ユーザ プリファレンスの指定

ホーム ページ、アカウント パスワード、タイム ゾーン、ダッシュボード、イベント ビューの各プリファレンスなど、単一のユーザ アカウントに関連付けられたプリファレンスを設定できます。

ユーザ ロールに応じて、パスワード、イベント ビューのプリファレンス、タイム ゾーンの設定、ホーム ページのプリファレンスなど、ユーザ アカウントに固有のプリファレンスを指定できます。詳細については、次の項を参照してください。

- 「パスワードの変更」（P.58-1）では、ユーザ アカウントのパスワードを変更する方法を説明します。
- 「ホーム ページの指定」（P.58-3）では、既存のページの 1 つをデフォルトのホーム ページとして使用する方法を説明します。この値を設定した後は、このページがアプライアンスにログインする際に最初に表示されるページになります。
- 「イベント ビュー設定の設定」（P.58-3）では、イベント プリファレンスによって、イベントの表示内容がどのように変化するかを説明します。
- 「デフォルトのタイム ゾーンの設定」（P.58-8）では、ユーザ アカウントのタイム ゾーンを設定する方法、およびその設定によって、表示されるイベントのタイムスタンプがどのように変化するかを説明します。
- 「デフォルトのダッシュボードの指定」（P.58-8）では、どのダッシュボードをデフォルトのダッシュボードとして使用するかを選択する方法を説明します。

パスワードの変更

ライセンス：任意

サポート対象デバイス：シリーズ 2、シリーズ 3

サポート対象防御センター：任意

すべてのユーザ アカウントはパスワードで保護されています。パスワードはいつでも変更することができ、ユーザー アカウントの設定によっては定期的にパスワードを変更しなければならない場合もあります。「期限切れのパスワードの変更」（P.58-2）を参照してください。

パスワードの強度チェックが有効の場合、パスワードは大文字と小文字が混在する少なくとも 8 つの英数字で、少なくとも 1 つの数字が含まれている必要があることに注意してください。パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。

注　LDAP または RADIUS ユーザの場合、Web インターフェイスを介してパスワードを変更することはできません。

パスワードを変更するには、次の手順を実行します。

アクセス：Any

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[Change Password] ページが表示されます。

ステップ 2　[Current Password] フィールドに、現在のパスワードを入力して、[Change] をクリックします。

ステップ 3　[New Password] および [Confirm] フィールドに、新しいパスワードを入力します。

ステップ 4　[Change] をクリックします。

新しいパスワードがシステムによって受け入れられると、成功を示すメッセージが表示されます。

期限切れのパスワードの変更

ライセンス：任意

サポート対象デバイス：シリーズ 2、シリーズ 3

サポート対象防御センター：任意

ユーザ アカウントの設定によっては、パスワードが期限切れになることがあります。パスワードの有効期間は、アカウントが作成されたときに設定され、変更できないことに注意してください。パスワードが期限切れになった場合、[Password Expiration Warning] ページが表示されます。

パスワードの期限切れ警告に応答するには、次のようにします。

アクセス：Any

ステップ 1　次の 2 つの選択肢があります。

- すぐにパスワードを変更するには、[Change Password] をクリックします。

  残りの警告日数がゼロの場合は、パスワードを変更する**必要があります**。また、パスワードの強度チェックが有効の場合、パスワードは大文字と小文字が混在する少なくとも 8 つの英数字で、少なくとも 1 つの数字が含まれている必要があります。パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。
- 後でパスワードを変更するには、[Skip] をクリックします。

ホーム ページの指定

ライセンス：任意

Web インターフェイス内のページをアプライアンスのホーム ページに指定できます。デフォルトのホーム ページはサマリー ダッシュボード（[Overview] > [Dashboards]）ですが、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例外で、[Welcome] ページが使用されます。

ホーム ページを指定するには、次のようにします。

アクセス：External Database User を除くすべてのユーザ

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[Change Password] ページが表示されます。

ステップ 2　[Home Page] をクリックします。

[Home Page] ページが表示されます。

ステップ 3　ホーム ページとして使用するページをドロップダウン リストから選択します。

ドロップダウン リスト内のオプションは、ユーザ アカウントのアクセス権限に基づいて表示されます。詳細については、「アカウント特権について」（P.48-60）を参照してください。

