SonicWall Secure Mobile Access 10.2.1
リリース ノート

このリリース ノートでは、SonicWall Secure Mobile Access (SMA) 10.2.1 日本語版リリースについて説明します。

バージョン:

- バージョン 10.2.1.12
- バージョン 10.2.1.11
- バージョン 10.2.1.10
- バージョン 10.2.1.9
- バージョン 10.2.1.8
- バージョン 10.2.1.7
- バージョン 10.2.1.6
- バージョン 10.2.1.5
- バージョン 10.2.1.4
- バージョン 10.2.1.3
- バージョン 10.2.1.2
- バージョン 10.2.1.1
- バージョン 10.2.1

バージョン 10.2.1.12

2024 年 4 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス (SMA) は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security (SSL/TLS) によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、ESXi、Microsoft Hyper-V、Amazon ウェブ サービス (AWS)、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.12 は、キャプチャ セキュリティ センター (CSC) と互換性があります。
- CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF (ウェブ アプリケーション ファイアウォール) 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。
- CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.12 は、次の SonicWall 装置でサポートされます。

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

このリリースには、次の新機能が含まれています。

セキュア モバイル アクセス 10.2.1.12 以降で、「連続ログイン失敗時に送信元 IP を遮断する」が追加されました。

「連続ログイン失敗時に送信元 IP を遮断する」は既定で有効化されている機能で、IP アドレスを遮断して装置へのアクセスを許可しないようにします。

詳細に関しては、『*SMA100 10.2 管理ガイド*』の「*連続ログイン失敗時に送信元 IP を遮断する*」セクションを参照してください。

追加の参考情報

SMA-4993。

バージョン 10.2.1.11

2024 年 2 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス（SMA）は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security（SSL/TLS）によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス（AWS）、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.11 は、キャプチャ セキュリティ センター（CSC）と互換性があります。
- CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF（ウェブ アプリケーション ファイアウォール）脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。
- CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.11 は、次の SonicWall 装置でサポートされます。

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

このリリースには、これまでに報告された問題に対する修正が含まれています。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3904	ウェブ アプリケーション ファイアウォールのグラフの接続数に統計がありません。
SMA-4716	デバイスが不安定です。
SMA-4764	10.2.1.9 にアップグレードすると、「仮想オフィス」のブックマークされたページが文字化けします。
SMA-4789	新モードで、名前に空白を含むボットネット ポリシーを追加すると、ポリシーが保存されません。
SMA-4795	NetExtender ユーザが、サーバ応答エラーによって初期パスワードの変更に失敗します。
SMA-4802	AWS 用 SMA 500v をインストールする際に、鍵ペアが authorized_keys に関連付けされません。
SMA-4805	SMA100 MFA の不適切なアクセス制御の脆弱性。
SMA-4820	演算子フィールドに「部分一致」を伴うウェブ アプリケーション ファイアウォール ルールが作成できません。
SMA-4821	不正な構文のログイン ポリシーの削除が、「Get user's setting failed (ユーザ設定の取得に失敗しました)」によって失敗します。
SMA-4829	完全なインポートと部分的なインポートのいずれを行っても、装置にアクセスできなくなってしまいます。
SMA-4857	EPC が失敗した時に、ユーザ定義のメッセージが表示されずに、既定のメッセージが表示されます。

確認されている問題点

該当なし。

追加の参考情報

該当なし。

バージョン 10.2.1.10

2023 年 11 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス（SMA）は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security（SSL/TLS）によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス（AWS）、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.10 は、キャプチャ セキュリティ センター（CSC）と互換性があります。
- CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF（ウェブ アプリケーション ファイアウォール）脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。
- CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.10 は、次の SonicWall 装置でサポートされます。

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

このリリースには、以下の新機能、廃止された機能、および、これまでに報告された問題に対する修正が含まれています。

新機能

Secure Mobile Access 10.2.1.10 以降に追加された機能は以下の通りです。

- Azure/AWS プラットフォーム用 SMA 装置に対する DNS 設定のカスタマイズ
- Azure/AWS プラットフォーム用 SMA 装置に対するデフォルト ゲートウェイのカスタマイズ
- 送信元 IP アドレスに対してロックアウトを有効にします。

詳細に関しては、『*SMA100 10.2 管理ガイド*』の「*新機能*」セクションを参照してください。

廃止された機能

この機能は、Secure Mobile Access 10.2.1.10 以降で廃止されました:

- 旧ユーザ インターフェース (UI) の廃止。

詳細に関しては、『*SMA100 10.2 管理ガイド*』の「*廃止された機能*」セクションを参照してください。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-4120	将来のリリースで、クライアント側の古い JavaScript ライブラリ (Jquery) のアップグレードが必要です。
SMA-4187	SMTP パスワードが平文で表示されます (読み取り専用アカウントでも同様)。隠蔽されるべきです。
SMA-4518	SYSNET より、PCI スキャン失敗の問題。

