Firepower ユーザ エージェント コンフィギュレーション ガイド

2018 年 7 月 23 日

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任となります。

Cisco Systems, Inc.
www.cisco.com
Cisco は世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号
は当社の Web サイト
（www.cisco.com/go/offices）をご覧ください。

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

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

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

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルとソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2017 年 Cisco Systems, Inc. All rights reserved.

CHAPTER 1 ユーザエージェントの概要 1-1
ユーザエージェントについて 1-2
ユーザ エージェントの基礎 1-2
複数のユーザ エージェントの展開 1-6
レガシー エージェントのサポート 1-6
バージョン 5.x のユーザ エージェントとアクセス制御について 1-6
バージョン 6.x のユーザ エージェント、ISE、およびアクセス制御について 1-7
ユーザエージェントでの FMC サポートの終了 1-7

CHAPTER 2 ユーザ エージェントの設定プロセス 2-1
ユーザ エージェントのセットアップ 2-1
Management Center 設定 2-3
ユーザエージェントに接続するためのバージョン 5.x の Defense Center の設定 2-3
ユーザエージェントに接続するためのバージョン 6.x の Management Center の設定 2-3
Active Directory サーバの設定 2-4
ロギング用の Active Directory サーバの設定 2-4
アイドル セッション タイムアウトの有効化 2-5
ドメイン コンピュータの設定 2-6
ユーザ エージェント コンピュータの設定 2-7
ユーザ エージェントのインストールに関するコンピュータの準備 2-7
ユーザ エージェントのユーザの作成 2-8
ユーザ権限の付与 2-9
ユーザ エージェント設定のバックアップ 2-19
ユーザ エージェントのインストール 2-20
ユーザ エージェントの設定 2-22
ユーザ エージェントのトラブルシューティング 2-35
Management Center に接続できない 2-35
ユーザ エージェントが応答しない 2-38
ユーザ エージェントが一部のログインを表示しない 2-39
ユーザ エージェントがリアルタイム イベントを処理しない 2-39
ユーザ エージェントにユーザ ログオフ イベントが表示されない 2-40
同じネットワーク内のユーザ エージェントと TS エージェント 2-40

ユーザエージェントの概要

Version 2.3 のユーザ エージェントは、Firepower システム の管理対象デバイスと連携してユーザデータを収集します。Firepower システム のバージョン 5.x または バージョン 6.x とともにエージェントを使用している場合は、ユーザ アクセス制御を実装するためにもユーザエージェントが不可欠です。

ユーザエージェントは最大 5 つの Microsoft Active Directory サーバをモニタし、Active Directory によって認証されるログインとログオフをレポートします。Firepower システムは、これらのレコードと、管理対象デバイス上でのトラフィックベースの検出により収集した情報を統合します。

注意 ユーザエージェントのサポート期間の終了が近づいています。Firepower Management Center バージョン 6.6 が、ユーザエージェントを有効にできる最後のバージョンです。Firepower Management Center 6.7 ではユーザエージェントを有効にできません。6.7 にアップグレードすると、アップグレードする前にユーザエージェントを無効にするように警告されます。

ユーザエージェントに関するリリース固有の用語や機能サポートについては、次の表を参照してください。

表 1-1　リリース固有のユーザエージェントの用語

概念	バージョン 5.x	バージョン 6.x
システム	FireSIGHT システム	Firepower System
ユーザ検出専用の機能	ネットワーク ディスカバリ	ネットワーク検出とアイデンティティ
ユーザ アイデンティティとユーザ アクティビティ データの分析	ユーザ認識	ユーザ認識
ユーザ制御へのユーザ アイデンティティとユーザ アクティビティの使用	アクセス コントロール	アクセス コントロール
管理側アプライアンス	Defense Center	Management Center
管理対象アプライアンス	管理対象デバイス	管理対象デバイス
サーバデータベース接続	ユーザ認識オブジェクト	レルム

ユーザエージェントについて

このセクションでは、Firepower システムにユーザ検出を実装する上でユーザエージェントが果たす役割に焦点を当てています。ユーザの探索、RNA/ネットワーク探索、およびアイデンティティ ソースに関連するすべての概念のより詳細な説明については、ご使用のシステムのコンフィギュレーション ガイドを参照してください。

詳細については、次の項を参照してください。

- ユーザ エージェントの基礎（1-2 ページ）
- 複数のユーザ エージェントの展開（1-6 ページ）
- レガシー エージェントのサポート（1-6 ページ）
- バージョン 5.x のユーザ エージェントとアクセス制御について（1-6 ページ）
- バージョン 6.x のユーザ エージェント、ISE、およびアクセス制御について（1-7 ページ）

ユーザ エージェントの基礎

Firepower システム は、組織の Active Directory サーバからユーザ ID とユーザアクティビティ情報の両方を取得できます。ユーザ エージェントでは、ユーザが Microsoft Active Directory サーバと認証する際に、そのユーザをモニタできます。

（注）ユーザ制御を実行するには、組織で Microsoft Active Directory が使用されている*必要があります*。Firepower システムは、Active Directory サーバをモニタするユーザ エージェントを使用してユーザと IP アドレスを関連付けます。その結果、アクセス制御ルールをトリガーできるようになります。

ユーザ エージェントのインストールと使用により、ユーザ コントロールを実行できるようになります。エージェントはユーザ名と 1 つ以上の IP アドレスを関連付け、この情報によりユーザの条件でアクセス制御規則をトリガーできます。

ユーザ制御を実行するためのユーザ エージェントの完全な設定には以下が含まれます。

- エージェントがインストールされているコンピュータ。
- Management Center とユーザ エージェント コンピュータとの間の接続。
- 各 Management Center から監視対象 Active Directory サーバへの接続。バージョン 5.x では、これらを*ユーザ認識オブジェクト*として設定します。バージョン 6.x では、これらをアイデンティティ *レルム*として設定します。

ユーザ制御の詳細については、各システムのコンフィギュレーション ガイドを参照してください。

ユーザ エージェントは、監視対象の Microsoft Active Directory サーバに TCP/IP でアクセスできる任意の Microsoft Windows Vista、Microsoft Windows 7、Microsoft Windows 8、Microsoft Windows Server 2008、または Microsoft Windows Server 2012 コンピュータにインストールできます。サポートされるオペレーティング システムの 1 つを実行する Active Directory サーバ上にエージェントをインストールすることもできますが、そのようにすると安全性は低くなります。

（注）ユーザ エージェントを Windows Server 2003 またはそれ以前のオペレーティング システムにインストールする場合、ユーザ エージェントは Active Directory コンピュータからのリアルタイム統計を収集できません。

Management Center 接続は、ログインとログオフがユーザエージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のログイン データは Management Center に報告されません。

エージェントのモニタリング、ポーリング、およびレポート

各ユーザ エージェントは、定期スケジュールされたポーリングまたはリアルタイム モニタリングのいずれかによって、暗号化されたトラフィックを使用して権限のあるログインをモニタできます。

次に示すのは、ユーザ エージェントが Management Center に報告するいくつかのイベントです。

- **ユーザ ログイン**：ユーザが、最後に表示されたユーザ名に関連していない IP アドレスを持つコンピュータにログインするときに発生します。

  つまりたとえば、月曜日にユーザ名 `james.harvey` が IP アドレス 192.0.2.100 にログインしたとします。火曜日に、`james.harvey` は IP アドレス 192.0.2.105 にログインします。このログインでは、Management Center でユーザ ログイン イベントがトリガーされます。

  ユーザ ログイン イベントは、ユーザがワークステーションに直接ログインするか、またはリモート デスクトップを使用するときに発生します。

- **ユーザ ログオフ**：ユーザが IP アドレスからログアウトするときに発生します。ユーザ ログオフ イベントは、コンピュータからユーザがログオフした直後ではなく設定可能な間隔で Management Center に報告されます。
- **新規ユーザ ID**：ユーザ名が IP アドレスに初めて関連付けられたときに発生する 1 回限りのイベント。
- **ユーザ ID の削除**：Management Center 管理者がユーザ ID を削除すると発生します。

ログイン データとログオフ データを組み合わせることで、ネットワークにログインしたユーザをより完全に把握できます。

Active Directory サーバのポーリングによって、エージェントは定義されたポーリング間隔でユーザ アクティビティ データをまとめて取得できます。リアルタイム モニタリングは、Active Directory サーバがデータを受信するとすぐに、ユーザ アクティビティ データをエージェントに送信します。

特定のユーザ名または IP アドレスに関連付けられたログインまたはログオフの報告を除外するように、エージェントを設定できます。これはたとえば次への繰り返しログインを除外するために役立てることができます。

- 共有サーバ（ファイル共有、プリント サーバなど）
- ユーザ エージェント コンピュータ
- Active Directory サーバ
- トラブルシューティング目的のコンピュータへのログイン

最大 5 つの Active Directory サーバをモニタし、暗号化されたデータを 5 つの Management Center に送信するように、エージェントを設定できます。

バージョン 5.x またはバージョン 6.x を使用してアクセス制御を実行すると、ユーザ エージェントが報告したログインによってユーザと IP アドレスが関連付けられ、その結果としてユーザ条件によるアクセス制御ルールがトリガーされます。

(注)　複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを防止する方法の詳細については、アイドル セッション タイムアウトの有効化（2-5 ページ）を参照してください。

表 1-2　ポーリングおよびモニタリングについての注記

概念	注記
ログイン検出	エージェントは、バージョン 5.2 以降を実行している Defense Center に対して、IPv6 アドレスを持つホストへのユーザ ログインを報告します。 エージェントは、バージョン 5.0.1 以降を実行している Defense Center に対して、権限のないユーザログインと NetBIOS ログインを報告します。 Active Directory サーバへのログインを検出するには、サーバの IP アドレスを使用して Active Directory サーバの接続を設定する必要があります。詳細については、ユーザ エージェントの Active Directory サーバ接続の設定（2-23 ページ）を参照してください。
ログオフ検出	エージェントは、バージョン 5.2 以降の Defense Center に対して、検出されたログオフを報告します。 ログオフはすぐに検出されない場合があります。ログオフに関連付けられたタイムスタンプは、ユーザがホストの IP アドレスにマップされなくなったことをエージェントが検出した時間であり、ユーザがホストからログオフした時間とは一致しない場合があります。
リアルタイム データの取得	Active Directory サーバで Windows Server 2008 または Windows Server 2012 を実行している必要があります。 ユーザ エージェント コンピュータは、Windows 7、Windows 8、Windows 10、または Windows Server の Server 2003 より新しいバージョンを実行している必要があります。

ユーザ エージェントのログイン データ

ユーザ エージェントは、ユーザがネットワークにログインするか、またはアカウントがその他の理由で Active Directory のクレデンシャルに対して認証されるときに、ユーザをモニタします。ユーザ エージェントは、ホストへの対話型ユーザ ログイン、リモート デスクトップ ログイン、ファイル共有認証、およびコンピュータ アカウント ログインを検出します。

ユーザエージェントは*権限を有した*ユーザのログインを報告します。権限のあるログインのデータ（たとえば、リモート デスクトップ ログインや、ユーザによるホストへの対話型ログインなど）によって、ホスト IP アドレスにマップされた現在のユーザが新たなログインからのユーザに変更されます。

ネットワーク検出のトラフィックベース検出では、*権限を持たない*ユーザによるログインが報告されます。権限のないログインでは、現在のユーザを変更しないか、ユーザも権限がない場合にのみ現在のユーザを変更します。

ただし、次の警告に注意してください。

- エージェントがファイル共有認証用のログインを検出した場合は、ホストに対するユーザ ログインを報告しますが、ホスト上の現在のユーザは変更しません。
- エージェントがホストに対するコンピュータ アカウント ログインを検出した場合は、NetBIOS Name Change 検出イベントを生成し、ホスト プロファイルに NetBIOS 名の変更が反映されます。
- 除外されたユーザ名のログインを検出した場合、エージェントは Management Center にログインを報告しません。

エージェントは、すべてのログインについて次の情報を Management Center に送信します。

- ユーザの LDAP ユーザ名

(注)　Unicode 文字を含むユーザ名は、Management Center により正しく表示されない場合があります。

- ログインまたはその他の認証の時刻
- ユーザのホストの IP アドレス、およびエージェントがコンピュータ アカウント ログインの IPv6 アドレスを報告した場合のリンクローカル アドレス

(注)　ユーザが Linux コンピュータでリモートデスクトップを使用して Windows コンピュータにログインした場合、エージェントはログインを検出すると、Linux コンピュータの IP アドレスではなく Windows コンピュータの IP アドレスを Management Center に報告します。

Management Center はユーザ アクティビティ データベースにログイン情報とログオフ情報を記録し、ユーザ データをユーザ データベースに記録します。ユーザ エージェントがユーザ ログインまたはログオフからのユーザ データを報告すると、報告されたユーザがユーザ データベース内のユーザのリストと照合してチェックされます。報告されたユーザがエージェントから報告された既存のユーザと一致した場合、報告されたデータがそのユーザに割り当てられます。報告されたユーザが既存のユーザと一致しなかった場合、新しいユーザが作成されます。

除外されたユーザ名に関連付けられたユーザ アクティビティは報告されませんが、関連するユーザ アクティビティは報告される場合があります。エージェントがコンピュータへのユーザ ログインを検出し、その後 2 人目のユーザ ログインを検出したときに、2 人目のユーザ ログインに関連付けられたユーザ名が報告対象から除外されていた場合、エージェントは元のユーザのログオフを報告します。ただし、2 人目のユーザのログインは報告されません。その結果、除外されたユーザがホストにログインしていた場合でも、IP アドレスにユーザはマップされません。

エージェントによって検出されるユーザ名に関する次の制限事項に注意してください。

- バージョン 5.0.2+ Defense Centerに報告されるドル記号($)で終わるユーザ名は、ネットワーク マップを更新しますが、ユーザ ログインとして表示されません。エージェントは、他のバージョンの Management Center に対してドル記号文字($)で終わるユーザ名を報告しません。
- Management Center では、Unicode 文字を含むユーザ名の表示が制限される場合があります。

Management Center で保存できる検出済みユーザの総数は、以下の内容によって異なります。

- バージョン 5.x では、RNA または FireSIGHT ライセンス
- バージョン 6.x では、Management Center モデル

ユーザ制限に達すると、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを削除する必要があります。

複数のユーザ エージェントの展開

ドメインごとに複数の Active Directory サーバがある場合は、複数のユーザ エージェントのインストールを検討できます。Active Directory サービスは認証情報は共有しますが、セキュリティ ログ（ユーザ エージェントが一部の情報を収集する場所）は共有しません。

したがって、ドメイン内に複数の Active Directory サーバがある場合、以下のいずれかを実行できます。

- 複数の Active Directory サーバと通信する 1 つのユーザ エージェントをインストールします。

  1 つのユーザ エージェントは、最大 5 つの Active Directory サーバと通信できます。

- 複数のユーザ エージェントをインストールし、それぞれが異なる Active Directory サーバまたはドメイン コント ローラと通信するようにします。

  次のような状況ではこのタイプの展開をお勧めします。

  – Active Directory サーバが地理的に分散している。Active Directory サーバに地理的に近接しているコンピュータには、ユーザ エージェントをインストールすることをお勧めします（または Active Directory サーバ コンピュータ自体にもインストールできますが、これは安全性が低くなります）。

