WatchGuard® Firebox® X Edge e-Series

リリース ノート: Release Notes for Firebox® X Edge e-Series v10.2

概要

WatchGuard は、Firebox® X Edge e-Series v10.2 のリリースを発表しました。

このリリースには、ユーザーから報告された Edge の不具合に関する修正が含まれています。修正された個所は、PPPoE、プロキシ、複数 WAN、Branch Office VPN などです。詳細については、「解決済みの問題」を参照してください。

このリリースでサポートされるアプライアンス

Firebox® X Edge e-Series v10.2 ソフトウェアは、Firebox® X Edge e-Series モデル上でのみ動作します。Edge、SOHO 6、SOHO 6 ワイヤレス、S6、S6 ワイヤレス、または SOHO モデルでは機能せず、インストールもできません。

Firebox® X Edge e-Series アプライアンスのご購入については、各社の経理担当者にお問い合わせください。

ソフトウェア ライセンスに関する重要な注意事項

Firebox® X Edge e-Series では、ソフトウェア ライセンスの以下の規定が適用されます。

- **登録:** 機能キーを受け取るには、LiveSecurity で Firebox X Edge e-Series を登録する必要があります。有効な機能キーを保有しない場合は、Edge からインターネットに接続できるユーザーは 1 人だけです。
- **LiveSecurity:** ソフトウェアのアップグレードをインストールするには、現行の LiveSecurity 登録が必要です。
- **WebBlocker:** WebBlocker 登録の有効期限が切れると、Edge デバイスは既定ですべての送信 HTTP トラフィックを拒否します。この動作は、[WebBlocker] > [設定] ページで制御することができます。
- **spamBlocker:** SpamBlocker 登録の有効期限が切れると、spamBlocker のメール検証が機能しなくなるため、すべてのメールが許可されます。

インストール

Firebox® X Edge v10.2 リリースをインストールするには、以下の手順に従います。既定では、v10.2 アプライアンス ソフトウェアは英語でのみインストールされます。追加の言語パックは、Edge Upgrade Wizard で以下のインストール手順に従って、Edge にインストールできます。Edge ユーザー インターフェイスの言語は、Edge Web インターフェイスの [管理] ページで変更できます。

Windows XP (またはその他の Vista 以外の Windows バージョン) 使用している場合

1. http://www.watchguard.com/support にアクセスし、LiveSecurity ユーザー名とパスフレーズでログインします。[ソフトウェアのダウンロード] ページへのリンクをたどって、Edge_10_2.exe ファイルをハード ディスクに保存します。
2. Edge v10.2 にアップグレードする前に、Edge を再起動することをお勧めします。
3. 手順 1 でダウンロードした Edge_10_2.exe ファイルをダブルクリックし、[Upgrade Wizard] ダイアログ ボックスに示される指示に従います。
4. 言語パックをインストールする場合は、Upgrade Wizard の実行中に適切な言語を選択します。Edge ユーザー インターフェイスの言語は、Quick Setup Wizard または Edge Web ユーザー インターフェイスの [管理] ページで選択します。

Windows Vista またはその他の Windows 以外のオペレーティング システム使用している場合

1. http://www.watchguard.com/support にアクセスし、LiveSecurity ユーザー名とパスフレーズでログインします。[ソフトウェアのダウンロード] ページへのリンクをたどって、Edge_10_2.zip ファイルをハード ディスクに保存します。このファイルを解凍します。
2. Edge v10.2 にアップグレードする前に、Edge を再起動することをお勧めします。
3. Firebox® X Edge の [システム ステータス] ページに接続します。
   接続するには、ブラウザのアドレス バーで「https://」と入力してから、Edge の信頼済みインタフェースの IP アドレスを入力します。既定の URL は https://192.168.111.1 です。
4. [システム ステータス] ページで、[更新] をクリックします。
5. [参照] をクリックします。yakfw.sysa-dl ファイルを選択し、[開く] をクリックします。
6. [更新] をクリックします。インストールを完了するには、Firebox Edge を再起動する必要があります。
7. 言語パックをインストールするには、手順 3 ～ 5 を繰り返しますが、手順 4 で以下のファイルのいずれかを選択します。
   フランス語: lang-fr-10.2-arm.wgpk-dl
   日本語: lang-ja-10.2-arm.wgpkg-dl
   簡体字中国語: lang-zh-10.2-arm.wgpkg-dl
8. Edge の再起動後、[管理] ページに移動してユーザー インターフェイスの言語を変更します。

