功した場合、テストの出力がページ下部に表示されます。

テストが失敗した場合は、接続のトラブルシューティングの提案事項につて基本 LDAP 認証接続の調整（61-16 ページ）を参照してください。表示されるエラー メッセージに、接続失敗の原因が示されていることに注意してください。

手順 6　[保存（Save）] をクリックします。

変更が保存され、[外部認証（External Authentication）] ページが表示されます。認証の変更がアプライアンスで行われる前に、オブジェクトが有効に設定されているシステム ポリシーをそのアプライアンスに適用する必要があることに注意してください。詳細については、外部認証の有効化（63-13 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

RADIUS 認証

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバで、認証オブジェクトを作成できます。

詳細については、次の各項を参照してください。

RADIUS 認証について

ライセンス：任意（Any）

RADIUS サーバで認証されたユーザが初めてログインすると、認証オブジェクトでそのユーザに指定されているロールがユーザに付与されます。どのユーザ ロールにもリストされていないユーザには、認証オブジェクトで選択されているデフォルト アクセス ロールが付与されます。認証オブジェクトでデフォルト アクセス ロールが選択されていない場合は、システム ポリシーのデフォルト アクセス ロールが付与されます。設定が認証オブジェクトのユーザ リストを介して付与されていない場合は、必要に応じてユーザのロールを変更できます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとすると、ユーザ アカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

（注） シリーズ 3 管理対象デバイスで外部認証を有効にする前に、シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除してください。

FireSIGHT システムの RADIUS 実装では、SecurID® トークンの使用がサポートされています。SecurID を使用したサーバによる認証を設定すると、そのサーバに対して認証されているユーザが、SecurID PIN の末尾に SecurID トークンを付加し、シスコ アプライアンスへのログイン時にそれをパスワードとして使用します。SecurID が FireSIGHT システム外部のユーザを認証するように適切に設定されている限り、これらのユーザは PIN と SecurID を使用して FireSIGHT システムにログインでき、アプライアンスでの追加の設定は不要です。

RADIUS 認証オブジェクトの作成

ライセンス：任意（Any）

RADIUS 認証オブジェクトの作成時に、認証サーバに接続できるようにする設定を定義します。また、特定のユーザおよびデフォルト ユーザにユーザ ロールを付与します。RADIUS サーバから、認証予定のユーザのカスタム属性が返される場合は、これらのカスタム属性を定義する必要があります。オプションで、シェル アクセス認証も設定できます。

認証オブジェクトを作成するには、ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできる必要があることに注意してください。

認証オブジェクトを作成する方法:

アクセス:管理

手順 1　[システム(System)] > [ローカル(Local)] > [ユーザ管理(User Management)] を選択します。

[ユーザ管理(User Management)] ページが表示されます。

手順 2　[外部認証(External Authentication)] タブをクリックします。

[外部認証(External Authentication)] ページが表示されます。

手順 3　[外部認証オブジェクトの作成(Create External Authentication Object)] をクリックします。

[外部認証オブジェクトの作成(Create External Authentication Object)] ページが表示されます。

手順 4　外部認証のためのユーザ データを取得するプライマリ認証サーバとバックアップ認証サーバを指定し、タイムアウト値と再試行値を設定します。詳細については、RADIUS 接続の設定(61-35 ページ)を参照してください。

手順 5　デフォルトのユーザ ロールを設定します。オプションで、ユーザを指定するか、または特定の FireSIGHT システム アクセス ロールを付与するユーザのユーザ属性値を指定します。詳細については、RADIUS ユーザ ロールの設定(61-37 ページ)を参照してください。

手順 6　オプションで、管理シェル アクセスを設定します。詳細については、管理シェル アクセスの設定(61-38 ページ)を参照してください。

手順 7　認証対象ユーザのプロファイルからカスタム RADIUS 属性が返される場合は、これらの属性を定義します。詳細については、カスタム RADIUS 属性の定義(61-39 ページ)を参照してください。

手順 8　認証が成功する必要があるユーザの名前とパスワードを入力して、設定をテストします。詳細については、ユーザ認証のテスト(61-40 ページ)を参照してください。

変更が保存されます。認証の変更がアプライアンスで行われる前に、オブジェクトが有効に設定されているシステム ポリシーをそのアプライアンスに適用する必要があることに注意してください。詳細については、外部認証の有効化(63-13 ページ)およびシステム ポリシーの適用(63-4 ページ)を参照してください。

RADIUS 接続の設定

ライセンス:任意(Any)

RADIUS 認証オブジェクトの作成時には、ローカル アプライアンス(管理対象デバイスまたは防御センター)が認証のために接続するプライマリおよびバックアップ サーバとサーバ ポートを最初に指定します。

(注)　RADIUS が正しく機能するためには、ファイアウォールで認証ポートとアカウンティング ポート(デフォルトでは 1812 および 1813)を開く必要があります。

バックアップ認証サーバを指定する場合は、プライマリ サーバへの接続試行操作のタイムアウトを設定できます。プライマリ認証サーバからの応答がない状態で [タイムアウト(Timeout)] フィールド(または LDAP サーバのタイムアウト)に指定された秒数が経過すると、アプライアンスはプライマリ サーバに対してクエリを再実行します。

アプライアンスがプライマリ認証サーバに対して再クエリを実行した後に、プライマリ認証サーバからの応答がない状態で [再試行回数(Retries)] フィールドに指定された回数を超え、[タイムアウト(Timeout)] フィールドに指定された秒数が再び経過すると、プライアンスはバックアップ サーバにロールオーバーします。

たとえば、プライマリ サーバで RADIUS が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。ただし RADIUS がプライマリ RADIUS サーバのポートで実行されており、何らかの理由（誤った設定またはその他の問題など）で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。

RADIUS 認証サーバを指定する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[外部認証（External Authentication）] タブをクリックします。

[外部認証（External Authentication）] ページが表示されます。

手順 3　[外部認証オブジェクトの作成（Create External Authentication Object）] をクリックします。

[外部認証オブジェクトの作成（Create External Authentication Object）] ページが表示されます。

手順 4　[認証方式（Authentication Method）] ドロップダウン リストから [RADIUS] を選択します。

RADIUS 設定オプションが表示されます。

手順 5　[名前（Name）] フィールドと [説明（Description）] フィールドに、認証サーバの名前と説明を入力します。

手順 6　認証データを取得するプライマリ RADIUS サーバの IP アドレスまたはホスト名を [プライマリ サーバのホスト名/IP アドレス（Primary Server Host Name/IP Address）] フィールドに入力します。

（注）　シェル認証では IPv6 アドレスはサポートされていません。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して認証オブジェクトをセットアップし、システム ポリシーの最初の認証オブジェクトとしてその IPv4 オブジェクトを使用します。

手順 7　オプションで、[プライマリ サーバ ポート（Primary Server Port）] フィールドでプライマリ RADIUS 認証サーバが使用するポートを変更します。

（注）　認証ポート番号とアカウンティング ポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの `/etc/services` ファイルの `radius` データと `radacct` データから RADIUS ポート番号を判断します。

手順 8　プライマリ RADIUS 認証サーバの秘密鍵を [RADIUS 秘密鍵（RADIUS Secret Key）] フィールドに入力します。

手順 9　認証データを取得するバックアップ RADIUS 認証サーバの IP アドレスまたはホスト名を [バックアップ サーバのホスト名/IP アドレス（Backup Server Host Name/IP Address）] フィールドに入力します。

手順 10　オプションで、[バックアップ サーバ ポート（Backup Server Port）] フィールドで、バックアップ RADIUS 認証サーバが使用するポートを変更します。

（注）　認証ポート番号とアカウンティング ポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの `/etc/services` ファイルの `radius` データと `radacct` データから RADIUS ポート番号を判断します。

手順 11　バックアップ RADIUS 認証サーバの秘密鍵を [RADIUS 秘密鍵（RADIUS Secret Key）] フィールドに入力します。

手順 12　[タイムアウト（Timeout）] フィールドに、接続を再試行するまでの経過秒数を入力します。

手順 13　[再試行回数（Retries）] フィールドに、バックアップ接続にロールオーバーする前に、プライマリ サーバ接続を試行する回数を入力します。

手順 14　RADIUS ユーザ ロールの設定（61-37 ページ）に進みます。

RADIUS ユーザ ロールの設定

ライセンス：任意（Any）

RADIUS サーバで既存のユーザに対してアクセス ロールを指定するには、FireSIGHT システムで使用される各アクセス ロールに対してユーザ名をリストします。これを行うと、RADIUS によって検出された、特定のロールに対して指定されていないユーザのデフォルト アクセス設定を設定できます。

ユーザがログインすると、FireSIGHT システムは RADIUS サーバを検査し、RADIUS 設定に基づいてアクセス権を付与します。

- ユーザに対して特定のアクセス権が設定されておらず、デフォルト アクセス ロールが選択されていない場合、新しいユーザがログインすると、FireSIGHT システムは RADIUS サーバに対してそのユーザを認証してから、システム ポリシーで設定されているデフォルト アクセス ロールに基づいてユーザ権限を付与します。
- 新しいユーザがどのリストにも指定されておらず、認証オブジェクトの [デフォルト ユーザ ロール（Default User Role）] リストでデフォルト アクセス ロールが選択されている場合、ユーザにはこのデフォルト アクセス ロールが割り当てられます。
- 1 つ以上の特定のロールのリストにユーザを追加すると、割り当てられているすべてのアクセス ロールがそのユーザに付与されます。

また、ユーザ名の代わりに属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。たとえば、Security Analyst とする必要があるすべてのユーザの [User-Category] 属性の値が [Analyst] である場合、これらのユーザにそのロールを付与するには、[セキュリティ アナリスト リスト（Security Analyst List）] フィールドに `User-Category=Analyst` と入力します。カスタム属性を使用してユーザ ロール メンバーシップを設定するには、その前に、カスタム属性を定義する必要があることに注意してください。詳細については、カスタム RADIUS 属性の定義（61-39 ページ）を参照してください。

外部認証されるが、特定のロールにリストされないすべてのユーザに、デフォルトのユーザ ロールを割り当てることができます。[デフォルト ユーザ ロール（Default User Role）] リストでは、複数のロールを選択できます。

FireSIGHT システムでサポートされているユーザ ロールの詳細については、RADIUS ユーザ ロールの設定（61-37 ページ）を参照してください。

FireSIGHT システム ユーザ管理ページで RADIUS ユーザ リスト メンバーシップが設定されているため、アクセス ロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。

注意　ユーザの最小アクセス設定を変更するには、[RADIUS 固有のパラメータ（RADIUS Specific Parameters）] セクションのリスト間でユーザを移動するかまたは RADIUS サーバでユーザの属性を変更する他に、システム ポリシーを再適用し、ユーザ管理ページで割り当てられているユーザ権限を削除する必要があります。

ユーザ リストに基づいてアクセスを設定する方法:

アクセス: 管理

手順 1　FireSIGHT システム ユーザ ロールに対応するフィールドに、各ユーザの名前を入力するか、またはこれらのロールに割り当てる必要がある属性と値のペアを指定します。ユーザ名と属性値のペアは、カンマで区切ります。

たとえば、ユーザ `jsmith` と `jdoe` に Administrator ロールを付与する場合は、[Administrator] フィールドに `jsmith, jdoe` と入力します。

もう 1 つの例として、[ユーザ カテゴリ（User-Category）] の値が [Maintenance] であるすべてのユーザに Maintenance User ロールを付与するには、[Maintenance User] フィールドに `User-Category=Maintenance` と入力します。

ユーザ アクセス ロールの詳細については、ユーザ ロールの設定（61-53 ページ）を参照してください。

手順 2　[デフォルト ユーザ ロール（Default User Role）] リストから、指定のどのグループにも属していないユーザのデフォルト最小アクセス ロールを選択します。

ヒント　複数のロールを選択するには、Ctrl キーを押しながらロール名をクリックします。

手順 3　管理シェル アクセスの設定（61-38 ページ）に進みます。

管理シェル アクセスの設定

ライセンス: 任意（Any）

RADIUS サーバを使用して、ローカル アプライアンス（管理対象デバイスまたは防御センター）で、シェル アクセスについてアカウントを認証することもできます。シェル アクセスを付与するユーザのユーザ名を指定します。シェル アクセスは、システム ポリシーの最初の認証オブジェクトでのみ設定できることに注意してください。認証オブジェクトの順序の管理については、外部認証の有効化（63-13 ページ）を参照してください。

（注）　シェル認証では IPv6 アドレスはサポートされていません。IPv6 アドレスを使用してプライマリ RADIUS サーバを設定し、管理シェル アクセスも設定すると、シェル アクセスの設定は無視されます。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して別の認証オブジェクトをセットアップし、システム ポリシーの最初の認証オブジェクトとしてそのオブジェクトを使用します。