  – Active Directory サーバのトラフィックの負荷が高い。

（注）　各ユーザ エージェントを、ドメイン コントローラの完全修飾ホスト名または IP アドレスと通信するように構成する必要があります。マルチドメイン システムでは、各ドメイン コントローラが別々の IP アドレスまたはホスト名を持つのが一般的です。

レガシー エージェントのサポート

Active Directory サーバにインストールされているバージョン 1.0（レガシー）のユーザエージェントは、引き続き Active Directory サーバから 1 つの Management Center にユーザログインデータを送信できます。レガシー エージェントの導入要件と検出機能に変更はありません。

レガシーエージェントを Active Directory サーバにインストールして、1 つの Management Center のみに接続する必要があります。ただし、ユーザ エージェントのステータス モニタ ヘルス モジュールではレガシー エージェントはサポートされないため、レガシー エージェントが接続されている Management Center ではこのモジュールを有効にしないでください。

今後のリリースでレガシー エージェントのサポートが停止される場合に備えてできるだけ早く Version 2.3 のユーザ エージェントを使用するように導入環境をアップグレードしてください。

バージョン 5.x のユーザ エージェントとアクセス制御について

ライセンス：Control

組織で Microsoft Active Directory サーバが使用されている場合、ユーザ エージェントをインストールして、Active Directory サーバを使用してユーザ アクティビティをモニタすることを推奨します。バージョン 5.x でユーザ制御を実行するには、ユーザ エージェントをインストールし、Defense Center への接続を設定する*必要があります*。

バージョン 6.x のユーザ エージェント、ISE、およびアクセス制御について

従来型ライセンス：Control

Smart ライセンス：Any

バージョン 6.0 では、ユーザ エージェントに代わって、Cisco Identity Services Engine（ISE）がサポートされるようになりました。ユーザ エージェントと ISE は、ユーザ アクセス制御のためのデータを収集するパッシブなアイデンティティ ソースです。バージョン 6.x でユーザ制御を実行するには、エージェントまたは ISE デバイスに接続されている Management Center 上の監視対象 Active Directory サーバに、アイデンティティ レルムを設定できます。レルム、アイデンティティ ソース、および ISE/ISE-PIC の詳細については、ご使用のシステムのコンフィギュレーション ガイドを参照してください。

ユーザエージェントでの FMC サポートの終了

Firepower Management Center バージョン 6.6 が、ユーザエージェントを有効にできる最後のバージョンです。Firepower Management Center 6.7 ではユーザエージェントを有効にできません。6.7 にアップグレードすると、アップグレードする前にユーザエージェントを無効にするように警告されます。

可能な限り早くユーザ エージェントの使用を停止し、Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）の使用に切り替えることを強く推奨します。

ユーザエージェントでは使用できない次の機能を活用できるようになります。

- バージョン 2016 までの Microsoft Active Directory のサポート
- 最大 10 の Microsoft Active Directory ドメインコントローラからの認証データの収集
- Kerberos SPAN をサポートするスイッチからの Active Directory 認証データの収集
- パッシブ/アクティブ冗長性のサポート
- ISE-PIC から ISE にアップグレードし、既存の Cisco ISE クラスタに Passive Identity Connector ノードを追加することができます。
- KVM、VMware、および Hyper-v のサポート
- 組織に適合するよう、ライセンスに応じて 3,000 および 30 万のセッションをサポートします。

ユーザ エージェントの設定プロセス

バージョン 2.3 のユーザエージェントを使用して最大 5 つの Microsoft Active Directory サーバからユーザログインデータを収集し、Management Center に送信するには、ユーザエージェントをインストールし、各 Management Center および Microsoft Active Directory サーバに接続して、全般的な設定を行う必要があります。詳細については、次の項を参照してください。

- ユーザ エージェントのセットアップ（2-1 ページ）
- Management Center 設定（2-3 ページ）
- Active Directory サーバの設定（2-4 ページ）
- ユーザ エージェント コンピュータの設定（2-7 ページ）
- ユーザ エージェントのインストール（2-20 ページ）
- ユーザ エージェントの設定（2-22 ページ）
- ユーザ エージェントのトラブルシューティング（2-35 ページ）

ユーザ エージェントのセットアップ

ユーザ エージェントは多段階の設定を行ってセットアップします。

ユーザ エージェントをセットアップするには、次の手順を実行します。

アクセス：管理

ステップ 1 それぞれの Management Center を、以下を実行するように設定します。

- エージェントをインストールするサーバの IP アドレスからのエージェント接続を許可する。
- Active Directory オブジェクトまたはレルムを設定して有効にする。オブジェクトを記述するために使用される用語は、使用している Management Center バージョンによって異なります。詳細については、次のいずれかのセクションを参照してください。
  - ユーザエージェントに接続するためのバージョン 5.x の Defense Center の設定（2-3 ページ）
  - ユーザエージェントに接続するためのバージョン 6.x の Management Center の設定（2-3 ページ）

ステップ 2 Active Directory サーバは、Management Center と通信するユーザ エージェントのイベントをログに記録するように構成します。詳細については、Active Directory サーバの設定（2-4 ページ）を参照してください。

ステップ 3　ドメイン上の各コンピュータを、Windows Management Instrumentation（WMI）がドメインのファイアウォールを通過することを許可するように構成します。詳細については、ドメイン コンピュータの設定（2-6 ページ）を参照してください。

ステップ 4　エージェントをインストールするコンピュータに、前提条件となるプログラムをインストールします。Active Directory サーバに対するコンピュータの TCP/IP アクセスをセットアップします。詳細については、ユーザ エージェントのインストールに関するコンピュータの準備（2-7 ページ）を参照してください。

ステップ 5　以前のユーザ エージェント インストールがあれば、必要に応じて構成設定を保持するためにエージェント データベースをバックアップします。詳細については、ユーザ エージェント設定のバックアップ（2-19 ページ）を参照してください。

ステップ 6　エージェントが Active Directory サーバに接続するのに必要な権限を設定します。詳細については、以下を参照してください。

- ドメイン ユーザへの限定的な特権の付与（概要）（2-9 ページ）
- ローカル ユーザへの特権の付与（2-9 ページ）

ステップ 7　コンピュータにエージェントをインストールします。

- 詳細については、ユーザ エージェントのインストール（2-20 ページ）を参照してください。
- 必要に応じて複数のユーザ エージェントをインストールするには、複数のユーザ エージェントの展開（1-6 ページ）を参照してください。

ステップ 8　1 つ以上の Microsoft Active Directory サーバへの接続を設定します。

ステップ 9　（オプション）エージェントのポーリング間隔と最大ポーリング時間を設定します。詳細については、ユーザ エージェントの Active Directory サーバ接続の設定（2-23 ページ）を参照してください。

ステップ 10　最大で 5 つの Management Center への接続を設定します。詳細については、ユーザ エージェントの Management Center 接続の設定（2-26 ページ）を参照してください。

ステップ 11　（オプション）ログインおよびログオフ データのポーリングから除外するユーザ名と IP アドレスのリストを設定します。詳細については、以下を参照してください。

- ユーザ エージェントの除外ユーザ名設定の構成（2-28 ページ）
- ユーザ エージェントの除外アドレス設定の構成（2-29 ページ）

ステップ 12　（オプション）次のようにエージェント ロギング設定を構成します。詳細については、ユーザ エージェントのロギング設定の構成（2-31 ページ）を参照してください。

ステップ 13　（オプション）エージェント名の設定、サービスの開始と停止、およびサービスの現在のステータスの表示を行います。詳細については、ユーザ エージェントの全般的な設定の構成（2-33 ページ）を参照してください。

ステップ 14　[保存（Save）] をクリックして、ユーザ エージェントの設定を保存します。

注意　Cisco TAC からの指示がないかぎり、エージェント メンテナンスの設定は変更*しないでください*。

Management Center 設定

ここでは、Management Center を準備してユーザ エージェントからユーザ データを受け取る方法を説明します。

ユーザエージェントに接続するためのバージョン 5.x の Defense Center の設定

バージョン 2.3 のユーザエージェントを使用して LDAP ログインデータをバージョン 5.x の Defense Center に送信する予定の場合は、以下のすべてを設定する必要があります。

- 各 Defense Center を、Active Directory サーバに接続する予定のエージェントからの接続を許可するように設定します。その接続によって、エージェントは Defense Center とのセキュアな接続を確立し、データを送信できるようになります。

  この接続の確立に関する詳細については、バージョン 5.x の『*FireSIGHT System User Guide*』の「Using User Agents to Report Active Directory Logins」を参照してください。

- ユーザアクセス制御を実装するには、組織内の少なくとも 1 つの Microsoft Active Directory サーバと Defense Center との間に接続を設定し、有効にしておく必要があります。バージョン 5.x では、これを *LDAP 接続*、または*ユーザ認識オブジェクト*と呼んでいます。

  この設定には、サーバの接続設定と認証フィルタの設定が含まれています。接続のユーザ アクセス制御パラメータとグループ アクセス制御パラメータで、アクセス制御ルールで使用可能なユーザとグループを指定します。この設定の詳細については、バージョン 5.x の『*FireSIGHT System User Guide*』の「Connecting to an LDAP Server for User Awareness and Control」を参照してください。

ユーザエージェントに接続するためのバージョン 6.x の Management Center の設定

バージョン 2.3 のユーザエージェントを使用してログインデータをバージョン 6.x の Management Center に送信するには、以下のすべてを設定する必要があります。

- 各 Management Center を、サーバへの接続を予定しているエージェントからの接続を許可するように設定します。その接続によって、エージェントは Management Center とのセキュアな接続を確立し、データを送信できるようになります。

  この接続の確立に関する詳細については、バージョン 6.x の『*Firepower Management Center Configuration Guide*』の「Configuring a User Agent Connection」を参照してください。

- ユーザアクセス制御を実装するには、組織内の少なくとも 1 つの Microsoft Active Directory サーバと Management Center との間に接続を設定し、有効にしておく必要があります。バージョン 6.x では、これを *レルム*と呼んでいます。

  レルムには、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。接続のユーザ ダウンロード設定で、アクセス制御ルールで使用可能なユーザとグループを指定します。この設定の詳細については、バージョン 6.x の『*Firepower Management Center Configuration Guide*』の「Creating a Realm」を参照してください。

Active Directory サーバの設定

ここでは、Active Directory のセキュリティ ログが有効になっていることを確認し、Active Directory サーバがログイン データをそれらのログに記録できるようにする方法を説明します。

ロギング用の Active Directory サーバの設定

Active Directory サーバがログイン データをログに記録していることを確認するには、次の手順を実行します。

ステップ 1　Active Directory サーバで、[スタート(Start)] > [すべてのプログラム(All Programs)] > [管理ツール(Administrative Tools)] > [イベント ビューア(Event Viewer)] をクリックします。

ステップ 2　[Windows ログ(Windows Logs)] > [セキュリティ(Security)] をクリックします。

ロギングが有効になっている場合は、セキュリティ ログが表示されます。ロギングが無効になっている場合は、セキュリティ ロギングの有効化について、MSDN の「How to configure Active Directory and LDS diagnostic event logging」を参照してください。

ステップ 3　WMI が Active Directory サーバ上のファイアウォールを通過することを許可します。Active Directory サーバが Windows Server 2008 または Windows Server 2012 を実行している場合、詳細については、MSDN の「Setting up a Remote WMI Connection」を参照してください。

Windows 2012 Server でログオン/ログオフ イベントの監査を有効にするには、次の手順を実行します。

ステップ 1　[スタート(Start)] > [管理ツール(Administrative Tools)] > [グループポリシー管理(Group Policy Management)] をクリックします。

ステップ 2　ナビゲーション ウィンドウで、[フォレスト: *ご使用のホスト名*(Forest: YourForestName)] を展開し、[ドメイン(Domains)] > *ご使用のホスト名* > [グループ ポリシー オブジェクト(Group Policy Objects)] を展開します。

ステップ 3　[デフォルトのドメイン ポリシー(Default Domain Policy)] を右クリックし、[編集(Edit)] を選択します。

ステップ 4　[コンピュータの構成(Computer Configuration)] > [ポリシー(Policies)] > [Windows の設定(Windows Settings)] > [セキュリティの設定(Security Settings)] > [監査ポリシーの詳細な構成(Advanced Audit Policy Configuration)] > [監査ポリシー(Audit Policies)] > [ログオン/ログオフ(Logon/Logoff)] を参照します。

ステップ 5　右側のウィンドウで、[監査ログオフ(Audit Logoff)] をダブルクリックします。

ステップ 6　[ログオフプロパティの編集(Edit Logoff Properties)] ダイアログ ボックスで、[次の監査イベントの設定(Configure the following audit events)] および [成功(Success)] をオンにします。

ステップ 7　[OK] をクリック

ステップ 8　[監査ログオン(Audit Logon)] に同じタスクを繰り返します。

（注）　ユーザ エージェントは、Windows セキュリティ ログ イベント 4634 により識別されたログオフ イベントを報告しません。ユーザ エージェントは、ドメイン コンピュータを照会してログオフするために、リモートの Windows Management Instrumentation（WMI）呼び出しを使用します。

アイドル セッション タイムアウトの有効化

ここでは、必要に応じてグループ ポリシーのアイドル セッション タイムアウトを有効にする方法について説明します。これにより、エージェントがホスト上の複数セッションによる余分なログインを検出して報告するのを防ぐことができます。

ターミナル サービス（2008 以前のバージョンの Windows Server）を使用すると、複数のユーザが 1 台のサーバに同時にログインできます。アイドル セッション タイムアウトを有効にすることにより、サーバにログインした複数セッションのインスタンスを減らすことができます。

リモート デスクトップ サービス（Windows Server バージョン 2012 以降）では、リモートでワークステーションにログインできるユーザは一度に 1 人だけです。ただし、ユーザがログアウトせずにリモート デスクトップ セッションを切断すると、そのセッションはアクティブなままになります。ユーザ入力がなくなると、アクティブなセッションは最終的にアイドル状態になります。

あるセッションがアイドル状態のときに別のユーザがリモート デスクトップ サービスを使用してワークステーションにログインすると、2 つのログインが Management Center に報告される可能性があります。アイドル セッション タイムアウトを有効にすると、それらのセッションは定義されたアイドル タイムアウト期間後に終了するため、ホスト上で複数のリモート セッションが実行されなくなります。

Citrix セッションは、リモート デスクトップ サービス セッションと同様に機能します。1 台のコンピュータ上で複数の Citrix ユーザ セッションを同時に実行することができます。アイドル セッション タイムアウトを有効にすると、ホスト上で複数の Citrix セッションが実行されなくなり、余分なログインの報告が減少します。

設定するセッション タイムアウトによっては、1 台のコンピュータに複数のセッションがログインしている状況が生じる可能性があります。

ターミナル サービスのセッション タイムアウトの有効化

このセクションは、2008 までの Windows Server バージョンに適用されます。

ターミナル サービスのセッション タイムアウトを有効にするには、Windows Server 2008 または Windows Server 2012 に対して、アイドル状態のターミナル サービスのセッション タイムアウトと、切断されたターミナル サービスのセッション タイムアウトのグループ ポリシー設定を更新します。これについては Microsoft TechNet の「Configure Timeout and Reconnection Settings for Terminal Services Sessions」で説明されています。

