FireSIGHT ユーザ エージェント構成ガイド

バージョン 2.2
2014 年 6 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、および推奨事項は、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になります。

Cisco Systems, Inc.
www.cisco.com
シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は当社の
Web サイトをご覧ください
www.cisco.com/go/offices

【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 ライセンスおよび限定保証は、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およびソフトウェアは、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. (1110R)

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。

© 2015 Cisco Systems, Inc. All rights reserved.

CHAPTER 1 はじめに 1-1
ユーザ エージェント バージョン 2.2 の主な変更点 1-1
ユーザ エージェントについて 1-2
ユーザ エージェントの機能について 1-2
レガシー エージェントのサポートについて 1-4
バージョン 5.x のエージェントとアクセス制御について 1-4
ユーザ データベースについて 1-5
ユーザ アクティビティ データベースについて 1-5
アクセス制御対象ユーザ データベースについて 1-6
ユーザ データ収集の制限事項 1-7

CHAPTER 2 ユーザ エージェントのセットアップ 2-1
バージョン 4.x の 防御センター に接続する準備 2-2
バージョン 5.x の防御センターに接続する準備 2-3
防御センターでのユーザ エージェントの設定 2-3
ユーザ アクセス制御を許可する LDAP 接続のセットアップ 2-4
Active Directory サーバに接続する権限の設定 2-4
アイドル セッション タイムアウトの有効化 2-6
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 エージェント設定のバックアップ 2-8
ユーザ エージェントのインストール 2-9
ユーザ エージェントの設定 2-10
ユーザ エージェントの Active Directory サーバ接続の設定 2-11
ユーザ エージェントの防御センター接続の設定 2-14
ユーザ エージェントの除外ユーザ名設定の構成 2-16
ユーザ エージェントの除外アドレス設定の構成 2-17
ユーザ エージェントのロギング設定の構成 2-18
ユーザ エージェントの全般的な設定の構成 2-20
ユーザ エージェントのメンテナンス設定の構成 2-20

はじめに

バージョン 2.2 のユーザ エージェントは、FireSIGHT 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。FireSIGHT システム バージョン 5.x とともにエージェントを使用する場合は、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 Microsoft Active Directory サーバを監視し、LDAP 経由で認証されたログインとログオフをレポートします。FireSIGHT システムでは、これらのレコードと、管理対象デバイスがネットワーク トラフィックを直接監視することで収集したデータが統合されます。

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 バージョン 2.2 の主な変更点（1-1 ページ）
- ユーザ エージェントについて（1-2 ページ）

ユーザ エージェント バージョン 2.2 の主な変更点

ユーザ エージェントをバージョン 2.2 にアップグレードする場合は、次の変更点に注意してください。

- バージョン 2.0 からバージョン 2.1.1 までのエージェントを削除するときは、データベースをバックアップして設定を保持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（2-8 ページ）」を参照してください。

  一方、バージョン 2.2 のエージェントは将来のアップグレードのために設定を自動的に保持します。バージョン 2.2 のエージェントをアンインストールおよび再インストールする場合は、データベースを手動でバックアップする必要はありません。
- エージェントは、設定された Active Directory サーバへのログインを検出できます。接続を設定するときは、[Local Login IP Address] フィールドから IP アドレスを選択します。
- 設定された Active Directory サーバ接続では、最大 64 文字のユーザ パスワードがサポートされます。
- エージェントは、1 分および 5 分の [Active Directory Server Max Poll Length] をサポートします。最大ポーリング時間を短くすると、リアルタイム モニタリングのパフォーマンスとログアウト検出が向上します。

ユーザ エージェントについて

この項では、FireSIGHT システムにユーザ ディスカバリ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 ディスカバリおよびネットワーク ディスカバリ（バージョン 4.x のマニュアルでは RNA）に関連するすべての概念の詳細については、アプライアンスで実行されている FireSIGHT システムのバージョンの『*FireSIGHT システム ユーザ 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 エージェントの機能について（1-2 ページ）
- レガシー エージェントのサポートについて（1-4 ページ）
- バージョン 5.x のエージェントとアクセス制御について（1-4 ページ）
- ユーザ データベースについて（1-5 ページ）
- ユーザ アクティビティ データベースについて（1-5 ページ）
- アクセス制御対象ユーザ データベースについて（1-6 ページ）
- ユーザ データ収集の制限事項（1-7 ページ）

ユーザ エージェントの機能について

FireSIGHT システムは、組織の LDAP サーバからユーザ アイデンティティ情報とユーザ アクティビティ情報の両方を取得します。ユーザ エージェントでは、Microsoft Active Directory サーバに対して Active Directory のクレデンシャルを認証するユーザを監視できます。

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 2003、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。また、サポートされるいずれかのオペレーティング システムを実行する Active Directory サーバにインストールすることもできます。

各エージェントは、定期的にスケジュールされたポーリングまたはリアルタイム モニタリングを通して、暗号化されたトラフィックを使用したログインを監視できます。ログインは、ユーザがワークステーションで、または、リモート デスクトップ ログイン経由でコンピュータにログインしたときに Active Directory サーバによって生成されます。

エージェントは、ユーザ ログオフを監視して報告することもできます。ログオフは、ホスト IP アドレスからログアウトしたユーザをエージェントが検出したときに、エージェント自体によって生成されます。また、ログオフは、ホストにログインしたユーザが変わったことをエージェントが検出したときにも生成され、その後で Active Directory サーバがユーザが変わったことを報告します。ログオフ データとログイン データを組み合わせれば、ネットワークにログインしたユーザのより完全なビューが形成されます。

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時間間隔でユーザ 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、繰り返し発生する共有サーバ（ファイル共有やプリント サーバなど）へのログインを除外したり、トラブルシューティングのためにマシンにログインするユーザを除外したりするのに役立ちます。