Admin アカウント以外は、RADIUS 認証オブジェクトで設定したシェル アクセス リストにより、アプライアンスでのシェル アクセスが完全に制御されます。システム ポリシーの適用時に、シェル ユーザはアプライアンスのローカル ユーザとして設定されます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとすると、ユーザ アカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

ログイン時に各シェル ユーザのホーム ディレクトリが作成されること、および(RADIUS 接続を無効にすることで)RADIUS シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは `/etc/password` 内の `/bin/false` に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

シェル ユーザは、小文字で構成されたユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

注意　シリーズ 3 防御センターでは、すべてのシェル ユーザに `sudoers` 特権が付与されます。シェル アクセスが付与されるユーザのリストを適切に制限してください。シリーズ 3 と仮想デバイスでは、外部認証ユーザに付与されるシェル アクセスのデフォルトは、**Configuration** レベルのコマンド ライン アクセスになります。このアクセスでも `sudoers` 特権が付与されます。

シェル アカウント認証を設定する方法:

アクセス: 管理

手順 1　[管理者シェル アクセス ユーザ リスト(Administrator Shell Access User List)] フィールドに、ユーザ名をカンマで区切って入力します。

(注)　シェル アクセス フィルタを指定しないことを選択すると、認証オブジェクトの保存時に、フィルタを空白のままにすることを確認する警告が表示されます。

手順 2　カスタム RADIUS 属性の定義(61-39 ページ)に進みます。

カスタム RADIUS 属性の定義

ライセンス: 任意(Any)

RADIUS サーバが、`/etc/radiusclient/` 内の `dictionary` ファイルに含まれていない属性の値を返し、これらの属性を使用してユーザにユーザ ロールを設定する予定の場合は、ログイン認証オブジェクトでこれらの属性を定義する必要があります。

RADIUS サーバでユーザ プロファイルを調べると、ユーザについて返される属性を見つけることができます。

属性を定義する場合は、英数字からなる属性名を指定します。属性名の中の単語を区切るには、スペースではなくダッシュを使用することに注意してください。また、指定する属性 ID は整数であり、`etc/radiusclient/dictionary` ファイルの既存の属性 ID と競合していてはなりません。属性のタイプ(文字列、IP アドレス、整数、または日付)も指定します。

たとえば、シスコ ルータが接続しているネットワーク上で RADIUS サーバが使用される場合、Ascend-Assign-IP-Pool 属性を使用して、特定の IP アドレス プールからログインするすべてのユーザに特定のロールを付与できます。Ascend-Assign-IP-Pool は、ユーザがログインできるアドレス プールを定義する整数属性であり、割り当てられる IP アドレス プールの番号を示す整数が指定されます。そのカスタム属性を宣言するには、属性名が Ascend-IP-Pool-Definition、属性 ID が 218、属性タイプが integer のカスタム属性を作成します。次に、Ascend-IP-Pool-Definition 属性値が 2 のすべてのユーザに対し、読み取り専用の Security Analyst 権限を付与するには、Ascend-Assign-IP-Pool=2 を [Security Analyst (Read Only)] フィールドに入力します。

RADIUS 認証オブジェクトの作成時に、そのオブジェクトの新しいディクショナリ ファイルが FireSIGHT システム アプライアンスの /var/sf/userauth ディレクトリに作成されます。認証オブジェクトに追加するカスタム属性はすべて、そのディクショナリ ファイルに追加されます。

カスタム属性を定義する方法:

アクセス:管理

手順 1　矢印をクリックして、[カスタム RADIUS 属性の定義（Define Custom RADIUS Attributes）] セクションを展開します。

属性フィールドが表示されます。

手順 2　[属性名（Attribute Name）] フィールドに、英数字とダッシュからなる属性名をスペースなしで入力します。

手順 3　[属性 ID（Attribute ID）] フィールドに、属性 ID を整数形式で入力します。

手順 4　[属性タイプ（Attribute Type）] ドロップダウン リストから、属性のタイプを選択します。

手順 5　認証オブジェクトにカスタム属性を追加するには、[追加（Add）] をクリックします。

ヒント　認証オブジェクトからカスタム属性を削除するには、その属性の横にある [削除（Delete）] をクリックします。

手順 6　ユーザ認証のテスト（61-40 ページ）に進みます。

ユーザ認証のテスト

ライセンス:任意（Any）

RADIUS 接続、ユーザ ロール、およびカスタム属性を設定したら、これらの設定をテストするため、認証できる必要があるユーザのユーザ クレデンシャルを指定できます。

ユーザ名として、テストするユーザのユーザ名を入力できます。

UI のページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。

ヒント　テスト ユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [追加のテスト パラメータ（Additional Test Parameters）] フィールドにユーザ情報を入力せずに [テスト（Test）] をクリックします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

ユーザ認証をテストする方法:

アクセス:管理

手順 1　[ユーザ名(User Name)] フィールドと [パスワード(Password)] フィールドに、RADIUS サーバへのアクセスの検証にクレデンシャルが使用されるユーザのユーザ名とパスワードを入力します。

たとえば、Example 社の `jsmith` のユーザ クレデンシャルを取得できるかどうかをテストするには、`jsmith` と入力します。

手順 2　[詳細の表示(Show Details)] を選択し、[テスト(Test)] をクリックします。

テストの成功を示すメッセージ、または欠落しているか訂正する必要がある設定を詳しく示すメッセージが表示されます。

手順 3　テストが成功した場合は [保存(Save)] をクリックします。

[外部認証(External Authentication)] ページが表示され、このページに新しいオブジェクトが示されます。

アプライアンスでオブジェクトを使用して RADIUS 認証を有効にするには、そのオブジェクトが有効になっているシステム ポリシーをアプライアンスに適用する必要があります。詳細については、外部認証の有効化(63-13 ページ)およびシステム ポリシーの適用(63-4 ページ)を参照してください。

RADIUS 認証オブジェクトの例

ライセンス:任意(Any)

ここでは、RADIUS サーバ認証オブジェクトの例を示し、FireSIGHT システム RADIUS 認証機能をどのように使用できるかを示します。詳細については、次の各項を参照してください。

- 例:RADIUS を使用したユーザの認証(61-41 ページ)
- 例:カスタム属性を使用したユーザの認証(61-43 ページ)

例:RADIUS を使用したユーザの認証

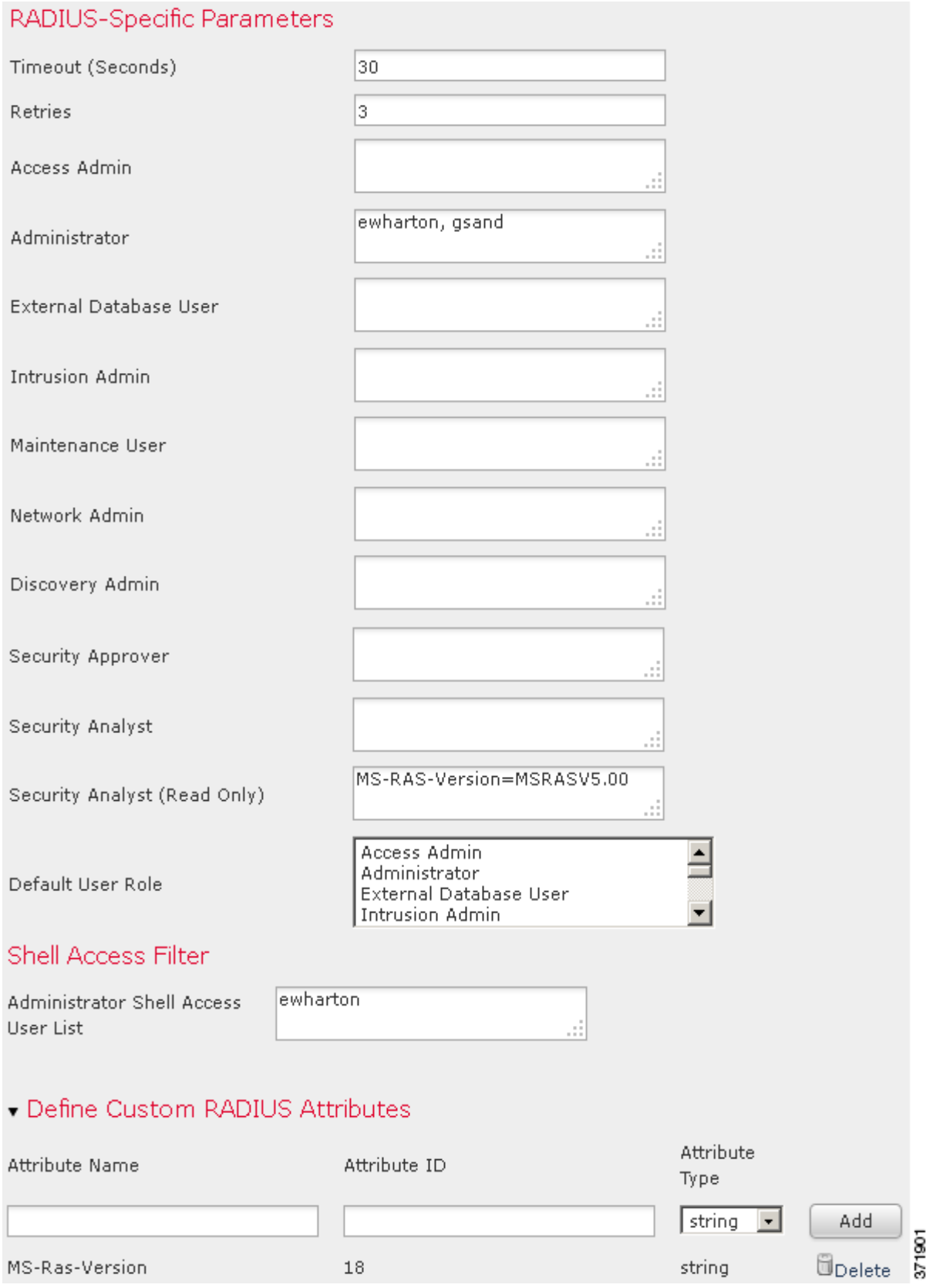
ライセンス:任意(Any)

次の図は、IP アドレスが 10.10.10.98 で FreeRADIUS が稼働しているサーバのサンプル RADIUS ログイン認証オブジェクトを示します。接続ではアクセスのためにポート 1812 が使用されること、および不使用期間が 30 秒を経過するとサーバ接続がタイムアウトになり、バックアップ認証サーバへの接続試行前に、サーバ接続が 3 回再試行されることに注意してください。

次の例は、RADIUS ユーザ ロール設定の重要な特徴を示します。

- ユーザ `ewharton` と `gsand` には、この認証オブジェクトが有効になっている FireSIGHT システム アプライアンスへの管理アクセスが付与されます。
- ユーザ `cbronte` には、この認証オブジェクトが有効になっている FireSIGHT システム アプライアンスへの Maintenance User アクセスが付与されます。
- ユーザ `cbronte` には、この認証オブジェクトが有効になっている FireSIGHT システム アプライアンスへの Security Analyst アクセスが付与されます。
- ユーザ `ewharton` は、シェル 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。

次の図に、この例のロール設定を示します。


RADIUS-Specific Parameters
Timeout (Seconds)
30
Retries
3
Access Admin
Administrator
ewharton, gsand
External Database User
Intrusion Admin
Maintenance User
Network Admin
Discovery Admin
Security Approver
Security Analyst
Security Analyst (Read Only)
MS-RAS-Version=MSRASV5.00
Default User Role
Access Admin
Administrator
External Database User
Intrusion Admin
Shell Access Filter
Administrator Shell Access User List
ewharton
Define Custom RADIUS Attributes
Attribute Name
Attribute ID
Attribute Type
string
Add
MS-Ras-Version
18
string
Delete
371901