グループ ポリシー オブジェクト マネージャのパスは次のとおりです。

```
Computer Configuration\Administrative Templates\Windows Components\Terminal
Services\Terminal Server\Session Time Limits
User Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal
Server\Session Time Limits
```

アイドル セッションや切断されたセッションが次のログオフ チェックの前にタイムアウトできるように、セッション タイムアウトをユーザ エージェントのログオフ チェックの頻度より短く設定してください。アイドル セッションまたは切断されたセッションのタイムアウトが必須の場合は、ユーザ エージェントのログオフ チェックの頻度をセッション タイムアウトよりも*長く*設定してください。ログオフ チェックの頻度の設定方法の詳細については、ユーザ エージェントの全般的な設定の構成（2-33 ページ）を参照してください。

設定が完了したら、ユーザ エージェント コンピュータの設定（2-7 ページ）に進みます。

リモート デスクトップのセッション タイムアウトの有効化

このセクションは、Windows Server バージョン 2012 以降に適用されます。

リモート デスクトップのセッション タイムアウトを有効にするには、アイドル状態のリモート セッション タイムアウトおよび切断されたセッション タイムアウトのグループ ポリシー設定を更新します。セッション タイムアウトの有効化の詳細については、Microsoft TechNet の「Session Time Limits」を参照してください。

アイドル セッションおよび切断されたセッションが次のログオフ チェックの前にタイムアウトできるように、リモート デスクトップのタイムアウトはユーザ エージェントのログオフ チェックの頻度より*短く*設定してください。アイドル セッションまたは切断されたセッションのタイムアウトが必須の場合は、ユーザ エージェントのログオフ チェックの頻度をリモート デスクトップのタイムアウトよりも*長く*設定してください。ログオフ チェックの頻度の設定方法の詳細については、ユーザ エージェントの全般的な設定の構成（2-33 ページ）を参照してください。

グループ ポリシー オブジェクト エディタのパスは次のとおりです。

```
User Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Session Time Limits
```

設定が完了したら、ユーザ エージェント コンピュータの設定（2-7 ページ）に進みます。

Citrix セッション タイムアウトの有効化

Citrix セッション タイムアウトを有効にするには、Citrix 社のマニュアルを参照してください（http://support.citrix.com/）。

ドメイン コンピュータの設定

ユーザ エージェントがログオフ イベントを Management Center に送信できるようにするには、WMI トラフィックがドメインに接続するすべてのコンピュータ上でファイアウォールを通過することを許可する必要があります。

次の選択肢があります。

- Windows ファイアウォールを使用して、ドメインの WMI を許可します。
- グループ ポリシー オブジェクト（GPO）を使用してファイアウォール ポリシーを構成します。これについては、Microsoft TechNet の Windows Firewall with Advanced Security Deployment Guide などの資料で説明されています。

ユーザ エージェント コンピュータの設定

Management Center と Active Directory サーバの準備が整ったら、エージェントをインストールして設定するコンピュータを準備します。

ユーザ エージェントのインストールに関するコンピュータの準備

ユーザ エージェントは、ここで説明する要件を満たしている Windows コンピュータにインストールできます。

コンピュータの設定

コンピュータは次のいずれかになります。

- （推奨）Active Directory サーバにアクセスできる信頼ネットワーク上のコンピュータ。このコンピュータは、ネットワーク管理者のみが使用できるようにする必要があります。

  このインストール方法は最も安全であるので推奨します。
- Active Directory サーバ。

ユーザ エージェントのインストールの前提条件

Windows コンピュータは、次の前提条件を満たしている必要があります。

- コンピュータで、Windows Vista、Windows 7、Windows 8、Windows Server 2008、または Windows Server 2012 が実行されていること。セキュリティ上の理由から、ユーザ エージェントは Active Directory サーバ コンピュータ *ではなく*、ドメイン コンピュータにインストールすることをお勧めします。
- コンピュータに Microsoft .NET Framework バージョン 4.0 クライアント プロファイルおよび Microsoft SQL Server Compact（SQL CE）バージョン 3.5 がインストールされていること。
  - Microsoft .NET Framework バージョン 4.0 クライアント プロファイル再頒布可能パッケージは、Microsoft のダウンロード サイトから入手できます（`dotNetFx40_Client_x86_x64.exe`）。
  - SQL Server Compact 3.5 は、Microsoft のダウンロード サイトから入手できます（`SSCERuntime-ENU.exe`）。

（注）　.NET Framework がない場合は、エージェント実行可能ファイル（`setup.exe`）を開始すると、該当ファイルをダウンロードするためのプロンプトが表示されます。詳細については、ユーザ エージェントのインストール（2-20 ページ）を参照してください。

- ユーザ エージェントを実行するユーザを作成します。これについては、ユーザ エージェントのユーザの作成（2-8 ページ）で説明しています。
- コンピュータが、監視対象の Active Directory サーバに TCP/IP でアクセスでき、Active Directory サーバと同じバージョンのインターネット プロトコルを使用していること。エージェントが Active Directory サーバをリアルタイムでモニタリングしている場合は、ログイン データを取得できるように、コンピュータの TCP/IP アクセスを常に有効にしておく必要があります。

(注)　ユーザ エージェントを Windows Server 2003 またはそれ以前のオペレーティング システムにインストールする場合、ユーザ エージェントは Active Directory コンピュータからのリアルタイム統計を収集できません。

- コンピュータが、データと IPv4 アドレスの報告先となる Management Center に TCP/IP でアクセスできること。
- IPv6 アドレスが設定されたホストからのログオフを検出する場合は IPv6 アドレスがコンピュータに設定されていて、IPv4 アドレスが設定されたホストからのログオフを検出する場合は IPv4 アドレスがコンピュータに設定されていること。
- コンピュータにレガシー エージェントまたはバージョン 2.x エージェントがまだインストールされていないこと。これらのエージェントは自動的にアンインストールされないため、既存のエージェントをアンインストールするには、Windows コントロール パネルの [プログラムの追加と削除(Add/Remove Programs)] を使用します。

注意　ユーザ エージェントの旧バージョンがインストールされている場合は、構成設定を保持するために、データベースをバックアップする必要があります。

ユーザ エージェントのユーザの作成(2-8 ページ)に進みます。

ユーザ エージェントのユーザの作成

必要最小限の権限でユーザ エージェントを実行できるようにするには、ユーザ エージェントのユーザ アカウントを作成する必要があります。

- 以前のバージョンのユーザ エージェントをアップグレードする場合には、この手順は必要ありません。

  その場合には、ユーザ エージェント設定のバックアップ(2-19 ページ)を参照してください。
- Active Directory サーバとは別のコンピュータ上でユーザ エージェントを実行するには、ユーザはドメイン ユーザである必要があります。
- Active Directory サーバ上でユーザ エージェントを実行するには、ユーザはローカル アカウントである必要があります。

新規ユーザを作成するには、次を実行します。

ステップ 1　Active Directory サーバに Domain Admins グループのメンバーとしてログインします。

ステップ 2　Active Directory サーバでユーザ エージェントを実行するには、ローカル ユーザ アカウントを作成します(このアカウントは Domain Admins グループに属している必要がありますが、ユーザは管理者グループに属している必要はありません)。

このセクションの残りの手順をスキップして、ユーザ権限の付与(2-9 ページ)に進みます。

ステップ 3　ドメイン ユーザを作成してユーザ エージェントを別のコンピュータで実行できるようにするには、[スタート(Start)] > [Active Directory ユーザとコンピュータ(Active Directory Users and Computers)] をクリックします。

ステップ 4　左側のウィンドウで、ユーザを追加するドメインとフォルダを展開します。

ステップ 5　ユーザを追加するフォルダを右クリックします。

ステップ 6　ポップアップ メニューから、[新規(New)] > [ユーザ(User)] をクリックします。

ステップ 7　画面の指示に従って、ドメイン ユーザを作成し、そのユーザに強力なパスワードを付与します。

注意　セキュリティ上の理由から、必ずこのユーザ アカウントはネットワーク管理者だけが知ることができるようにします。

ユーザ権限の付与

ここでは、次の可能性について説明します。

- Active Directory サーバ上の Domain Admins グループにローカル ユーザを追加する。

  この方法は簡単ですが、安全性が低いためにお勧めしません。ローカル ユーザへの特権の付与(2-9 ページ)を参照してください。

- ドメイン ユーザにユーザ エージェントを実行する最小限の特権を付与する。ドメイン ユーザへの限定的な特権の付与(概要)(2-9 ページ)を参照してください。

ローカル ユーザへの特権の付与

Active Directory サーバでユーザ エージェントを実行するには、Domain Admins グループにユーザを追加する必要があります。ユーザ エージェントをインストールしやすくするために、必要に応じて管理者グループにもユーザを追加できます。

ドメイン ユーザへの限定的な特権の付与(概要)

ここでは、ユーザ エージェントを実行する最小限の特権をドメイン ユーザに付与するために必要な作業の概要を示します。例については、ドメイン ユーザに限定的な特権を付与する(ステップバイステップの例)(2-10 ページ)を参照してください。

ドメイン ユーザに限定的な特権を付与するには、次の手順を実行します。

ステップ 1　Active Directory サーバに Domain Admins グループのメンバーとしてログインします。

ステップ 2　ユーザ エージェント ユーザを次のグループに追加します。

- **分散 COM ユーザ**
- **イベントログリーダー**

ステップ 3　Windows Management Instrumentation(WMI)コントロール コンソールを使用して、ユーザに `Root\CIMV2` ノードに対する次の権限を付与します(これについては Microsoft TechNet で説明されています)。

- **メソッドの実行**
- **アカウントの有効化**
- **リモートの有効化**
- **セキュリティの読み取り**

ステップ 4　ユーザ エージェントが Active Directory サーバのリアルタイム処理を使用できるようにします。

- Windows ファイアウォール ルールに対するグループ ポリシー オブジェクト（GPO）セキュリティ ポリシーを作成して、リモート プロシージャ コール（RPC）エンドポイント マッパー サービスへのインバウンド ネットワーク トラフィックが許可されるようにします（これについては Microsoft TechNet で説明されています）。
- Windows ファイアウォール ルールに対する GPO セキュリティ ポリシーを作成して、ランダム RPC ポート上のインバウンド トラフィックが許可されるようにします（これについては Microsoft TechNet で説明されています）。

リアルタイム処理の詳細については、ユーザ エージェントの Active Directory サーバ接続の設定（2-23 ページ）を参照してください。

ステップ 5　`gupdate /force` コマンドまたは同等のポリシーを使用して、グループ ポリシー オブジェクト（GPO）を更新します。

ドメイン ユーザに限定的な特権を付与する（ステップバイステップの例）

ここでは、ユーザ エージェントを実行する最小限の特権をドメイン ユーザに付与するステップバイステップの例を示します。

このセクションの手順に従うには、ご使用のシステムが次を使用していることが前提です。

- Windows Server 2012
- ユーザ エージェント ユーザ名は `limited.ua`。
- ドメイン名は `sesame.example.com`。
- ユーザ エージェントが 1 つの Active Directory サーバと 1 つの Firepower Management Center に接続している。
- ユーザ エージェントが Active Directory サーバからイベントをリアルタイムで処理している。

ユーザへの Windows Management Instrumentation（WMI）権限の付与

ここでは、ドメイン ユーザ WMI 特権を Active Directory サーバ上の `Root > CIMV2` ノードに付与して、ユーザがドメイン コンピュータからのログオフを取得できるようにする方法について説明します。

ドメイン ユーザに WMI 権限を付与するには、次の手順に従います。

ステップ 1　Active Directory サーバに Domain Admins グループのメンバーとしてログインします。

ステップ 2　ユーザ エージェント ユーザを次のグループに追加します。

- **分散 COM ユーザ**
- **イベントログリーダー**

ステップ 3　[開始（Start）] をクリックして、`wmimgmt.msc` を入力します。

ステップ 4　[コンソール ルート（Console Root）] > [WMI コントロール（ローカル）（WMI Control (Local)）] を右クリックし、[プロパティ（Properties）] をクリックします。

ステップ 5　[WMI コントロール（ローカル）のプロパティ（WMI Control (Local) Properties）] ダイアログボックスで、[セキュリティ（Security）] タブをクリックします。

ステップ 6　[ルート（Root）] > [CIMV2] をクリックします。

ステップ 7　[セキュリティ（Security）] をクリックします。

ステップ 8　[ROOT\CIMV2 のセキュリティ（Security for ROOT\CIMV2）] ダイアログ ボックスで、[追加（Add）] をクリックします。

ステップ 9　[選択するオブジェクト名を入力してください（Enter the object names to select）] フィールドで、`limited.ua` と入力して、[名前の確認（Check Names）] をクリックします。

Windows によりユーザ名が検索され、フィールドに表示されます。

ステップ 10　[OK] をクリック

ステップ 11　ユーザに次の権限を付与します。

- メソッドの実行
- アカウントの有効化
- リモートの有効化
- セキュリティの読み取り

ステップ 12　[Root\CIMV2 のセキュリティ（Security for Root\CIMV2）] ダイアログ ボックスで、[OK] をクリックします。

ステップ 13　[WMI コントロール プロパティ（WMI Control Properties）] ダイアログ ボックスで、[OK] をクリックします。

WMI 権限のテスト

ユーザ エージェントに Active Directory サーバに対する WMI 権限を付与したら、その権限を、ユーザ エージェントをインストールするコンピュータからテストする必要があります。

WMI の権限をテストするには、次の手順を実行します。

ステップ 1　ユーザ エージェントをインストールするドメインのコンピュータにログインします。

ステップ 2　検索フィールドに `wbemtest` と入力します。（Windows のバージョンによっては、[スタート（Start）] をまずクリックする必要があります。）

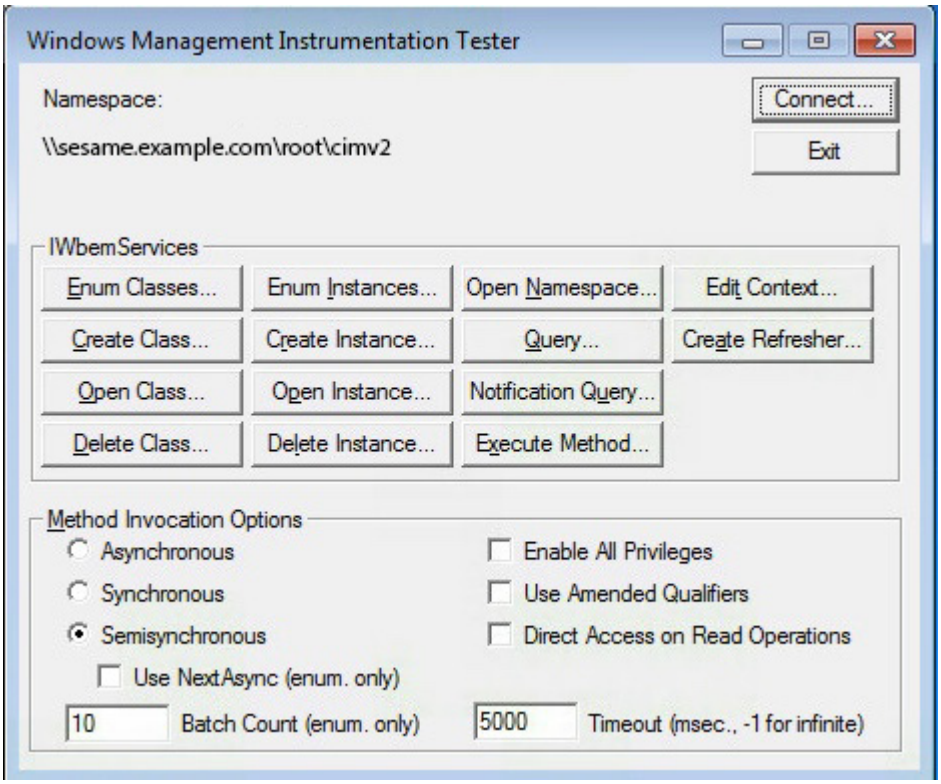
ステップ 3　[Windows Management Instrumentation テスト（Windows Management Instrumentation Tester）] ダイアログ ボックスで、[接続（Connect）] をクリックします。