最大 5 つのサーバを監視し、その暗号化されたデータを 5 つの防御センターに送信するように、各エージェントを設定できます。

エージェントは、検出されたすべてのログインおよびログオフのうち、除外されたユーザ名または IP アドレスを含まないレコードを防御センターに送信します。防御センターはこれらのレコードをユーザ アクティビティとして記録し、報告します。エージェントは、防御センターのバージョンを検出し、適切なデータ形式でログイン レコードを送信します。これにより、管理対象デバイスで直接検出されたユーザ アクティビティが補完されます。バージョン 5.x の FireSIGHT システム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。

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 の資格情報に対して認証されるときに、ユーザを監視します。バージョン 2.2 のユーザ 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 アカウントのログインに加えて、ユーザ ログオフとユーザがログオフしたリモート デスクトップ セッションを検出します。

検出されるログインのタイプに応じて、エージェントによるログインの報告方法と、ホスト プロファイルでのログインの表示方法が決まります。ホストに対して*信頼できるユーザ ログイン*が行われると、ホスト IP アドレスにマッピングされている現在のユーザが新しいログインのユーザに変更されます。その他のログインでは、現在のユーザは変更されません。ただし、ホスト上の既存のユーザがホストに対して信頼できるユーザ ログインを行わなかった場合にのみ、ホストの現在のユーザが変更されます。そのような場合、予期されるユーザがログインしなくなったときに、そのユーザのログオフが生成されます。ネットワーク ディスカバリによって検出されたユーザ ログインでは、ホスト上の既存のユーザがホストに対して信頼できるユーザ ログインを行わなかった場合にのみ、ホストの現在のユーザが変更されます。エージェントによって検出されたログインは、ネットワーク マップに対して次のような影響を与えます。

- ユーザによるホストへの対話型ログインまたはリモート デスクトップ ログインを検出した場合、エージェントはそのホストに対する信頼できるユーザ ログインを報告し、ホストの現在のユーザを新しいユーザに変更します。
- ファイル共有認証のログインを検出した場合、エージェント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。
- エージェントが除外されたユーザ名からのログインを検出した場合は、防御センターにログインを報告しません。

ログインまたはその他の認証が実行されると、エージェントは次の情報を防御センターに送信します。

- ユーザの LDAP ユーザ名
- 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、およびコンピュータ アカウントのログインでエージェントが IPv6 アドレスを報告する場合はリンクローカル 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 アドレスを防御センターに報告します。

防御センターは、ログインとログオフの情報をユーザ アクティビティとして記録します。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のリストに照ら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は、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は、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活動は報告されませんが、関連するユーザ活動が報告される場合があります。エージェントがマシンに対するユーザ ログインを検出してから、2 人目のユーザ ログインを検出し、その 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から除外されていた場合は、1 人目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、除外されたユーザはホストにログインしていますが、IP アドレスにユーザはマッピングされません。

エージェントによって検出されるユーザ名については、次の制限事項に注意してください。

- バージョン 5.0.2+ 防御センターに報告されるドル記号（$）で終わるユーザ名は、ネットワーク マップを更新しますが、ユーザ ログインとして表示されません。エージェントは、他のバージョンの防御センターに対してドル記号文字（$）で終わるユーザ名を報告しません。
- 防御センターでは、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。

防御センターで保存できる検出済みユーザの総数は、RNA または FireSIGHT ライセンスによって異なります。ライセンス 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、手動でデータベースから古いユーザやアクティブでないユーザを削除するか、データベースからすべてのユーザをパージする必要があります。

レガシー エージェントのサポートについて

Active Directory LDAP 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 防御センター 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は変わっていません。それらは Active Directory サーバ上にインストールして、1 つの防御センターにだけ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 モジュールはレガシー エージェントをサポートしないため、レガシー エージェントが接続されている防御センター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、できるだけ早くバージョン 2.2 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 LDAP サーバが使用されている場合は、ユーザ エージェントをインストールし、Active Directory サーバを介してユーザ アクティビティを監視することをシスコでは推奨しています。バージョン 5.x でユーザ制御を実行する場合は、ユーザ エージェントをインストールして使用する**必要があります**。エージェントによってユーザと 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。1 つのエージェントを使用して、最大 5 つの Active Directory サーバでユーザ アクティビティを監視できます。

エージェントを使用するには、エージェントに接続された各防御センターと監視対象 LDAP サーバ間の接続を設定する必要があります。この接続は、ユーザ エージェントによってログインとログオフが検出されたユーザのメタデータを取得するために使用されるだけでなく、アクセス制御ルール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。ユーザ ディスカバリのために LDAP サーバを設定する方法の詳細については、『*FireSIGHT システム ユーザ ガイド*』を参照してください。

注　Microsoft Active Directory サーバにインストールされているレガシー エージェントは、Active Directory の資格情報で認証されるユーザも監視します。ただし、今後のリリースでレガシー エージェントのサポートが終了する場合に備えて、できるだけ早くバージョン 2.2 のユーザ エージェントに移行してください。

ユーザ データベースについて

ライセンス: FireSIGHT

ユーザ データベースには、管理対象デバイスまたはユーザ エージェントで検出された各ユーザのレコードが格納されます。防御センターで保存できる検出済みユーザの総数は、FireSIGHT ライセンスによって異なります。ライセンスされた制限に達すると、ほとんどの場合、このシステムはデータベースへの新しいユーザの追加を停止します。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消去する必要があります。

ただし、信頼できるユーザ ログインは優先されます。制限に達しているときに、以前に検出されていないユーザの信頼できるユーザ ログインをシステムが検出すると、長時間にわたってアクティブでない状態のユーザをシステムが削除し、新しいユーザに置き換えます。

ユーザ データベースの内容は、防御センターの Web インターフェイスを使用して表示できます。検出済みユーザの表示、検索、および削除については、『*FireSIGHT システム ユーザ ガイド*』を参照してください。

ユーザ アクティビティ データベースについて

ライセンス: FireSIGHT

ユーザ アクティビティ データベースには、ネットワーク上のユーザ アクティビティのレコードが格納されます。これらのアクティビティは、ユーザ エージェントが監視している Active Directory LDAP サーバとの接続から取得されるか、またはネットワーク ディスカバリによって取得されます。このシステムは、次の場合にイベントをログに記録します。