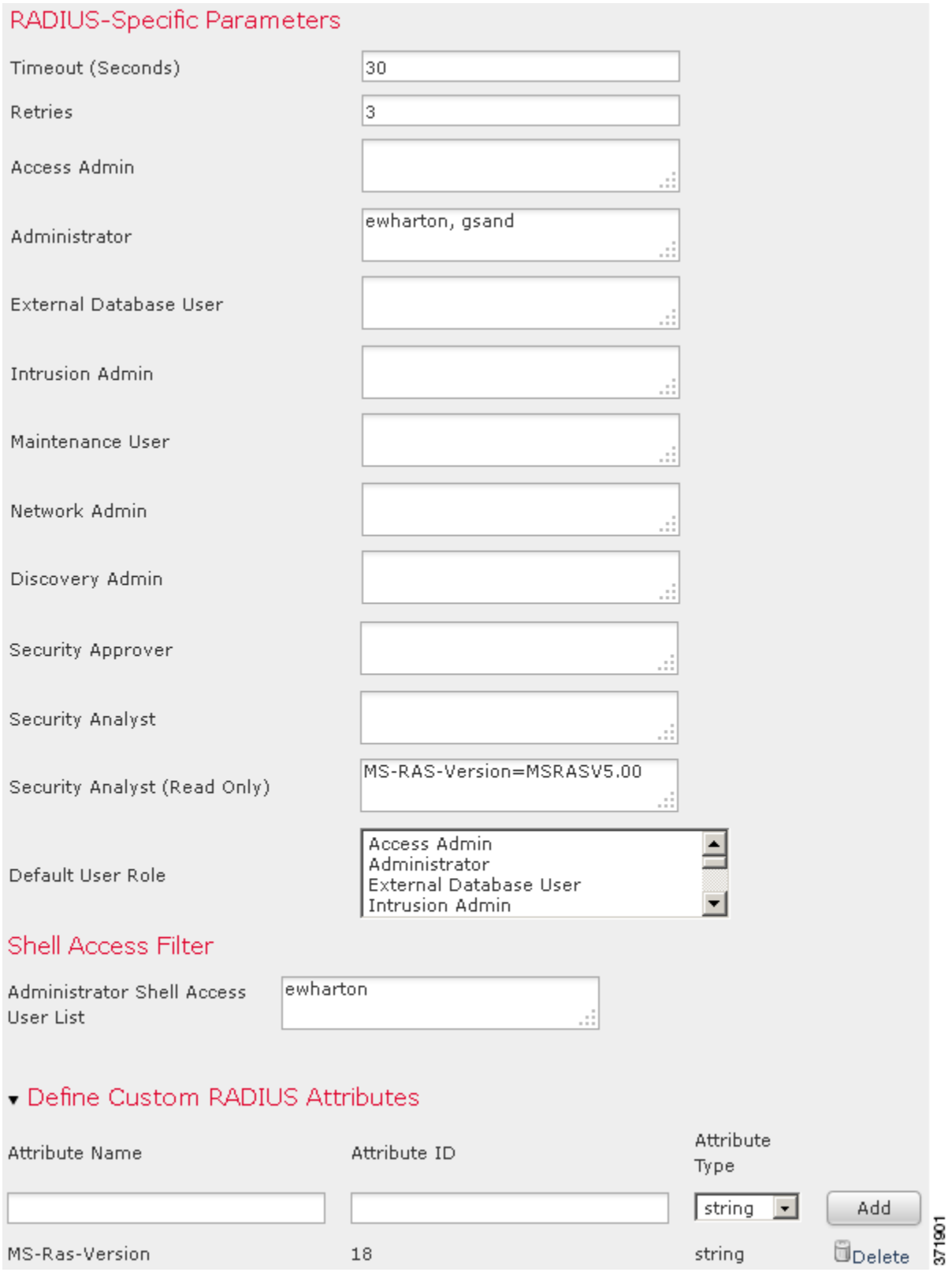
例:カスタム属性を使用したユーザの認証

ライセンス:任意(Any)

属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ FreeRADIUS サーバのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモート アクセス サーバが使用されているため、1 つ以上のユーザの `MS-RAS-Version` カスタム属性が返されます。`MS-RAS-Version` カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモート アクセス サーバ経由で RADIUS にログインするすべてのユーザに対し、Security Analysts (Read Only) ロールが付与される必要があります。このため、属性と値のペア `MS-RAS-Version=MSRASV5.00` を [Security Analyst (Read Only)] フィールドに入力します。


RADIUS-Specific Parameters
Timeout (Seconds)
30
Retries
3
Access Admin
Administrator
ewharton, gsand
External Database User
Intrusion Admin
Maintenance User
Network Admin
Discovery Admin
Security Approver
Security Analyst
Security Analyst (Read Only)
MS-RAS-Version=MSRASV5.00
Default User Role
Access Admin
Administrator
External Database User
Intrusion Admin
Shell Access Filter
Administrator Shell Access User List
ewharton
Define Custom RADIUS Attributes
Attribute Name
Attribute ID
Attribute Type
string
Add
MS-Ras-Version
18
string
Delete
371901

RADIUS 認証オブジェクトの編集

ライセンス: 任意（Any）

既存の認証オブジェクトを編集できます。オブジェクトがシステム ポリシーで使用されている場合、ポリシーが適用された時点での設定が、ポリシーを再適用するまで有効になります。

認証オブジェクトを編集する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[外部認証（External Authentication）] タブをクリックします。

[外部認証（External Authentication）] ページが表示されます。

手順 3　編集するオブジェクトの横にある編集アイコン（  ）をクリックします。

[外部認証オブジェクトの作成（Create External Authentication Object）] ページが表示されます。

手順 4　必要に応じてオブジェクト設定を変更します。

手順 5　[保存（Save）] をクリックします。

変更が保存され、[外部認証（External Authentication）] ページが再び表示されます。認証の変更がアプライアンスで行われる前に、オブジェクトが有効に設定されているシステム ポリシーをそのアプライアンスに適用する必要があることに注意してください。詳細については、外部認証の有効化（63-13 ページ）およびシステム ポリシーの適用（63-4 ページ）を参照してください。

認証オブジェクトの削除

ライセンス: 任意（Any）

削除できる認証オブジェクトは、システム ポリシーで現在有効ではない認証オブジェクトです。

認証オブジェクトを削除する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[外部認証（External Authentication）] タブをクリックします。

[外部認証（External Authentication）] ページが表示されます。

手順 3　削除するオブジェクトの横にある削除アイコン（  ）をクリックします。

オブジェクトが削除され、[外部認証（External Authentication）] ページが表示されます。

ユーザ アカウントの管理

ライセンス：任意（Any）

Administration アクセスが付与されている場合は、Web インターフェイスを使用して防御センターまたは管理対象デバイスでユーザ アカウントを表示および管理（アカウントの追加、変更、削除など）できます。また、カスタム ユーザ ロールを作成および変更し、ユーザ ロール エスカレーションを設定できます。Administrator アクセス権が付与されていないユーザ アカウントでは、管理機能へのアクセスが制限されています。表示されるナビゲーション メニューは、ユーザのタイプによって異なります。

ユーザ アカウントの管理の詳細については、次の項を参照してください。

- ユーザ アカウントの表示（61-46 ページ）では、[ユーザ管理（User Management）] ページへのアクセス方法を説明します。このページでは、ユーザ アカウントを追加、アクティブ化、非アクティブ化、編集、削除できます。
- 新しいユーザ アカウントの追加（61-47 ページ）では、新しいユーザ アカウントを追加するときに使用できるさまざまなオプションについて説明します。
- コマンド ライン アクセスの管理（61-49 ページ）では、仮想デバイスまたは シリーズ 3 のローカル デバイス ユーザにコマンド ライン インターフェイス アクセス権を割り当てる方法について説明します。
- 外部認証ユーザ アカウントの管理（61-50 ページ）では、外部認証ユーザの追加方法と、FireSIGHT システム内で管理できるユーザ設定の内容を説明します。
- ユーザ特権とオプションの変更（61-59 ページ）では、既存のユーザ アカウントにアクセスして変更する方法を説明します。
- 制限付きユーザ アクセス プロパティについて（61-59 ページ）では、制限付きデータ アクセスを使用して、ユーザ アカウントに対して使用可能なデータを制限する方法を説明します。
- ユーザ アカウントの削除（61-60 ページ）では、ユーザ アカウントを削除する方法について説明します。
- ユーザ アカウント特権について（61-61 ページ）には、各種ユーザ アカウントでアクセスできるメニューとオプションをまとめた表が収録されています。

ユーザ アカウントの表示

ライセンス：任意（Any）

[ユーザ管理（User Management）] ページでは、既存のアカウントを表示、編集、削除できます。[認証方式（Authentication Method）] 列でユーザの認証タイプを確認できます。[パスワード有効期間（Password Lifetime）] 列には、ユーザ パスワードの残りの有効日数が示されます。[アクション（Action）] 列のアイコンを使用して、ユーザの詳細を編集したり、ユーザをアクティブまたは非アクティブにしたりできます。外部認証ユーザの場合、サーバの認証オブジェクトが無効であると、[認証方式（Authentication Method）] 列に [外部（無効）（External (Disabled)）] が表示されます。

[ユーザ管理(User Management)] ページにアクセスする方法:

アクセス:管理

手順 1　[システム(System)] > [ローカル(Local)] > [ユーザ管理(User Management)] を選択します。

[ユーザ管理(User Management)] ページに、各ユーザと、ユーザ アカウントのアクティブ化、非アクティブ化、編集、または削除のオプションが表示されます。

[ユーザ管理(User Management)] ページで実行できるアクションについては、以降の項を参照してください。

- 新しいユーザ アカウントの追加(61-47 ページ)
- ユーザ ロールの設定(61-53 ページ)
- ユーザ特権とオプションの変更(61-59 ページ)
- 制限付きユーザ アクセス プロパティについて(61-59 ページ)
- ユーザ パスワードの変更(61-60 ページ)
- ユーザ アカウントの削除(61-60 ページ)

新しいユーザ アカウントの追加

ライセンス:任意(Any)

サポートされるデバイス:機能に応じて異なる

新しいユーザ アカウントをセットアップするときに、そのアカウントでアクセスできるシステムの部分を制御できます。ユーザ アカウントの作成時に、ユーザ アカウントのパスワードの有効期限と強度を設定できます。シリーズ 3 デバイスのローカル アカウントの場合、ユーザに付与するコマンド ライン アクセスのレベルも設定できます。

新しいユーザを追加するには、次の手順を実行します

アクセス:管理

手順 1　[システム(System)] > [ローカル(Local)] > [ユーザ管理(User Management)] を選択します。

[ユーザ管理(User Management)] ページが表示されます。

手順 2　[ユーザの作成(Create User)] をクリックします。

[ユーザの作成(Create User)] ページが表示されます。

手順 3　[ユーザ名(User Name)] フィールドに、新しいユーザの名前を入力します。

新しいユーザ名は、英数字とハイフン文字のみからなり、スペースを使用せず、32 文字以下の長さにする必要があります。ユーザ名では、大文字と小文字が区別されます。

手順 4　このユーザがログイン時に外部ディレクトリ サーバに対して認証されるようにするには、[外部認証方式を使用する(Use External Authentication Method)] を選択します。

このオプションを有効にすると、パスワード管理オプションが非表示になります。ユーザのアクセス ロールの設定を続行するには、ステップ 8 に移動してください。

外部ディレクトリ サーバに対してユーザを認証する場合は、防御センターを使用して、使用するサーバの認証オブジェクトを作成し、次に認証が有効な状態でシステム ポリシーを適用します。また、これらのユーザが FireSIGHT システム アプライアンスにログインするには、外部認証サー

バが使用可能である必要があります。詳細については、認証オブジェクトの管理（61-5 ページ）および外部認証の有効化（63-13 ページ）を参照してください。

手順 5　[パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに、パスワード（最大 32 文字の英数字）を入力します。

パスワード強度の検査を有効にする場合は、パスワードは 8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。

（注）　アプライアンスで STIG 準拠を有効にするには、シェル アクセス ユーザのパスワード設定の詳細について『*FireSIGHT システムSTIG Release Notes*』を参照してください。

手順 6　その他のユーザ アカウント ログイン オプションを設定します。

詳細については、ユーザ アカウント ログイン オプションの表を参照してください。

手順 7　シリーズ 3 デバイスの Web インターフェイスでローカル ユーザを作成する場合は、[コマンドライン インターフェイス アクセス（Command-Line Interface Access）] でユーザのコマンド ライン インターフェイス アクセス レベルを割り当てることができます。

- ユーザに対しコマンド ラインへのアクセスを無効にするには、[なし（None）] を選択します。
- ユーザがシェルにログインし、特定のコマンド サブセットにアクセスできるようにするには、[基本（Basic）] を選択します。
- ユーザがシェルにログインし、すべてのコマンド ライン オプション（アプライアンスでエキスパート モードが有効な場合はエキスパート モードも含む）を使用できるようにするには、[設定（Configuration）] を選択します。

  コマンド ライン アクセスの詳細については、コマンド ライン アクセスの管理（61-49 ページ）を参照してください。

手順 8　ユーザに付与するアクセス ロールを選択します。

（注）　すべての物理管理対象デバイスでは、シスコから提供される事前定義のユーザ ロールは、Administrator、Maintenance User、および Security Analyst に限定されています。

詳細については、ユーザ ロールの設定（61-53 ページ）を参照してください。

手順 9　[保存（Save）] をクリックします。

ユーザが作成され、[ユーザ管理（User Management）] ページが再度表示されます。

ヒント　[ユーザ管理（User Management）] ページの内部認証ユーザの名前の横にあるスライダをクリックして、非アクティブなユーザを再度アクティブにするか、またはアクティブ ユーザ アカウントを削除せずに無効にします。