ステップ 4　[接続（Connect）] ダイアログ ボックスに、次の情報を入力します。

- [名前空間（Namespace）] フィールド：Active Directory サーバの名前とパスを、`\\namespace\root\cimv2` の形式で入力します。この例では、`\\sesame.example.com\root\cimv2` と入力します。
- [資格情報（Credentials）] フィールド：ユーザ名を `domain\username` の形式で [ユーザ（User）] フィールドに、およびユーザのパスワードを [パスワード（Password）] フィールドに入力します。この例では、ユーザ名は `sesame\limited.ua` です。
- 通常、このダイアログ ボックスの他のオプションを変更する必要はありません。

ステップ 5　[接続(Connect)] をクリックします。

接続が成功すると、次のように [Windows Management Instrumentation テスト(Windows Management Instrumentation Tester)] ダイアログ ボックスが表示されます。



エラーが表示される場合は、以下のことを試します。

- 「RPC サーバを使用できません(The RPC server is unavailable)」は、名前空間が正しくないかまたは Active Directory サーバがアクセス不能であること(ネットワーク問題、サーバがダウンしているなど)を示しています。
- 「アクセスは拒否されました(Access is denied)」は、ユーザ名またはパスワードが正しくないことを示しています。

ステップ 6　テストが成功したら、[クエリ(Query)] をクリックします。

ステップ 7　[クエリ(Query)] ダイアログ ボックスに、次のように入力します。

```
select * from Win32_NTLogEvent where Logfile = 'Security' and (EventCode=672 or
EventCode=4768 or EventCode=538 or EventCode=4364 or EventCode=528 or EventCode=4624 or
EventCode=4634) and TimeGenerated > "date-code"
```

日付コードは Microsoft 日時コードで、YYYYMMDDHHMMSS.*fractionalSecond-utc_timezone_offset* の形式です。

たとえば、米国中央タイム ゾーン(UTC - 6 時間)において、2017 年 5 月 1 日深夜にクエリを実行するために、次を入力します。

```
select * from Win32_NTLogEvent where Logfile = 'Security' and (EventCode=672 or
EventCode=4768 or EventCode=538 or EventCode=4364 or EventCode=528 or EventCode=4624 or
EventCode=4634) and TimeGenerated > "20170501000000.000000-600"
```

ステップ 8　[クエリの種類(Query Type)] リストから、[WQL] をクリックします。

ステップ 9　[適用（Apply）] をクリックします。

クエリは新しいダイアログ ボックスで表示されます。

エラー「無効なクラスです（`Invalid class`）」または「無効なクエリです（`Invalid query`）」が表示される場合は、コマンド構文を確認して再試行します。結果が表示されない場合は、日付コードを確認します。

ステップ 10　ログの表示が終了したら、[閉じる（Close）] をクリックします。

ステップ 11　[Windows Management Instrumentation テスト（Windows Management Instrumentation Tester）] ダイアログ ボックスで、[終了（Exit）] をクリックします。

ユーザ エージェントに分散コンポーネント オブジェクト管理（DCOM）へのアクセスを許可する

このセクションでは、DCOM アクセスを許可して、ユーザ エージェントが Active Directory サーバ上のオブジェクトにリモートにアクセスできるようにする方法について説明します。

ユーザに DCOM アクセスを付与するには、次の手順を実行します。

ステップ 1　Active Directory サーバに Domain Admins グループのメンバーとしてログインします。

ステップ 2　[スタート（Start）] > [ファイル名を指定して実行（Run）] をクリックし、`dcomcnfg` を入力し、Enter を押します。

ステップ 3　[コンポーネント サービス（Component Services）] ウィンドウで、[コンポーネント サービス（Component Services）] > [コンピュータ（Computers）] をクリックします。

ステップ 4　[マイ コンピュータ（My Computer）] を右クリックし、[プロパティ（Properties）] をクリックします。

ステップ 5　[コンピュータのプロパティ（Computer Properties）] ダイアログ ボックスで、[COM セキュリティ（COM Security）] タブをクリックします。

ステップ 6　[起動とアクティブ化のアクセス許可（Launch and Activation Permissions）] で、[制限の編集（Edit Limits）] をクリックします。

ステップ 7　[起動とアクティブ化のアクセス許可（Launch and Activation Permissions）] ダイアログ ボックスで、[追加（Add）] をクリックします。

ステップ 8　[選択するオブジェクト名を入力してください（Enter the object names to select）] フィールドに、`limited.ua` を入力して、[名前の確認（Check Names）] をクリックします。

ステップ 9　名前が一致する場合は、[OK] をクリックします。

ステップ 10　ユーザに**リモートからの起動**および**リモートからのアクティブ化**権限を付与します。

ステップ 11　[起動とアクティブ化のアクセス許可（Launch and Activation Permissions）] ダイアログ ボックスで、[OK] をクリックします。

ステップ 12　[コンピュータ プロパティ（My Computer Properties）] ダイアログボックスで、[OK] をクリックします。

Active Directory セキュリティ ログへのアクセスを許可するグループ オブジェクト ポリシーを更新するには、次の手順に従います。

ステップ 1　[スタート(Start)] > [すべてのプログラム(All Programs)] > [管理ツール(Administrative Tools)] > [グループ ポリシー管理(Group Policy Management)] を選択します。

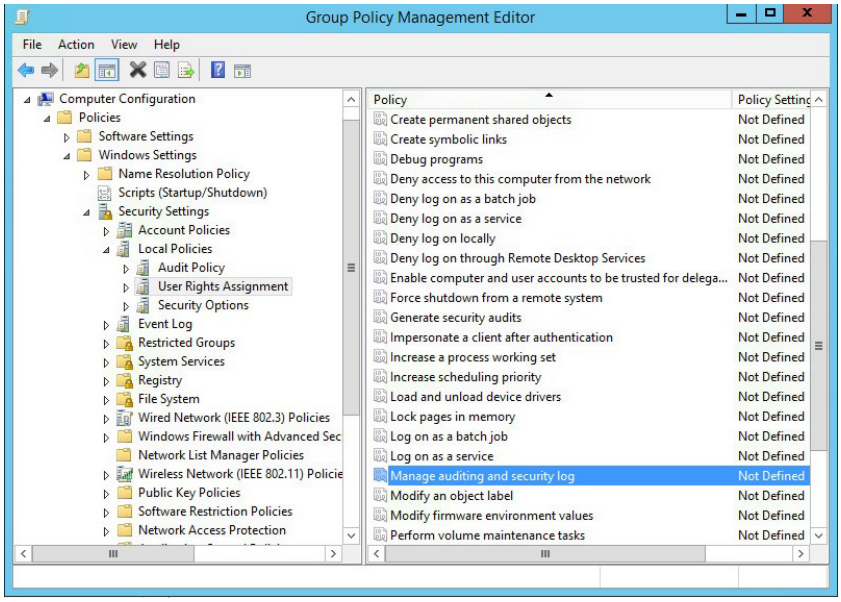
ステップ 2　ナビゲーション ウィンドウで、[フォレスト: *ご使用のホスト名*(Forest: YourForestName)] を展開し、[ドメイン(Domains)] > *ご使用のホスト名* > [グループ ポリシー オブジェクト(Group Policy Objects)] を展開します。

ステップ 3　[デフォルトのドメイン ポリシー(Default Domain Policy)] を右クリックし、[編集(Edit)] を選択します。

ステップ 4　[コンピュータの構成(Computer Configuration)] > [ポリシー(Policies)] > [Windows の設定(Windows Settings)] > [セキュリティの設定(Security Settings)] > [ローカル ポリシー(Local Policies)] > [ユーザ権利の割り当て(User Rights Assignment)] を参照します。

ステップ 5　右側のウィンドウで、[監査とセキュリティ ログの管理(Manage auditing and security log)] をダブルクリックします。

次の図は例を示しています。



ステップ 6　[これらのポリシーの設定を定義する(Define these policy settings)] をオンにします。

ステップ 7　[ユーザまたはグループを追加(Add User or Group)] をクリックします。

ステップ 8　[ユーザとグループ名(User and group names)] フィールドで、ユーザ エージェントのユーザ名を入力するか、または [参照(Browse)] をクリックしてそれを見つけます。

ステップ 9　[監査とセキュリティ ログの管理(Manage auditing and security log)] プロパティ ダイアログ ボックスで、[OK] をクリックします。

Windows ファイアウォールのグループ ポリシー オブジェクト ルールの作成

このセクションは、ユーザ エージェントが Active Directory サーバのリアルタイム イベント処理を使用するために必要です。リアルタイムのイベント処理の詳細については、ユーザ エージェントの Active Directory サーバ接続の設定（2-23 ページ）を参照してください。

インバウンド リモート プロシージャ コール（RPC）のネットワーク トラフィックを許可するには、グループ ポリシー管理でセキュリティが強化された Windows ファイアウォール ノードを使用して、2 つのファイアウォール ルールを作成します。

- 最初のルールでは、RPC エンドポイント マッパー サービスへの着信トラフィックを許可します。これはクライアントがサービスとの通信に使用する必要がある動的に割り当てられたポート番号で応答します。
- 2 番目のルールでは、動的に割り当てられたポート番号に送信されるネットワーク トラフィックを許可します。

2 つのルールを使用すると、RPC 動的ポート リダイレクトを受信したコンピュータのみを送信元、RPC エンドポイント マッパーによって割り当てられたポート番号のみを送信先としてネットワーク トラフィックが許可され、コンピュータを保護できます。

後述の手順で説明するタスクは、ユーザ エージェントがアクセスする必要のあるすべての Active Directory サーバ上で実行してください。

RPC トラフィックを許可するために GPO ファイアウォール ルールを作成するには、次の手順を実行します。

ステップ 1　まだそうしていない場合は、Active Directory サーバに Domain Admins グループのメンバーとしてログインします。

ステップ 2　[スタート（Start）] > [管理ツール（Administrative Tools）] を選択します。

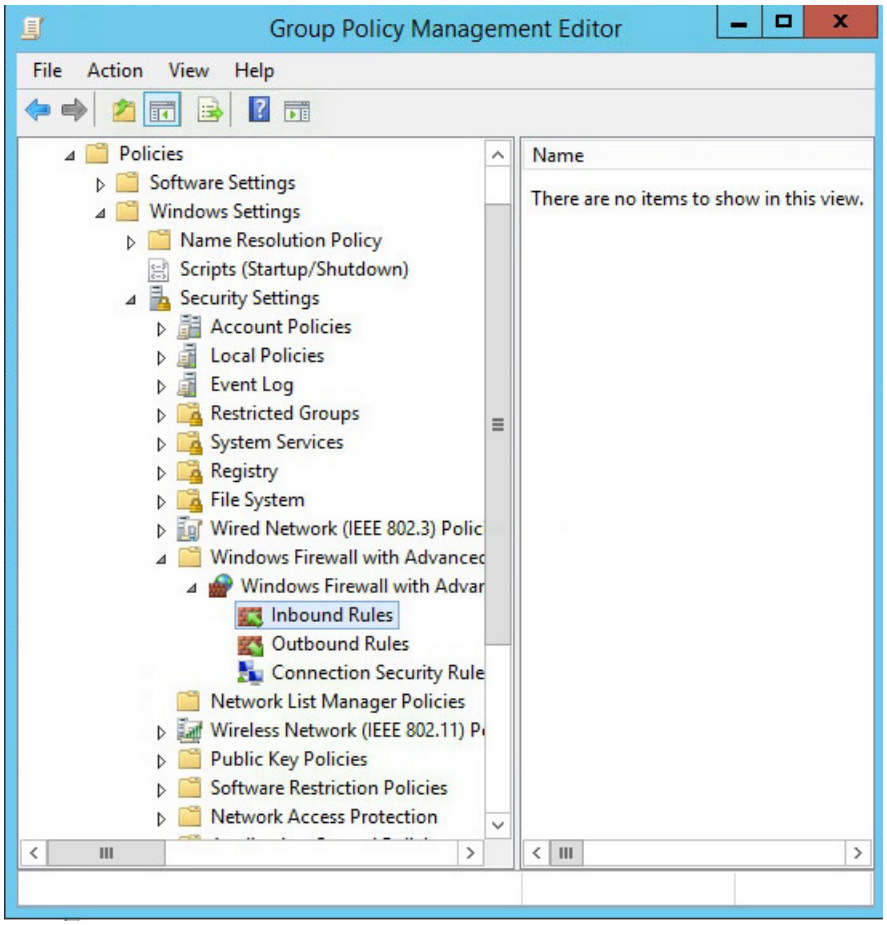
ステップ 3　[管理ツール（Administrative Tools）] ウィンドウで、[グループ ポリシー管理（Group Policy Management）] をダブルクリックします。

ステップ 4　ナビゲーション ウィンドウで、[フォレスト：ご使用のドメイン名（Forest：*YourForestName*）] を展開し、[ドメイン（Domains）] > *ご使用のドメイン名* > [グループ ポリシー オブジェクト（Group Policy Objects）] を展開し、変更する GPO を右クリックして、[編集（Edit）] をクリックします。

通常は、[既定のドメイン ポリシー（Default Domain Policy）] を編集する必要があります。

ステップ 5　左側のウィンドウで、[コンピュータの構成（Computer Configuration）] > [ポリシー（Policies）] > [Windows の設定（Windows Settings）] > [セキュリティの設定（Security Settings）] > [セキュリティが強化された Windows ファイアウォール（Windows Firewall with Advanced Security）] > [セキュリティが強化された Windows ファイアウォール（Windows Firewall with Advanced Security）] を展開します。