問題番号	問題の詳細
SMA-4557	NTP サーバを有効にすると、1 分 ～ 2 分で時間がリセットされるため、TOTP 接続に失敗します。
SMA-4596	パス関連の問題があります。
SMA-4597	Azure 用 SMA で、カスタム設定の有無にかかわらず DNS 設定を調整できません。
SMA-4620	SMA-4499 の問題により、重複したデバイスがデバイス管理に表示されます。
SMA-4625	「仮想オフィス」ポータルにログインして、接続するために NetExtender をクリックすると、DNS 接尾辞がクライアントに供給されません。NetExtender を直接使った場合は正しく動作します。
SMA-4656	Azure プラットフォーム用 SMA 500v のファームウェアを 10.2.1.7-50sv から 10.2.1.8-53sv にアップグレードすると、SMA 装置にアクセスできなくなります。
SMA-4661	SMA が接続要求の認証を中止します。ウェブ ポータルにログインすると、「ERROR = Socket Creation Failed（エラー = ソケット作成失敗）」が発生します。
SMA-4668	ユーザ定義の「ウェブ アプリケーション ファイアウォール」ルールのクロス サイド スクリプトが、httpd プロセスの再起動ループを起こします。
SMA-4674	ダウンロードされた NetExtender インストーラが検証できません。信頼される SSL VPN サーバへの接続と NAC エージェントに問題がないことを確認してください。
SMA-4675	10.2.1.9 で、EasyAccess 関連により httpd プロセスがデバイスの再起動に失敗します。設定のインポートができません。
SMA-4678	[%] を入力しても、ワンタイム パスワード電子メールに件名情報が含まれていません。
SMA-4679	SMA 10.2.1.9 バージョンで Connet Agent バージョン 1.1.46 を使用すると、仮想オフィスで EPC 確認に失敗します。
SMA-4682	SonicWall 仮想 SMA の Webshell – マルウェア分析。
SMA-4698	「イベント ログの電子メール送信先」の電子メール アドレス フィールドに電子メール アドレスが入力されているにもかかわらず、イベント ログの手動送信に失敗します。
SMA-4705	KVM プラットフォーム用 SMA 500v で、10.2.1.0-17sv から 10.2.1.1-19sv にアップグレードすると、ライセンスの同期に失敗します。
SMA-4713	10.2.1.9 バージョンにアップグレードすると、soniclicense.global.sonicwall.com への接続に失敗します。
SMA-4724	「Let's Encrypt」の証明書が自動的に更新されません。
SMA-4759	認証済 RCE。
SMA-4783	SMA 100 装置で、重複した AD ユーザによって MFA がバイパスされます。
SMA-4761	ワンタイム パスワード メッセージで、日本語や中国語などの Unicode 文字が文字化けします。
SMA-4784	EPC エージェントのシグネチャ証明書が失効してるため、EPC のインストールと更新ができません。
SMA-4787	NetExtender Windows が OPSWAT パッケージを検証できず、接続に失敗します。

追加の参考情報

SMA-4702

バージョン 10.2.1.9

2023 年 8 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス（SMA）は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security（SSL/TLS）によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス（AWS）、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.9 は、キャプチャ セキュリティ センター（CSC）と互換性があります。
- CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF（ウェブ アプリケーション ファイアウォール）脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。
- CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.9 は、次の SonicWall 装置でサポートされます。

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

このリリースには、これまでに報告された問題に対する修正が含まれています。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3108	PCI スキャンが、一般的に使用される素数を SMA が使用していることを検出しました。
SMA-3414	メモリの使用率が高くなると、デバイスが再起動します。
SMA-3704	AWS プラットフォーム上の SMA 500v が正常に起動した後、1 時間以内にオフラインになります。
SMA-3712	メモリの使用率が 98% に達すると、デバイスが再起動します。
SMA-3798	デバイスが外部ユーザをログ オフした後に、削除できないローカル ユーザが作成されます。
SMA-3867	DHCP が複数のクライアント要求に対して同一の IP アドレスをリースします。
SMA-3889	ローカル ユーザを削除できません。
SMA-3947	電子メール設定を設定しようとすると、未知のエラーが表示されます。
SMA-3967	新モードで証明書ページが表示されません。
SMA-3971	ブックマークされたウェブサイトが正しく表示されません。
SMA-4018	Mac Pro デバイスで、Mobile Connect、MacOS、WireGuard および Connect Tunnel が動作しません。
SMA-4035	https://デバイス IP/_api_/v1/doc.json に脆弱性があります。
SMA-4039	ユーザ アカウント名の文字制限に問題があります。
SMA-4047	ユーザ定義ポートを使用した NetExtender で、Duo 認証に失敗します。

問題番号	問題の詳細
SMA-4096	記号 "&" が含まれたクライアント証明書を新モードで使用すると、ログインに失敗します。
SMA-4116	EPC のバージョンを更新できません。
SMA-4117	ユーザ名の大文字と小文字の区別を無効にするオプション。
SMA-4130	HTTPS ブックマークで画像が読み込まれません。
SMA-4154	セッションに関係のない IP アドレスがログの送信元 IP アドレスに表示されます。
SMA-4191	日本語 UI の問題: iPerf > iPref。
SMA-4236	macOS のブラウザで、クライアント証明書の EPC 確認に失敗します。Mobile Connect では動作します。
SMA-4329	新モードで、地域 IP の国に色づけがされていません。
SMA-4352	10.2.1.7 にアップグレードした後、PHP インジェクション攻撃 – 単一ユーザの問題があります。
SMA-4482	10.2.1.7-50sv が動作している SMA 400 の誤検知の事例 (シリアル番号: 18B1694D3E10)。
SMA-4515	仮想オフィスにユーザ定義ポートを構成すると、デバイスが再起動します。
SMA-4529	10.2.1.7-50sv.jpn を工場出荷時の状態で開始した後に GUI にアクセスすると、内部サーバ エラーが表示されます。
SMA-4615	10.2.1.8 にアップグレードした後、WAF が妨げられることで、ポータルからウェブサイトにアクセスできなくなります。

確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-4491	アップグレード ビルドで、ESXi-VA の UI と CLI からセーフ モード オプションが削除されています。