- 個別のログインまたはログオフを検出したとき
- 新しいユーザを検出したとき
- 手動でユーザが削除されたとき
- データベース内に存在しないユーザをシステムが検出したものの、FireSIGHT のライセンス制限に達したためにそのユーザを追加できなかったとき

システムによって検出されたユーザ アクティビティは、防御センターの Web インターフェイスを使用して表示できます。ユーザ アクティビティの表示、検索、および削除については、『*FireSIGHT システム ユーザ ガイド*』を参照してください。バージョン 2.2 の FireSIGHT システム ユーザ エージェントを使用してバージョン 5.x の防御センターに LDAP ログイン データを送信する場合は、エージェントを接続する各防御センターで各エージェントの接続を設定する必要があります。その接続によって、エージェントは防御センターとのセキュアな接続を確立し、ログイン データを送信できるようになります。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 データは防御センターに報告されません。

また、ユーザ アクセス制御を実装する予定がある場合は、設定済みのユーザ認識パラメータを使用して、データを収集する各 Microsoft Active Directory サーバへの接続をセットアップする必要があります。

アクセス制御対象ユーザ データベースについて

ライセンス: Control

アクセス制御対象ユーザ データベースには、FireSIGHT システムでユーザ制御を実行するためのアクセス制御ルールで使用できるユーザとグループが格納されます。これらのユーザは、次の 2 つのタイプに分かれます。

- *アクセス制御対象ユーザ*は、ユーザ制御を実行するためのアクセス制御ルールに追加できるユーザです。防御センター と LDAP サーバ間の接続を設定する際は、アクセス制御対象ユーザが属すべきグループを指定します。
- *非アクセス制御対象ユーザ*とは、その他の検出されたユーザです。

防御センター に保存できるアクセス制御対象ユーザの総数は、FireSIGHT ライセンスによって異なります。

『*FireSIGHT システム User Guide*』の説明に従って、防御センター と LDAP サーバ間の接続を設定するときに、アクセス制御対象ユーザが属すべきグループを指定します。

バージョン 2.2 の FireSIGHT システム ユーザ エージェントを使用して、バージョン 5.x の防御センターに LDAP ログインおよびログオフ データを送信する場合は、エージェントを接続する各防御センターで各エージェントの接続を設定する必要があります。その接続によって、エージェントは防御センターとのセキュアな接続を確立し、ユーザ アクティビティ データを送信できるようになります。

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ユーザ アクティビティ データは防御センターに報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。

また、ユーザ アクセス制御を実装する予定がある場合は、設定済みのユーザ認識パラメータを使用して、データを収集する各 Microsoft Active Directory サーバへの接続をセットアップする必要があります。

ユーザ データ収集の制限事項

ライセンス: FireSIGHT

次の表に、ユーザ データ収集の制限事項（一般的な制限またはエージェントに特に関連する制限）を示します。

表 1-1　　ユーザ データ収集の制限事項

制限事項	説明
ユーザ制御	ユーザ制御を実行するには、組織で Microsoft Active Directory LDAP サーバを使用している必要があります。システムは、Active Directory からアクセス コントロール ルールで使用可能なユーザとグループを取得し、Active Directory サーバにインストールされたユーザ エージェントから報告されたログインとログオフを使用してユーザを IP アドレスに関連付けます。
ログインの検出	エージェントは、バージョン 5.2 以降を実行している防御センターに対して 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防御センターに対して信頼できないユーザ ログインと NetBIOS ログインを報告します。 また、エージェントは、実際のユーザ名からの権限のあるログインを、バージョン 4.10.x+ を実行している防御センターに報告します。 Active Directory サーバへのログインを検出する場合は、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（2-11 ページ）」を参照してください。 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た場合、エージェントはそのホストから適切にログインを検出できないことがあります。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（2-6 ページ）を参照してください。
ログオフの検出	エージェントは、検出したログオフをバージョン 5.2+ 防御センターに報告します。 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実際の時間とは一致しない場合があります。 ログオフは、ユーザがホスト IP アドレスからログアウトしたことをエージェントが検出したときに、エージェント自体によって生成されます。また、ログオフは、ホストにログインしたユーザが変わったことをエージェントが検出したときにも生成され、その後で Active Directory サーバがユーザが変わったことを報告します。
リアルタイム データ検索	Active Directory サーバは、Windows Server 2008 または Windows Server 2012 を実行している必要があります。

表 1-1　ユーザ データ収集の制限事項（続き）

制限事項	説明
複数のユーザによる同じホストへの複数のログイン	システムは、特定のホストにログインするユーザは一度に 1 人だけであり、ホストの現在のユーザが最後の権限のあるユーザ ログインであると見なします。権限のないログインだけがホストにログインしている場合は、最後にログインしたものが現在のユーザと見なされます。複数のユーザがリモート セッション経由でログインしている場合は、Active Directory サーバによって報告された最後のユーザが防御センターに報告されるユーザです。
同じユーザによる同じホストへの複数のログイン	システムは、ユーザが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。あるユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。 ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。
Unicode 文字	ユーザ インターフェイスは Unicode 文字を含むユーザ名を正しく表示しない場合があります。 エージェントは、Unicode 文字を含むユーザ名をバージョン 4.10.x 防御センターに報告しません。
ユーザ データベース内の LDAP ユーザ アカウント	ユーザ認識または RUA LDAP サーバで LDAP ユーザを削除または無効化するか、あるいは防御センターに報告する対象からユーザ名を除外した場合、防御センターはユーザ データベースからそのユーザを削除せず、そのユーザは引き続きデータベースに登録されるユーザのライセンス制限に照らしてカウントされます。ユーザをデータベースから手動でパージする必要があります。バージョン 5.x では、ユーザ ライセンス制限がアクセス制御対象ユーザにも同時に適用されることに注意してください。アクセス制御対象ユーザのユーザ カウントは、LDAP 設定により取得されるユーザ数に応じて異なります。

ユーザ エージェントのセットアップ

バージョン 2.2 のユーザ エージェントを使用して Microsoft Active Directory サーバからユーザ ログイン データを収集し、それを防御センターに送信するには、ユーザ エージェントをインストールし、それを各防御センターおよび Microsoft Active Directory サーバに接続して、全般的な設定を構成する必要があります。