次の図は例を示しています。



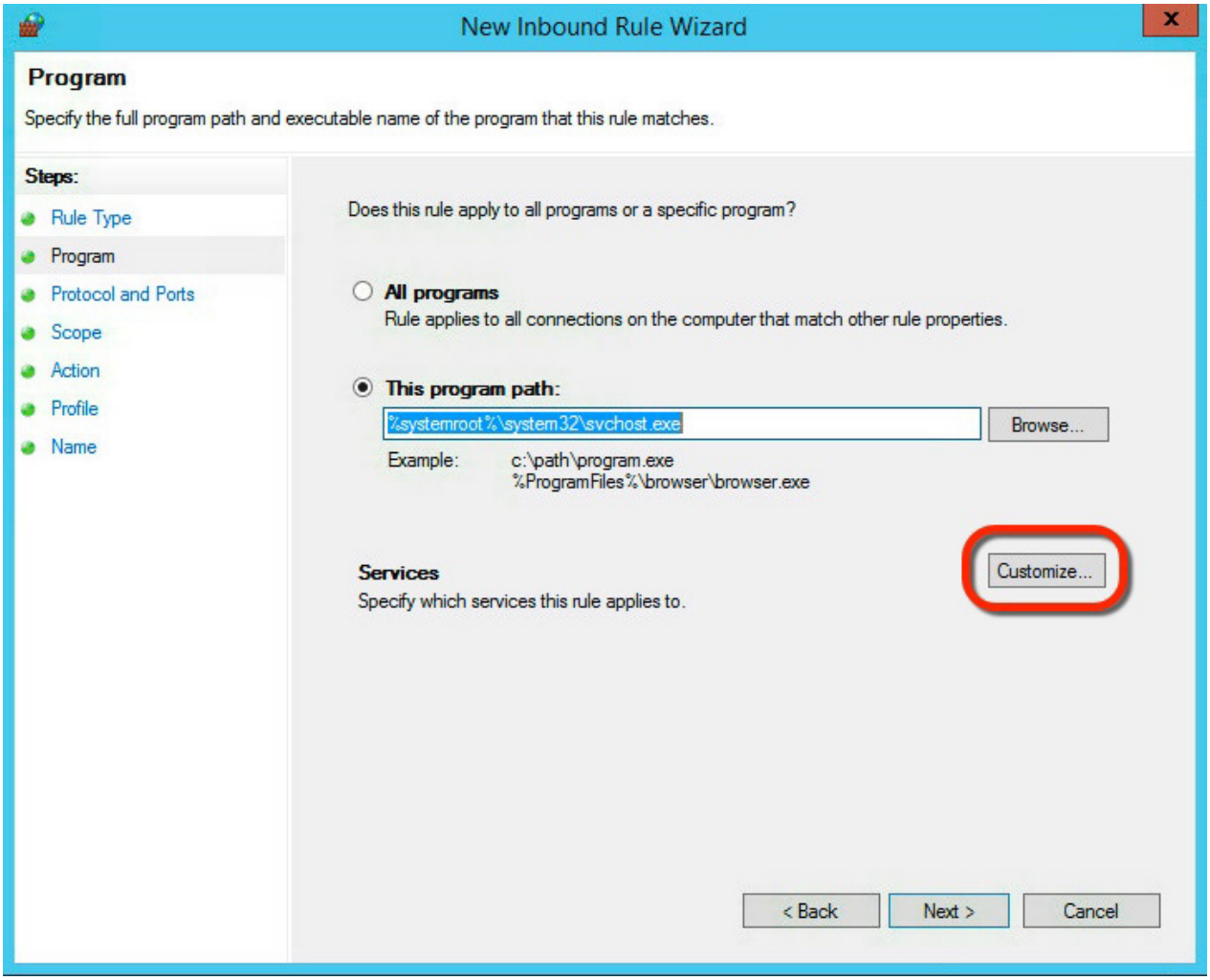
ステップ 6　[受信の規則(Inbound Rules)] を右クリックして、[新しい規則(New Rule)] をクリックします。

ステップ 7　[新規の受信の規則ウイザード(New Inbound Rule Wizard)] ダイアログ ボックスで、[カスタム(Custom)] をクリックし、[次へ(Next)] をクリックします。

ステップ 8　[このプログラム パス(This program path)] をクリックし、`%systemroot%\system32\svchost.exe` を入力します。

ステップ 9　サービスの横で、[カスタマイズ(Customize)] をクリックします。

次の図は例を示しています。



ステップ 10　[サービス設定のカスタマイズ(Customize Service Settings)] ダイアログ ボックスで、[このサービスに適用する(Apply to this service)] をクリックし、短い名前 **RpcSs** の [リモート プロシージャ コール(RPC) (Remote Procedure Call(RPC))] を選択し、[OK] をクリックします。

ステップ 11　[次へ(Next)] をクリックします。処理の確認が求められます。

ステップ 12　[プロトコルおよびポート(Protocol and Ports)] ダイアログ ボックスで、[プロトコルの種類(Protocol type)] に [TCP] をクリックします。

ステップ 13　[ローカル ポート(Local port)] で、[RPC エンドポイント マッパー(RPC Endpoint Mapper)] を選択して、[次へ(Next)] をクリックします。

ステップ 14　[スコープ(Scope)] ページの、[このルールはどのリモート IP アドレスに適用されますか(Which remote IP addresses does this rule apply to?)] セクションで、[これらの IP アドレス(These IP addresses)] をし、[追加(Add)] をクリックして、ユーザ エージェント コンピュータの IP アドレスを入力します。

ステップ 15　[次へ(Next)] をクリックします。

ステップ 16　[アクション(Action)] ページで、[接続を許可する(Allow the connection)] を選択し、[次へ(Next)] をクリックします。

ステップ 17　[プロファイル(Profiles)] ページで、[ドメイン(Domain)] のみをオンにして、[次へ(Next)] をクリックします。

ステップ 18　[名前(Name)] ページで、このルールを識別する名前を入力して、[完了(Finish)] をクリックします。

動的にマップされたポートを許可する GPO ルールを作成するには、次の手順を実行します。

ステップ 1　Windows ファイアウォールのグループ ポリシー オブジェクト ルールの作成(2-15 ページ)の 1 ～ 4 の手順を完了させます。

ステップ 2　[新規の受信の規則ウイザード(New Inbound Rule Wizard)] ダイアログ ボックスで、[カスタム(Custom)] をクリックし、[次へ(Next)] をクリックします。

ステップ 3　[このプログラム パス(This program path)] をクリックし、`%systemroot%\system32\svchost.exe` を入力します。

ステップ 4　サービスの横で、[カスタマイズ(Customize)] をクリックします。

ステップ 5　[サービス設定のカスタマイズ(Customize Service Settings)] ダイアログ ボックスで、[このサービスに適用する(Apply to this service)] をクリックし、短い名前 **EventLog** の [Windows イベント ログ(Windows Event Log)] を選択し、[OK] をクリックします。

ステップ 6　[次へ(Next)] をクリックします。処理の確認が求められます。

ステップ 7　[プロトコルおよびポート(Protocol and Ports)] ダイアログ ボックスで、[プロトコルの種類(Protocol type)] に [TCP] をクリックします。

ステップ 8　[ローカル ポート(Local port)] で、[RPC 動的ポート(RPC Dynamic Ports)] をクリックして、[次へ(Next)] をクリックします。

ステップ 9　[スコープ(Scope)] ページで、[これらの IP アドレス(These IP addresses)] をクリックし、[追加(Add)] をクリックして、ユーザ エージェント コンピュータの IP アドレスを入力します。

ステップ 10　[次へ(Next)] をクリックします。

ステップ 11　[アクション(Action)] ページで、[接続を許可する(Allow the connection)] をクリックし、[次へ(Next)] をクリックします。

ステップ 12　[プロファイル(Profiles)] ページで、[ドメイン(Domain)] のみをオンにして、[次へ(Next)] をクリックします。

ステップ 13　[名前(Name)] ページで、このルールを識別する名前を入力して、[完了(Finish)] をクリックします。

GPO ポリシーを適用するには、次の手順を実行します。

ステップ 1　新しい GPO ポリシーを、`gpupdate /force` コマンドまたは同等のメソッドを使用して適用します。

GPO ポリシーの適用の詳細については、次の参照資料を参照してください。

- Microsoft TechNet の「GPO Policy for Beginners」
- Microsoft TechNet の「Policy Processing」

(注)　昇格された権限を使用して、`gpupdate /force` コマンドを実行する必要があります。Active Directory サーバに管理者としてログインするか、コマンド プロンプトを管理者として実行します(コマンド プロンプトを右クリックして、[管理者として実行(Run as Administrator)] をクリックします)。

ユーザ エージェント設定のバックアップ

ユーザ エージェントの旧バージョンがインストールされている場合は、ユーザ エージェントの新しいバージョンをインストールすると、既存の設定が削除されます。既存の構成設定を保持するには、ユーザ エージェントの新しいバージョンをインストールする前に、データベースをバックアップします。

(注)　バージョン 2.2 以降のユーザ エージェントがインストールされている場合は、データベースをバックアップする必要はありません。ユーザ エージェントの新しいバージョンをインストールするときに、構成設定が自動的にインポートされます。ユーザ エージェントのインストール(2-20 ページ)に進みます。

構成設定を保持するには、次の手順を実行します。

ステップ 1　エージェントがインストールされているコンピュータで、[スタート(Start)] > [プログラム(Programs)] > [Cisco] > [Active Directory 用の Cisco FirePOWER ユーザ エージェントの設定(Configure Cisco Firepower User Agent for Active Directory)] をクリックします。

ステップ 2　エージェント サービスを停止するには、停止ボタン(■)をクリックします。

ステップ 3　エージェントがインストールされているコンピュータで `CiscoUserAgent.sdf` を見つけ、このファイルをローカルでコピーします。

(注)　2.2 以前のバージョンから更新している場合は、`SourcefireUserAgent.sdf` を見つけて、コピーします。ファイルのコピーを作成し、名前を `CiscoUserAgent.sdf` に変更します。

ステップ 4　Cisco ユーザエージェントを、[コントロールパネル(Control Panel)] の [プログラムの追加と削除(Add/Remove Programs)] オプションを使用してアンインストールします。エージェントを削除します。

ステップ 5　ユーザ エージェントの最新バージョンをインストールします。詳細については、ユーザ エージェントのインストール(2-20 ページ)を参照してください。

ステップ 6　エージェントがインストールされているコンピュータで、[スタート(Start)] > [プログラム(Programs)] > [Cisco] > [Active Directory 用の Cisco FirePOWER ユーザ エージェントの設定(Configure Cisco Firepower User Agent for Active Directory)] を選択します。

ステップ 7　エージェント サービスを停止するには、停止ボタン(■)をクリックします。

ステップ 8　エージェントの最新バージョンがインストールされているコンピュータで `CiscoUserAgent.sdf` を見つけます。現在のファイルを、エージェントの旧バージョンから作成したローカル バックアップに置き換えます。

ステップ 9　最新バージョンのエージェントがインストールされているコンピュータで、[スタート(Start)] > [プログラム(Programs)] > [Cisco] > [Active Directory 用の Cisco FirePOWER ユーザ エージェントの設定(Configure Cisco Firepower User Agent for Active Directory)] を選択します。

ステップ 10　▶ をクリックしてサービスを開始します。

ユーザ エージェントのインストール(2-20 ページ)に進みます。

ユーザ エージェントのインストール

ライセンス: FireSIGHT または該当なし

Active Directory サーバに接続する権限を設定した後、およびアイドル状態のリモート セッションのタイムアウト後に、エージェントをインストールします。

注意　ユーザ エージェントの旧バージョンがインストールされている場合は、構成設定を保持するため、インストールの前にデータベースのバックアップを実行する必要があります。詳細については、ユーザ エージェント設定のバックアップ(2-19 ページ)を参照してください。

デフォルトでは、エージェントは、**ローカル システム** アカウントを使用するサービスとして動作します。エージェントが実行されている Windows コンピュータがネットワークに接続されている場合、ユーザがコンピュータにアクティブにログインしていなくても、このサービスはユーザ データのポーリングと送信を続けます。

エージェントごとに、1 つ以上の Active Directory サーバと最大 5 つの Management Center への接続を設定できます。Management Center の接続を追加する前に、必ず Management Center の設定にエージェントを追加してください。詳細については、以下を参照してください。

- ユーザエージェントに接続するためのバージョン 5.x の Defense Center の設定(2-3 ページ)
- ユーザエージェントに接続するためのバージョン 6.x の Management Center の設定(2-3 ページ)

1 つ以上のユーザ エージェントの展開の詳細については、複数のユーザ エージェントの展開(1-6 ページ)を参照してください。

高可用性構成では、両方の Management Center をエージェントに追加して、プライマリとセカンダリの両方に対するユーザ ログイン データの更新を可能にし、両方のデータが最新になるようにします。

ユーザ エージェントをインストールするには、次の手順を実行します。

アクセス:任意(Any)

ステップ 1　ユーザ エージェントのユーザの作成(2-8 ページ)で作成したユーザとして、ユーザ エージェントをインストールする Windows コンピュータにログインします。

- 旧バージョンのユーザ エージェントをアップグレードする場合は、同じコンピュータにログインします。
- (推奨)Active Directory サーバとは別のコンピュータにユーザ エージェントをインストールするには、そのコンピュータにログインします。
- Active Directory サーバにユーザ エージェントをインストールするには、Domain Admins グループ、および必要であれば管理者グループのメンバーとして、Active Directory サーバにログインします。

ステップ 2　ユーザ エージェント セットアップ ファイル（Cisco_Firepower_User_Agent_for_Active_Directory_2.3-10.zip）をサポート サイトからダウンロードします。

（注）　サポート サイトから直接、ユーザ エージェントのセットアップ ファイルを含む圧縮アーカイブをダウンロードします。破損する可能性があるため、ファイルは電子メールでは転送しないでください。

ステップ 3　.zip ファイルを右クリックし、[すべて展開（Extract All）] を選択します。

ステップ 4　ファイルを展開するフォルダを選択します。

エージェントをインストールするにはハード ドライブ上に 3 MB の空き領域が必要です。エージェント ローカル データベース用に、ハード ドライブで 4 GB を割り当てることを推奨します。

ステップ 5　ファイルを展開したフォルダで、setup.exe をダブルクリックします。

（注）　setup.exe をダブルクリックします（setup.msi では*ありません*）。setup.msi はユーザ エージェントのインストール前に前提条件ソフトウェアを確認しませんが、それによりエージェントのインストールまたは実行がエラーになる可能性があります。

ヒント　管理者グループのメンバーではないアカウントを使用しており、Windows コンピュータに新しいアプリケーションをインストールする権限を持っていない場合は、インストールを開始するための適切な権限を持っている管理者グループに属するユーザに昇格させる必要があります。エスカレーションオプションにアクセスするには、setup.exe ファイルを右クリックして、[別のユーザとして実行（Run As）] をクリックします。該当するユーザを選択して、そのユーザのパスワードを入力します。

ステップ 6　インストールを続行するにはライセンス契約に同意する必要があります。

ステップ 7　エージェントをインストールする Windows コンピュータ上に Microsoft .NET Framework バージョン 4.0 クライアント プロファイルと SQL Server Compact 3.5 の両方がインストールされていない場合は、該当ファイルをダウンロードするためのプロンプトが表示されます。ファイルをダウンロードしてインストールします。

ステップ 8　ウィザード内のプロンプトに従ってエージェントをインストールします。

コンピュータでユーザ アカウント制御が有効になっている場合、変更を行う許可を求めるすべてのプロンプトに対して [はい（Yes）] と応答する必要があります。

ステップ 9　エージェントの設定を開始するには、ユーザ エージェントの設定（2-22 ページ）を参照してください。

ユーザ エージェントの設定

ライセンス:FireSIGHT または該当なし

エージェントをインストールしたら、Active Directory サーバからデータを受信して、その情報を Management Center に報告し、レポートから特定のユーザ名と IP アドレスを除外して、ステータスメッセージをローカルイベントログまたは Windows アプリケーションログに記録するようにエージェントを設定します。