コマンド ライン アクセスの管理

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3、仮想

シリーズ 3 または仮想デバイスでは、コマンド ライン インターフェイス アクセスをローカル デバイス ユーザに割り当てることができます。

仮想デバイスのユーザにコマンド ライン アクセスを割り当てることができますが、コマンドはコマンド ライン インターフェイスから使用することに注意してください。詳細については、コマンドライン リファレンス（D-1 ページ）を参照してください。

ユーザが実行できるコマンドは、ユーザに割り当てられているアクセスのレベルによって決まります。[コマンドライン インターフェイス アクセス（Command-Line Interface Access）] を [なし（None）] に設定すると、ユーザはコマンド ラインでアプライアンスにログインできなくなります。ユーザがクレデンシャルを指定すると、ユーザが開始したセッションはすべて閉じます。ユーザ作成時に、アクセス レベルはデフォルトで [なし（None）] に設定されます。[コマンドライン インターフェイス アクセス（Command-Line Interface Access）] を [基本（Basic）] に設定すると、ユーザは特定のコマンド セットだけを実行できます。

表 61-3　基本のコマンド ライン コマンド

configure password	interfaces
終了	lcd
exit	link-state
ヘルプ	log-ips-connection
history	managers
ログアウト	memory
?	model
??	mpls-depth
access-control-config	NAT
alarms	network
arp-tables	network-modules
audit-log	ntp
bypass	perfstats
クラスタリング	portstats
cpu	power-supply-status
データベース	process-tree
device-settings	processes
ディスク	routing-table
disk-manager	serial-number
dns	stacking
expert	summary
fan-status	時刻
fastpath-rules	traffic-statistics
gui	version
ホスト名	virtual-routers
hyperthreading	virtual-switches
inline-sets	

[コマンドライン インターフェイス アクセス(Command-Line Interface Access)] を [設定(Configuration)] に設定すると、ユーザはすべてのコマンド ライン オプションにアクセスできます。このアクセス レベルをユーザに割り当てるときには注意してください。

注意　外部認証ユーザに付与されるシェル アクセスは、デフォルトで [設定(Configuration)] レベルのコマンド ライン アクセスになります。これにより、すべてのコマンド ライン ユーティリティの権限が付与されます。外部認証ユーザのシェル アクセスの詳細については、シェル アクセスについて(61-9 ページ)およびシェル アクセスの設定(61-26 ページ)を参照してください。

外部認証ユーザ アカウントの管理

ライセンス: 任意(Any)

外部認証が有効になっているアプライアンスに外部認証ユーザがログインすると、認証オブジェクトでグループ メンバーシップを指定して設定したデフォルト アクセス ロールが、アプライアンスによりユーザに付与されます。アクセス グループ設定を設定していない場合、アプライアンスは、システム ポリシーで設定されているデフォルト ユーザ ロールを付与します。ただし、ユーザがアプライアンスにログインする前に、ユーザをローカルで追加すると、[ユーザ管理(User Management)] ページで設定するユーザ特権によってデフォルト設定がオーバーライドされます。

デフォルト ユーザ ロールの選択の詳細については、外部認証の有効化(63-13 ページ)およびユーザ特権について(61-4 ページ)を参照してください。外部認証ユーザのデフォルト ユーザ ロールとして、事前定義のユーザ ロールとカスタム ユーザ ロールの両方を設定できることに注意してください。詳細については、ユーザ ロールの設定(61-53 ページ)を参照してください。

次のすべての条件が満たされている場合には、内部認証ユーザが外部認証に変換されます。

- LDAP(CAC を使用する場合および使用しない場合)または RADIUS 認証を有効にしている。
- LDAP サーバまたは RADIUS サーバでユーザに対して同一ユーザ名が存在する。
- ユーザが、LDAP または RADIUS サーバに保存されているそのユーザのパスワードを使用してログインする。

防御センターではシステム ポリシーの外部認証だけを有効にできることに注意してください。管理対象デバイスで外部認証を使用するには、防御センターを使用して管理対象デバイスにポリシーを適用する必要があります。

外部認証ユーザがアプライアンスに初めてログインすると、アプライアンスは、ローカル ユーザ レコードを作成して、これらのクレデンシャルを一連のアクセス許可に関連付けます。ユーザ ログインの詳細については、アプライアンスへのログイン(2-1 ページ)を参照してください。初回ログイン後、そのローカル ユーザ レコードのアクセス許可がグループ メンバーシップまたはリスト メンバーシップを介して付与されていない場合は、そのアクセス許可を以下のように変更できます。

- 外部認証ユーザ アカウントのデフォルト ロールとして特定のアクセス ロールが設定されている場合、ユーザは外部アカウント クレデンシャルを使用してアプライアンスにログインでき、この際にシステム管理者による追加の設定は必要ありません。
- アカウントが外部で認証され、デフォルトではアクセス権限が付与されない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザ(またはシステム管理者)は、ユーザ機能へ適切なアクセス権を付与する権限を変更することができます。

ヒント　システムでは、シェル アクセス ユーザのローカル ユーザ アカウントは作成されません。シェル アクセスは、シェル アクセス フィルタ、または LDAP サーバに設定されている PAM ログイン属性、あるいは RADIUS サーバ上のシェル アクセスリストによってすべて制御されます。

ユーザ アクセスの変更の詳細については、ユーザ特権とオプションの変更（61-59 ページ）を参照してください。FireSIGHT システム インターフェイスでは、外部認証ユーザのパスワード管理および外部認証ユーザの非アクティブ化は実行できないことに注意してください。外部認証ユーザの場合、LDAP グループ メンバーシップ、RADIUS リスト メンバーシップ、または属性値によってアクセス ロールが割り当てられているユーザの FireSIGHT システム ユーザ管理ページでは、最小アクセス権を削除することができません。外部認証ユーザの [ユーザの編集（Edit User）] ページでは、外部認証サーバの設定により付与された権限は、[外部変更（Externally Modified）] ステータスでマークされます。

ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理（User Management）] ページの [認証方式（Authentication Method）] 列に、[外部 - ローカル変更（External - Locally Modified）] というステータスが表示されます。

シェル ユーザは、小文字で構成されたユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

注意　シリーズ 3 防御センターでは、すべてのシェル ユーザに `sudoers` 特権が付与されます。シェル アクセスが付与されるユーザのリストを適切に制限してください。シリーズ 3 と仮想デバイスでは、外部認証ユーザに付与されるシェル アクセスのデフォルトは、**Configuration** レベルのコマンド ライン アクセスになります。このアクセスでも `sudoers` 特権が付与されます。シェル アクセスのセットアップの詳細については、シェル アクセスについて（61-9 ページ）およびシェル アクセスの設定（61-26 ページ）を参照してください。

ユーザ ログイン設定の管理

ライセンス：任意（Any）

各ユーザ アカウントのパスワードの変更方法と変更する条件、およびユーザ アカウントが無効になる条件を制御できます。Web インターフェイス ログイン セッションのタイムアウトを設定している場合は、このタイムアウトからユーザを除外できます。次の表に、パスワードおよびアカウント アクセスの調整に使用できるオプションの一部について説明します。

シリーズ 3 管理対象デバイス上のローカル認証ユーザの場合、Web インターフェイスのユーザ パスワードを変更すると、コマンド ライン インターフェイスのパスワードも変更されることに注意してください。

[パスワード強度の確認（Check Password Strength）] オプションを有効にすると、最小パスワード長が自動的に 8 文字に設定されます。また、[最小パスワード長（Minimum Password Length）] に 8 文字を超える値を設定すると、いずれか大きい方の値が適用されます。

（注）　[外部認証方式を使用する（Use External Authentication Method）] を有効にした後は、ログイン オプションが表示されなくなります。ログイン設定の管理に外部認証サーバを使用します。

表 61-4　ユーザ アカウント ログイン オプション

オプション	説明
[外部認証方式を使用する（Use External Authentication Method）]	このユーザのクレデンシャルを外部で認証する場合に、このチェックボックスをオンにします。 **（注）** ユーザに対してこのオプションを選択した場合に外部認証サーバが使用できないと、そのユーザは Web インターフェイスにログインできますが、どの機能にもアクセスできません。
[最大ログイン失敗回数（Maximum Number of Failed Logins）]	各ユーザが、ログイン試行の失敗後に、アカウントがロックされるまでに試行できるログインの最大回数を示す整数を、スペースなしで入力します。デフォルト設定は 5 回です。ログイン失敗回数を無制限にするには、0 を使用します。
[最小パスワード長（Minimum Password Length）]	ユーザのパスワードの必須最小長（文字数）を示す整数を、スペースなしで入力します。デフォルト設定は 8 です。値 0 は、最小長が必須ではないことを示します。
[パスワードの有効期限の残り日数（Days Until Password Expiration）]	ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は 0 で、パスワードは期限切れにならないことを示します。
[パスワード期限切れまでの警告日数（Days Before Password Expiration Warning）]	パスワードが実際に期限切れになる前に、ユーザがパスワードを変更する必要があるという警告が表示される日数を入力します。デフォルト設定は 0 日間です。 **注意** 警告日数は、パスワードの残りの有効期間の日数**未満**である必要があります。
[ログオン時にパスワードを強制リセットする（Force Password Reset on Login）]	初回ログイン時に、ユーザが強制的に各自のパスワードを変更するようにするには、このオプションを選択します。
[パスワード強度の確認（Check Password Strength）]	強力なパスワードを必須にするには、このオプションを選択します。強力なパスワードは 8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。
[ブラウザ セッション タイムアウトを免除（Exempt from Browser Session Timeout）]	操作が行われなかったことが原因でユーザのログイン セッションが終了しないようにするには、このオプションを選択します。Administrator ロールが割り当てられているユーザを除外することはできません。セッション タイムアウトの詳細については、ユーザ インターフェイスの設定（63-31 ページ）を参照してください。

ユーザ ロールの設定

ライセンス：任意（Any）

各 FireSIGHT システム ユーザには、1 つ以上のユーザ アクセス ロールが関連付けられています。たとえばアナリストは、ネットワークのセキュリティを分析するためイベント データへのアクセスが必要ですが、FireSIGHT システム自体の管理機能へのアクセスが必要となることはありません。たとえばユーザ ロールを使用して、アナリストには Security Analyst アクセスを付与し、FireSIGHT システムを管理する 1 人以上のユーザに対して Administrator ロールを予約しておくことができます。FireSIGHT システムには、さまざまな管理者とアナリスト向けに設計された 10 の事前定義ユーザ ロールがあります。また、特別なアクセス権限を持つカスタム ユーザ ロールを作成することもできます。

ユーザがアクセスできる Web インターフェイスのメニューとその他のオプションは、ロールによって異なります。事前定義のユーザ ロールには、一連の事前定義のアクセス権限が含まれており、カスタム ユーザ ロールには、作成者が指定する詳細なアクセス権限が含まれています。

[ユーザ ロール（User Roles）] ページでユーザ ロールを設定します。

[ユーザ ロール（User Roles）] ページにアクセスする方法：

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[ユーザロール（User Roles）] タブをクリックします。

[ユーザロール（User Roles）] ページが表示され、すべての事前定義ユーザ ロールとカスタム ユーザ ロール、およびロールのアクティブ化、非アクティブ化、編集、コピー、削除、エクスポートのためのオプションが表示されます。

この 2 種類のユーザ ロールの設定の詳細については、以降の項を参照してください。

- 事前定義ユーザ ロールの管理（61-53 ページ）
- カスタム ユーザ ロールの管理（61-56 ページ）
- 事前定義ユーザ ロールのカスタム コピーの作成（61-57 ページ）
- カスタム ユーザ ロールの削除（61-58 ページ）

事前定義ユーザ ロールの管理

ライセンス：任意（Any）

FireSIGHT システムには、組織のニーズに対応するためのさまざまなアクセス権限セットを提供する 10 の事前定義ユーザ ロールがあります。[ユーザ ロール（User Roles）] ページでは、事前定義ユーザ ロールに「シスコ Provided」というラベルが付いています。管理対象デバイスは、10 の事前定義ユーザ ロールのうち 3 つのユーザ ロール（Administrator、Maintenance User、および Security Analyst）にだけアクセスできることに注意してください。

事前定義ユーザ ロールは編集できませんが、そのアクセス権限セットをカスタム ユーザ ロールのベースとして使用できます。カスタム ユーザ ロールの作成と編集については、カスタム ユーザ ロールの管理（61-56 ページ）を参照してください。また、事前定義ユーザ ロールを編集できないため、事前定義ユーザ ロールが別のユーザ ロールにエスカレーションするように設定することができません。詳細については、ユーザ ロール エスカレーションの管理（61-71 ページ）を参照してください。

次の表に、使用可能な事前定義ロールの簡単な説明を示します。各ロールで使用可能なメニューおよびオプションのリストについては、ユーザ アカウント特権について（61-61 ページ）を参照してください。