更新後、[システム ステータス] ページには、新しいバージョンが "10.2 June 3 2008 Build 179920" と表示されます。

注 現在 Edge で Edge v8.0.x ソフトウェアを使用している場合、このリリースをインストールするには特定のアップグレード パスに従う必要があります。次の表で、アップグレード パスを判断してください。

現在実行中のバージョン	インストールの順序
Edge e-Series v8.0	Edge e-Series v8.0.1 > v8.0.3 -> v10.2
Edge e-Series v8.0.3 以降	Edge e-Series v10.2

Edge に現在インストールされているソフトウェアのバージョンが不明な場合は、Edge の管理インターフェイスにログインし、[システム ステータス] ページを表示します。Edge e-Series v8.0.3 ソフトウェアを入手するには、WatchGuard テクニカル サポートに連絡してください。

シングル サインオン (SSO) エージェント ソフトウェアをインストールするには、以下の手順に従います。

1. http://www.watchguard.com/support にアクセスし、LiveSecurity ユーザー名とパスフレーズでログインします。[ソフトウェアのダウンロード] ページへのリンクをたどって、WatchGuard Single Sign-On Agent 10.2 をダウンロードします。`WG-Authentication-Gateway.exe` ファイルをハード ディスクに保存します。
2. 静的 IP アドレスを持つドメイン コンピュータにこのファイルをインストールし、Setup Wizard の入力を完了します。SSO エージェント ソフトウェアはドメイン コントローラにインストールすることをお勧めします。

WebBlocker および Quarantine Server ソフトウェアをローカルにインストールするには、次の手順に従います。

1. http://www.watchguard.com/support にアクセスし、LiveSecurity ユーザー名とパスフレーズでログインします。[ソフトウェアのダウンロード] ページへのリンクをたどって、`WGEdge10_2QWB.exe` ファイルをハード ディスクに保存します。
2. ローカル コンピュータにこのファイルをインストールし、Setup Wizard の入力を完了します。

解決済みの問題

全般

- WAN1 がワイヤレス クライアントとして構成されているときに、MAC アドレスの無効化機能が正しく動作するようになりました。[23459]
- Edge で、1 - 1 NAT の IP のサブネットが標準のクラス C (/24) であるとは想定されなくなりました。外部インターフェイスからのサブネット マスクが 1 - 1 NAT サブネットに使用されます。[27320]
- インターフェイスの変更後に WPA 共有キーが消失する原因となる日本語バージョンの WatchGuard System Manager (WSM) v10.1 の問題が修正されました。[27214]
- Edge の再起動をスケジュールするオプションが [管理] ページで使用できるようになりました。[27383]
- Quick Setup Wizard の実行後にシリアル番号の "評価単位" が Edge で表示される原因となる問題が修正されました。[27147]
- ベネズエラの新しいタイム ゾーン オプション (GMT - 4:30) が追加されました。[22975]

認証

- ユーザーが正しくないユーザー名またはパスワードを使用して Edge から認証を得ようとすると、RADIUS サーバーが使用できないと誤って示すログ メッセージが表示されなくなりました。[23362]
- ユーザー アカウントの [セッションのアイドル タイムアウト] 設定が正しく動作するようになり、[セッションの最大タイムアウト] 設定と同じではなくなりました。[23820]

シングル サインオン (SSO)

- SSO エージェントが複数ドメインで機能し、親および子のドメインに関係なく認証情報を取得するようになりました。[26905]