エージェントを設定するには、次の手順を実行します。

アクセス:任意(Any)

ステップ 1　エージェントがインストールされているコンピュータで、[スタート(Start)] > [プログラム(Programs)] > [Cisco] > [Active Directory 用の Cisco FirePOWER ユーザ エージェントの設定(Configure Cisco Firepower User Agent for Active Directory)] を選択します。

次の表に、エージェントを設定する場合に実行可能な操作とエージェントの設定場所の説明を示します。

表 2-1　ユーザ エージェントの設定操作

目的	操作
エージェント名の変更、ログオフ チェックの頻度の変更、サービスの開始と停止、スケジュール優先度の設定	[全般(General)] タブをクリックします。詳細については、ユーザ エージェントの全般的な設定の構成(2-33 ページ)を参照してください。
Active Directory サーバの追加、変更、または削除、Active Directory サーバ データのリアルタイムでの取得の有効化、Active Directory サーバのポーリング間隔と最大ポーリング時間の変更	[Active Directory サーバ(Active Directory Servers)] タブをクリックします。詳細については、ユーザ エージェントの Active Directory サーバ接続の設定(2-23 ページ)を参照してください。
Management Center の追加または削除	[Firepower Management Centers] タブをクリックします。詳細については、ユーザ エージェントの Management Center 接続の設定(2-26 ページ)を参照してください。
レポートから除外するユーザ名の追加、変更、または削除	[除外ユーザ名(Excluded Usernames)] タブをクリックします。詳細については、ユーザ エージェントの除外ユーザ名設定の構成(2-28 ページ)を参照してください。
レポートから除外する IP アドレスの追加、変更、または削除	[除外アドレス(Excluded Addresses)] タブをクリックします。詳細については、ユーザ エージェントの除外アドレス設定の構成(2-29 ページ)を参照してください。
イベント ログの表示、エクスポート、クリア、Windows アプリケーション ログへの記録、メッセージの保持期間の変更	[ログ(Logs)] タブをクリックします。詳細については、ユーザ エージェントのロギング設定の構成(2-31 ページ)を参照してください。

表 2-1　ユーザ エージェントの設定操作（続き）

目的	操作
Cisco TAC から指示されたトラブルシューティングおよびメンテナンス タスクの実行	[ログ（Logs）] タブを選択して、[ログ内のデバッグ メッセージを表示（Show Debug Messages in Log）] を有効にしてから、[メンテナンス（Maintenance）] タブをクリックします。詳細については、ユーザ エージェントのメンテナンス設定の構成（2-33 ページ）を参照してください。
エージェント設定の変更の保存	[保存（Save）] をクリックします。未保存の変更がある場合には、そのことを示すメッセージが表示されます。
エージェント設定に対する変更を保存せずにエージェントを閉じる	[キャンセル（Cancel）] をクリックします。

ユーザ エージェントの Active Directory サーバ接続の設定

ライセンス：FireSIGHT または該当なし

ユーザ エージェントから 1 つ以上の Active Directory サーバへの接続を追加し、次を構成できます。

- エージェントがリアルタイムでログインおよびログオフ データを取得するか、または Active Directory サーバのデータを定期的にポーリングするか。
- エージェントがユーザ アクティビティ データをポーリングする頻度、または接続が失われた場合に Active Directory サーバとのリアルタイム接続の確立または再確立を試行する頻度。
- エージェントが Active Directory サーバ自体にログインするために報告する IP アドレス。
- Active Directory サーバとの接続の確立または再確立時にエージェントが取得するログインおよびログオフ データの量。

ユーザ エージェントがリアルタイムでデータを取得するように設定されていて、リアルタイム モニタリングが利用できない場合は、リアルタイム モニタリングが再び利用可能になるまで、エージェントは代わりに Active Directory サーバのデータをポーリングしようとします。

ヒント　シスコでは、ユーザ エージェントが大量のユーザ アクティビティを取得する場合に、リアルタイム データ取得の代わりにポーリングを設定することを推奨しています。アクティビティの多い環境では、ポーリング間隔を 1 分に設定し、最大ポーリング時間を 10 分以下に設定してください。

リアルタイム モニタリングを使用するには、Active Directory サーバで Windows Server 2008 以降が実行されている必要があります。

（注）　ユーザ エージェントを Windows Server 2003 またはそれ以前のオペレーティング システムにインストールする場合、ユーザ エージェントは Active Directory コンピュータからのリアルタイム統計を収集できません。

ユーザ エージェントでは、タブ選択時の Active Directory サーバの最新のポーリング ステータス、エージェントに報告された最後のログイン、およびエージェントが最後に Active Directory サーバをポーリングした時間を確認できます。

エージェントが Active Directory サーバをリアルタイムでポーリングしているかどうか、タブ選択時のリアルタイム データの取得ステータスも確認できます。サーバのステータスの詳細については、次の表を参照してください。

表 2-2　Active Directory サーバのステータス

Active Directory サーバのステータス	ポーリングの可用性	リアルタイムの可用性
`available`	サーバのポーリングが利用できます。	サーバのリアルタイム データ取得が利用できます。
`unavailable`	サーバのポーリングが利用できません。	サーバのリアルタイム データ取得が利用できないか、サーバがポーリング用に設定されています。
`pending`	サーバ構成は追加されましたが、通信はまだ開始していません。	サーバ構成を追加して保存してから、ユーザ エージェントとの通信を開始するまでには、いくらかの時間がかかります。`pending` ステータスが続く場合は、ユーザ エージェントとサーバとの間の通信を確認してください。
`unknown`	エージェントは起動されていますが、ステータスをまだ取得できません。または、エージェントが Active Directory サーバをまだチェックしていません。	エージェントは起動されていますが、ステータスをまだ取得できません。または、エージェントが Active Directory サーバをまだチェックしていません。

（注）　各ユーザ エージェントが互いの接続を検出するたびに余分なログインが報告されるため、同じ Active Directory ドメイン コントローラに複数のユーザ エージェントを接続しないでください。複数のユーザ エージェントを接続する場合は、同じ Active Directory サーバをポーリングしているエージェントを実行している他のすべてのホストの IP アドレスとエージェントがログイン時に使用するユーザ名を除外するように、各ユーザ エージェントを設定してください。詳細については、ユーザ エージェントの除外アドレス設定の構成（2-29 ページ）を参照してください。

Active Directory サーバの接続を設定するには、次の手順を実行します。

アクセス：任意（Any）

ステップ 1　必要に応じて、ユーザ エージェントがインストールされているコンピュータにログインします。

ステップ 2　[スタート（Start）] > [（すべての）プログラム（（All）Programs）] > [Cisco] > [Cisco Firepower Agent for Active Directory の設定（Configure Cisco Firepower Agent for Active Directory）] をクリックします。

ステップ 3　[Active Directory サーバ（Active Directory Servers）] タブをクリックします。

ステップ 4　次の選択肢があります。

- サーバへの新しい接続を追加するには、[追加（Add）] をクリックします。
- 既存の接続を変更するには、サーバ名をダブルクリックします。
- 既存の接続を削除するには、サーバ名をクリックして [削除（Remove）] をクリックします。

ステップ 5　[サーバ名/IP アドレス（Server Name/IP Address）] フィールドで、Active Directory サーバまたはドメイン コントローラの完全修飾サーバ名または IP アドレスを入力します。Active Directory サーバへのログインを検出するには、IP アドレスを入力します。

エージェントが Active Directory サーバにインストールされている場合は、エージェントがインストールされているサーバを追加するために、サーバ名として `localhost` を入力します。必要に応じて、ユーザ名とパスワードを追加できます。これらの情報を省略すると、その Active Directory サーバへ認証を行っているユーザのログオフを検出できません。ユーザ名とパスワードを入力したかどうかに関係なく、サーバをポーリングできます。

（注）　Active Directory システムに複数のドメイン コントローラがある場合は、ユーザ エージェントと通信させるドメイン コントローラのホスト名または IP アドレスを入力します（Active Directory ドメイン コントローラはそのセキュリティ ログを共有しないので、各コントローラへの個別のユーザ エージェント接続が必要です）。分散システムまたはトラフィックが多いシステムでは、必要に応じて 1 つ以上のユーザ エージェントをインストールできます。これについては、複数のユーザ エージェントの展開（1-6 ページ）で説明しています。

ステップ 6　[許可されたユーザ（Authorized User）] および [パスワード（Password）] フィールドに、Active Directory サーバのユーザ ログインおよびログオフ データをクエリする権限を持つユーザ名とパスワードを入力します。

プロキシを使用して認証するには、完全修飾ユーザ名を入力します。

デフォルトでは、エージェントがインストールされているコンピュータへのログイン時に使用したアカウントのドメインが [ドメイン（Domain）] フィールドに自動的に入力されています。

（注）　ユーザ パスワードに含まれる文字が 65 文字以上の場合、新しいサーバ接続を設定できません。この機能を使用できるようにするには、パスワードを短くしてください。

ステップ 7　[ドメイン（Domain）] フィールドに、Active Directory ドメインの名前を入力します。

ステップ 8　Active Directory サーバへのログインを検出するには、[ローカル ログイン IP アドレス（Local Login IP Address）] フィールドから IP アドレスを選択します。このフィールドには、[サーバ名/IP アドレス（Server Name/IP Address）] フィールドに指定されたサーバに関連付けられているすべての IP アドレスがエージェントによって自動的に入力されています。

[サーバ名/IP アドレス（Server Name/IP Address）] フィールドが空であるか、または `localhost` を含んでいる場合は、ローカル ホストに関連付けられているすべての IP アドレスがこのフィールドに入力されています。

ステップ 9　ユーザ エージェントがこの Active Directory サーバからリアルタイムでログイン イベントを取得できるようにするには、[リアルタイム イベントを処理（Process realtime events）] をクリックします。

ステップ 10　[追加（Add）] をクリックして新規サーバを追加するか、または [保存（Save）] をクリックして既存のサーバへの変更を保存します。

このサーバ接続定義が Active Directory サーバのリストに表示されます。複数のサーバ接続が設定されている場合は、[ホスト（Host）]、[最終報告（Last Reported）]、[ポーリング ステータス（Polling Status）]、[最終ポーリング（Last Polled）]、[リアルタイム ステータス（Real Time Status）]、または [リアルタイム（Real Time）] の列ヘッダーをクリックすると、それぞれの列でソートできます。

(注)　設定時にユーザ エージェントが Active Directory サーバに接続できない場合、そのサーバは追加できません。エージェントがサーバに TCP/IP でアクセスできること、使用したクレデンシャルで接続できること、および Active Directory サーバへの接続を正しく設定していることを確認してください。詳細については、Active Directory サーバの設定 (2-4 ページ)を参照してください。

ステップ 11　(オプション)エージェントが Active Directory サーバのユーザ ログイン データを自動的にポーリングする間隔を変更するには、[Active Directory サーバのポーリング間隔(Active Directory Server Polling Interval)] リストから時間を選択します。

設定を保存すると、選択した分数が経過した後で次のポーリングが開始され、その間隔で繰り返されます。ポーリングにかかる時間が選択した間隔よりも長い場合、次のポーリングは前のポーリングが終了した後の次の間隔で開始されます。

Active Directory サーバに対するリアルタイム イベント処理が有効になっていて、ユーザ エージェントとサーバの接続が失われている場合、エージェントは応答を受信してリアルタイム データの取得が可能になるまでポーリングを試行し続けます。接続が確立されると、リアルタイム データの取得が再開されます。

ステップ 12　(オプション)エージェントが Active Directory サーバのユーザ ログイン データをポーリングするための接続を最初に確立(または再確立)するときの最大ポーリング時間を変更するには、[Active Directory サーバの最大ポーリング時間(Active Directory Server Max Poll Length)] リストから時間を選択します。

(注)　ユーザ エージェントでは、各ポーリングのユーザ アクティビティ データをスキップする設定を保存できません。[Active Directory サーバの最大ポーリング時間(Active Directory Server Max Poll Length)] リストに保存する値を、[Active Directory サーバのポーリング間隔(Active Directory Server Polling Interval)] リストから選択した値より小さくすることはできません。

ステップ 13　設定の変更を保存してエージェントに適用するには、[保存(Save)] をクリックします。

ステップ 14　次の選択肢があります。

- Management Center の接続を追加または削除するには、[Firepower Management Centers] タブを選択します。詳細については、ユーザ エージェントの Management Center 接続の設定 (2-26 ページ)を参照してください。

  ユーザ ログインおよびログオフ データを報告するには、エージェントに少なくとも 1 つの Management Center を追加する必要があります。

- エージェントを設定する場合は、表 2-1 (2-22 ページ)で説明されているいずれかの操作を実行します。

ユーザ エージェントの Management Center 接続の設定

ライセンス:FireSIGHT または該当なし

Active Directory ユーザデータを、ユーザエージェントから最大 5 つの Management Center に送信できます。エージェントでは、タブ選択時の Management Center のステータス(エージェントが最初に起動したときの `available`、`unavailable`、または `unknown`)や、エージェントによって報告された最後のログインを確認することもできます。

接続を追加する前に、必ず Management Center の設定にユーザエージェントを追加してください。詳細については、ユーザエージェントに接続するためのバージョン 5.x の Defense Center の設定（2-3 ページ）、ユーザエージェントに接続するためのバージョン 5.x の Defense Center の設定（2-3 ページ）、またはユーザエージェントに接続するためのバージョン 6.x の Management Center の設定（2-3 ページ）を参照してください。

（注）　バージョン 5.x では、Management Center は Defense Center と呼ばれています。

高可用性構成では、両方の Management Center をエージェントに追加し、プライマリとセカンダリの両方に対するユーザ ログインおよびログオフ データの更新を有効にして、両方で最新のデータが保持されるようにします。

Management Center の接続を設定するには、次の手順を実行します。

アクセス：任意（Any）

ステップ 1　必要に応じて、ユーザ エージェントがインストールされているコンピュータにログインします。

ステップ 2　[スタート（Start）] > [（すべての）プログラム（（All）Programs）] > [Cisco] > [Cisco Firepower Agent for Active Directory の設定（Configure Cisco Firepower Agent for Active Directory）] をクリックします。

ステップ 3　[Firepower Management Centers] タブをクリックします。

ステップ 4　[追加（Add）] をクリックします。

ステップ 5　追加する Management Center のホスト名または IP アドレスを入力します。

ステップ 6　[追加（Add）] をクリックします。

Management Center 接続の設定が追加されます。ホスト名または IP アドレスを複数回追加することはできません。ホスト名と IP アドレスの両方を使って Management Center を追加しないでください。Management Center に複数のネットワークアダプタがある場合は、異なる IP アドレスを使用して複数回追加しないでください。

複数の Management Center 接続が設定されている場合は、[ホスト（Host）]、[ステータス（Status）]、または [最終報告（Last Reported）] の列見出しをクリックすると、それぞれの列でソートできます。

（注）　設定時にユーザエージェントが Management Center に接続できない場合は、その Management Center を追加できません。エージェントが Management Center に TCP/IP でアクセスできることを確認します。