ユーザ エージェントをセットアップするには、以下を行います。

アクセス: Admin

ステップ 1 エージェントをインストールするコンピュータの IP アドレスから行われるエージェント接続を許可するように、各防御センターを設定します。詳細については、以下を参照してください。

- バージョン 4.x の 防御センター に接続する準備（2-2 ページ）
- バージョン 5.x の防御センターに接続する準備（2-3 ページ）

注 バージョン 5.x の防御センターを使用してユーザ制御を実行する場合は、防御センターでユーザ認識パラメータを使用して Microsoft Active Directory サーバへの LDAP 接続を設定する必要もあります。

ステップ 2 エージェントが Active Directory サーバに接続するのに必要な Windows とユーザの権限を設定します。詳細については、Active Directory サーバに接続する権限の設定（2-4 ページ）を参照してください。

ステップ 3 必要に応じて、アイドル状態のリモート セッションに対するタイムアウトを有効にします。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（2-6 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、Active Directory サーバに接続する権限の設定（2-4 ページ）を参照してください。

ステップ 5 必要に応じて、旧バージョンのユーザ エージェントの構成設定を保持するために、エージェント データベースのバックアップを実行します。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（2-8 ページ）を参照してください。

ステップ 6 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（2-9 ページ）を参照してください。

ステップ 7 最大で 5 つの Microsoft Active Directory サーバへの接続を設定します。必要に応じて、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（2-11 ページ）を参照してください。

ステップ 8　防御センター への接続を、最大で 5 つ設定します。詳細については、ユーザ エージェントの防御センター接続の設定（2-14 ページ）を参照してください。

ステップ 9　必要に応じて、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、ユーザ エージェントの除外ユーザ名設定の構成（2-16 ページ）およびユーザ エージェントの除外アドレス設定の構成（2-17 ページ）を参照してください。

ステップ 10　必要に応じて、エージェントの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（2-18 ページ）を参照してください。

ステップ 11　必要に応じて、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（2-20 ページ）を参照してください。

ステップ 12　[Save] をクリックして、エージェントの設定を保存します。

注意　サポートから指示されないかぎり、エージェントのメンテナンス設定は変更しないでください。

バージョン 4.x の 防御センター に接続する準備

ユーザ エージェントを使用して LDAP ユーザのログイン情報を収集する場合、最初のステップとして、Active Directory サーバに接続するエージェントからの接続を許可するように、各防御センターを設定します。この項では、バージョン 4.x の防御センターでエージェント接続を承認する手順について説明します。

ユーザ エージェントに接続するように防御センターを設定するには、以下を行います。

アクセス: Admin

ステップ 1　[Operations] > [Configuration] > [RUA] を選択します。

ステップ 2　[Add RUA Agent] をクリックします。

ステップ 3　[Name] フィールドに、エージェントの識別に役立つ名前を入力します。

ステップ 4　[Hostname or IP address] フィールドに、ユーザ エージェントを配置するコンピュータの IP アドレスまたはホスト名を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように防御センターを設定することはできません。

注　IPv6 アドレスまたは IPv6 アドレスに解決できないホスト名を持つユーザ エージェントは追加できません。

ステップ 5　[Add RUA Agent] をクリックします。

設定した IP アドレスでエージェントからの接続を許可するように防御センターが設定されます。

ヒント　防御センター とエージェント間の接続を削除するには、削除する接続の横にある [Delete] をクリックします。

ステップ 6　Active Directory サーバに接続する権限の設定（2-4 ページ）に進みます。

バージョン 5.x の防御センターに接続する準備

バージョン 2.2 のユーザ エージェントを使用してバージョン 5.x の防御センターに LDAP ログイン データを送信する場合は、エージェントが接続する各防御センターで各エージェントの接続を設定する必要があります。その接続によって、エージェントは防御センター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。

また、ユーザ アクセス制御を実装する予定がある場合は、設定済みのユーザ認識パラメータを使用して、データを収集する各 Microsoft Active Directory サーバへの接続をセットアップする必要があります。

詳細については、次の項を参照してください。

- 防御センターでのユーザ エージェントの設定（2-3 ページ）
- ユーザ アクセス制御を許可する LDAP 接続のセットアップ（2-4 ページ）

防御センターでのユーザ エージェントの設定

ユーザ エージェントを使用して LDAP ユーザのログイン情報を収集する場合、最初のステップとして、Active Directory サーバに接続するエージェントからの接続を許可するように、各防御センターを設定します。この章では、バージョン 5.x の防御センターでエージェント接続を承認する手順について説明します。

ユーザ エージェントに接続するように防御センターを設定するには、以下を行います。

アクセス: Admin/Discovery Admin

ステップ 1　[Policies] > [Users] を選択します。

ステップ 2　[Add User Agent] をクリックします。

ステップ 3　[Name] フィールドに、エージェントの識別に役立つ名前を入力します。

ステップ 4　[Hostname or IP address] フィールドに、エージェントを配置するコンピュータの IP アドレスまたはホスト名を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように防御センターを設定することは**できません**。

注　IPv6 アドレスまたは IPv6 アドレスに解決できないホスト名を持つユーザ エージェントは追加できません。

ステップ 5　[Add User Agent] をクリックします。

これで、防御センターは設定されたホストのユーザ エージェントに接続できるようになります。

ステップ 6　次の選択肢があります。

- ユーザ制御を実行する場合は、ユーザ アクセス制御を許可する LDAP 接続のセットアップ（2-4 ページ）に進みます。
- ユーザ制御を実行しない場合は、Active Directory サーバに接続する権限の設定（2-4 ページ）に進みます。

ユーザ アクセス制御を許可する LDAP 接続のセットアップ

ユーザ制御を実行する（つまり、ユーザ条件によるアクセス制御ルールを作成する）場合は、防御センターと組織の少なくとも 1 つの Microsoft Active Directory サーバ間の接続を設定して有効にする必要があります。*LDAP 接続*または*ユーザ認識認証オブジェクト*と呼ばれるこの設定には、サーバの接続設定と認証フィルタ設定が含まれます。接続のユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータは、アクセス コントロール ルールで使用可能なユーザとグループを指定します。