表 61-5　事前定義ユーザ ロール

[ユーザ権限（User Roles）]	権限（Privileges）
Access Admin	アクセス制御、SSL インスペクション、およびファイル ポリシー機能にアクセスするためのアクセス権を提供します。ただし、Access Admin はアクセス コントロール ポリシーを適用することはできません。Access Admin は、[ポリシー（Policies）] メニューでアクセス制御、SSL インスペクション、およびファイル関連オプションにアクセスできます。
Administrator	分析およびレポート機能、ルールおよびポリシーの設定、システム管理、およびすべての保守機能へのアクセスを提供します。Administrator はすべてのメニュー オプションにアクセスできるため、セッションでセキュリティが侵害されると、高いセキュリティ リスクが生じます。このため、ログイン セッション タイムアウトから Administrator を除外することはできません。 セキュリティ上の理由から、Administrator ロールの使用を制限する必要があることに注意してください。 このロールは、管理対象デバイスでも使用可能です。
Discovery Admin	ネットワーク検出、相関、およびユーザ アクティビティ機能へのアクセスを提供します。Discovery Admin は、[ポリシー（Policies）] メニューの関連オプションにアクセスできます。
External Database User	JDBC SSL 接続をサポートするアプリケーションを使用した FireSIGHT システム データベースへの読み取り専用アクセスを提供します。サードパーティ アプリケーションを FireSIGHT システム アプライアンスに対して認証するには、データベースへのアクセスの有効化（64-8 ページ） の説明に従い、システム設定でデータベース アクセスを有効にする必要があることに注意してください。Web インターフェイスでは、External Database User は [ヘルプ（Help）] メニューのオンライン ヘルプ関連オプションだけにアクセスできます。このロールの機能には Web インターフェイスが含まれていないため、容易なサポートとパスワード変更の目的でのみアクセスが提供されます。
Intrusion Admin	すべての侵入ポリシー、侵入ルール、およびネットワーク解析ポリシーの機能にアクセスするためのアクセス権を提供します。Intrusion Admin は、[ポリシー（Policies）] メニューの侵入関連オプションにアクセスできます。Intrusion Admin は、侵入またはネットワーク解析ポリシーをアクセス制御ポリシーの一部として適用できないことに注意してください。
Maintenance User	モニタ機能と保守機能へのアクセスを提供します。Maintenance User は、[ヘルス（Health）] メニューと [システム（System）] メニューの保守関連オプションにアクセスできます。 このロールは、管理対象デバイスでも使用可能です。
ネットワーク管理者	アクセス制御、SSL インスペクション、およびデバイス設定機能にアクセスするためのアクセス権を提供します。Network Admin は、アクセス制御、SSL インスペクション、および [ポリシー（Policies）] メニューと [デバイス（Devices）] メニューのデバイス関連オプションにアクセスできます。
Security Analyst	セキュリティ イベント分析機能（イベント ビュー、レポート、ホスト、ホスト属性、サービス、脆弱性、クライアント アプリケーション、ヘルス イベントへの読み取り専用アクセスなど）へのアクセスを提供します。Security Analyst は、[概要（Overview）]、[分析（Analysis）]、[ヘルス（Health）]、および [システム（System）] メニューの分析関連オプションにアクセスできます。 このロールは、管理対象デバイスでも使用可能です。

表 61-5　事前定義ユーザ ロール（続き）

[ユーザ権限（User Roles）]	権限（Privileges）
Security Analyst (Read Only)	セキュリティ イベント分析機能（イベント ビュー、レポート、ホスト、ホスト属性、サービス、脆弱性、クライアント アプリケーション、ヘルス イベントなど）への読み取り専用アクセスを提供します。Security Analyst は、[概要（Overview）]、[分析（Analysis）]、[ヘルス（Health）]、および [システム（System）] メニューの分析関連オプションにアクセスできます。
Security Approver	アクセス制御、侵入、ファイル、SSL、およびネットワーク検出ポリシーへの制限付きアクセスを提供します。Security Approver は、これらのポリシーを表示し、ネットワーク検出、侵入、およびアクセス制御ポリシーを適用できますが、ポリシーを変更することはできません。[ポリシー（Policies）] メニューのポリシー関連オプションにアクセスできます。

ユーザに Event Analyst ロールを割り当てるときに、そのユーザの削除権限を、そのユーザにより作成されるレポート プロファイル、検索、ブックマーク、カスタム テーブル、およびカスタム ワークフローの削除だけに制限できます。詳細については、新しいユーザ アカウントの追加（61-47 ページ）を参照してください。

その他のロールが割り当てられていない外部認証ユーザには、LDAP または RADIUS 認証オブジェクトとシステム ポリシーでの設定に基づいて最小アクセス権が付与されることに注意してください。追加の権限をこれらのユーザに割り当てることができますが、最小アクセス権を削除または変更するには、次の操作を行う必要があります。

- 認証オブジェクト内のリスト間でユーザを移動するか、または外部認証サーバのユーザの属性値またはグループ メンバーシップを変更します。
- システム ポリシーを再度適用します。
- [ユーザ管理（User Management）] ページでそのユーザ アカウントからアクセスを削除します。

事前定義ユーザ ロールは削除できませんが、非アクティブにすることができます。ロールを非アクティブにすると、そのロールが割り当てられているすべてのユーザから、そのロールと関連するアクセス許可が削除されます。

注意　非アクティブにされたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして [ユーザ設定（User Preferences）] メニューにアクセスできますが、FireSIGHT システムにはアクセスできません。

ユーザ ロールをアクティブ化または非アクティブ化する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[ユーザロール（User Roles）] タブをクリックします。

[ユーザ ロール（User Roles）] ページが表示されます。

手順 3　アクティブまたは非アクティブにするユーザ ロールの横にあるスライダをクリックします。

（注）　Lights-Out Management を含むロールが割り当てられているユーザがログインしているときに、このロールを非アクティブにしてから再度アクティブにする場合、またはユーザのログイン セッション中にバックアップからユーザまたはユーザ ロールを復元する場合、そのユーザは Web インターフェイスに再度ログインして、IPMItool コマンドへのアクセスを再度取得する必要があります。詳細については、Lights-Out 管理の使用（64-28 ページ）を参照してください。

カスタム ユーザ ロールの管理

ライセンス:任意（Any）

事前定義ユーザ ロールの他に、特別なアクセス権限を含むカスタム ユーザ ロールを作成できます。カスタム ユーザ ロールには、メニューベースのアクセス許可およびシステム アクセス許可の任意のセットを割り当てることができます。また、最初から独自に作成したり、事前定義されたユーザ ロールを基に作成したりできます。事前定義ユーザ ロールと同様に、カスタム ロールは外部認証ユーザのデフォルト ロールとして使用できます。事前定義ロールとは異なり、カスタム ロールは変更、削除できます。

選択可能なアクセス許可は階層構造になっており、FireSIGHT システム メニュー レイアウトに基づいています。アクセス許可にサブページが含まれているか、または単純なページ アクセスよりも詳細なアクセス許可が含まれている場合、このアクセス許可は拡張可能です。その場合、上位アクセス許可によって、ページ ビュー アクセス、およびそのページの関連機能への詳細な下位アクセス権が付与されます。たとえば [相関イベント（Correlation Events）] アクセス許可は [相関イベント（Correlation Events）] ページへのアクセスを付与し、[相関イベントの変更（Modify Correlation Events）] チェックボックスは、ユーザがそのページで使用可能な情報を編集、削除できるようにします。「Manage」という単語が含まれているアクセス許可は、他のユーザが作成する情報を編集および削除できる権限を付与します。

ヒント　メニュー構造に含まれていないページまたは機能の権限は、上位または関連ページにより付与されます。たとえば、Modify Intrusion Policy 特権があれば、ネットワーク解析ポリシーの変更もできます。

カスタム ユーザ ロールに制限付き検索を適用できます。これにより、イベント ビューアでユーザに対して表示されるデータが制限されます。制限付き検索を設定するには、最初に、プライベートの保存済み検索を作成し、該当するメニュー ベースのアクセス許可の下で、[制限付き検索（Restricted Search）] ドロップダウン メニューからその検索を選択します。詳細については、検索の実行（60-2 ページ）を参照してください。

防御センターでカスタム ユーザ ロールを設定するときには、すべてのメニュー ベースのアクセス許可を付与できます。管理対象デバイスでカスタム ユーザ ロールを設定するときには、デバイス機能に関連する一部のアクセス許可だけを使用できます。設定できるメニュー ベースのアクセス許可と、事前定義ユーザ ロールとの関係については、次の項を参照してください。

- [分析（Analysis）] メニュー（61-63 ページ）
- [ポリシー（Policies）] メニュー（61-66 ページ）
- [デバイス（Devices）] メニュー（61-68 ページ）
- [オブジェクト マネージャ（Object Manager）]（61-69 ページ）
- [ヘルス（Health）] メニュー（61-69 ページ）
- [システム（System）] メニュー（61-69 ページ）
- [ヘルプ（Help）] メニュー（61-71 ページ）

[システム アクセス許可（System Permissions）] で選択できるオプションでは、外部データベースに対してクエリを実行したり、ターゲット ユーザ ロールのアクセス許可にエスカレーションしたりすることができるユーザ ロールを作成できます。詳細については、データベースへのアクセスの有効化（64-8 ページ）およびユーザ ロール エスカレーションの管理（61-71 ページ）を参照してください。

オプションで、新しいカスタム ユーザ ロールを作成する代わりに、別のアプライアンスからカスタム ユーザ ロールをエクスポートし、ご使用のアプライアンスにインポートできます。インポートしたロールは、適用する前に、ニーズに合わせて編集できます。詳細については、設定のエクスポート（A-1 ページ）および設定のインポート（A-5 ページ）を参照してください。

カスタム ユーザ ロールを作成する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[ユーザロール（User Roles）] タブをクリックします。

[ユーザ ロール（User Roles）] ページが表示されます。

手順 3　[ユーザ ロールの作成（Create User Role）] をクリックします。

[ユーザ ロール エディタ（User Role Editor）] ページが表示されます。

手順 4　[名前（Name）] フィールドに、新しいユーザ ロールの名前を入力します。

英数字またはハイフン文字を使用できます。スペースは使用しないでください。ロール名は 75 文字以下でなければなりません。ユーザ ロール名では、大文字と小文字が区別されます。

手順 5　オプションで、[説明（Description）] フィールドに新しいロールの説明を入力します。

ロールの説明は 255 文字以下でなければなりません。

手順 6　新しいロールのアクセス許可を選択します。

選択されていないアクセス許可を選択すると、その権限の下位のアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が選択されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。選択されたアクセス許可の下位のアクセス許可がすべて選択されていない場合、イタリック テキストで表示されます。

カスタム ロールのベースとして使用する事前定義ユーザ ロールをコピーすることを選択すると、その事前定義ロールに関連付けられているアクセス許可が事前に選択されることに注意してください。事前定義ユーザ ロールのコピーの詳細については、事前定義ユーザ ロールのカスタム コピーの作成（61-57 ページ）を参照してください。

現在のエスカレーション ターゲット ロールは、ロール エスカレーション チェックボックスの横に表示されます。このチェックボックスをオンにすると、割り当てられているユーザのパスワードまたは指定されている別のユーザ ロールのパスワードのいずれかを使用してエスカレーションを認証することを選択できます。詳細については、ユーザ ロール エスカレーションの管理（61-71 ページ）を参照してください。

手順 7　[保存（Save）] をクリックします。

カスタム ユーザ ロールが作成され、[ユーザ ロール（User Roles）] ページが再度表示されます。

事前定義ユーザ ロールのカスタム コピーの作成

ライセンス: 任意（Any）

新しいカスタム ロールのベースとして使用する既存のロールをコピーできます。これにより、[ユーザ ロール エディタ（User Role Editor）] で既存のロールのアクセス許可が事前に選択されるので、あるロールをモデルとして別のロールを作成できます。

事前定義ユーザ ロールのカスタム コピーを作成する方法:

アクセス:管理

手順 1　[システム(System)] > [ローカル(Local)] > [ユーザ管理(User Management)] を選択します。

[ユーザ管理(User Management)] ページが表示されます。

手順 2　[ユーザロール(User Roles)] タブをクリックします。

[ユーザ ロール(User Roles)] ページが表示されます。

手順 3　コピーするユーザ ロールの横にあるコピー アイコン( )をクリックします。

[ユーザ ロール エディタ(User Role Editor)] ページが表示され、コピーされたロールのアクセス許可が事前に選択されます。

カスタム ユーザ ロールと事前定義ユーザ ロールの両方をこの方法でコピーできることに注意してください。

カスタム ユーザ ロールの削除

ライセンス:任意(Any)