ステップ 4　[Save] をクリックします。

ホーム ページのプリファレンスが保存されます。

イベント ビュー設定の設定

ライセンス：任意

[Event View Settings] ページを使用して、FireSIGHT システムのイベント ビューの特性を設定します。イベント ビュー設定は、特定のユーザ ロールでのみ使用可能であることに注意してください。External Database User ロールを持つユーザは、イベント ビュー設定のユーザ インターフェイスの一部を表示できますが、それらの設定を変更しても意味のある結果は生じません。詳しくは、以下にリンクされている個々の項を参照してください。

イベントのプリファレンスを設定するには、次のようにします。

アクセス：機能に応じて異なる

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[User Preferences] ページが表示されます。

ステップ 2　[Event View Settings] をクリックします。

[Event View Settings] ページが表示されます。

ステップ 3　イベント ビューの基本特性を設定します。

詳細については、「イベントのプリファレンス」（P.58-4）を参照してください。

ステップ 4　ファイルのダウンロードのプリファレンスを設定します。

詳細については、「ファイルのプリファレンス」（P.58-4）を参照してください。

ステップ 5　デフォルトの時間枠を設定します（複数可）。

詳細については、「デフォルトの時間枠」（P.58-5）を参照してください。

ステップ 6　デフォルトのワークフローを設定します。

詳細については、「デフォルトのワークフロー」（P.58-7）を参照してください。

ステップ 7　[Save] をクリックします。

変更が反映されます。

イベントのプリファレンス

ライセンス：任意

[Event View Settings] ページの [Event Preferences] セクションを使用して、FireSIGHT システムのイベント ビューの基本特性を設定します。このセクションはすべてのユーザ ロールで使用可能ですが、イベントを表示できないユーザには、ほとんどまたはまったく意味がありません。

以下のフィールドが [Event Preferences] セクションに示されます。

- [Confirm “All” Actions] フィールドは、イベント ビューのすべてのイベントに影響を与える操作について、アプライアンスがユーザに確認を要求するかどうかを制御します。

  たとえば、この設定が有効である場合、イベント ビューで [Delete All] をクリックすると、アプライアンスがデータベースからの削除を実行する前に、現在の制約を満たすすべてのイベント（現在のページに表示されていないイベントを含む）を削除することをユーザが確認する必要があります。

- [Resolve IP Addresses] フィールドは、可能な場合には常に、アプライアンスがイベント ビューで IP アドレスの代わりにホスト名を表示するようにします。

  多数の IP アドレスが含まれている場合、このオプションを有効にすると、イベント ビューの表示に時間がかかる可能性があることに注意してください。この設定が有効になるためには、システム設定で DNS サーバを設定している必要があることにも注意してください。「ネットワーク設定の構成」（P.51-9）を参照してください。

- [Rows Per Page] フィールドは、ドリル ダウン ページとテーブル ビューに表示する、ページごとのイベントの行数を制御します。

- [Refresh Interval] フィールドは、イベント ビューの更新間隔を分数で設定します。「0」を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。

ファイルのプリファレンス

ライセンス：任意

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[Event View Settings] ページの [File Preferences] セクションを使用して、ローカル ファイル ダウンロードの基本特性を設定します。このセクションは、Administrator、Security Analyst、または Security Analyst（読み取り専用）ユーザ ロールを持つユーザのみが使用できます。

検出されたファイルのダウンロードをアプライアンスがサポートしていない場合、これらのオプションは無効になることに注意してください。DC500 ではMalware ライセンスを使用できないので、それらのアプライアンスを使用してファイルをダウンロードしたり、これらのオプションを変更したりすることはできません。

以下のフィールドが [File Preferences] セクションに示されます。

- [Confirm 'Download File' Actions] チェック ボックスは、ファイルをダウンロードするたびに [File Download] ポップアップ ウィンドウが表示され、警告が示されて続行するかキャンセルするかを選択するためのプロンプトが出されるようにするかどうかを制御します。