注　ユーザ制御を実行する場合は、Microsoft Active Directory を使用する**必要があります**。システムは、Active Directory サーバ上で実行されているユーザ エージェントを使用してユーザを IP アドレスに関連付けます。この関連付けによって、アクセス制御ルールが呼び出されます。

ユーザ認識設定を使った LDAP 接続の設定方法の詳細については、『*FireSIGHT システム ユーザ ガイド*』を参照してください。

Active Directory サーバに接続する権限の設定

エージェントに関するすべての前提条件を満たすようにコンピュータを準備できたら、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て、Active Directory サーバがこれらのログにログイン データを記録できるようにします。次に、ユーザ権限と Windows のセキュリティ権限を設定して、エージェントが Active Directory サーバと通信し、セキュリティ ログにアクセスしてログイン データ（および必要に応じてログオフ データ）を取得できるようにします。

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、以下を行います。

ステップ 1　Active Directory サーバで、[Start] > [All Programs] > [Administrative Tools] > [Event Viewer] を選択します。

ステップ 2　[Windows Logs] > [Security] を選択します。

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、http://technet.microsoft.com/en-us/library/cc779487(v=ws.10).aspx でセキュリティ ログの有効化の詳細を参照してください。

エージェントが Active Directory サーバと通信できるようにするには、以下を行います。

ステップ 1　Active Directory サーバのリモート管理のファイアウォール ルールを有効にします。次の選択肢があります。

- Active Directory サーバで Windows Server 2003 が実行されている場合は、http://technet.microsoft.com/en-us/library/cc738900%28v=ws.10%29.aspx で詳細を参照してください。
- Active Directory サーバで Windows Server 2008 または Windows Server 2012 が実行されている場合は、http://msdn.microsoft.com/en-us/library/aa822854%28VS.85%29.aspx で詳細を参照してください。

ログイン データを取得する権限をエージェントに付与するには、以下を行います。

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上でユーザを作成します。

注　Active Directory サーバ接続を設定するときに、これらの資格情報を使用します。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（2-11 ページ）」を参照してください。

ステップ 2　このユーザのために Active Directory サーバの RPC を有効にします。次の選択肢があります。

- Active Directory サーバで Windows Server 2008 R2 または Windows Server 2012 が実行されていて、ユーザが Administrators グループのメンバーでない場合は、ユーザに DCOM のリモート アクセス、リモート起動、およびアクティブ化権限を付与します。詳細については、http://msdn.microsoft.com/en-us/library/Aa393266.aspx を参照してください。
- Active Directory サーバで他のサポート対象バージョンの Microsoft Windows が実行されている場合は、RPC がすでに有効になっています。

ログオフ データを取得する権限をエージェントに付与するには、以下を行います。

ステップ 1　作成したユーザに管理者権限を付与して、Active Directory サーバに対して認証するすべてのワークステーションにユーザが確実にログインできるようにします。

セキュリティ ログにアクセスする権限をエージェントに付与するには、以下を行います。

ステップ 1　作成したユーザに Active Directory サーバの WMI ルート/CIMV2 ネームスペースへの完全なアクセス権限を付与します。詳細については、http://technet.microsoft.com/en-us/library/cc787533%28v=WS.10%29.aspx を参照してください。

アイドル セッション タイムアウトの有効化（2-6 ページ）に進みます。

アイドル セッション タイムアウトの有効化

Active Directory サーバに接続する権限を設定した後は、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ことができます。これは、エージェントがホストの複数のセッションによる余分なログインを検出して報告することを防ぐのに役立ちます。

ターミナル サービスでは、複数のユーザが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の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。別のユーザがリモート デスクトップを使用してワークステーションにログインした場合は、2 つのセッションが実行されています。実行中のセッションが複数あるため、エージェントは余分なログインを報告す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、これらのセッションは定義されたアイドル タイムアウト期間が経過した後で終了するため、ホスト上で複数のリモート セッションが実行されることを防止できます。

Citrix セッションは、リモート デスクトップ セッションと同様に機能します。1 つのコンピュータ上で複数の Citrix ユーザ セッションが実行されてい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、ホスト上で複数の Citrix セッションが実行されることを防止できるため、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、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引き続き発生する可能性があります。

ターミナル サービスのセッション タイムアウトを有効にするには、以下を行います。

ステップ 1　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 タイムアウトに関するグループ ポリシー設定を更新します。次の選択肢があります。

- Active Directory サーバで Windows Server 2008 または Windows Server 2012 が実行されている場合は、http://technet.microsoft.com/en-us/library/cc754272(v=ws.10).aspx でセッション タイムアウトの有効化の詳細を参照してください。
- Active Directory サーバで Windows Server 2003 が実行されている場合は、http://technet.microsoft.com/en-us/library/cc758177(v=ws.10).aspx でセッション タイムアウトの有効化の詳細を参照してください。

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 タイムアウトを設定済みのログオフ チェック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、設定済みのログオフ チェック頻度をセッション 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 (2-20 ページ) を参照してください。

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、以下を行います。

ステップ 1　アイドル状態のリモート セッションのタイムアウトと切断されたセッションのタイムアウトに関するグループ 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、http://technet.microsoft.com/en-us/library/ee791886%28v=ws.10%29.aspx を参照してください。

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 タイムアウトを設定済みのログオフ チェック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、設定済みのログオフ チェック頻度をセッション 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（2-20 ページ）を参照してください。

Citrix セッションのタイムアウトを有効にするには、以下を行います。

ステップ 1　Citrix のオンライン ドキュメント（http://support.citrix.com/）を参照してください。

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）に進みます。

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

各ユーザ エージェントをインストールする Windows コンピュータに接続するように防御センターを設定した後は、次の前提条件を満たすように Windows コンピュータをセットアップします。