追加の参考情報

このセクションでは、本リリースでの追加の参照情報のリストを示します。

問題番号	問題の詳細
SMA-4349	日本語ファームウェアで WAF レポートが正しく出力されません。
SMA-4012	メモリ使用率が高くなります。

バージョン 10.2.1.8

2023 年 5 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス（SMA）は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security（SSL/TLS）によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス（AWS）、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.8 は、キャプチャ セキュリティ センター（CSC）と互換性があります。
- CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF（ウェブ アプリケーション ファイアウォール）脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。
- CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.8 は、次の SonicWall 装置でサポートされます。

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

このリリースには、セキュリティの強化と、これまでに報告された問題に対する修正が含まれています。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-4401	セキュリティの堅牢化。
SMA-4471	地域 IP ポリシーが米国へのすべてのトラフィックを遮断するように構成されている場合、EPC（OPSWAT ライブラリ）の更新が動作しません。

バージョン 10.2.1.7

2023 年 3 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス（SMA）は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security（SSL/TLS）によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス (AWS)、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.7 は、キャプチャ セキュリティ センター (CSC) と互換性があります。
- CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF (ウェブ アプリケーション ファイアウォール) 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。
- CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.7 は、次の SonicWall 装置でサポートされます。

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

セキュリティの強化

- 新しいファームウェアの入手可能の通知
  アップグレード用の新しいファームウェアが利用可能であることを通知するために、「システム > ライセンス」ページにファームウェア アップグレードの通知を追加しました。高レベルのセキュリティ対策と最適な性能を得るために、最新のファームウェア バージョンを使用することを推奨します。
  詳細に関しては、SMA100 10.2.1『*管理ガイド*』の「*新しいファームウェアの入手可能の通知*」セクションを参照してください。

- OpenSSL バージョンのアップグレード
  OpenSSL ライブラリが、最新のバージョン 1.1.1t に更新されました。この最新のバージョンは、CVE-2022-4304 に記載されている OpenSSL の脆弱性が修正されています: タイミングベースのサイド チャンネルが OpenSSL RSA 復号化の実装に存在します。
  詳細に関しては、SMA100 10.2.1『*管理ガイド*』の「*OpenSSL バージョンのアップグレード*」セクションを参照してください。
- 追加のセキュリティの強化
  - SMA100 自身を防御するために、WAF（ウェブ アプリケーション ファイアウォール）を強制します。
  - 2FA（2 段階認証）、パスワード失効、および、WAF（ウェブ アプリケーション ファイアウォール）の有効化を含む、セキュリティ構成を警告します。
  - SMA 500v を AWS または Azure 環境に展開する際に、ユーザが追加した起動後に自動的に実行されるユーザ定義スクリプトを無効にします。
    ⓘ **メモ:** セキュリティ強制のため、SMA 500vに展開されたユーザ スクリプトは今後動作しなくなります。バージョン 10.2.1.7 にアップグレードする前に存在していたユーザ スクリプトは、アップグレード以降動作しなくなります。
  - ファームウェアの整合性を確認するために、追加のセキュリティ確認がされます。
  - トラフィック制限 – ファームウェアの整合性に問題が検知された場合、SMA はそれ自身が始動した送信通信を制限します。アプリケーションまたはネットワーク上のリソースに対するユーザの VPN アクセスには影響しません。
  - まれな状況で、ファームウェアの整合性確認が偽陽性の状態になり、SMA はそれ自身が始動した送信電子メール/Syslog 通信を制限します。さらなる確認と分析により、送信電子メール/Syslog 通信は通常の動作に復旧します。

  詳細に関しては、SMA100 10.2.1『*管理ガイド*』の「*追加のセキュリティの強化*」セクションを参照してください。

ファームウェアのアップグレード

SMA100 シリーズのファームウェア アップグレードに関する情報については、次の『ナレッジ ベース』の記事を参照してください。

- SMA100 シリーズのファームウェアのアップグレード方法について
- 追加で必要な SMA 100 シリーズ 10.X および 9.X ファームウェア更新
- SMA100 シリーズのアップグレード パス
- SMA 100 シリーズ 10.2.1.7 での OpenSSL ライブラリの更新

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3940	内部 SSH デーモン構成の問題により、PCI スキャン テストでそれに脆弱性があると表示されます。
SMA-4179	CVE-2022-4304: タイミングベースのサイド チャンネルが OpenSSL RSA 復号化の実装に存在します。

バージョン 10.2.1.6

2022 年 8 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス (SMA) は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security (SSL/TLS) によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス (AWS)、Azure および KVM が動作する仮想装置として利用できます。

重要

SonicWall 製品の OpenSSL 無限ループの潜在的な影響に関する情報については、次の「ナレッジ ベース」記事を必ずご確認ください。

- セキュリティ通告: 証明書解析時の OpenSSL 無限ループ (CVE-2022-0778)。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.6 は、キャプチャ セキュリティ センター (CSC) と互換性があります。
- CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

- CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。
- SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.6 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

NetExtender バージョン	サポート対象ファイアウォール ファームウェア
Windows 10/11 用 NetExtender クライアント 10.2.331 および Linux 用 NetExtender クライアント 10.2.845	GEN 6 – 6.4.5.9-93n、GEN 7 – 7.0.1-5030 以降

NetExtender バージョン	サポート対象 SMA ファームウェア
Windows 10/11 用 NetExtender クライアント 10.2.331 および Linux 用 NetExtender クライアント 10.2.845	10.2.1.6-37sv 10.2.1.5-34sv

新機能

- Windows 10/11 用 NetExtender 10.2.331 および Linux 用 NetExtender 10.2.845 のサポート

メモ: 最新の NetExtender バージョンは、SMA 100 シリーズ ファームウェアの最新バージョンとともに使用することを推奨します。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3437	地域 IP フィルタが、遮断した国を遮断しません。
SMA-3518	再起動すると、AWS の展開が利用なくなり、ライセンスが失われます。