ステップ 7　設定の変更を保存してエージェントに適用するには、[保存（Save）] をクリックします。更新された設定がエージェントに適用されます。

ステップ 8　次の選択肢があります。

- （オプション）除外ユーザ名リストのユーザ名を追加または削除するには、[除外ユーザ名（Excluded Usernames）] タブを選択します。詳細については、ユーザ エージェントの除外ユーザ名設定の構成（2-28 ページ）を参照してください。
- （オプション）除外 IP アドレス リストの IP アドレスを追加または削除するには、[除外アドレス（Excluded Addresses）] タブを選択します。詳細については、ユーザ エージェントの除外アドレス設定の構成（2-29 ページ）を参照してください。

- (オプション)ログ メッセージを表示したり、ロギングを設定したりするには、[ログ(Logs)] タブを選択します。詳細については、ユーザ エージェントのロギング設定の構成(2-31 ページ)を参照してください。
- (オプション)エージェントの全般的な設定を構成するには、[全般(General)] タブをクリックします。詳細については、ユーザ エージェントの全般的な設定の構成(2-33 ページ)を参照してください。
- エージェントを設定する場合は、表 2-1(2-22 ページ)で説明されているいずれかの操作を実行します。

ユーザ エージェントの除外ユーザ名設定の構成

ライセンス: FireSIGHT または該当なし

ログインまたはログオフ イベントのポーリング時に除外するユーザ名を最大 500 件定義できます。除外されたユーザ名によるログインまたはログオフ イベントを取得した場合、エージェントはそのイベントを Management Center に報告しません。

ユーザ名を除外する前に報告されたログインおよびログオフ イベントは影響を受けません。除外ユーザ名リストからユーザ名を削除すると、その後のそのユーザ名のログインおよびログオフ イベントは Management Center に報告されます。

あるユーザによるすべてのログインおよびログオフ イベントを、すべてのドメインから除外するか、または特定のドメインから除外するかを選択できます。コンマ区切り値(CSV)ファイルに保存されるユーザ名とドメインのリストをエクスポートおよびインポートすることもできます。Management Center にすでに報告されたユーザを除外した場合、データベースからホストをパージしないかぎり、そのユーザはホストからマッピング解除されないことに注意してください。

たとえば、Active Directory サーバとは別のコンピュータにユーザ エージェントをインストールした場合、このオプションを使用して、ユーザ エージェント ユーザを Management Center にログインしないように除外できます。

除外ユーザ名を設定するには、次の手順を実行します。

アクセス:任意(Any)

ステップ 1　必要に応じて、ユーザ エージェントがインストールされているコンピュータにログインします。

ステップ 2　[スタート(Start)] > [(すべての)プログラム((All)Programs)] > [Cisco] > [Cisco Firepower Agent for Active Directory の設定(Configure Cisco Firepower Agent for Active Directory)] をクリックします。[除外ユーザ名(Excluded Usernames)] タブを選択します。

ステップ 3　入力可能な次の行の [ユーザ名(Username)] 列に除外するユーザ名を入力します。

除外ユーザ名にドル記号文字($)や引用符文字(")を含めることはできません。

ステップ 4　(オプション)ユーザ名に関連付けられたドメインを [ドメイン(Domain)] 列に入力します。

行ごとに 1 つのドメインのみ定義できます。ドメインを指定しない場合、すべてのドメインのユーザ名が除外されます。

ステップ 5　ユーザ名をさらに追加するには、ステップ 3 および 4 を繰り返します。複数の除外ユーザ名が設定されている場合は、[ユーザ名(Username)] または [ドメイン(Domain)] の列ヘッダーをクリックすると、それぞれの列でソートできます。

ステップ 6　行を削除する場合、次の選択肢があります。

- 行を強調表示して Del キーを押します。
- ユーザ名の末尾にポインタを置いて、ユーザ名が削除されるまで Back Space キーを押します。

行が削除されます。

複数の行を削除するには、Ctrl キーを押した状態で複数の行をクリックして選択し、それから Delete キーを押します。

ステップ 7　ユーザ名とドメインのリストをコンマ区切り値（CSV）ファイルにエクスポートするには、[リストのエクスポート（Export List）] をクリックします。ファイルの保存先のファイル パスを選択します。

ファイルが保存されます。デフォルトのファイル名は `Cisco_user_agent_excluded_users.csv` です。

ステップ 8　ユーザ名とドメインのリストをコンマ区切り値（CSV）ファイルからインポートするには、[リストのインポート（Import List）] をクリックします。アップロードするファイルを選択します。

既存のユーザ名がクリアされ、ファイル内のユーザ名がロードされます。重複するユーザ名を含むファイルをアップロードすることはできません。ファイルに構文エラーがある場合、ファイルをアップロードできません。

コンマ区切り値（CSV）ファイル内のエントリは、次の形式になっている必要があります。

```
"username","domain"
```

ドメインの値はオプションですが、プレースホルダとして引用符が必要です。

ステップ 9　[保存（Save）] をクリックして設定の変更を保存し、エージェントに適用します。

ステップ 10　次の選択肢があります。

- 除外 IP アドレス リストの IP アドレスを追加または削除するには、[除外アドレス（Excluded Addresses）] タブを選択します。詳細については、ユーザ エージェントの除外アドレス設定の構成（2-29 ページ）を参照してください。
- エージェントを設定する場合は、表 2-1（2-22 ページ）で説明されているいずれかの操作を実行します。

ユーザ エージェントの除外アドレス設定の構成

ライセンス：FireSIGHT または該当なし

ログイン イベントのポーリング時に除外する IPv4 および IPv6 アドレスを最大 100 件設定できます。除外された IP アドレスを含むログインまたはログオフイベントを取得した場合、ユーザ エージェントはそのイベントを Management Center に報告しません。

IP アドレスを除外する前に報告されたログインおよびログオフ イベントは影響を受けません。除外アドレス リストから IP アドレスを削除すると、その後のそのアドレスのログインおよびログオフ イベントは Management Center に報告されます。

たとえば、Active Directory サーバとは別のコンピュータにユーザ エージェントをインストールした場合、このオプションを使用して、ユーザ エージェント ユーザを Management Center にログインしないように除外できます。

（注）　同じネットワーク内でユーザ エージェントと TS エージェントの両方を使用する場合は、重大ではないエラーが Firepower Management Center に記録されないようにするために、TS エージェントの IP アドレスを除外する必要があります。TS エージェントとユーザ エージェントの両方が同じユーザのログインを検出すると、重大ではないエラーがログに書き込まれます。

除外 IP アドレスを設定するには、次の手順を実行します。

アクセス：任意（Any）

ステップ 1　必要に応じて、ユーザ エージェントがインストールされているコンピュータにログインします。

ステップ 2　[スタート（Start）] > [（すべての）プログラム（（All）Programs）] > [Cisco] > [Cisco Firepower Agent for Active Directory の設定（Configure Cisco Firepower Agent for Active Directory）] をクリックします。[除外アドレス（Excluded Addresses）] タブを選択します。

ステップ 3　入力可能な次の行の [アドレス（Address）] 列に、除外する IP アドレスを入力します。IP アドレスをさらに追加するには、この手順を繰り返します。

複数の除外 IP アドレスが設定されている場合は、[アドレス（Address）] の列ヘッダーをクリックすると、それぞれの列でソートできます。

無効な IP アドレスを入力した場合は、行のヘッダーに感嘆符アイコン（ ）が表示されます。無効なアドレスを修正しないと、他のアドレスを入力できません。

ステップ 4　IP アドレスを削除するには、行を強調表示して Del キーを押します。

IP アドレスが削除されます。複数の行を削除するには、Ctrl キーを押した状態で複数の行をクリックして選択し、それから Delete キーを押します。

ステップ 5　IP アドレスのリストをコンマ区切り値（CSV）ファイルにエクスポートするには、[リストのエクスポート（Export List）] をクリックします。ファイルの保存先のファイル パスを選択します。

ファイルが保存されます。デフォルトのファイル名は `Cisco_user_agent_excluded_addresses.csv` です。

ステップ 6　IP アドレスのリストをコンマ区切り値（CSV）ファイルからインポートするには、[リストのインポート（Import List）] をクリックします。アップロードするファイルを選択します。

既存の IP アドレスがクリアされ、ファイル内の IP アドレスがロードされます。重複する IP アドレスを含むファイルをアップロードすることはできません。ファイルに構文エラーがある場合、ファイルをアップロードできません。

ステップ 7　[保存（Save）] をクリックして設定の変更を保存し、エージェントに適用します。

ステップ 8　次の選択肢があります。

- ログ メッセージを表示したり、ロギングを設定したりするには、[ログ（Logs）] タブを選択します。詳細については、ユーザ エージェントのロギング設定の構成（2-31 ページ）を参照してください。
- エージェントを設定する場合は、表 2-1（2-22 ページ）で説明されているいずれかの操作を実行します。

ユーザ エージェントのロギング設定の構成

ライセンス:FireSIGHT または該当なし

[ログ(Logs)] タブには、エージェントによってログに記録されたステータス メッセージが最大 250 件表示されます。エージェントは、次のイベントが発生したときにステータス メッセージをローカル イベント ログに記録します。

- エージェントが Active Directory サーバからのデータのポーリングに成功した。
- エージェントが Active Directory サーバへの接続に失敗した。
- エージェントが Active Directory サーバからのデータ取得に失敗した。
- エージェントが Management Center への接続に成功した。
- エージェントが Management Center への接続に失敗した。

エージェントは、タイムスタンプおよび重大度レベルとともに各ステータス メッセージをログに記録します。次の表に、重大度のレベルを低い方から順に示します。

表 2-3　ユーザ エージェントのロギングの重大度レベル

レベル	カラー	説明
デバッグ	グレー	このイベントは、デバッグのためにログに記録されます。 これらのメッセージは、デフォルトでは表示されません。
情報	緑色	このイベントは、エージェントの通常の動作と一致します。
警告	黄色	これは予期しないイベントですが、エージェントの通常の動作は必ずしも中断されません。
エラー	赤色	これは予期しないイベントであり、エージェントの通常の動作は中断されます。

エージェントはローカル イベント ログに加えて Windows アプリケーション ログにもステータス メッセージを記録できます。エージェントは、ローカル イベント ログの内容をコンマ区切り値(CSV)ファイルにエクスポートすることもできます。

ステータス メッセージを保存するかどうかや、ステータス メッセージの保存期間を設定したり、すべてのステータス メッセージのイベント ログをクリアしたりできます。また、デバッグ ステータス メッセージの表示や [メンテナンス(Maintenance)] タブへのアクセスなどのメンテナンス オプションも設定できます。

(注)　デバッグ ステータス メッセージは、7 日間保存された後、イベント ログから削除されます。ステータス メッセージの保存期間を設定したり、イベント ログをクリアしたりしても、デバッグ ステータス メッセージの保存には影響しません。

ユーザ エージェントのロギング設定を構成するには、次の手順を実行します。

アクセス:任意(Any)

ステップ 1　必要に応じて、ユーザ エージェントがインストールされているコンピュータにログインします。

ステップ 2　[スタート(Start)] > [(すべての)プログラム((All)Programs)] > [Cisco] > [Cisco Firepower Agent for Active Directory の設定(Configure Cisco Firepower Agent for Active Directory)] をクリックします。

ステップ 3　[ログ(Logs)] タブをクリックします。

ステップ 4　Cisco TAC から指示された場合は、イベント ログ内のデバッグ ステータス メッセージを表示するために [ログ内のデバッグ メッセージを表示（Show Debug Messages in Log）] を選択し、[メンテナンス（Maintenance）] タブを有効にしますページ。

（注）　このオプションは、Cisco TAC から使用を推奨された場合のみ選択してください。

ステップ 5　Windows アプリケーション ログとローカル イベント ログの両方にデバッグ以外のステータス メッセージを記録するには、[Windows アプリケーション ログにメッセージを記録（Log Messages to Windows Application Log）] を選択します。

Windows アプリケーション ログを表示するには、Windows イベント ビューアを開きます。

ステップ 6　ステータス メッセージがローカル イベント ログに保存されてから自動的に削除されるまでの期間を設定するには、[メッセージのキャッシュ サイズ（Message Cache Size）] ドロップダウン リストから期間を選択します。

ローカル イベント ログに記録されたステータス メッセージは、[メッセージのキャッシュ サイズ（Message Cache Size）] ドロップダウン リストで選択された期間だけ保存された後、削除されます。

（注）　[メッセージのキャッシュ サイズ（Message Cache Size）] の設定は、ローカル イベント ログにのみ影響し、[Windows アプリケーション ログにメッセージを記録（Log Messages to Windows Application Log）] を選択した場合でも Windows アプリケーション ログには影響しません。

ステップ 7　最後の更新後にログに記録された新しいステータス メッセージを表示するには、[更新（Refresh）] をクリックします。

最後の更新後に新しいステータス メッセージがログに記録された場合は、新しいステータス メッセージがあることを示すメッセージが表示されます。更新の結果 250 件を超えるメッセージが表示される場合、最も古いステータス メッセージが [ログ（Logs）] タブ ページから削除されます。250 件を超えるメッセージを表示するには、ログをエクスポートします。詳細については、ステップ 8 を参照してください。

ステップ 8　ローカル イベント ログの内容をコンマ区切り値（CSV）ファイルにエクスポートするには、[ログのエクスポート（Export Logs）] をクリックします。

コンマ区切り値（CSV）ファイルには、すべてのイベント ログ ステータス メッセージとデバッグ メッセージが格納されます。

ステップ 9　ローカル イベント ログからデバッグ以外のすべてのステータス メッセージを削除するには、[イベント ログのクリア（Clear Event Log）] をクリックします。

エージェントがメッセージを削除したことを示すステータス メッセージを除き、ローカル イベントがクリアされます。

ステップ 10　設定の変更を保存してエージェントに適用するには、[保存（Save）] をクリックします。

ステップ 11　次の選択肢があります。

- エージェントの全般的な設定を構成するには、[全般（General）] タブを選択します。詳細については、ユーザ エージェントの全般的な設定の構成（2-33 ページ）を参照してください。
- エージェントを設定する場合は、表 2-1（2-22 ページ）で説明されているいずれかの操作を実行します。

ユーザ エージェントの全般的な設定の構成

ライセンス:FireSIGHT または該当なし

[全般(General)] タブには、ユーザ エージェントの基本設定が含まれています。エージェントがログイン データを報告するときに Management Center に報告されるエージェント名を変更できます。また、エージェント サービスの開始と停止、ログオフ チェックの頻度の変更、および現在のサービス ステータスの表示もできます。

ユーザ エージェントの全般的な設定を構成するには、次の手順を実行します。

アクセス:任意(Any)

ステップ 1　エージェントがインストールされているコンピュータで、[スタート(Start)] > [プログラム(Programs)] > [Cisco] > [Active Directory 用の Cisco FirePOWER ユーザ エージェントの設定(Configure Cisco Firepower User Agent for Active Directory)] を選択します。

ステップ 2　エージェント サービスを開始するには、開始ボタン( )をクリックします。

ステップ 3　エージェント サービスを停止するには、停止ボタン( )をクリックします。

ステップ 4　(オプション)[エージェント名(Agent Name)] でエージェント名を変更します。デフォルトのエージェント名は `Cisco FUAfAD` です。文字、数字、下線(_)、およびハイフン(-)を入力できます。