- コンピュータで Windows Vista、Windows 7、Windows 8、Windows Server 2003、Windows Server 2008、または Windows Server 2012 が実行されていること。コンピュータが Active Directory サーバである必要はありません。
- 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。この .NET Framework は、.NET Framework バージョン 4.0 クライアント プロファイルの再頒布可能パッケージ（`dotNetFx40_Client_x86_x64.exe`）として Microsoft から入手できます。SQL CE は、実行可能ファイル（`SSCERuntime-ENU.exe`）として Microsoft から入手できます。

注　.NET Framework と SQL CE が両方ともインストールされていない場合は、エージェントの実行可能ファイル（`Sourcefire_User_Agent_2.2-9_Setup.exe`）を開いたときに、適切なファイルをダウンロードするように求められます。詳細については、「ユーザ エージェントのインストール（2-9 ページ）」を参照してください。

- コンピュータが、監視する 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 プロトコルを使用すること。エージェントが Active Directory サーバをリアルタイムで監視する場合は、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する必要があります。
- コンピュータが、データと IPv4 アドレスの報告先となる防御センターに TCP/IP でアクセスできること。

- IPv6 アドレスを持つホストからログオフを検出する場合は、コンピュータが IPv6 アドレスを持っていること。IPv4 アドレスを持つホストからログオフを検出する場合は、コンピュータが IPv4 アドレスを持っていること。
- 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 のエージェントが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、コントロール パネルの [Add/Remove Programs] を開きます。

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、データベースのバックアップを実行する必要があります。

ユーザ エージェント設定のバックアップ（2-8 ページ）に進みます。

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。これら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（2-9 ページ）に進みます。

構成設定を保持するには、以下を行います。

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、[Start] > [Programs] > [Sourcefire] > [Configure User Agent] を選択します。

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

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 `C:\SourcefireUserAgent.sdf` を見つけ、このファイルをローカルでコピーします。

ステップ 4　Sourcefire ユーザ エージェントをアンインストールするため、コントロール パネルに移動して [Add/Remove Programs] を開きます。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（2-9 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、[Start] > [Programs] > [Sourcefire] > [Configure User Agent] を選択します。

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

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 `C:\SourcefireUserAgent.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されたローカル バックアップに置き換えます。

ステップ 9　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、[Start] > [Programs] > [Sourcefire] > [Configure User Agent] を選択します。

ステップ 10　再生ボタン（▶）をクリックして起動します。エージェント サービスが起動します。

ユーザ エージェントの設定（2-10 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

Active Directory サーバに接続する権限を設定した後は、アイドル状態のリモート セッションのタイムアウトを設定したかどうかにかかわらず、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（2-8 ページ）を参照してください。

エージェントは、**Local System** アカウントを使用してサービスとして実行されます。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は、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 データをポーリングし、送信し続けます。

注　サービス設定を変更しないでください。異なるアカウントを使用すると、エージェントが正常に機能しません。

エージェントごとに、5 つの Active Directory サーバと 5 つの.防御センター への接続を設定できます。防御センター の接続を追加する前に、必ず、防御センター 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、バージョン 4.x の 防御センター に接続する準備（2-2 ページ）または バージョン 5.x の防御センターに接続する準備（2-3 ページ）を参照してください。

高可用性設定では、両方の防御センター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 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。

ユーザ エージェントをインストールするには、以下を行います。

アクセス: すべて

ステップ 1　サポート サイトからユーザ エージェントのセットアップ ファイル（`Sourcefire_User_Agent_2.2-9_Setup.zip`）をダウンロードします。

注　セットアップ ファイルは電子メールで転送せずに、サポート サイトから直接ダウンロードしてください。セットアップ ファイルを電子メールで転送すると、破損することがあります。

ステップ 2　エージェントをインストールする Windows コンピュータにセットアップ ファイルをコピーして、ファイルを解凍します。

エージェントをインストールするには、ハード ドライブに 3 MB の空き容量が必要です。シスコでは、ハード ドライブ上の 4 GB をエージェントのローカル データベースに割り当てることを推奨しています。

ステップ 3　セットアップ実行可能ファイル（`Sourcefire_User_Agent_2.2-9_Setup.exe`）を開きます。

ヒント　Administrators グループのメンバーでないアカウントを使用していて、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がない場合は、インストールを開始するための適切な権限を持つグループに属するユーザに昇格する必要があります。エスカレーションのオプションにアクセスするには、`Sourcefire_User_Agent_2.2-9_Setup.exe` ファイルを右クリックして、[Run As] を選択します。適切なユーザを選択し、そのユーザのパスワードを入力します。

ステップ 4　エージェントをインストールする Windows コンピュータに Microsoft .NET Framework バージョン 4.0 クライアント プロファイルと SQL CE バージョン 3.5 が両方ともインストールされていない場合は、適切なファイルをダウンロードするように求められます。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 5　ウィザード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。

ステップ 6　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（2-10 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

エージェントがインストールされたら、Active Directory サーバからデータを受信し、その情報を防御センターに報告し、レポートから特定のユーザ名と IP アドレスを除外し、ローカル イベント ログまたは Windows アプリケーション ログにステータス メッセージを記録するようにエージェントを設定できます。

エージェントを設定するには、以下を行います。

アクセス: すべて

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、[Start] > [Programs] > [Sourcefire] > [Configure Sourcefire User Agent] を選択します。

次の表で、エージェントの設定時に実行できる操作と、それらを設定する場所について説明します。

表 2-1　　ユーザ エージェントの設定操作

目的	場所
エージェント名の変更、ログオフ チェック頻度の変更、サービスの開始と停止、スケジュール優先度の設定	[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（2-20 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 サーバのリアルタイム データ取得の有効化、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 Servers] 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 Active Directory サーバ接続の設定（2-11 ページ）」を参照してください。
防御センターの追加または削除	[Sourcefire DCs] タブを選択します。詳細については、「ユーザ エージェントの防御センター接続の設定（2-14 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	[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（2-16 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	[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（2-17 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	[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（2-18 ページ）」を参照してください。
サポート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	[Logs] タブを選択し、[Show Debug Messages in Log] を有効にしてから、[Maintenance] タブを選択します。詳細については、「ユーザ エージェントのメンテナンス設定の構成（2-20 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	[Save] をクリックします。[Save] の下に、未保存の変更があることを示すメッセージが表示されます。
エージェント設定の変更を保存せずにエージェントを閉じる	[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