問題番号	問題の詳細
SMA-3521	Windows のログイン画面に NetExtender ダイアルアップが表示されません。
SMA-3551	WireGuard トンネルがセッション制限に達しても切断されません。
SMA-3607	HTTP ブックマークが動作しません
SMA-3628	装置が無作為に応答しなくなり、ユーザが切断されます。
SMA-3637	10.2.0.9 から 10.2.1.4 にアップグレードした後に、ボットネットの追加、および、地域 IP ポリシーの編集または削除をすると、エラーが表示されます。
SMA-3652	手動アップグレードのライセンス テキスト ボックスが Hyper-V、Azure と AWS で利用できます。
SMA-3667	管理者に送信されるワンタイム パスワード エラーと警告電子メールに、ユーザ情報が記載されていません。
SMA-3684	SMA 装置のセキュリティ設定を有効にすると、侵入テストで低レベルの危険度が見つかります。
SMA-3688	ポータル設定を変更した後に、装置が動作を停止します。
SMA-3692	[脆弱性] SonicWall SMA 100 ヘルプ バッファ オーバーフロー
SMA-3701	展開後の `.tar` ファイルの表示と読み取りができません。
SMA-3714	Windows 用 NetExtender 10.2.324 バージョンが EPC 確認に失敗します。
SMA-3715	Hyper-V 用 SMA で、EPC Windows 10 ポリシーが動作しません。
SMA-3720	EPC をアップグレードすると、NetExtender の接続に失敗します。
SMA-3723	SMA 100 上の複数の古い 3PL とバージョン開示の脆弱性
SMA-3727	「**新しいファームウェアが利用可能になった時に通知する**」オプションが動作しません。
SMA-3728	Windows バージョンに対する EPC 確認に失敗します。
SMA-3756	コンピュータ システム上で Windows ユーザを切り替えると、プロファイルが既に作成されていたとしても、ユーザ名のない新しいプロファイルが作成されます。
SMA-3759	SMA 10.2.1.5 バージョンが、要求中にヘッダーへのコードの挿入を許可します。
SMA-3766	証明書に誤りがあることを示す代わりに、警告メッセージ「***certificate chain too long. Do you want to proceed? Hostname for this server does not match hostname in certificate (証明書チェーンが長すぎます。続行しますか? このサーバのホスト名と証明書のホスト名が一致しません)***」が表示されます。
SMA-3774	装置からのレポートが正確ではありません。
SMA-3775	WireGuard NetExtender クライアントが、グループ レベルからのクライアント ルートを取得しません。
SMA-3777	NetExtender を 10.2.324 にアップグレードすると、Windows のネットワーク ログイン機能が利用できません。
SMA-3824	Windows 10 バージョンで、EPC 確認に失敗します。

追加の問題点

SMA-3872

バージョン 10.2.1.5

2022 年 4 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス (SMA) は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security (SSL/TLS) によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス (AWS)、Azure および KVM が動作する仮想装置として利用できます。

重要

SonicWall 製品の OpenSSL 無限ループの潜在的な影響に関する情報については、次の「ナレッジ ベース」記事を必ずご確認ください。

- セキュリティ通告: 証明書解析時の OpenSSL 無限ループ (CVE-2022-0778)。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.5 は、キャプチャ セキュリティ センター (CSC) と互換性があります。
  CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。
  CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。
  SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.5 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

NetExtender バージョン	サポート対象ファイアウォール ファームウェア
Windows 10/11 用 NetExtender クライアント 10.2.324 および Linux 用 NetExtender クライアント 10.2.839	GEN 6/6.5 – 6.4.5.9-93n、GEN 7 – 7.0.1-5030 以降

NetExtender バージョン	サポート対象 SMA ファームウェア
Windows 10/11 用 NetExtender クライアント 10.2.324 および Linux 用 NetExtender クライアント 10.2.839	10.2.1.5-34sv

新機能

- Windows 10/11 用 NetExtender 10.2.324 および Linux 用 NetExtender 10.2.839 のサポート。

ⓘ **メモ:** 最新の NetExtender バージョンは、SMA 100 シリーズ ファームウェアの最新バージョンとともに使用することを推奨します。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3141	AJAX 呼び出しで予期しない 403 状況になるため、HTTP ブック マークが動作せず、SQL インジェクション攻撃を受けます。
SMA-3240	ファームウェアを 10.2.0.8 にアップグレードした後、Windows と macOS 上の HTTP リソースが動作を停止します。
SMA-3390	状況ページで、地域 IP の解決が動作せず、「不明」になります。
SMA-3392	SMA が NetExtender に反対側のクライアント IP アドレスを無作為に割り当てます。