プロキシ

- 外部インターフェイスが PPPoE を使用するように構成されているときのすべてのプロキシの MTU 処理が向上しました。MTU 処理が向上したため、ユーザーから報告されていた、Yahoo メールや AOL メールによる添付ファイルの受信の問題や Yahoo の検索機能を使用したときの処理速度の低下の問題のほか、www.mappy.fr などの Web サイトの一部にアクセスするときの問題が解消されます。[21771] [27093] [26762]
- スパムではない電子メールが、POP3 プロキシから "Message is classified as not spam (POP3-Proxy)" とログに正しく記録されるようになりました。[23431]
- 送信プロキシで IM - ICQ アクションが [拒否] に設定されているときに ICQ がブロックされるようになりました。[22804]
- v10.2 にアップグレードしても、v8.6.x 以前のバージョンで作成された WebBlocker のカスタムの拒否メッセージの内容は失われません。[26903]
- [デバッグ] ページにあるプロキシのログ記録オプションが正しく動作するようになりました。[23680]

spamBlocker

- SMTP プロキシに対して spamBlocker を構成している場合、検疫された確認済みのスパムのログ メッセージは、"ProxyQuarantine: SMTP Confirmed" ではなく、"ProxyQuarantine: SMTP Confirmed spam" と表示されるようになりました。[23733]

複数 WAN/WAN フェールオーバー

- WAN1 で受信した ping 要求への応答が、WAN1 で正しく実行されるようになりました。[23556]
- WAN フェールオーバーに対応するように Edge を構成した後、Edge を再起動する必要はなくなりました。[23578]

VPN

- v8.6.x から v10.x にアップグレードした後に、ローカルおよびリモートの両方に FQDN を使用するアグレッシブ モードのトンネルに障害が発生しなくなりました。[27319] [27331]
- ローカル ID のタイプが IPV4_ADDR のドメイン名として誤って構成されていても、Iked デーモンがクラッシュすることはなくなりました。[26924]
- BOVPN 設定の変更が含まれる構成を保存する間、BOVPN トラフィックで Edge が暗号化されないままになる問題が修正されました。[23597]
- WAN フェールオーバーおよび VPN フェールオーバーを使用して 2 つの Edge デバイスが構成されている場合、両方のデバイスで WAN1 の ping ホストが到達不能になっても、これらの Edge デバイス間に VPN トンネルが正しく確立されるようになりました。[23780]
- [VPN 統計] ページに、受信および送信の両方のパケット数情報が表示されるようになりました。[25799]

既知の問題

ネットワーク構成

- WAN1 の [ワイヤレス クライアント構成] タブは、すべての Edge e-series モデルで使用できます。Firebox X Edge e-Series Wireless を保有していない場合は、このワイヤレス タブを使用しないでください。[23910]

1 - 1 NAT

- IPSec トラフィックに対して 1 - 1 NAT は使用できません。[13516]

DHCP

- DHCP 中継サーバーは Edge DHCP サーバーより優先されません。[16796]
- DHCP リース時間が常に GMT で報告されます。[15431]
- 従来の MUVPN with IPSec クライアント ソフトウェアを使用し、DHCP 内部クライアント用の Mobile VPN 既定ルート (0.0.0.0/0) トンネルを作成すると、クライアントは IP アドレスを更新できないため、DHCP リースがタイムアウトすると接続が終了します。この構成を使用している場合は、DHCP リース タイムアウトを 8 時間以上に設定してください。[15912]

複数 WAN/WAN フェールオーバー

- 特定のインターフェイス (WAN1) へのポリシー ベースのルーティングを構成しているとき、Edge でラウンド ロビンの使用が続行されることがあります。この状態になると、他のインターフェイス (WAN2) から送信されるパケットがポリシー ベースのルーティング ルール インターフェイス (WAN1) IP と表示されます。[27602]
- 複数 WAN を使用していると、WAN 2 (eth3) から送信されるすべてのパケットが、最初のインターフェイス eth1 (信頼済み) または eth2 (任意) から送信されたとログ ファイルに示されます。[27519]
- WAN1 とリモート IPSec ゲートウェイが同じサブネット上に存在する場合、BOVPN トンネルのフェールオーバーが正しく機能しないことがあります。[15935]
- Ping の間隔が、構成された間隔より 2 秒長くなります。[15598]
- IPSec トンネルでは、常に WAN1 を使用してネゴシエートが試行されます。Edge を複数 WAN に対応するように構成する場合、フェールオーバーが発生しない限り、すべての IPSec トンネルで WAN1 が使用されます。[23704]
- 複数 WAN を使用するように Edge が構成されている場合、ポリシーベースのルーティング機能を使用して、すべてのポリシーのトラフィックで使用する外部インターフェイスを選択できます。既定では、外部インターフェイスが選択され、負荷分散が適用されます。WAN1 または WAN2 を選択した場合、変更を反映するために Edge を再起動する必要があります。[23519]
- Edge が、モデムへの WAN フェールオーバーに対応するように構成されている場合、大量のトラフィックが送信されると IPSec トンネル接続でキーが正しく再生されない場合があります。[23560]