1 つのエージェントから最大 5 つの Active Directory サーバへの接続を追加して、次の項目を設定できます。

- 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や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 サーバとの接続を確立または再確立するときに、エージェントが取得するログインおよびログオフのデータの量

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、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 分を超えない値に設定してください。

Active Directory サーバで Windows Server 2003 が実行されている場合は、Active Directory サーバをリアルタイムで監視するようにエージェントを設定できません。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。

エージェントでは、タブを選択した時点の Active Directory サーバのポーリング 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表示できます。エージェントがリアルタイムで Active Directory サーバをポーリングしているかどうかや、タブを選択した時点のリアルタイム データ取得のステータスを表示することもできます。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。
unavailabl	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	サーバ設定が追加されましたが、まだ保存されていません。	サーバ設定が追加されましたが、まだ保存されていません。
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　複数の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を報告するため、同じ Active Directory サーバに複数のユーザ 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、各エージェントの設定において、同じ Active Directory サーバをポーリングしている他の全ホストの IP アドレスを除外し、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（2-17 ページ）を参照してください。

Active Directory サーバ接続を設定するには、以下を行います。

アクセス: すべて

ステップ 1　[Active Directory Servers] タブを選択します。

ステップ 2　次の 2 つのオプションから選択できます。

- サーバへの新しい接続を追加するには、[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。

ヒント　既存の接続を削除するには、サーバ名を選択して [Remove] をクリックします。

ステップ 3　[Server Name/IP Address] フィールドに、Active Directory サーバの完全識別サーバ名または 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場合は、IP アドレスを入力します。

注　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` と入力します。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。

ステップ 4　Active Directory サーバのユーザ ログインおよびログオフ データを照会する権利を持つユーザ名とパスワードを入力します。プロキシ経由でユーザを認証するには、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 [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 個以上の場合は、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 5　[Domain] フィールドに、Active Directory サーバがドメインになっているドメインを入力します。

ステップ 6　Active Directory サーバへのログインを検出するには、[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、[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。

[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 7　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、[Process real-time events] を選択します。

ステップ 8　[Add] をクリックします。

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、[Host]、[Last Reported]、[Polling Status]、[Last Polled]、[Real-time Status]、または [Real-time] 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　設定時にエージェントが Active Directory サーバに接続できない場合は、そのサーバを追加できません。エージェントがサーバに TCP/IP でアクセスできること、使用した資格情報で接続できること、および Active Directory サーバへの接続を正しく設定したことを確認してください。詳細については、「Active Directory サーバに接続する権限の設定 (2-4 ページ)」を参照してください。

ステップ 9　必要に応じて、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 Server Polling Interval] ドロップダウン 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発生し、その間隔で繰り返します。ポーリングにかかる時間が選択した間隔より長い場合、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 サーバに対してリアルタイム データ取得が有効になっていて、エージェントがサーバと接続できなくなっている場合、エージェントは応答を受信してリアルタイム データ取得が利用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 データ取得が再開されます。

ステップ 10　必要に応じて、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）したときの最大ポーリング時間を変更するには、[Active Directory Server Max Poll Length] ドロップダウン リストから時間を選択します。

注　[Active Directory Server Max Poll Length] ドロップダウン リストに保存する値を、[Active Directory Server Polling Interval] ドロップダウン 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。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。

ステップ 11　設定変更を保存してエージェントに適用するには、[Save] をクリックします。

ステップ 12　次の選択肢があります。

- 防御センター接続を追加または削除するには、[Sourcefire DCs] タブを選択します。詳細については、ユーザ エージェントの防御センター接続の設定 (2-14 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 つの防御センターを追加する必要があります。

- エージェントを設定するために、表 2-1 (2-11 ページ) に示されている操作をどれでも実行できます。

ユーザ エージェントの防御センター接続の設定

ライセンス: FireSIGHT

1 つのエージェントから最大 5 つの防御センターへの接続を追加できます。エージェントでは、タブを選択した時点の防御センターのステータス（`available`、`unavailable`、またはエージェントが最初に起動したときの `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表示することもできます。接続を追加する前に、必ず防御センター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、バージョン 4.x の 防御センター に接続する準備 (2-2 ページ) またはバージョン 5.x の防御センターに接続する準備 (2-3 ページ) を参照してください。

高可用性設定では、両方の防御センター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。

防御センター接続を設定するには、以下を行います。

アクセス: すべて

ステップ 1　[Sourcefire DCs] タブを選択します。

ステップ 2　[Add] をクリックします。

ステップ 3　追加する防御センターのホスト名または IP アドレスを入力します。

ステップ 4　[Add] をクリックします。

防御センター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防御センターを追加しないでください。防御センターがマルチホームの場合は、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。

複数の防御センター接続が設定されている場合は、[Host]、[Status]、または [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　設定時にエージェントが防御センターに接続できない場合は、その防御センターを追加できません。エージェントが防御センターに TCP/IP でアクセスできることを確認します。

ステップ 5　設定変更を保存してエージェントに適用するには、[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 6　次の選択肢があります。

- 必要に応じて、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、[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（2-16 ページ）を参照してください。
- 必要に応じて、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、[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（2-17 ページ）を参照してください。
- 必要に応じて、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、[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（2-18 ページ）を参照してください。
- 必要に応じて、エージェントの全般的な設定を構成するには、[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（2-20 ページ）を参照してください。
- エージェントを設定するために、表 2-1（2-11 ページ）に示されている操作をどれでも実行できます。

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

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防御センターに報告しません。ユーザ名を除外する前に報告されたログインまたはログオフ 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、そのユーザ名の以後のログインおよびログオフ イベントは防御センターに報告されます。

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。カンマ区切り値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。防御センター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。

除外ユーザ名を設定するには、以下を行います。

アクセス: すべて

ステップ 1　[Excluded Usernames] タブを選択します。

ステップ 2　入力可能な次の行の [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 3　必要に応じて、ユーザ名に関連付けられたドメインを [Domain] 列に入力します。ドメインは各行に 1 つだけ定義できます。ドメインを指定しない場合は、すべてのドメインのユーザ名が除外されます。