問題番号	問題の詳細
SMA-3405	NetExtender を使用すると、ユーザが内部リソースまたはインターネットに断続的にアクセスできなくなります。
SMA-3411	NetExtender 接続を切断しても、ユーザ ライセンスがすぐに解放されません。
SMA-3421	ユーザにメッセージ「Failed to get WireGuard parameters (WireGuard パラメータの取得に失敗しました)」が表示されます。
SMA-3432	Werkzeug ライブラリと Python インタプリタにバージョン開示の脆弱性があります。
SMA-3436	Windows 7 上で、EPC が Windows Defender を検知できません。
SMA-3470	新モードのポータル ログインで、パスワード表示ボタンを無効にします。
SMA-3492	ネイティブ ブックマーク認証で、Azure AD に参加したコンピュータの PIN は動作しますが、パスワードが失敗します。
SMA-3501	インターネット トラフィックが内部プロキシ設定を通してルートされません。最新の NetExtender 10.2.319 で無視されます。
SMA-3509	SMA Connect Agent のインストールに失敗します。アップデートを試みると、最新版と表示されます。
SMA-3522	POST 認証コマンド インジェクションの脆弱性があります。
SMA-3553	WireGuard トンネル プロトコルを使用すると、リソースにアクセスできません。
SMA-3559	システムが休止状態/スリープから復旧しても、AOV を使用した NetExtender が自動的に再接続しません。
SMA-3568	NetExtender Windows クライアント v10.2.322 で、バッファ オーバーフローが発生します。
SMA-3573	新モードで、RDP ブックマークの自動ログインが無効化されています。
SMA-3582	10.2.1.4 の GUI が適切に日本語翻訳されていません。
SMA-3599	WireGuard プロトコルを使用すると、無動作時タイムアウトがリセットされません。
SMA-3606	SMA100 OpenSSL CVE-2022-0778 DoS の脆弱性。
SMA-3610	NetExtender OpenSSL CVE-2022-0778 DoS の脆弱性。
SMA-3640	SMA 500v で、SMA/オーバービュー/レポートがダウンロードされません。

確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-3652	手動アップグレード テキスト ボックスが Hyper-V、KVM、Azure と AWS で利用できます。

バージョン 10.2.1.4

2022 年 1 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス (SMA) は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security (SSL/TLS) によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス (AWS)、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.4 は、キャプチャ セキュリティ センター (CSC) と互換性があります。

  CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

  CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。

  SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.4 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

NetExtender バージョン	サポート対象ファイアウォール ファームウェア
Windows 10/11 用 NetExtender クライアント 10.2.322 および Linux 用 NetExtender クライアント 10.2.835	GEN 6/6.5 – 6.4.5.9-92n、GEN 7 – 7.0.1-5030

NetExtender バージョン	サポート対象 SMA ファームウェア
Windows 10/11 用 NetExtender クライアント 10.2.322 および Linux 用 NetExtender クライアント 10.2.835	10.2.1.4-31sv

新機能

- Windows 10/11 用 NetExtender 10.2.322 および Linux 用 NetExtender 10.2.835 のサポート

ⓘ **メモ:** 最新の NetExtender バージョンは、SMA 100 シリーズ ファームウェアの最新バージョンとともに使用することを推奨します。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3361	ユーザ裁量が選択されている場合、パスワードを変更できません。
SMA-3335	接続パラメータ状況の最初の初期化中に、NetExtender が停止します。
SMA-3227	NetExtender 10.2.319 にアップグレードした後に、Google に関連するサイトへの接続が遅くなるか、または、到達できなくなります。
SMA-3310	NetExtender クライアント 10.2.319 を使用した後に、DNS 解決が動作しません。
SMA-3309	新しい NetExtender 10.2.319 でトラフィックが通過しません。

問題番号	問題の詳細
SMA-3307	バックアップに失敗するため、ゲスト(Azure)エージェントの更新が必要です。
SMA-3291	10.2.1.2 にアップグレードした後、Windows オペレーティング システムで接続後のスクリプトが動作しません。 ⓘ | **メモ:** これは 10.2.1.3 までの既知の問題です。10.2.1.4 で修正されました。
SMA-3284	UPN 名を使用すると、新・旧の両方のモードで「ドメイン試行タイムアウト」が発生します。
SMA-3282	Linux の NetExtender で WireGuard プロトコルを使用すると、DUO が動作しません。
SMA-3262	「**内部設定**」ページの「**定期的再起動**」に、誤った時刻が表示されます。
SMA-3242	10.2.1.2 と 10.2.1.3 にアップグレードした後、VoIP 通信に接続できません
SMA-3189	10.2.1.1 にアップグレードした後に、仮想オフィスから NetExtedner が起動できません。
SMA-3137	「Let's Encrypt」の証明書が自動的に更新されません。
SMA-3126	Linux 上の CMD プロンプトを使用した NetExtender で、SAML と Dual ユーザがログインできません。
SMA-2893	SND がワンタイム パスワードを入力しなくても検出します。

確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-3411	NetExtender 接続を切断しても、ユーザ ライセンスがすぐに解放されません。

追加の参考情報

SMA-3428

バージョン 10.2.1.3

2021 年 12 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス(SMA)は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理

対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security (SSL/TLS) によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス (AWS)、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.3 は、キャプチャ セキュリティ センター (CSC) と互換性があります。

  CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

  CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。

  SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.3 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
  - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
  - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

- SMA100 製品と WireGuard との統合。この機能についての情報は、サポート ポータル (https://www.sonicwall.com/ja-jp/support/technical-documentation/) で入手できる『*WireGuard Feature Guide (英語)*』をご覧ください。