事前定義ユーザ ロールとは異なり、不要になったカスタム ロールは削除できます。カスタム ロールを完全に削除せずに無効にするには、カスタム ロールを非アクティブ化します。詳細については、事前定義ユーザ ロールの管理(61-53 ページ)を参照してください。各自のユーザ ロール、またはシステム ポリシーでデフォルト ユーザ ロールとして設定されているロールは削除できないことに注意してください。詳細については、外部認証の有効化(63-13 ページ)を参照してください。

カスタム ユーザ ロールを削除する方法:

アクセス:管理

手順 1　[システム(System)] > [ローカル(Local)] > [ユーザ管理(User Management)] を選択します。

[ユーザ管理(User Management)] ページが表示されます。

手順 2　[ユーザロール(User Roles)] タブをクリックします。

[ユーザ ロール(User Roles)] ページが表示されます。

手順 3　削除するカスタム ロールの横にある削除アイコン( )をクリックします。

カスタム ロールが削除されます。

削除されたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして [ユーザ設定(User Preferences)] メニューにアクセスできますが、FireSIGHT システムにはアクセスできません。

ユーザ特権とオプションの変更

ライセンス: 任意（Any）

システムにユーザ アカウントを追加したら、アクセス権限、アカウント オプション、パスワードをいつでも変更できます。パスワード管理オプションは、外部ディレクトリ サーバに対して認証されるユーザには適用されないことに注意してください。これらの設定は外部サーバで管理します。ただし、外部認証されるアカウントを含め、すべてのアカウントのアクセス権を設定する必要があります。

外部認証ユーザの場合、LDAP グループ メンバーシップ、RADIUS リスト メンバーシップ、または属性値によってアクセス ロールが割り当てられているユーザの FireSIGHT システム ユーザ管理ページでは、最小アクセス権を削除することができません。ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理（User Management）] ページの [認証方式（Authentication Method）] 列に、[外部 - ローカル変更（External - Locally Modified）] というステータスが表示されます。

ユーザの認証を外部認証から内部認証に変更した場合は、ユーザの新しいパスワードを指定する必要があることに注意してください。

ユーザ アカウント権限を変更する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　変更するユーザの横にある編集アイコン（ ）をクリックします。

[ユーザの編集（Edit User）] ページが表示されます。

手順 3　必要に応じて 1 つ以上のアカウントを変更します。

- 外部サーバでユーザを認証する方法の説明については、外部認証ユーザ アカウントの管理（61-50 ページ）を参照してください。
- 内部認証ユーザのパスワード設定の変更については、ユーザ ログイン設定の管理（61-51 ページ）を参照してください。
- FireSIGHT システム機能のアクセスを付与するロールの設定の詳細については、ユーザ ロールの設定（61-53 ページ）を参照してください。

制限付きユーザ アクセス プロパティについて

ライセンス: 任意（Any）

イベント ビューアであるユーザ ロールが表示できるデータを制限するには、そのロールに制限付き検索を適用します。ユーザに割り当てられたロールを作成または編集するときに、この情報を指定できます。制限付きアクセスを使用してカスタム ロールを作成するには、[メニュー ベースのアクセス許可（Menu Based Permissions）] リストから制限するテーブルを選択し、次に [制限付き検索（Restrictive Search）] ドロップダウン リストからプライベート保存検索を選択します。詳細については、カスタム ユーザ ロールの管理（61-56 ページ）を参照してください。

ユーザ パスワードの変更

ライセンス: 任意（Any）

内部認証ユーザの [ユーザ管理（User Management）] ページで、ユーザ パスワードを変更できます。LDAP または RADIUS サーバで外部認証ユーザのパスワードを管理する必要があることに注意してください。

（注） アプライアンスで STIG 準拠または Lights-Out Management（LOM）を有効にすると、異なるパスワード制限が適用されます。STIG 準拠を有効にしたシステムでのシェル アクセス ユーザのパスワード設定の詳細については、『*FireSIGHT システムSTIG Release Notes*』を参照してください。LOM ユーザ用システム パスワードのパスワード設定の詳細については、Lights-Out 管理ユーザ アクセスの有効化（64-25 ページ）を参照してください。

ユーザ パスワードを変更する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　ユーザ名の横にある編集アイコン（）をクリックします。

[ユーザの編集（Edit User）] ページが表示されます。

手順 3　[パスワード（Password）] フィールドに、新しいパスワード（最大 32 文字の英数字）を入力します。

手順 4　[パスワードの確認（Confirm Password）] フィールドに、新しいパスワードをもう一度入力します。

ユーザ アカウントのパスワード強度検査が有効な場合は、パスワードは 8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。

手順 5　ユーザ設定に、必要なその他のすべての変更を行います。

- パスワード オプションの詳細については、ユーザ ログイン設定の管理（61-51 ページ）を参照してください。
- ユーザ ロールの詳細については、ユーザ ロールの設定（61-53 ページ）を参照してください。

手順 6　[保存（Save）] をクリックします。

パスワードが変更され、その他のすべての変更が保存されます。

ユーザ アカウントの削除

ライセンス: 任意（Any）

admin アカウント以外のユーザ アカウントはシステムからいつでも削除できます。admin アカウントは削除できません。

ユーザ アカウントを削除するには、次の手順を実行します。

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　アカウントを削除するユーザの横の削除アイコン（ ）をクリックします。アカウントが削除されます。

ユーザ アカウント特権について

ライセンス: 任意（Any）

ここでは、FireSIGHT システムの設定可能なユーザ アクセス許可と、これらのアクセス許可にアクセスできるユーザ ロールのリストを示します。ここに記載されているアクセス許可は、カスタム ユーザ ロールの作成時に表示される [メニュー ベースのアクセス許可（Menu Based Permissions）] リストの順序に従っています。管理対象デバイスでは使用できないアクセス許可があります。防御センターでのみ使用可能なアクセス許可には、そのことが記されています。詳細については、カスタム ユーザ ロールの管理（61-56 ページ）を参照してください。

DC500 防御センターと シリーズ 2 デバイスでは制限付き機能セットがサポートされているため、これらのアプライアンスに適用されないアクセス許可があることに注意してください。シリーズ 2 アプライアンス機能の要約については、各デバイス モデルでサポートされるアクセス制御機能の表を参照してください。

このマニュアルで、これ以降のすべての表で使用されるアクセスの表記の詳細については、アクセスの表記規則（1-24 ページ）を参照してください。ここでは、Web ベース インターフェイスの各メイン メニューに関連付けられているユーザ ロール特権を示します。

[概要（Overview）] メニュー

ライセンス: 任意（Any）

次の表は、[概要（Overview）] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。Security Approver、Discovery Admin、Intrusion Admin、Access Admin、Network Admin、および External Database User の各ロールには、[概要（Overview）] メニューのアクセス許可がありません。

表 61-6　[概要(Overview)] メニュー

権限	管理	Maint User	Security Analyst	Security Analyst (RO)
ダッシュボード	Yes	Yes	Yes	Yes
ダッシュボードの管理	Yes	No	No	No
[アプライアンス情報ウィジェット(Appliance Information Widget)]	Yes	Yes	Yes	Yes
[アプライアンス ステータス ウィジェット(Appliance Status Widget)] *(防御センターのみ)*	Yes	Yes	Yes	Yes
[コリレーション イベント ウィジェット(Correlation Events Widget)]	Yes	No	Yes	Yes
[現行インターフェイス ステータス ウィジェット(Current Interface Status Widget)]	Yes	Yes	Yes	Yes
[現行セッション ウィジェット(Current Sessions Widget)]	Yes	No	No	No
[カスタム分析ウィジェット(Custom Analysis Widget)] *(防御センターのみ)*	Yes	No	Yes	Yes
[ディスク使用率ウィジェット(Disk Usage Widget)]	Yes	Yes	Yes	Yes
[インターフェイス トラフィック ウィジェット(Interface Traffic Widget)]	Yes	Yes	Yes	Yes
[侵入イベント ウィジェット(Intrusion Events Widget)] *(防御センターのみ)*	Yes	No	Yes	Yes
[ネットワーク コリレーション ウィジェット(Network Correlation Widget)] *(防御センターのみ)*	Yes	No	Yes	Yes
[製品ライセンス ウィジェット(Product Licensing Widget)] *(防御センターのみ)*	Yes	Yes	No	No
[製品アップデート ウィジェット(Product Updates Widget)]	Yes	Yes	No	No
[RSS フィード ウィジェット(RSS Feed Widget)]	Yes	Yes	Yes	Yes
[システム負荷ウィジェット(System Load Widget)]	Yes	Yes	Yes	Yes
[システム時刻ウィジェット(System Time Widget)]	Yes	Yes	Yes	Yes
[ホワイト リスト イベント ウィジェット(White List Events Widget)] *(防御センターのみ)*	Yes	No	Yes	Yes
[レポート(Reporting)] *(防御センターのみ)*	Yes	No	Yes	Yes
[レポート テンプレートの管理(Manage Report Templates)] *(防御センターのみ)*	Yes	No	Yes	Yes
要約	Yes	No	Yes	Yes
[侵入イベント統計(Intrusion Event Statistics)] *(防御センターのみ)*	Yes	No	Yes	Yes
侵入イベント パフォーマンス(Intrusion Event Performance)	Yes	No	No	No
[侵入イベント グラフ(Intrusion Event Graphs)] *(防御センターのみ)*	Yes	No	Yes	Yes
[ディスカバリ統計(Discovery Statistics)] *(防御センターのみ)*	Yes	No	Yes	Yes

表 61-6　[概要(Overview)] メニュー(続き)

権限	管理	Maint User	Security Analyst	Security Analyst (RO)
[ディスカバリ パフォーマンス(Discovery Performance)] *(防御センターのみ)*	Yes	No	No	No
[接続サマリ(Connection Summary)] *(防御センターのみ)*	Yes	No	Yes	Yes

[分析(Analysis)] メニュー

ライセンス:任意(Any)

次の表は、[分析(Analysis)] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。異なる見出しの下に複数回出現する権限は、最初に出現する表にのみ示されています。ただし、サブメニューの見出しを示す場合を除きます。Security Approver、Intrusion Admin、Access Admin、Network Admin、および External Database User の各ロールには、[分析(Analysis)] メニューのアクセス許可がありません。[分析(Analysis)] メニューは防御センターでのみ使用可能です。

表 61-7　[分析(Analysis)] メニュー

メニュー	管理	Discovery Admin	Maint User	Security Analyst	Security Analyst (RO)
[アプリケーション統計(Application Statistics)]	Yes	No	No	Yes	Yes
[地理位置情報統計(Geolocation Statistics)]	Yes	No	No	Yes	Yes
[ユーザ統計(User Statistics)]	Yes	No	No	Yes	Yes
[URL カテゴリの統計(URL Category Statistics)]	Yes	No	No	Yes	Yes
[URL レピュテーション統計(URL Reputation Statistics)]	Yes	No	No	Yes	Yes
[SSL 統計(SSL Statistics)]	Yes	No	No	Yes	Yes
[アプリケーション別侵入イベントの統計(Intrusion Event Statistics by Application)]	Yes	No	No	Yes	Yes
[ユーザ別侵入イベントの統計(Intrusion Event Statistics by User)]	Yes	No	No	Yes	Yes
[セキュリティ インテリジェンス カテゴリ統計(Security Intelligence Category Statistics)]	Yes	No	No	Yes	Yes
[傾向別ファイル ストレージ統計(File Storage Statistics by Disposition)]	Yes	No	No	Yes	Yes
[タイプ別ファイル ストレージ統計(File Storage Statistics by Type)]	Yes	No	No	Yes	Yes
[ダイナミック ファイル分析統計(Dynamic File Analysis Statistics)]	Yes	No	No	Yes	Yes
コンテキスト エクスプローラ(Context Explorer)	Yes	No	No	Yes	Yes

表 61-7　[分析(Analysis)] メニュー(続き)