認証

- [ユーザー認証を要求する (ローカル ユーザー アカウントを有効にする)] という設定がオンになっていない場合、インターネットにアクセスする匿名ユーザーは、"アクティブ セッション" として登録されませんが、ユーザー ライセンスの 1 つを使用します。[26493]
- Vista でシングル サインオン エージェントを使用すると、現在のユーザーを列挙しようとしたリモート コンピュータに "アクセスが拒否されました" というメッセージが返されます。[23590]
- Edge でユーザーが認証されても、Edge がシングル サインオン用に構成されている場合、ユーザーは Edge からログオフできません。[23708]

  回避策

  必要に応じて、[自動セッション終了を有効にする] 設定により、認証セッションの時間を短くしてください。

- 同一のコンピュータ上で複数のユーザーが認証される場合は、シングル サインオンを有効にしないことを強くお勧めします。
- シングル サインオンが機能するようにするには、Active Directory 認証を使用する必要があります。LDAP 認証では、シングル サインオンはサポートされていません。

プロキシ

- 最初の BitTorrent 接続は、TCP-UDP (送信) プロキシで正常にブロックされます。このとき、BitTorrent は、HTTP プロキシまたは HTTP フィルタ ポリシーを正常に通過する TCP ポート 80 で接続しようとします。[27474]
- HTTP プロキシの安全でないファイル名のパターン機能を使用すると、ファイル名のパターンが URI 全体に適用されて一部のリダイレクトがブロックされることがあります。[23758]

  回避策

  安全でないファイルの種類を許可してコンテンツの種類でのブロックを利用するか、問題が発生したときに、安全でないファイル名のパターンを既定リストから削除します。

- 送信プロキシを有効にすると、アウトバウンド SIP 接続は SIP プロキシに正しく送信されません。[23546、全プラットフォーム]

  回避策

  SIP 接続を直接処理するように SIP プロキシを構成します。

- 外部 PBX を使用して、1 つの信頼済みエンドポイントから同じ Firebox の背後にある別の信頼済みエンドポイントを呼び出しできません。これは一般に NAT の「ヘアピン」シナリオとして知られています。[23872]
- SMTP プロキシで uuencode および binhex の添付ファイルが完全に除去されません。添付ファイル ヘッダーのごく一部が、拒否メッセージとともに電子メールの本文に残ります。[22989]
- VoIP の導入は複雑になることが多く、多数の標準プロトコルと独自プロトコルを使用します。現在のプロキシは、基本的な音声およびビデオの転送用に、H.323 および SIP プロトコルを使用する標準ベースのトラフィックだけをサポートしています。VoIP 業界では、これらの新しいプロキシはより厳密に Application Layer Gateway (ALG) と呼ばれています。一部の ALG の機能、サービス、および構成はサポートされていないことがあります。サポートされない機能にはデータ ファイル転送 (チャット、ホワイトボード、ファックス送信などの用途) やトラフィック制御 (QoS) があり、また、プロトコルごとに後述する制限があります。これらの変動的な要素のため、実際の環境内で互換性テストおよび相互運用性テストを行ってから製品を導入することを強くお勧めします。
- H.323 プロキシでは、音声およびビデオのトラフィック用に NAT Traversal がサポートされています。このリリースでは、H.323 GateKeeper (PBX ホスティング/トランキング) および T.120 マルチメディアはサポートされていません。このため、プロキシの使用はポイント ツー ポイントのシナリオ (テレビ会議など) に限定されます。互換性と相互運用性は保証できませんが、ポイント ツー ポイントの音声およびビデオの接続性は、一般的なソフトウェア クライアントおよびテレビ会議ハードウェアで実証されています。
- 透過的な SIP プロキシでは、音声およびビデオのトラフィック用に NAT Traversal がサポートされています。通常のスタンドアロン SIP レジスタ - プロキシの PBX 登録機能はありませんが、代わりに SIP トラフィックに透過的な Application Layer Gateway が提供されています。透過的な SIP プロキシではこの PBX トラフィックのパススルーはサポートされませんが、独自のレジスタ - プロキシ サーバーでこれらの接続をルーティングする必要があります。このリリースでは、透過的な SIP プロキシは Firebox の外部セグメントにある PBX でのみテスト済みです (ホストシナリオ、トランキングなし)。互換性および相互運用性は保証できませんが、音声およびビデオのポイント ツー ポイント接続は代表的なソフトウェア クライアントを使用して実証されています。ホストされたオーディオ接続は、さまざまな電話機を使用して実証されています。