  メモ: SMA 10.2.1.3 の WireGuard 機能は、テクニカル プレビュー ビルドです。WireGuard の完全なサポートは、SMA 10.2.2 以降で利用できる予定です。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3235	脆弱性: SMA100 で、複数の認証されないファイル エクスプローラ ヒープ ベースとスタック ベースのバッファ オーバーフロー。
SMA-3233	脆弱性: SMA100 で、POST 認証 RCE。
SMA-3231	脆弱性: SMA100 で、getBookmarks ヒープ ベースのバッファ オーバーフロー。
SMA-3229	新モードで、パスワード変更ダイアログが表示されません。旧モードでは表示されます。
SMA-3228	10.2.1.2 にアップグレードした後、NetExtender/Mobile Connect ユーザの DUO RADIUS 認証が動作しません。
SMA-3217	脆弱性: SMA100 で、重大な認証されないスタックベースのバッファ オーバーフロー。
SMA-3213	「Let's Encrypt」証明書が動作しません。
SMA-3208	脆弱性: SMA100 で、認証されない「混乱した代理」。
SMA-3207	脆弱性: SMA100 で、認証されない CPU 枯渇の脆弱性。
SMA-3206	脆弱性: SMA100 で、認証されないファイル アップロード パス横断の脆弱性
SMA-3204	脆弱性: SMA100 で、root として認証されたコマンド インジェクションの脆弱性。
SMA-3199	ユーザ ログインの顧客ロゴをクリックすると、管理コンソールにリダイレクトされます。
SMA-3138	ユーザ定義資格情報を伴う SSHv2 ブックマークを使用して SonicWall ファイアウォールに接続すると、エラーが発生します。
SMA-3111	脆弱性: HTTP ホスト ヘッド値の反映。
SMA-1980	セキュリティの問題: SMA エージェント/NetExtender が、個別のデバイス ID を割り当てません。

確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-3282	Linux の NetExtender で WireGuard プロトコルを使用すると、DUO が動作しません。
SMA-3281	「地域 IP とボットネット フィルタ > ポリシー」ページで地域 IP ポリシーを追加すると、警告メッセージ「国が選択されていません」が表示されます。
SMA-3262	診断設定ページの「定期的再起動」の時刻に誤りがあります。
SMA-3249	Linux の NetExtender で、複雑なパスワードに対するローカル パスワード更新のエラー メッセージに誤りがあります。

バージョン 10.2.1.2

2021 年 10 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス (SMA) は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security (SSL/TLS) によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス (AWS)、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。
- SMA 10.2.1.2 は、キャプチャ セキュリティ センター (CSC) と互換性があります。

  CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

  CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。

  SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.2 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

- SMA100 製品と WireGuard との統合。この機能についての情報は、サポート ポータル (https://www.sonicwall.com/ja-jp/support/technical-documentation/) で入手できる『*WireGuard Feature Guide (英語)*』をご覧ください。

  メモ: SMA 10.2.1.2 の WireGuard 機能は、テクニカル プレビュー ビルドです。WireGuard の完全なサポートは、SMA 10.2.2 以降で利用できる予定です。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-3121	ユーザが新 UI で仮想オフィスにログインする際、SMS ワンタイム パスワードを有効にした後にエラー メッセージが表示されます。
SMA-3112	10.2.1.1 にアップグレードした後、新モードで「ドメイン試行タイムアウト」が発生します。
SMA-3057	「ウェブ アプリケーション ファイアウォール > 状況」に、更新をインストールするためのボタンがありません。
SMA-3028	10.2.1.1 にアップグレードした後、NetExtender/Mobile Connect クライアント バージョンのオプションと表示がありません。
SMA-3006	10.2.1 にアップグレードした後、AD ユーザにエラー「ログインに失敗しました。適切なグループが見つかりません」が発生します。
SMA-2978	Linux の NetExtender で、自己署名証明書エラーが発生します。
SMA-2938	デバイス管理が有効化されている場合、Windows 7 のみで SMA Connect Agent がクラッシュするため、SMA で承認が行われません。
SMA-2935	10.2.1.x にアップグレードした後、NetExtender/Mobile Connect ユーザの DUO RADIUS 認証が動作しません。仮想オフィスは動作します。
SMA-2917	地域 IP データベースがエラー番号 2 によって同期しません。
SMA-2904	ユーザ定義ロゴに対して、ユーザ定義 URL を追加する必要があります。

確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-3213	「Let's Encrypt」証明書が動作しません。
SMA-3199	ユーザ ログインの顧客ロゴをクリックすると、管理コンソールにリダイレクトされます。
SMA-3126	Linux の cmd で起動した NetExtender クライアントを使用すると、SMAL ユーザがログインできません。
SMA-2941	EPC の属性が「スキャンされたファイル システム」に設定されている場合、10.2.1.0 にアップグレードした後に EPC 更新が失敗します。

バージョン 10.2.1.1

2021 年 9 月

セキュア モバイル アクセスについて

セキュア モバイル アクセス (SMA) は、拡張性と安全性に優れたモバイル アクセスを企業にもたらすと同時に、信頼できないアプリケーション、WiFi の無断使用、および、モバイル マルウェアを遮断します。SMA 装置は、管理対象と管理対象外のデバイスを含むすべてのプラットフォームで、単一のゲートウェイと共通のユーザ エクスペリエンスを提供します。トラフィックは Secure Sockets Layer/Transport Layer Security (SSL/TLS) によって暗号化され、不正なユーザから保護されます。

SMA は、物理装置、または、VMWare ESXi、Microsoft Hyper-V、Amazon ウェブ サービス (AWS)、Azure および KVM が動作する仮想装置として利用できます。

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。

- SMA 10.2.1.1 は、キャプチャ セキュリティ センター（CSC）と互換性があります。

  CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

  CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。

  SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1.1 は、以下の SonicWall 装置でサポートされます:

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
    - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
    - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

- 「修正された問題点」に一覧されている問題のメンテナンス修正

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-1583	各 500v インスタンス下のハイパーバイザ（VMWare、HyperV、Azure、AWS、その他）から分析データを取得できません。
SMA-2541	EPC 確認が失敗したにもかかわらず、EPC 確認が AOV セッションで繰り返し実行されます。
SMA-2746	10.2.1 へアップグレードした後に、CIFS ファイル共有ブックマークが意図したとおりに動作しません。
SMA-2836	新モードを使用してログインしようとすると、ドメイン取得の試行がタイムアウトします。
SMA-2846	ネットワークの変更を検知した際に、「VPN 常時有効」を有効にした NetExtender が自動的に再接続しません。
SMA-2847	フォルダ内のファイル名に ASCII 以外の文字が含まれている場合、フォルダのダウンロードに失敗します。
SMA-2851	HTTP DoS 設定により、オフロード ポータルが破棄されます。