メニュー	管理	Discovery Admin	Maint User	Security Analyst	Security Analyst (RO)
接続イベント	Yes	No	No	Yes	Yes
[接続イベントの変更(Modify Connection Events)]	Yes	No	No	Yes	No
[接続サマリ イベント(Connection Summary Events)]	Yes	No	No	Yes	Yes
[接続サマリ イベントの変更(Modify Connection Summary Events)]	Yes	No	No	Yes	No
セキュリティ インテリジェンス イベント	Yes	No	No	Yes	Yes
[セキュリティ インテリジェンス イベントの変更(Modify Security Intelligence Events)]	Yes	No	No	Yes	No
[侵入(Intrusion)]	Yes	No	No	Yes	Yes
侵入イベント	Yes	No	No	Yes	Yes
[侵入イベントの変更(Modify Intrusion Events)]	Yes	No	No	Yes	No
[ローカル ルールを表示(View Local Rules)]	Yes	No	No	Yes	Yes
[確認済みイベント(Reviewed Events)]	Yes	No	No	Yes	Yes
[クリップボード(Clipboard)]	Yes	No	No	Yes	Yes
[インシデント(Incidents)]	Yes	No	No	Yes	Yes
ファイル	Yes	No	No	Yes	Yes
マルウェア イベント	Yes	No	No	Yes	Yes
[Malware イベントの編集(Modify Malware Events)]	Yes	No	No	Yes	No
ファイル イベント	Yes	No	No	Yes	Yes
[ファイル イベントの変更(Modify File Events)]	Yes	No	No	Yes	No
キャプチャ ファイル(Captured Files)	Yes	No	No	Yes	Yes
[キャプチャされたファイルの変更(Modify Captured Files)]	Yes	No	No	Yes	No
File Trajectory	Yes	No	No	Yes	Yes
[ファイルのダウンロード(File Download)]	Yes	No	No	Yes	Yes
[ダイナミック ファイル分析(Dynamic File Analysis)]	Yes	No	No	Yes	No
Hosts	Yes	No	No	Yes	Yes
[ネットワーク マップ(Network Map)]	Yes	No	No	Yes	Yes
Hosts	Yes	No	No	Yes	Yes
[ホストの変更(Modify Hosts)]	Yes	No	No	Yes	No
Indications of Compromise	Yes	No	No	Yes	Yes

表 61-7　[分析(Analysis)] メニュー(続き)

メニュー	管理	Discovery Admin	Maint User	Security Analyst	Security Analyst (RO)
[侵害の兆候の変更(Modify Indications of Compromise)]	Yes	No	No	Yes	No
サーバ	Yes	No	No	Yes	Yes
[サーバの変更(Modify Servers)]	Yes	No	No	Yes	No
脆弱性(Vulnerabilities)	Yes	No	No	Yes	Yes
[脆弱性の変更(Modify Vulnerabilities)]	Yes	No	No	Yes	No
ホスト属性(Host Attributes)	Yes	No	No	Yes	Yes
[ホスト属性の変更(Modify Host Attributes)]	Yes	No	No	Yes	No
アプリケーション	Yes	No	No	Yes	Yes
アプリケーション詳細(Application Details)	Yes	No	No	Yes	Yes
[アプリケーション詳細の変更(Modify Application Details)]	Yes	No	No	Yes	No
[ホスト属性の管理(Host Attribute Management)]	Yes	No	No	No	No
検出イベント(Discovery Events)	Yes	No	No	Yes	Yes
[ディスカバリ イベントの変更(Modify Discovery Events)]	Yes	No	No	Yes	No
Users	Yes	Yes	No	Yes	Yes
ユーザ アクティビティ(User Activity)	Yes	Yes	No	Yes	Yes
[ユーザ アクティビティ イベントの変更(Modify User Activity Events)]	Yes	Yes	No	Yes	No
Users	Yes	Yes	No	Yes	Yes
[ユーザの変更(Modify Users)]	Yes	Yes	No	Yes	No
脆弱性(Vulnerabilities)	Yes	No	No	Yes	Yes
[サードパーティの脆弱性(Third-party Vulnerabilities)]	Yes	No	No	Yes	Yes
[サードパーティの脆弱性の変更(Modify Third-party Vulnerabilities)]	Yes	No	No	Yes	No
相関(Correlation)	Yes	Yes	No	Yes	Yes
相関イベント(Correlation Events)	Yes	Yes	No	Yes	Yes
[コリレーション イベントの変更(Modify Correlation Events)]	Yes	Yes	No	Yes	No
ホワイトリスト イベント(White List Events)	Yes	Yes	No	Yes	Yes
[ホワイト リスト イベントの変更(Modify White List Events)]	Yes	Yes	No	Yes	No
ホワイトリスト違反(White List Violations)	Yes	Yes	No	Yes	Yes
[修復ステータス(Remediation Status)]	Yes	Yes	No	No	No

表 61-7　[分析(Analysis)] メニュー(続き)

メニュー	管理	Discovery Admin	Maint User	Security Analyst	Security Analyst (RO)
[修復ステータスの変更(Modify Remediation Status)]	Yes	Yes	No	No	No
カスタム(Custom)	Yes	No	No	Yes	Yes
カスタム ワークフロー(Custom Workflows)	Yes	No	No	Yes	Yes
[カスタム ワークフローの管理(Manage Custom Workflows)]	Yes	No	No	Yes	Yes
カスタム テーブル(Custom Tables)	Yes	No	No	Yes	Yes
[カスタム テーブルの管理(Manage Custom Tables)]	Yes	No	No	Yes	Yes
検索(Search)	Yes	No	Yes	Yes	Yes
[検索の管理(Manage Search)]	Yes	No	No	No	No
[ブックマーク(Bookmarks)]	Yes	No	No	Yes	Yes
[ブックマークの管理(Manage Bookmarks)]	Yes	No	No	Yes	Yes

[ポリシー(Policies)] メニュー

ライセンス:任意(Any)

次の表は、[ポリシー(Policies)] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。External Database User、Maintenance User、Security Analyst、および Security Analyst (Read Only)の各ロールには、[ポリシー(Policies)] メニューでのアクセス許可がありません。[ポリシー(Policies)] メニューは防御センターでのみ使用可能です。

Intrusion Policy および Modify Intrusion Policy 特権があれば、ネットワーク解析ポリシーの作成および修正もできることに注意してください。

表 61-8　[ポリシー(Policies)] メニュー

メニュー	Access Admin	管理者	Discovery Admin	Intrusion Admin	ネットワーク管理者	Security Approver
アクセス制御	Yes	Yes	No	No	Yes	Yes
アクセス コントロール リスト	Yes	Yes	No	No	Yes	Yes
アクセス制御ポリシーの変更 (Modify Access Control Policy)	Yes	Yes	No	No	Yes	No
管理者ルールの変更(Modify Administrator Rules)	Yes	Yes	No	No	Yes	No
ルート ルールの変更(Modify Root Rules)	Yes	Yes	No	No	Yes	No
[侵入ポリシーの適用(Apply Intrusion Policies)]	No	Yes	No	No	No	Yes

表 61-8　[ポリシー(Policies)] メニュー(続き)

メニュー	Access Admin	管理者	Discovery Admin	Intrusion Admin	ネットワーク管理者	Security Approver
アクセス コントロール ポリシーの適用(Apply Access Control Policies)	No	Yes	No	No	No	Yes
[侵入(Intrusion)]	Yes	Yes	No	Yes	No	Yes
侵入ポリシー(Intrusion Policy)	No	Yes	No	Yes	No	Yes
[ルール エディタ(Rule Editor)]	No	Yes	No	Yes	No	No
E メール	No	Yes	No	Yes	No	No
[侵入ポリシーの変更(Modify Intrusion Policy)]	No	Yes	No	Yes	No	No
ファイル ポリシー	Yes	Yes	No	No	No	No
[ファイル ポリシーの変更(Modify File Policy)]	Yes	Yes	No	No	No	No
ネットワーク ディスカバリ(Network Discovery)	No	Yes	Yes	No	No	Yes
[カスタムフィンガープリント(Custom Fingerprinting)]	No	Yes	Yes	No	No	No
[カスタム トポロジ(Custom Topology)]	No	Yes	Yes	No	No	No
[ネットワーク検出の変更(Modify Network Discovery)]	No	Yes	Yes	No	No	No
[ネットワーク検出の適用(Apply Network Discovery)]	No	Yes	No	No	No	Yes
SSL	Yes	Yes	No	No	Yes	Yes
SSL ポリシーの変更(Modify SSL Policy)	Yes	Yes	No	No	Yes	No
管理者ルールの変更(Modify Administrator Rules)	Yes	Yes	No	No	Yes	No
ルート ルールの変更(Modify Root Rules)	Yes	Yes	No	No	Yes	No
SSL ポリシーの適用(Apply SSL Policy)	No	Yes	No	No	No	Yes
アプリケーション ディテクタ(Application Detectors)	No	Yes	Yes	No	No	No
[ユーザ サードパーティ マッピング(User 3rd Party Mappings)]	No	Yes	Yes	No	No	No
[カスタム サービス フィンガープリント(Custom Product Mappings)]	No	Yes	Yes	No	No	No
Users	No	Yes	No	No	No	No
相関(Correlation)	No	Yes	No	No	No	No
[ポリシー管理(Policy Management)]	No	Yes	No	No	No	No
[ルール管理(Rule Management)]	No	Yes	No	No	No	No

表 61-8　[ポリシー(Policies)] メニュー(続き)

メニュー	Access Admin	管理者	Discovery Admin	Intrusion Admin	ネットワーク管理者	Security Approver
[ホワイト リスト(White List)]	No	Yes	No	No	No	No
[トラフィック プロファイル(Traffic Profiles)]	No	Yes	No	No	No	No
アクション(Actions)	No	Yes	Yes	No	No	No
アラート(Alerts)	No	Yes	Yes	No	No	No
[インパクト フラグ アラート(Impact Flag Alerts)]	No	Yes	Yes	No	No	No
[ディスカバリ イベント アラート(Discovery Event Alerts)]	No	Yes	Yes	No	No	No
スキャナ(Scanners)	No	Yes	Yes	No	No	No
[スキャン結果(Scan Results)]	No	Yes	Yes	No	No	No
[スキャン結果の変更(Modify Scan Results)]	No	Yes	Yes	No	No	No
グループ(Groups)	No	Yes	No	No	No	No
モジュール(Modules)	No	Yes	No	No	No	No
[インスタンス(Instances)]	No	Yes	No	No	No	No

[デバイス(Devices)] メニュー

ライセンス:任意(Any)

[デバイス(Devices)] メニューの表には、[デバイス(Devices)] メニューの各オプションとそのサブ権限にアクセスするために必要なユーザ ロール特権を順に示します。X はユーザ ロールにアクセス権があることを示します。Access Admin、Discovery Admin、External Database User、Maintenance User、Security Approver、Security Analyst、および Security Analyst(Read Only)の各ロールには、[デバイス(Devices)] メニューでのアクセス許可がありません。[デバイス(Devices)] メニューは防御センターでのみ使用可能です。

表 61-9　[デバイス(Devices)] メニュー

メニュー	管理	ネットワーク管理者
デバイス管理	Yes	Yes
[デバイスの変更(Modify Devices)]	Yes	Yes
[デバイスの変更を適用(Apply Device Changes)]	Yes	Yes
NAT	Yes	Yes
[NAT リスト(NAT List)]	Yes	Yes
[NAT ポリシーの変更(Modify NAT Policy)]	Yes	Yes
[NAT ルールの適用(Apply NAT Rules)]	Yes	No
VPN	Yes	Yes
[VPN の変更(Modify VPN)]	Yes	Yes
[VPN の変更を適用(Apply VPN Changes)]	Yes	Yes

[オブジェクト マネージャ（Object Manager）]

ライセンス：任意（Any）

[オブジェクト マネージャ（Object Manager）] アクセス許可は、Access Admin、Administrator、Network Admin の各ユーザ ロールに対して使用可能です。[オブジェクト マネージャ（Object Manager）] アクセス許可は防御センターでのみ使用可能です。

FireAMP

ライセンス：任意（Any）

FireAMP アクセス許可は、Administrator ユーザ ロールのみに対して使用可能です。このアクセス許可は、防御センターでのみ使用可能です。

[ヘルス（Health）] メニュー

ライセンス：任意（Any）

次の表は、[ヘルス（Health）] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示します。Access Admin、Discovery Admin、Intrusion Admin、External Database User、Network Admin、および Security Approver の各ロールには、[ヘルス（Health）] メニューでのアクセス許可がありません。[ヘルス（Health）] メニューは防御センターでのみ使用可能です。

表 61-10　[ヘルス（Health）] メニュー

メニュー	管理	Maint User	Security Analyst	Security Analyst（RO）
ヘルス ポリシー（Health Policy）	Yes	Yes	No	No
[正常性ポリシーの変更（Modify Health Policy）]	Yes	Yes	No	No
[正常性ポリシーの適用（Apply Health Policy）]	Yes	Yes	No	No
ヘルス イベント（Health Events）	Yes	Yes	Yes	Yes
[正常性イベントの変更（Modify Health Events）]	Yes	Yes	No	No

[システム（System）] メニュー

ライセンス：任意（Any）

次の表は、[システム（System）] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示します。Access Admin、Discovery Admin、Intrusion Admin、External Database User、および Security Approver の各ロールには、[システム（System）] メニューでのアクセス許可はありません。