注意　シスコは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

ファイルをダウンロードする際には、いつでもこのオプションを無効にできることに注意してください。ファイルのダウンロード方法について詳しくは、「保存されているファイルの別の場所へのダウンロード」（P.34-4）を参照してください。

- 検出されたファイルをダウンロードすると、そのファイルを含むパスワード保護された.zip アーカイブがシステムによって作成されます。[Zip File Password] フィールドは、zip ファイルへのアクセスを制限するためにユーザが使用するパスワードを定義します。このフィールドを空欄にすると、パスワードなしのアーカイブ ファイルがシステムによって作成されます。
- [Show Zip File Password] チェック ボックスによって、[Zip File Password] フィールドにプレーン テキストを表示するかまたは不明瞭な文字を表示するかを切り替えます。このフィールドをオフにすると、[Zip File Password] には不明瞭な文字が表示されます。

デフォルトの時間枠

ライセンス：任意

時間枠（時間範囲と呼ばれることもある）は、任意のイベント ビューでイベントに時間制約を課します。[Event View Settings] ページの [Default Time Windows] セクションを使用して、時間枠のデフォルトの動作を制御します。

このセクションへのユーザ ロール アクセスは以下のとおりです。

- Administrators と Maintenance Users は、セクション全体にアクセスできます。
- Security Analysts と Security Analysts（読み取り専用）は、[Audit Log Time Window] 以外のすべてのオプションにアクセスできます。
- Access Admins、Discovery Admins、External Database Users、Intrusion Admins、Network Admins、および Security Approvers は、[Events Time Window] オプションにのみアクセスできます。

デフォルトの時間枠設定に関係なく、イベントの分析中にいつでも手動で個別のイベント ビューの時間枠を変更できることに注意してください。また、時間枠の設定は、現在のセッションにだけ有効であることにも注意してください。ログアウトしてから再びログインすると、時間枠は、このページで設定したデフォルトにリセットされます。詳細については、「イベント時間の制約の設定」（P.47-27）を参照してください。

以下のように、デフォルトの時間枠を設定できる 3 つのタイプのイベントがあります。

- [Events Time Window] は、時間で制約できるほとんどイベントのために単一のデフォルトの時間枠を設定します。
- [Audit Log Time Window] は、監査ログのためにデフォルトの時間枠を設定します。
- [Health Monitoring Time Window] は、ヘルス イベントのためにデフォルトの時間枠を設定します。

時間枠は、ユーザ アカウントがアクセスできるイベント タイプにのみ設定できます。すべてのユーザ タイプは、イベントの時間枠を設定できます。Administrators、Maintenance Users、および Security Analysts は、ヘルス モニタリングの時間枠を設定できます。Administrators と Maintenance Users は、監査ログの時間枠を設定できます。

すべてのイベント ビューが時間で制約できるとは限らないので、時間枠の設定によって、ホスト、ホスト属性、アプリケーション、クライアント、脆弱性、ユーザの ID、ホワイトリスト違反を表示するイベント ビューは影響を受けないことに注意してください。

複数の時間枠を使用して、上記の各タイプのイベントに 1 つずつ適用するか、または**単一の**時間枠を使用して、それをすべてのイベントに適用することができます。単一の時間枠を使用すると、3 つのタイプの時間枠用の設定が非表示になり、新しく [Global Time Window] 設定が表示されます。

以下の 3 つのタイプの時間枠があります。

- *静的*は、特定の開始時刻から特定の終了時刻までに生成されたすべてのイベントを表示します
- *拡張*は、特定の開始時刻から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠が拡張され、新しいイベントがイベント ビューに追加されます。
- *スライディング*は、特定の開始時刻（たとえば 1 日前）から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠は「スライド」し、設定した範囲内（この例では直前の 1 日）のイベントだけが表示されます。

すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。

次のオプションは、[Time Window Settings] ドロップダウン リストに表示されます。

- [Show the Last - Sliding] オプションにより、指定した長さのスライドするデフォルトの時間枠を設定できます。

  アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。

- [Show the Last - Static/Expanding] により、指定した長さのデフォルトの時間枠を静的または拡張のどちらかに設定できます。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、特定の開始時間（1 時間前など）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。

- [Current Day - Static/Expanding] オプションにより、現在の日付のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。