問題番号	問題の詳細
SMA-2854	"X-Frame-Options" に "sameorigin" が設定されている場合、フレームが表示されません。
SMA-2856	新 UI モードで SMS ワンタイム パスワード オプションに切り替えると、常にワンタイム パスワードが起動されます。
SMA-2859	ワンタイム パスワードのユーザ裁量が有効の場合、ユーザ ポータルに設定オプションが表示されません。
SMA-2861	新モードで、ユーザが作成したブックマークを編集できません。
SMA-2866	Azure AD SSO で正常に認証した後に、タブのリソースが利用できません。
SMA-2867	10.2.0.6 にアップグレードした後に、アプリケーション オフロード ポータルが読み込まれません。
SMA-2892	NetExtender 10.2.313 クライアントを伴う 10.2.1.0 にアップグレードした後に、エラー「Your password has expired (パスワードの期限が切れました)」が表示され、接続できません。
SMA-2903	Azure の SMA 500v で、CPU とメモリ使用率が高く表示されます。
SMA-2905	バックアップ SMA にフェイルオーバーした際に、OKTA を使用した SAML 認証 が失敗します。
SMA-2587	10.2.1 にアップグレードした後に、装置のメモリ使用率が常に 92% を維持します。
SMA-2912	SMA 500v ESXi のファームウェアを 10.2.1.0 にアップグレードした後に、装置がクラッシュします。
SMA-2913	10.2.1.0 にアップグレードした後に、NetExtender クライアントのアドレス範囲が枯渇しています。
SMA-2587	装置を再起動した後に、SMTP パスワードが失敗します。
SMA-2939	NetExtender で接続すると、NetExtender クライアントの IP アドレスではなく、装置の IP アドレスがトラフィックに表示されます。
SMA-2940	2 段階認証 (2FA) を有効にすると、パスワード変更の入力画面が表示されません。
SMA-2947	公開しているポータルに、プライベート IP が表示されます。
SMA-2949	エラー メッセージ「Update Signature failed, error code 500 (シグネチャの更新に失敗しました。エラー コード 500)」により、シグネチャの更新が頻繁に失敗します。
SMA-2950	SAML 認証で、SMA Connect が NetExtender を起動しません。
SMA-2951	バックアップ システムがプライマリの役割に切り替わらず、IP の所有権を得ることができません。
SMA-2954	Pcap と netstat の結果に、NX IP ではなく SMA IP として通信が表示されます。
SMA-2957	認証済み SMA100 の任意のコマンド インジェクションの脆弱性。
SMA-2959	未認証 SMA100 の任意のファイルを削除する脆弱性。
SMA-3002	Net-SNMP パッケージに、NULL ポインタの確認が不十分である脆弱性があります (SNMP DoS)。
SMA-3015	高可用性でのコマンド インジェクションによるローカル権限昇格。

確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-2496	「既存のセッションからログアウトしたことを確認する」を伴った「多重ログインを禁止する」が意図したとおりに動作しません。
SMA-2904	SMA ポータルでユーザ定義ロゴの URL を設定できません。
SMA-2941	装置を 10.2.1.0 にアップグレードした後に、属性オプションの「スキャンされたファイル システム」が設定されている場合、EPC 更新が失敗します。
SMA-3001	装置を 9.0.0.10-28sv から 10.2.1.1-19sv にアップグレードした後に、証明書ドメインを使用してログインできません。 **応急:** • TLS 1.3 オプションを無効にします • ドメインを編集し、信頼された CA 証明書を確認します

アップグレード情報

最新ファームウェアの取得方法、SonicWall 装置のファームウェア イメージのアップグレード方法、および他の装置から構成設定をインポートする方法については、サポート ポータル (https://www.sonicwall.com/ja-jp/support/technical-documentation/) から入手できる『*SonicWall SMA アップグレード ガイド*』を参照してください。

バージョン 10.2.1

2021 年 6 月

互換性とインストールの注意事項

- 最も一般的なブラウザがサポートされますが、ダッシュボードの画像をリアルタイムで表示するには、Google Chrome を推奨します。
- MySonicWall アカウントが必須です。

- SMA 10.2.1 は、Capture Security Center (CSC) との互換性があります。

  CSC は、登録されたすべての SMA 装置の全体状況を表示するクラウド ダッシュボードを提供します。ダッシュボードには、時間範囲を選択するスライダー、および、警告、脅威、WAF 脅威、認証、VPN アクセス、ブックマーク アクセス、アクティブ デバイスと地図上のユーザの数、また、脅威種別が表示されます。

  CSC にログインするには、https://cloud.sonicwall.com で MySonicWall の資格情報を使用してください。

  SMA ダッシュボードの表示、登録の完了、および、クラウド管理を行うには、「SMA」タイルをクリックします。

SonicWall SMA 10.2.1 は、次の SonicWall 装置でサポートされます。

- SMA 200/400
- SMA 210/410
- ESXi 用 SMA 500v
  - VMware ESXi 6.0 以降への展開がサポートされています。
- Hyper-V 用 SMA 500v
  - Hyper-V サーバ バージョン 2016 および 2019 への展開がサポートされています。
- AWS 用 SMA 500v
- Azure 用 SMA 500v
- KVM 用 SMA 500v