表 61-11　[システム(System)] メニュー

メニュー	管理	Maint User	ネットワーク管理者	Security Approver	Security Analyst
[ローカル(Local)]	Yes	No	No	No	No
設定(Configuration)	Yes	No	No	No	No
登録	Yes	No	No	No	No
[ハイ アベイラビリティ(High Availability)] *(DC1000、DC1500、DC2000、DC3000、DC3500、DC4000 のみ)*	Yes	No	No	No	No
eStreamer	Yes	No	No	No	No
[ホスト入力クライアント(Host Input Client)] *(防御センターのみ)*	Yes	No	No	No	No
ユーザ管理	Yes	No	No	No	No
Users	Yes	No	No	No	No
ユーザの役割	Yes	No	No	No	No
[ログイン認証(Login Authentication)] *(防御センターのみ)*	Yes	No	No	No	No
[システム ポリシー(System Policy)] *(防御センターのみ)*	Yes	No	No	No	No
[システム ポリシーの適用(Apply System Policy)] *(防御センターのみ)*	Yes	No	No	No	No
[システム ポリシーの変更(Modify System Policy)] *(防御センターのみ)*	Yes	No	No	No	No
変更点	Yes	No	No	No	No
[ルール アップデート(Rule Updates)] *(防御センターのみ)*	Yes	No	No	No	No
[ルール アップデート インポート ログ(Rule Update Import Log)] *(防御センターのみ)*	Yes	No	No	No	No
ライセンス	Yes	No	No	No	No
モニタリング(Monitoring)	Yes	Yes	Yes	Yes	Yes
監査(Audit)	Yes	No	No	No	No
[監査ログの変更(Modify Audit Log)]	Yes	No	No	No	No
Syslog	Yes	Yes	No	No	No
タスク ステータス(Task Status)	Yes	Yes	Yes	Yes	Yes
[他のユーザのタスクの表示(View Other Users' Tasks)]	Yes	No	No	No	No
統計情報(Statistics)	Yes	Yes	No	No	No
ツール	Yes	Yes	No	No	Yes
[バックアップ管理(Backup Management)]	Yes	Yes	No	No	No
[バックアップの復元(Restore Backup)]	Yes	Yes	No	No	No
スケジューリング	Yes	Yes	No	No	No

表 61-11　[システム(System)] メニュー(続き)

メニュー	管理	Maint User	ネットワーク管理者	Security Approver	Security Analyst
[他のユーザのスケジュール済みタスクの削除(Delete Other Users' Scheduled Tasks)]	Yes	No	No	No	No
インポート/エクスポート(Import/Export)	Yes	No	No	No	No
[ディスカバリ データの消去(Discovery Data Purge)] *(防御センターのみ)*	Yes	No	No	No	Yes
[Whois]	Yes	Yes	No	No	Yes

[ヘルプ(Help)] メニュー

ライセンス:任意(Any)

[ヘルプ(Help)] メニューとその権限には、すべてのユーザ ロールがアクセスできます。[ヘルプ(Help)] メニュー オプションを制限することはできません。

ユーザ ロール エスカレーションの管理

ライセンス:任意(Any)

カスタム ユーザ ロールにアクセス許可を付与し、パスワードを設定することで、ベース ロールの特権に加え、他のターゲット ユーザ ロールの特権を一時的に取得できます。これにより、あるユーザが不在であるときにそのユーザを別のユーザに容易に置き換えることや、拡張ユーザ特権の使用状況を緊密に追跡することができます。

たとえば、ユーザのベース ロールに含まれている特権が非常に限られている場合、そのユーザは管理アクションを実行するために Administrator ロールにエスカレーションします。ユーザが各自のパスワードを使用するか、または指定された別のユーザのパスワードを使用することができるように、この機能を設定できます。2 番目のオプションでは、該当するすべてのユーザのための 1 つのエスカレーション パスワードを容易に管理できます。詳細については、エスカレーションに使用するカスタム ユーザ ロールの設定(61-72 ページ)を参照してください。

エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけであることに注意してください。カスタム ユーザ ロールまたは事前定義ユーザ ロールを使用できます。各エスカレーションはログイン セッション期間中保持され、監査ログに記録されます。

この機能の設定および使用方法の詳細については、以降の項を参照してください。

- エスカレーション ターゲット ロールの設定(61-72 ページ)
- エスカレーションに使用するカスタム ユーザ ロールの設定(61-72 ページ)
- ユーザ ロールのエスカレーション(61-74 ページ)

エスカレーション ターゲット ロールの設定

ライセンス:任意（Any）

各自のユーザ ロール（事前定義またはカスタム）をシステム全体でのエスカレーション ターゲット ロールとして機能するように割り当てることができます。これは、他のロールからのエスカレーション先となるロールです（エスカレーションが可能な場合）。

エスカレーション ターゲット ロールを設定する方法:

アクセス:管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[ユーザ ロール（User Roles）] をクリックします。

[ユーザ ロール（User Roles）] ページが表示されます。

手順 3　[アクセス許可エスカレーションの設定（Configure Permission Escalation）] をクリックします。

[アクセス許可エスカレーションの設定（Configure Permission Escalation）] ダイアログボックスが表示されます。

手順 4　ドロップダウン リストからユーザ ロールを選択します。

手順 5　[OK] をクリックして変更を保存します。

変更が保存され、[ユーザ ロール（User Roles）] ページが表示されます。

（注）　エスカレーション ターゲット ロールの変更は即時に反映されます。エスカレーションされたセッションのユーザには、新しいエスカレーション ターゲットのアクセス許可が付与されます。

エスカレーションに使用するカスタム ユーザ ロールの設定

ライセンス:任意（Any）

ユーザ ロール エスカレーション機能を使用するには、最初にエスカレーション権限を持つカスタム ユーザ ロールを設定し、そのエスカレーション パスワードを選択して、そのロールをユーザに割り当てる必要があります。詳細については、新しいユーザ アカウントの追加（61-47 ページ）およびユーザ ロールの設定（61-53 ページ）を参照してください。

カスタム ロールのエスカレーション パスワードを設定するときには、部門のニーズを考慮してください。多数のエスカレーション ユーザを容易に管理するには、別のユーザを選択し、そのユーザのパスワードをエスカレーション パスワードとして使用することができます。そのユーザのパスワードを変更するか、またはそのユーザを非アクティブにすると、そのパスワードを必要とするすべてのエスカレーション ユーザが影響を受けます。このことにより、特に一元管理できる外部認証ユーザを選択した場合に、ユーザ ロール エスカレーションをより効率的に管理できます。

エスカレーションに使用するカスタム ユーザ ロールを設定する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　[ユーザ ロール（User Roles）] をクリックします。

[ユーザ ロール（User Roles）] ページが表示されます。

手順 3　[ユーザ ロールの作成（Create User Role）] をクリックして新しいカスタム ユーザ ロールを作成するか、既存のカスタム ユーザ ロールの横の編集アイコン（  ）をクリックします。

[ユーザ ロール エディタ（User Role Editor）] ページが表示されます。

手順 4　カスタム ユーザ ロールの名前、説明、およびメニュー ベースのアクセス許可を選択します。

詳細については、カスタム ユーザ ロールの管理（61-56 ページ）の手順を参照してください。

手順 5　[システム アクセス許可（System Permissions）] で、[このロールをエスカレーション先として設定する:（Set this role to escalate to:）] チェックボックスをオンにします。

エスカレーション パスワード オプションが表示されます。

手順 6　このロールがエスカレーションするときに使用するパスワードを選択します。以下の 2 つの対処法があります。

- このロールが割り当てられているユーザがエスカレーション時に各自のパスワードを使用できるようにするには、[割り当てられているユーザのパスワードを認証に使用する（Authenticate with the assigned user's password）] を選択します。
- このロールが割り当てられているユーザが、別のユーザのパスワードを使用するようにするには、[指定されているユーザのパスワードを認証に使用する（Authenticate with the specified user's password）] を選択し、そのユーザ名を入力します。

（注）　別のユーザのパスワードで認証するときには、任意のユーザ名（非アクティブなユーザまたは存在しないユーザを含む）を入力できます。エスカレーションにパスワードが使用されるユーザを非アクティブにすると、そのパスワードを必要とするロールが割り当てられているユーザのエスカレーションが不可能になります。この機能を使用して、必要に応じてエスカレーション機能をただちに削除できます。

手順 7　[保存（Save）] をクリックします。

変更が保存され、[ユーザ ロール（User Roles）] ページが再度表示されます。これで、このロールが割り当てられているユーザはターゲット ユーザ ロールにエスカレーションできます。ユーザへのユーザ ロールの割り当ての詳細については、新しいユーザ アカウントの追加（61-47 ページ）を参照してください。

ユーザ ロールのエスカレーション

ライセンス:任意（Any）

エスカレーション対象のアクセス許可が含まれているカスタム ユーザ ロールが割り当てられているユーザは、いつでもターゲット ロールのアクセス許可にエスカレーションできます。エスカレーションはユーザ設定に影響しないことに注意してください。割り当てられているユーザ ロールがユーザ ロール エスカレーション向けに設定されていない場合、[ユーザ（User）] メニューの [アクセス許可のエスカレーション（Escalate Permissions）] オプションは表示されません。

ユーザ アクセス許可をエスカレーションする方法:

アクセス:任意（Any）

手順 1　[ローカル（Local）] > [ユーザ（User）] > [アクセス許可のエスカレーション（Escalate Permissions）] を選択します。

[ユーザ アクセス許可のエスカレーション（Escalate User Permissions）] ダイアログボックスが表示されます。

手順 2　認証パスワードを入力します。

手順 3　[エスカレーション（Escalate）] をクリックします。

これで、現行ロールに加え、エスカレーション ターゲット ロールのすべてのアクセス許可が付与されました。

エスカレーションはログイン セッションの残り期間にわたって保持されることに注意してください。ベース ロールの特権だけに戻すには、ログアウトしてから新しいセッションを開始する必要があります。

シスコ Security Manager からのシングル サインオンの設定

ライセンス:任意（Any）

サポートされるデバイス:ASA FirePOWER

シングル サインオン（SSO）により、シスコ Security Manager（CSM）バージョン 4.7 以上と防御センターを統合できます。これにより、ログインのために追加認証なしで CSM から防御センターにアクセスできます。ASA FirePOWER デバイスの ASA モジュールの管理では、デバイスの FirePOWER モジュールに適用されるポリシーの変更が必要となる場合もあります。CSM で防御センターを管理することを選択し、Web ブラウザで起動します。管理元の防御センターが高可用性ペアのメンバーの場合、SSO を使用すると、プライマリ ピアに移動します。

ユーザ ロールに基づくアクセスがある場合、CSM でクロス起動したデバイスの [デバイス管理（Device Management）] ページの [デバイス（Device）] タブに移動します。それ以外の場合は、[サマリ ダッシュボード（Summary Dashboard）] ページ（[概要（Overview）] > [ダッシュボード（Dashboards）]）に移動します。ただしダッシュボードにアクセスできないユーザ アカウントの場合は、[ようこそ（Welcome）] ページが使用されます。

防御センターに SSO を行うには、その前に、CSM から防御センターへの一方向暗号化認証パスをセットアップする必要があります。NAT 環境では、防御センターと CSM は NAT 境界の同じ側に存在している必要があります。通信を有効にするには、CSM と防御センターが相互を認識できるように、次の基準を指定する必要があります。

- CSM から、接続を識別する SSO 共有暗号キーを生成する必要があります。防御センターでこのキーを入力する必要があります。
- 防御センターで、CSM サーバのホスト名または IP アドレスとサーバ ポートを指定します。高可用性を使用する場合は、プライマリ ピアで SSO を設定します。
- 暗号化認証パラメータを検証するため、SSO アクセスを持たせるすべてのユーザに対し、CSM と防御センターで同じユーザ名（大文字小文字を区別）をセットアップする必要があります。

防御センターで STIG 準拠が有効な場合、システムにより SSO が無効化されます。詳細については、STIG コンプライアンスの有効化（63-27 ページ）を参照してください。

（注）　組織で認証に CAC が使用されている場合は、シングル サインオンでログインできません。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

シングル サインオンをセットアップする方法:

アクセス: 管理

手順 1　CSM から SSO 共有暗号キーを生成します。

詳細については、CSM のマニュアルを参照してください。

手順 2　防御センターで [システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 3　[CSM シングル サインオン（CSM Single Sign-on）] を選択します。

[CSM シングル サインオン（CSM Single Sign-on）] ページが表示されます。

手順 4　**CSM ホスト名**または **IP** アドレスとサーバの**ポート**を入力します。

手順 5　CSM から生成した**共有キー**を入力します。

手順 6　オプションで、防御センターのプロキシ サーバを使用して CSM と通信する場合は、[接続にプロキシを使用する（Use Proxy For Connection）] チェックボックスをオンにします。詳細については、管理インターフェイスのオプションについて（64-10 ページ）を参照してください。

手順 7　[送信（Submit）] をクリックします。

CSM 証明書が表示されます。

手順 8　[証明書の確認（Confirm Certificate）] をクリックして証明書を保存します。

これで CSM から防御センターにログインできるようになります。追加のログインを実行する必要はありません。