WebBlocker

- WebBlocker の構成によって HTTPS 接続が正常にブロックされている場合、拒否メッセージはクライアントに返信されません。ブロックされた HTTPS 接続はログ ファイルに正確に記録されます。[22515]

spamBlocker

- [Quarantine Server] > [自動削除ルールの編集] ダイアログ ボックスで、[件名に特定のテキストが含まれるメッセージの自動削除] ルールの変更が Quarantine Server に保存されません。このルールは、削除されていると UI で示されますが、有効になったままです。このルールを無効にするには、[件名に特定のテキストが含まれるメッセージの自動削除] のチェック ボックスをオフにします。[26796]
- Virus Outbreak Detection (VOD) が有効になっている spamBlocker と Gateway AV の両方を使用して電子メールをスキャンする場合、スパムでもウィルスでもある電子メール メッセージが SMTP プロキシで検出されると、SMTP プロキシは VOD 用に構成されたアクションをメッセージに適用します。具体的には、VOD アクションが [除去] に設定されている場合、添付ファイルはメッセージから削除されて復元できません。VOD アクションが [ロック] に設定されている場合、添付ファイルは検疫メッセージ内でロックされます。[23709, 23711]
- spamBlocker が電子メール メッセージに Virus Outbreak Detection (VOD) の兆候を検出すると、電子メールの添付ファイルはすべて除去または検疫されます。送信元のクライアントが HTML 形式で電子メールを送信した場合、電子メールの本文もこの対象になります。
- 複数パートの添付ファイルを持つ電子メール メッセージ (組み込みの電子メール メッセージなど) の感染が VOD によって検出された場合、Firebox に [除去] アクションが構成されていると、添付ファイルの拒否メッセージとともに添付ファイルの電子メール ヘッダーの一部が配信された添付ファイルに残ります。ウィルス関連コンテンツは必ず除去されるため、このヘッダー情報によって問題が発生することはありません。[23550]
- Edge がプライマリ DNS サーバーにアクセスできない場合、spamBlocker は機能しません。[18159]

Gateway AV/IPS

- タイム ゾーンが変更されても、署名更新ログ メッセージには以前の日時情報が表示されます。Edge を再起動するまで、正しいタイム ゾーンが表示されません。[17754]

ワイヤレス

- 一部のレガシー ワイヤレス クライアント ハードウェアおよびソフトウェアでは、クライアントがワイヤレス ネットワークの 1 つに既に接続している場合に、すべてのワイヤレス ネットワークが表示されないことがあります。別の Edge のワイヤレス ネットワークに接続する必要がある場合は、ワイヤレス ネットワーク アダプタを無効にしてから、再度有効にしてください。
- WAN1 インターフェイスがワイヤレス クライアントとして構成されている場合、トラフィック制御機能は正しく機能しません。[23757]
- Windows XP SP1 を実行中のワイヤレス クライアントでは、Edge が WPA2 のみを認証に使用するように構成されていると、接続できないことがあります。[23808]
- Edge のフロント パネルの WAP ライトは、Edge がワイヤレス アクセス ポイントとして構成されている場合、または外部 WAN1 インターフェイスがワイヤレス クライアントとして構成されている場合に点灯します。[23121]
- ワイヤレス ゲスト アカウントを有効にすると、Edge の再起動時に Edge DHCP サーバーが 3 回停止する場合があります。これは予想される状況であり、DHCP サーバーは Edge の再起動後 2 分以内に正常に機能します。[23792]
- XBOX 360 ワイヤレス クライアントを使用して、Edge へのワイヤレス接続を確立することはできません。[27481]
- Edge で以前のワイヤレス ゲスト サービス (Edge v8.0 ～ Edge v8.5) を実行している場合、Edge v10.2 にアップグレードした後、ゲスト サービスを再度構成する必要があります。