新機能

Secure Mobile Access 10.2.1 に追加された機能は以下の通りです。

- **システム レポート**

  すべてのサポートされる基本および詳細の組み合わせを使用したシステム情報、システム状況、脅威、使用中のユーザ、およびアクティビティに関する機能性レポートを生成できます (英語のみ)。レポートは、日次、週次、月次でスケジュールできます。

- **HTML5 SSH 鍵ファイル認証のサポート**

  これまでに HTML SSH でサポートされていた認証方式は、ユーザ名とパスワードのみでした。特にクラウド環境内で、多くの SSH サーバが鍵ファイル認証サイトとして使用されるようになったため、鍵ファイル認証方式のサポートが追加されました。

  - HTML5 SSH ブックマークは、識別ファイル認証をサポートします
  - HTML5 SSH 機能は、識別ファイルとユーザ情報をブラウザのローカル記憶領域に保存できます
  - HTML5 SSH 機能は、保存された情報を SSH サーバに自動ログインするために使用できます

- **移行ツール**

  SMA プラットフォームの構成を移行する機能が開発されました。移行元デバイス インターフェースを移行先デバイス インターフェースに割り当てることで。主要なネットワーク構成を引き継ぐことができます。この新しいツールは、高可用性などのデバイス/ネットワークに関連する機能を無効にします。また、*ポリシー*などのデバイスに関連する機能構成のみを変換します。構成移行シナリオに関しては、『SMA100: 構成移行ツール』のナレッジ ベース記事を参照するか、サポートにご連絡ください。

- KVM 上の 500v **SMA**

  KVM 用 SMA 500v は、SMA 物理装置で利用できるほとんどの機能をサポートした SMA 500v 装置を KVM 環境で動作させることができます。

- **「コンテンツ セキュリティ ヘッダー」の「許可されたホスト」オプション**

  サードパーティのリソースをサポートする「コンテンツ セキュリティ ヘッダー」に「許可されたホスト」オプションを追加できます。サードパーティ URL を「**コンテンツ セキュリティ ポリシー設定**」に入力するには、装置の内部設定にアクセスする必要があります。

- **NetExtender と Mobile Connect クライアントで DUO セキュリティ認証のサポート**

  SMA のログインで、「**DUO セキュリティ認証**」をサポートします。「DUO セキュリティ認証」ログインは、新モードと旧モードの両方で、ウェブ ブラウザや Mobile Connect クライアントなどの異なるクライアントをサポートします。

- **「安全なネットワークの検出」のための「保護されたホスト」**

  「**安全なネットワークを検出する**」が有効の場合、新しい「**保護されたホスト**」設定を使用して、SMA はSSL 証明書が信頼されているかどうかを確認します。これにより、保護されたホストを「常に有効」な VPN 接続に追加することができるようになります。安全なネットワークが検知されなかった場合、クライアントは VPN に接続します。

- **iPerf 統合**

  ネットワーク性能の測定と調整をするために、iPerf を SMA に統合できます。iPerf は、あらゆるネットワーク上で標準化された性能測定を生成し、クライアントとサーバの両方として機能できます。iPerf は、エンド クライアント マシンおよびバックエンド リソース ホストとしての SMA 装置間での一方向または両方向のスループットを測定するデータ ストリームも作成できます。iPerf に含まれる出力は、転送されたデータ量と測定されたスループットのタイムスタンプが付けられたレポートです。

これらの新機能に関する詳細は、『*Secure Mobile Access 10.2 管理ガイド*』の「***新機能***」セクションを参照してください。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

問題番号	問題の詳細
SMA-2587	装置を再起動すると、すべてのログが削除されます。
SMA-2581	移行ツールは、低いモデルから高いモデルへのメッセージを伴って検証されるべきです。
SMA-2566	特定の状況下において、装置がライセンスを消費します。
SMA-2561	SRA 4600 からインポートされた設定が SMA へのログインを許可しません。
SMA-2539	「VPN 常時有効」機能が特定のドメインに対して期待通り有効になりません。
SMA-2393	日次ログ電子メールが期待通り送信されません。
SMA-2317	アップグレードに必要な「**システム > 設定**」ページが空白で、期待通りに動作しません。
SMA-2268	「エンド ポイント制御 (EPC)」検査が、誤ったシリアル番号を含む不正な周辺機器 ID を返します。
SMA-1847	SecureDNS を使用すると、「安全なネットワークの検出 (SND)」が失敗します。
SMA-1392	Linux クライアント上の NetExtender で DUO 認証が期待通り動作しません。
SMA-1187	「パスワード変更を許可する」の機能が期待通り動作しません。

確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

問題番号	問題の詳細
SMA-2720	新しいユーザ インターフェースで、SMS OTP（ワン タイム パスワード）オプションと「モバイル アプリを使用する」または「電子メールを使用する」などの認証方式間を切り替えて、SMS OTP オプションに切り替えると、常に OTP を起動します。
SMA-2563	フォルダ内のファイル名に ASCII 文字以外が含まれていると、そのフォルダのダウンロードが正しく機能しません。
SMA-2496	「既存のセッションからログアウトしたことを確認する」を伴った「多重ログインを禁止する」が期待通り動作しません。
SMA-1962	SharePoint を使用して Excel と Word ファイルを開くことができません。

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。

サポート ポータルでは、次のことができます。

- ナレッジベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする。
- ビデオ チュートリアルを視聴する。
- MySonicWall にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- SonicWall University に登録して、トレーニングと技術認定を得る。

このドキュメントについて

メモ: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SMA 100 シリーズ Secure Mobile Access リリース ノート
更新日 – 2024 年 4 月
ソフトウェア バージョン – 10.2.1.12
232-005740-00 Rev Q