ステップ 4　ユーザ名をさらに追加するには、ステップ 2 および 3 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、[Username] または [Domain] 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。

ステップ 5　行を削除するには、次の選択肢があります。

- 行を強調表示して Delete 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 Backspace 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 キーを押しながら複数の行をクリックして選択し、Delete キーを押します。

ステップ 6　ユーザ名とドメインのリストをカンマ区切り値ファイルにエクスポートするには、[Export List] をクリックします。ファイルを保存するファイル 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 `Sourcefire_user_agent_excluded_users.csv` です。

ステップ 7　ユーザ名とドメインのリストをカンマ区切り値ファイルからインポートするには、[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は、ファイルをアップロードできません。

カンマ区切り値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。

"*user name*","*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 8　[Save] をクリックして設定変更を保存し、エージェントに適用します。

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 9　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、[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（2-17 ページ）を参照してください。
- エージェントを設定するために、表 2-1（2-11 ページ）に示されている操作をどれでも実行できます。

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

ログイン イベントのポーリング時に除外する IPv4 または 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、エージェントはそのイベントを防御センターに報告しません。IP アドレスを除外する前に報告されたログインまたはログオフ 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、そのアドレスの以後のログインおよびログオフ イベントは防御センターに報告されます。

除外 IP アドレスを設定するには、以下を行います。

アクセス: すべて

ステップ 1　[Excluded Addresses] タブを選択します。

ステップ 2　入力可能な次の行の [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、[Address] 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。

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かぎり、他のアドレスを入力できません。

ステップ 3　IP アドレスを削除するには、行を強調表示して Delete 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 キーを押しながら複数の行をクリックして選択し、Delete キーを押します。

ステップ 4　IP アドレスのリストをカンマ区切り値ファイルにエクスポートするには、[Export List] をクリックします。ファイルを保存するファイル 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 `Sourcefire_user_agent_excluded_addresses.csv` です。

ステップ 5　IP アドレスのリストをカンマ区切り値ファイルからインポートするには、[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は、ファイルをアップロードできません。

ステップ 6　[Save] をクリックして設定変更を保存し、エージェントに適用します。

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 7　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、[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（2-18 ページ）を参照してください。
- エージェントを設定するために、表 2-1（2-11 ページ）に示されている操作をどれでも実行できます。

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

[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
- エージェントがシスコ アプライアンスへの接続に成功した
- エージェントがシスコ アプライアンス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、重大度をレベルの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	色	説明
debug	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。
information	緑	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。
warning	黄	これは予期され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。
error	レッド	これは予期され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 ログの内容をカンマ区切り値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を指定したり、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 [Maintenance] タブへのアクセスなどのメンテナンス オプションを設定することもできます。

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、以下を行います。

アクセス: すべて

ステップ 1　[Logs] タブを選択します。

ステップ 2　サポート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 [Show Debug Messages in Log] を選択し、[Maintenance] タブを有効にします。

[Logs] タブにデバッグ メッセージが表示されます。[Maintenance] タブが利用可能になります。

注　このオプションは、サポートから指示された場合にのみ選択してください。

ステップ 3　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、[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 4　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、[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、[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　[Message Cache Size] の設定は、ローカル イベント ログにのみ影響し、[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 5　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、[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モが表示されます。更新の結果 250 件を超えるメッセージが表示された場合は、最も古いステータス メッセージが [Logs] タブから削除されます。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 6 を参照してください。

ステップ 6　ローカル イベント ログの内容をカンマ区切り値ファイルにエクスポートするには、[Export Logs] をクリックします。

カンマ区切り値ファイルには、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 7　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、[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 8　設定変更を保存してエージェントに適用するには、[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 9　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、[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（2-20 ページ）を参照してください。
- エージェントを設定するために、表 2-1（2-11 ページ）に示されている操作をどれでも実行できます。

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

[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防御センターに報告す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 チェック頻度の変更、および現在のサービス ステータスの表示を行うこともできます。

ユーザ エージェントの全般的な設定を構成するには、以下を行います。

アクセス: すべて

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、[Start] > [Programs] > [Sourcefire] > [Configure User Agent] 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、再生ボタン( )をクリックします。

エージェント サービスが起動します。

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。

エージェント サービスが停止します。

ステップ 4　必要に応じて、[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 SFADUA 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　必要に応じて(バージョン 5.2 以降の場合)、エージェントがログオフ データをチェックする頻度を変更するには、[Logout Check Frequency] ドロップダウン 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　必要に応じて、エージェントのスケジュールの優先度を変更するには、[Priority] ドロップダウン 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 アクティビティを監視して取得する場合にのみ、[High] を選択します。

ステップ 7　設定を保存するには、[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　エージェントを設定するために、表 2-1(2-11 ページ)に示されている操作をどれでも実行できます。

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

エージェントは、構成設定に加えて、ユーザと IP 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 [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 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、[Maintenance] タブ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、以下を行います。

アクセス: すべて

ステップ 1　[Logs] タブを選択します。

ステップ 2　[Show Debug Messages in Log] を選択して [Maintenance] タブを有効にします。

ステップ 3　[Maintenance] タブを選択します。

ステップ 4　保存されているすべてのユーザと IP のマッピング データをクリアするには、[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 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、防御センターのデータベースに保存されているユーザと IP のマッピング データには影響しません。

ステップ 5　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、[Clear logon event log cache] をクリックします。

エージェントはローカル イベント ログから、保存されているすべてのログイン イベント データを削除します。

ステップ 6　エージェントが設定済みの防御センター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、[Clear reporting state cache] をクリックします。

エージェントは、設定されている 防御センター に対して最後に報告したログイン情報とログオフ情報に関する情報をすべて削除します。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ているすべての Active Directory サーバを手動でポーリングし、[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（2-11 ページ）」を参照してください。

ステップ 7　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、[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 8　エージェントを設定するために、表 2-1（2-11 ページ）に示されている操作をどれでも実行できます。