VPN

- Edge の信頼済みネットワークと同じサブネット内にあるリモート ネットワークへの BOVPN トンネルを使用して Edge が構成されている場合、信頼済みインターフェイスがアクセス不能になることがあります。信頼済み BOVPN ネットワークとリモートの BOVPN ネットワークとの間でネットワークが重複するように Edge を構成しないでください。[27106]
- IKE のキー再生成が頻繁に発生するように構成されていると、Edge のメモリ使用量が増加します。これにより、Edge の管理接続の速度が低下することがあります。既定の IPSec のキー再生成設定を変更する場合は、トンネルでのキー再生成が 1 時間に 2 回以下になるようにしてください。[24221]
- WSM の管理下で v8.6.2 とともにインストールされている Edge では、キー再生成の発生以後にトンネルを通過するトラフィックがない場合に、有効期限に基づいてキーが再生成されたトンネルに赤色の感嘆符が表示されます。このトンネルをトラフィックが通過すると、赤色の感嘆符は表示されなくなり、トンネルは正常に動作します。[22412]
- BOVPN トンネルで H.323 を使用する Avaya の電話により、Edge が再起動される場合があります。[24191]
- Cisco VPN クライアントを使用している場合、Edge を経由した Mobile VPN with IPSec の送信接続が確立されないことがあります。[19183]

Mobile VPN with SSL

- SSL クライアントが Edge に接続されている場合、管理者が SSL 構成を変更しても、SSL クライアントは Edge から切断されません。ユーザーは、手動で切断してから再接続して、新しい構成ファイルを取得する必要があります。[23921]
- [Firebox ユーザー] ページで既定のグループを編集すると、[Mobile VPN with SSL によるリモート アクセスを許可] チェック ボックスがオンになりますが、有効にはならないため変更できません。[23449]
- Mobile VPN with SSL クライアントを Windows 2000 Pro コンピュータにインストールすることはできません。[23667]
- Mobile VPN with SSL クライアントは信頼済みネットワークから Edge に接続できません。[22547]

  回避策

  任意ネットワークから Edge に接続するように Mobile VPN with SSL クライアントを構成します。

- Mobile VPN with SSL Mac クライアントは、Firebox への接続が失われた (切断ではなく) ときに構成をチェックしません。VPN 接続を再度確立するには、切断してから再度接続する必要があります。[23109]

SNMP

- SNMP v3 を使用するように Edge を構成する場合、パスワードは 8 文字以上でないと正しく機能しません。[23531]

トラフィック制御

- IPSec 用のトラフィック制御では、最も限定的なルールではなく、VPN-ANY ルールが使用されます。[24206]

ログ記録とリアルタイムな監視

- Edge の UI で [システム ステータス] ページを選択すると、"httpd doInclude: INCLUDE failed for "lang.inc" result code was -1" というエラーがログ ファイルに示されることがあります。このログ メッセージは情報メッセージであり、無視してかまいません。[27322]
- Edge が従来の WatchGuard セキュリティ イベント プロセッサ ログ サーバーにログ メッセージを送信すると、ログが切り詰められて表示されます。[27430]
- 信頼済みネットワークと任意ネットワークとの間のトラフィックは、イベント ログ ファイルに表示されません。[15611]
- [ネットワーク] > [トラフィック制御] ページで [トラフィックの優先順位をログに記録する。] を有効にしても、プロキシ ポリシーで生成されるログ メッセージには優先順位が含まれません。[23164]

Edge を出荷時の既定設定にリセットする

- 出荷時の既定の設定に戻しても、構成ファイルが消去されません。[15174]

> **回避策**
>
> Edge を出荷時の既定の設定に戻す場合、構成ファイルを消去するには、Firebox X Edge e-Series のリセット ボタンを必ず 45 秒以上押してください。