- [Current Week - Static/Expanding] オプションにより、現在の週のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、日曜日の午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 1 週間を超えて分析を続けた場合、この時間枠は 1 週間よりも長くなる可能性があることに注意してください。

デフォルトのワークフロー

ライセンス：任意

ワークフローは、アナリストがイベントの評価に使用するデータが示された一連のページです。アプライアンスには、各イベント タイプに少なくとも 1 つの定義済みのワークフローが付属しています。たとえば、Security Analyst の場合、実行する分析のタイプに応じて、それぞれが侵入イベントのデータを別の形式で示している、10 の異なる侵入イベントのワークフローから選択できます。

アプライアンスは、イベント タイプごとのデフォルトのワークフローによって設定されます。たとえば、[Events by Priority and Classification（優先度および分類に基づいたイベント）] ワークフローが、侵入イベントのデフォルトになります。つまり、侵入イベント（確認済みの侵入イベントを含む）を表示するたびに、アプライアンスは [Events by Priority and Classification（優先度および分類に基づいたイベント）] ワークフローを表示します。

ただし、[Event View Settings] ページの [Default Workflows] セクションを使用して、各イベント タイプのデフォルトのワークフローを変更できます。

設定可能なデフォルトのワークフローは、ユーザ ロールによって異なることに注意してください。たとえば、侵入イベントのアナリストは、デフォルトのディスカバリ イベントのワークフローを設定できません。ワークフローの一般情報については、「ワークフローの概要と使用」（P.47-1）を参照してください。

デフォルトのタイム ゾーンの設定

ライセンス：任意

イベントの表示に使用するタイム ゾーンを、アプライアンスが使用している標準 UTC 時間から変更できます。タイム ゾーンを設定すると、それは現在のユーザ アカウントにのみ適用され、タイム ゾーンをさらに変更するときまで有効となります。

注意　タイム ゾーン機能は、デフォルトのシステム クロックが UTC 時間に設定されていると想定しています。ローカル タイム ゾーンを使用するようにアプライアンスのシステム クロックを変更した場合は、アプライアンスで正確なローカル時刻が表示されるように、それを変更して UTC 時間に戻す必要があります。防御センターと管理対象デバイスの時間を同期させる方法について詳しくは、「時刻の同期」（P.50-26）を参照してください。

タイム ゾーンを変更するには、次のようにします。

アクセス：Any

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[Change Password] ページが表示されます。

ステップ 2　[Time Zone Settings] をクリックします。

[Time Zone Preference] ページが表示されます。

ステップ 3　左側のリスト ボックスで、使用するタイム ゾーンを含む大陸または地域を選択します。

たとえば、北米、南米、カナダで標準のタイム ゾーンを使用する場合は、[America] を選択します。

ステップ 4　右側のリスト・ボックスで、使用するタイム ゾーンに対応するゾーン（都市名）を選択します。

たとえば、東部標準時を使用する場合は、最初のタイム ゾーン ボックスで [America] を選択した後に、[New York] を選択します。

ステップ 5　[Save] をクリックします。

タイム ゾーンが設定されます。

デフォルトのダッシュボードの指定

ライセンス：任意

アプライアンスにあるダッシュボードの 1 つをデフォルトのダッシュボードとして指定できます。デフォルトのダッシュボードは、[Overview] > [Dashboards] を選択すると表示されます。デフォルトのダッシュボードが定義されていない場合は、[Dashboard List] ページが表示されます。ダッシュボードの一般情報については、「ダッシュボードの使用」（P.3-1）を参照してください。

デフォルトのダッシュボードを指定するには、次のようにします。

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　ユーザ名の下にあるドロップダウン リストから、[User Preferences] を選択します。

[Change Password] ページが表示されます。

ステップ 2　[Dashboard Settings] をクリックします。

[Dashboard Settings] ページが表示されます。

ステップ 3　デフォルトとして使用するダッシュボードをドロップダウン リストから選択します。

[None] を選択した場合、[Overview] > [Dashboards] を選択すると [Dashboard List] ページが表示されます。その後、表示するダッシュボードを選択できます。

ステップ 4　[Save] をクリックします。

デフォルトのダッシュボードのプリファレンスが保存されます。