ステップ 5　(オプション)エージェントがログオフ データを確認する頻度を変更し、[ログアウト確認頻度(Logout Check Frequency)] リストから期間を選択します。ログオフ データのチェックを無効にするには、**0** を選択します。

ステップ 6　(オプション)エージェントのスケジュールの優先度を変更するには、[優先度(Priority)] リストからレベルを選択します。エージェントが大量のユーザアクティビティをモニタして取得し、パフォーマンスに影響を与えている場合のみ、[高(High)] を選択します。

ステップ 7　設定を保存するには、[保存(Save)] をクリックします。

ステップ 8　エージェントを設定する場合は、表 2-1(2-22 ページ)で説明されているいずれかの操作を実行します。

ユーザ エージェントのメンテナンス設定の構成

ライセンス:FireSIGHT または該当なし

エージェントは、構成設定に加えて、ユーザと IP アドレスのマッピング情報、ローカル イベント ログ、およびレポート状態情報を SQL CE データベースに保存します。エージェントの [メンテナンス(Maintenance)] タブでは、メンテナンスのためにデータベースの一部をクリアできます。キャッシュされているユーザと IP アドレスのマッピング情報およびローカル イベント ログ情報をクリアできます。レポート状態のキャッシュもクリアできますが、その場合は、設定された Active Directory サーバの手動ポーリングが強制実行されます。

注意　サポートから指示されないかぎり、[メンテナンス(Maintenance)] タブ ページの設定は変更*しないでください。*

ユーザ エージェントのメンテナンス設定を構成するには、次の手順を実行します。

アクセス：任意（Any）

ステップ 1　エージェントがインストールされているコンピュータで、[スタート（Start）] > [プログラム（Programs）] > [Cisco] > [Active Directory 用の Cisco FirePOWER ユーザ エージェントの設定（Configure Cisco Firepower User Agent for Active Directory）] を選択します。

ステップ 2　[ログ（Logs）] タブをクリックします。

ステップ 3　[ログ内のデバッグ メッセージを表示（Show Debug Messages in Log）] をクリックして [メンテナンス（Maintenance）] タブを有効にします。

ステップ 4　[メンテナンス（Maintenance）] タブをクリックします。

ステップ 5　保存されているすべてのユーザと IP アドレスのマッピング データをクリアするには、[ユーザ マッピング データ キャッシュをクリア（Clear user mapping data cache）] をクリックします。

エージェントのローカル データベースから、保存されているすべてのユーザと IP アドレスのマッピング データが削除されます。エージェントのローカル データベースをクリアしても、Management Center のデータベースに保存されているユーザと IP アドレスのマッピング データは影響を受けません。

ステップ 6　保存されているすべてのログイン イベント データをクリアするには、[ログオン イベント ログ キャッシュをクリア（Clear logon event log cache）] をクリックします。

ステップ 7　エージェントが設定済みの Management Center にログインおよびログオフ情報を最後に報告した時間に関するデータをクリアするには、[レポート ステート キャッシュをクリア（Clear reporting state cache）] をクリックします。

エージェントは設定済みの Management Center にログインおよびログオフ情報を最後に報告した時間に関するすべての情報を削除します。次のポーリング間隔の開始時に、エージェントは設定されたすべての Active Directory サーバを手動でポーリングし、[Active Directory サーバの最大ポーリング時間（Active Directory Server Max Poll Length）] フィールドで定義された期間内の情報を取得します。詳細については、ユーザ エージェントの Active Directory サーバ接続の設定（2-23 ページ）を参照してください。

ステップ 8　ログに記録されるデバッグ メッセージの詳細レベルを設定するには、[デバッグ ログ レベル（Debug Log Level）] ドロップダウン リストからロギングの詳細レベルを選択します。

ステップ 9　エージェントを設定する場合は、表 2-1（2-22 ページ）で説明されているいずれかの操作を実行します。

ユーザ エージェントのトラブルシューティング

続くいくつかのセクションでは、ユーザ エージェントの使用時に発生する可能性がある問題の解決策について説明します。

- Management Center に接続できない（2-35 ページ）
- ユーザ エージェントが応答しない（2-38 ページ）
- ユーザ エージェントが一部のログインを表示しない（2-39 ページ）
- ユーザ エージェントがリアルタイム イベントを処理しない（2-39 ページ）
- ユーザ エージェントにユーザ ログオフ イベントが表示されない（2-40 ページ）
- 同じネットワーク内のユーザ エージェントと TS エージェント（2-40 ページ）

Management Center に接続できない

このセクションでは、ユーザ エージェントの Firepower Management Center への接続を妨げる可能性のある次の問題について説明します。

- ユーザ エージェントがアイデンティティ ソースではない（2-35 ページ）
- 不正な Windows の暗号（2-36 ページ）

ユーザ エージェントがアイデンティティ ソースではない

ユーザ エージェントの [Firepower Management Centers] タブ ページで、Management Center のステータスが [使用不可（unavailable）] である場合は、Management Center でアイデンティティ ソースとしてユーザ エージェントを追加したことを確認してください。ユーザ エージェント設定の詳細については、*コンフィギュレーション ガイド*を参照してください。

バージョン 6.X の Management Center でユーザ エージェント アイデンティティ ソースを確認するには、次の手順を実行します。

ステップ 1　管理者として Management Center にログインします。

ステップ 2　[システム（System）] > [統合（Integration）] をクリックします。

ステップ 3　[アイデンティティの送信元（Identity Sources）] タブをクリックします。

ステップ 4　[ユーザ エージェント（User Agent）] をクリックします。

ステップ 5　ユーザ エージェントが定義されていることを確認し、その IP アドレスを確認します。何らかの変更を行った場合は、[保存（Save）] をクリックします。

ステップ 6　ユーザ エージェントの [Firepower Management Centers] タブ ページで Management Center のステータスを再度確認します。

Management Center が正しく設定されていて、それでも接続できない場合は、次のことを試してみます。

- ユーザ エージェントで設定した Management Center のホスト名または IP アドレスを再確認します。
- Management Center にホスト名でアクセスしている場合は、`nslookup hostname` コマンドを使用して、ホスト名が IP アドレスに解決されることを確認します。
- Management Center に IP アドレスでアクセスする場合、`ping ip-address` コマンドを使用して、それがユーザ エージェントのコンピュータでアクセス可能であることを確認します。

不正な Windows の暗号

ユーザ エージェントがインストールされている Windows マシンに適切な暗号がインストールされていない場合は、次の現象が発生します。

- ユーザ エージェントは、ユーザ エージェントの [Firepower Management Center] タブページで、Firepower management Center を [使用不可（unavailable）] として表示します。
- Firepower Management Center は、Active Directory ドメイン コントローラからユーザとグループをダウンロードできます。

この状況は比較的まれで、Windows マシンの暗号を制限している場合にのみ適用されます。

使用可能な暗号のリストを表示するには、次のようにします。

ステップ 1　ユーザ エージェント マシンにログインします。

ステップ 2　コマンド プロンプトで、`gpedit.msc` と入力し、Enter キーを押します。

ステップ 3　[コンピュータの設定（Computer Configuration）] > [管理用テンプレート（Administrative Templates）] > [ネットワーク（Network）] > [SSL 構成設定（SSL Configuration Settings）] の順にクリックします。

ステップ 4　[SSL 構成設定（SSL Configuration Settings）] で、[SSL 暗号スイートの順位（SSL Cipher Suite Order）] を選択します。

ステップ 5　暗号リストを設定して、次のセクションに示す 1 つ以上の暗号を含めます。

Firepower Management Center でサポートされている暗号

Firepower Management Center は、ユーザ エージェントと接続するために次の暗号をサポートしています。暗号は OpenSSL 形式で示されています。Windows の暗号は通常、RFC 形式で記載されています。暗号名を変換するには、`https://testssl.sh` サイトの『RFC mapping list』を参照してください。

注意　すべての暗号が安全なわけではないため、どの暗号を選択するかを決定する際には注意してください。安全な暗号の詳細については、Open Web Application Security Project（OWASP）などのリソースを参照してください。たとえば、『TLS Cipher String Cheat Sheet』などを参照できます。

サポート対象の暗号方式は次のとおりです。

AES256-GCM-SHA384
AES256-SHA
AES256-SHA256
CAMELLIA256-SHA
DES-CBC3-SHA
ECDH-ECDSA-AES256-GCM-SHA384
ECDH-ECDSA-AES256-SHA
ECDH-ECDSA-AES256-SHA384
ECDH-ECDSA-DES-CBC3-SHA
ECDH-RSA-AES256-GCM-SHA384
ECDH-RSA-AES256-SHA
ECDH-RSA-AES256-SHA384
ECDH-RSA-DES-CBC3-SHA
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA384
ECDHE-ECDSA-DES-CBC3-SHA
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-DES-CBC3-SHA
EDH-DSS-DES-CBC3-SHA
EDH-RSA-DES-CBC3-SHA
PSK-3DES-EDE-CBC-SHA
PSK-AES256-CBC-SHA
SRP-DSS-3DES-EDE-CBC-SHA
SRP-DSS-AES-128-CBC-SHA
SRP-DSS-AES-256-CBC-SHA
SRP-RSA-3DES-EDE-CBC-SHA
SRP-RSA-AES-128-CBC-SHA
SRP-RSA-AES-256-CBC-SHA

ユーザ エージェントが応答しない

ユーザ エージェントからデータが送られてきていないと思われる場合は、次のいずれかの操作を行うことができます。

- ユーザ エージェントのコンピュータにログインし、そのステータスを確認します。詳細については、ユーザ エージェントの全般的な設定の構成（2-33 ページ）を参照してください。
- Management Center でユーザ エージェントの正常性ポリシーをセットアップして、そのステータスをモニタします。これについては続く手順で説明しています。

  ユーザ エージェントの正常性ポリシーにより、Management Center がユーザ エージェントからハートビートを受信しない場合には通知が出されます。詳細については、コンフィギュレーション ガイドを参照してください。

6.X の Management Center でユーザ エージェントの正常性ポリシーを設定するには、次の手順を実行します。

ステップ 1　Management Center に、管理者特権またはメンテナンス ユーザ権限を持つユーザとしてログインします。

ステップ 2　[システム（System）] > [正常性（Health）] > [ポリシー（Policy）] をクリックします。

ステップ 3　[ポリシーの作成（Create Policy）] をクリックします。

ステップ 4　[ポリシーの作成（Create Policy）] タブで、次の情報を入力します。

- [ポリシーのコピー（Copy Policy）] リスト。**デフォルトの正常性ポリシー**などの任意のポリシーを選択します。
- [新規ポリシー名（New Policy Name）] フィールド：このポリシーを識別する名前を入力します。
- [新規ポリシーの説明（New Policy Description）] フィールド：オプションのポリシーの説明を入力します。

  新規ポリシーが表示されます。

ステップ 5　（編集）をクリックします。

ステップ 6　左側の列で、[ユーザ エージェントのステータス モニタ（User Agent Status Monitor）] をクリックします。

ステップ 7　右側の列で、[オン（On）] をクリックします。

ステップ 8　ページの下部で、[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。

ステップ 9　ポリシー名の横にある （適用）をクリックします。

ステップ 10　画面の指示に従って、管理対象デバイスにポリシーを適用します。

ステップ 11　任意の時点でユーザ エージェントをモニタするには、[正常性（Health）] > [モニタ（Monitor）] をクリックするか、または Management Center の （モニタ）アイコンに表示されるメッセージを監視します。

ユーザ エージェント ハートビートが管理対象デバイスによって検出されない場合、次のようなメッセージが表示されます。

```
Some user agents are not up-to-date
```

ユーザ エージェントが一部のログインを表示しない

ユーザ エージェントは、IP アドレスごとにユーザ名を追跡します。同じユーザが同じ IP アドレスに複数回ログインするとしても、そのユーザのユーザ ログイン イベントが Management Center に表示されるのは 1 回のみです。

次のシナリオは、1 ユーザによる複数回のユーザ ログイン イベントを示しています。

- ユーザが別々の IP アドレス（デスクトップと携帯電話など）からログインする。
- ユーザ `patricia.nolan` が次の IP アドレスから並びの順序どおりログインする。
  - 192.0.2.102
  - 192.0.2.210
  - 192.0.2.102

  `patricia.nolan` がいずれかの IP アドレスからログアウトしても問題ありません。Management Center は固有の IP アドレスごとに 1 つずつ、少なくとも 2 つのログインイベントを報告します（言い替えると、Management Center は最後のログインを、それが最初のものと同じ IP アドレスからであるため報告しません）。

ユーザ エージェントがリアルタイム イベントを処理しない

リアルタイム イベントを Active Directory サーバから処理できるようにするために、ユーザ エージェントは、Active Directory サーバへのリモート プロシージャ コール（RPC）アクセスを必要とします。延長期間のリアルタイム処理のステータスが、ユーザ エージェントの [Active Directory サーバ（Active Directory Servers）] タブ ページで `unknown` または `unavailable` と表示される場合、ユーザ エージェント ログでエラーを探して、このセクションで説明されている他の提案を試してみてください。

リアルタイム処理の問題をトラブルシューティングするには、次の手順を実行します。

ステップ 1　必要に応じて、ユーザ エージェントがインストールされているコンピュータにログインします。

ステップ 2　[スタート（Start）] > [（すべての）プログラム（（All）Programs）] > [Cisco] > [Cisco Firepower Agent for Active Directory の設定（Configure Cisco Firepower Agent for Active Directory）] をクリックします

ステップ 3　[ログ（Logs）] タブをクリックします。

ステップ 4　[ログ内のデバッグ メッセージを表示（Show debug messages in log）] をオンにします。

ステップ 5　ログ メッセージを確認して、[ログのエクスポート（Export logs）] をクリックし、ログ メッセージをファイルにエクスポートします。

ステップ 6　次のようなメッセージを見つけます。

```
"error","[2317] - Unable to attach event listener to host or IP address. Check firewall
settings on AD server. RPC server is unavailable
```

上記のメッセージは、Active Directory サーバのファイアウォールの設定に問題があることを示しています。ユーザ エージェントに分散コンポーネント オブジェクト管理（DCOM）へのアクセスを許可する（2-13 ページ）に記載されている手順を確認して、もう一度やり直してください。

ファイアウォールを問題箇所として分離するには、必要に応じて Active Directory サーバのファイアウォールを数分間無効にして、ユーザ エージェントがリアルタイム イベントを処理できるかどうかを確認してください。

ステップ 7　ユーザ エージェントで Active Directory サーバ構成の削除と再追加を試行してください。

ユーザ エージェントにユーザ ログオフ イベントが表示されない

Management Center でユーザ ログオフ イベントが表示されない場合は、WMI にすべてのドメイン コンピュータ上のファイアウォールの通過を許可していることを確認します。詳細については、ドメイン コンピュータの設定（2-6 ページ）を参照してください。

同じネットワーク内のユーザ エージェントと TS エージェント

ターミナル サービス（TS）エージェントとユーザ エージェントの両方を使用する場合、ユーザ エージェントから TS エージェントの IP アドレスを除外することによって、重大ではないエラーのログを回避できます。TS エージェントとユーザ エージェントの両方によって同じユーザが検出されると、重大ではないエラーがログに書き込まれます。

詳細については、ユーザ エージェントの除外アドレス設定の構成（2-29 ページ）を参照してください。