ユーザー インターフェイス

- Edge v10.2 ソフトウェアには、ユーザー インターフェイスに影響しないバグ修正が多数あります。v10.2 リリースでのユーザー インターフェイスの変更はローカライズされていません。ローカライズされた v10.1 リリースから v10.2 リリースにアップグレードする場合は、新しい UI 要素が英語のままになっていることに注意してください。ローカライズされたヘルプ コンテンツの更新事項はありません。
- Quick Setup Wizard で機能キーを入力した後、2 回目のログイン プロンプトが表示されます。[21994]
- Edge を v8.x から v10.1 にアップデートした後、新しいユーザー インターフェイス オプションとすべての新機能を表示するには、ブラウザ キャッシュの削除が必要な場合があります。[20457]
- Internet Explorer v7 を使用して Firebox X Edge e-Series を管理する場合、証明書セキュリティの警告が表示されます。IE および Firefox の他のすべてのバージョンと違って、IE7 の警告は表現が強く、操作の中止を勧める内容となっています。このメッセージは無視できます。Firebox X Edge では、IP アドレスを既定設定から変更することができるので、Firebox の証明書には IP アドレスが含まれていません。要求された IP アドレスと証明書が一致しないため、この警告が表示されます。[14434]

シングル サインオン (SSO) 実装の注意点

Firebox X Edge v10.0 リリースでは、現在 Active Directory ユーザー認証を使用している Firebox 管理者のシングル サインオン (SSO) がサポートされています。SSO が機能するためには、SSO エージェント ソフトウェア (WatchGuard Authentication Gateway ソフトウェア) を、ネットワーク上の静的 IP アドレスを持つドメイン コンピュータにインストールする必要があります。SSO エージェント ソフトウェアをインストールするコンピュータに Microsoft .NET Framework 2.0 がインストールされていることを確認してください。シングル サインオンは、Windows 2000 Advanced Server ドメイン コントローラおよび Windows 2003 ドメイン コントローラで検証済みです。

シングル サインオン エージェント ソフトウェアをインストールする前に、ユーザー アカウントを作成する必要があります。このソフトウェアは、作成するユーザー アカウントの権限で実行されます。

- ユーザー アカウントを Domain Admin グループに追加し、Domain Admin グループをユーザーのプライマリ グループとして設定する必要があります。
- ユーザー アカウントは、無期限のパスワードで構成する必要があります。
- このユーザー アカウントは、サービスとしてログオンする権限で構成する必要があります ([ドメイン セキュリティ ポリシー]、[ローカル ポリシー]、[ユーザー権利の割り当て]、[サービスとしてログオン] の順に選択)。
- SSO エージェント ソフトウェアをインストールするコンピュータの IP アドレスを、Edge 構成の SSO 例外リストに追加する必要があります ([Firebox ユーザー] > [設定])。

実装の注意点

- ユーザーが SSO を使用して認証を行うすべてのコンピュータで、印刷およびファイル共有が有効になっていることを確認します。
- ユーザーが SSO を使用して認証を行うすべてのコンピュータで、NetBIOS および SMB ポートがブロックされていないことを確認します。NetBIOS では TCP/UDP ポート 137、138、139 を、SMB では TCP ポート 445 を使用します。
- ユーザーが SSO を使用して認証を行うすべてのコンピュータが、完全に信頼できるドメイン メンバーであることを確認します。

ユーザー ドキュメント

Edge v10.2 リリースのドキュメントの変更内容は、WatchGuard の Web サイト (www.watchguard.com/help/documentation) で入手可能な更新済みの英語のヘルプ システムに含まれています。このリリースでは、Edge のユーザー ガイドは更新されていません。

技術サポート

技術サポートについては、電話または Web サイト (http://www.watchguard.com/international/jp/support.asp) で WatchGuard テクニカル サポートにお問い合わせください。テクニカル サポートへのお問い合わせ時には、登録した製品シリアル番号、LiveSecurity キーまたはパートナー ID をお知らせください。

	電話番号
米国のエンド ユーザー	877.232.3531
米国以外のエンド ユーザー	+1 206.613.0456
WatchGuard 正規販売代理店	206.521.8375