CA SiteMinder Federation Standalone

Federation Standalone リリース ノート

r12.52 SP1

ca technologies

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: ようこそ 7

第 2 章: オペレーティング システムのサポート 9

第 3 章: 新機能 11

r12.52 SP1 の新機能 11

第 4 章: 変更された機能 13

OpenSSL のアップグレード 13

第 5 章: 12.5 で修正された問題 15

XML シグネチャ ラッピング攻撃に対する保護（168095） 15

第 6 章: 12.52 で修正された問題 17

HTTP ヘッダを取得できない（173924） 17
アイドルおよび最大の Cookie タイムアウト値が変更された（173107） 17
アサーティング パーティで認証リクエストの ACS URL が受け入れられない（170971） 18
設定をバックアップするための XPSExport コマンド構文が正しくない（173659） 18
ユーザ データベース設定が失敗する（173170） 19
Apache Web サーバの CSR リクエストのサイズが間違っている 19
国名ドロップダウン リストに値が表示されない（171912） 19
SAML 認証方式が認証に失敗する（170507/173913） 20
fedmanager.sh スクリプトで ${LOGNAME} の代わりに $(logname) が使用される（170497） 20
12.1 SP3 から 12.5 へのアップグレードが失敗する（169579） 20
オープン形式の Cookie で必要なフラグ（168080） 21
ログ設定ファイルが更新されていない（171956） 21
Log4j.properties ファイルが省略され SSL コマンド構文が正しくない（165412） 22
フェールオーバおよび負荷分散のプロセスに明確化が必要（145146） 22

第 7 章: r12.52 SP1 で修正された問題 23

ログ ファイル（53337）の正しくないファイル名 23

nohup.out ログの名前が正しく設定されない（172212） 23
ñ 文字で SiteMinder の検索が失敗する（168418） 24

第 8 章: マニュアル 25

CA SiteMinder® Federation Standalone マニュアル選択メニュー 25

第 9 章: 国際化サポート 27

第 10 章: サード パーティ製ソフトウェアの使用許諾契約書 29

付録 A: アクセシビリティ機能 31

製品拡張機能 31

第 1 章: ようこそ

CA SiteMinder® Federation Standalone をご利用いただき、誠にありがとうございます。 これらのリリース ノートには、製品のインストールに関する注意事項、オペレーティング システムのサポート、既知の問題、および CA テクニカル サポートへの問い合わせに関する情報が含まれています。

第 2 章: オペレーティング システムのサポート

CA SiteMinder® Federation Standalone 用のサポートされているオペレーティング システムのリストについては、製品のプラットフォーム サポート マトリックスを参照してください。

プラットフォーム マトリックスにアクセスする方法

1. テクニカル サポート サイトにログインします。
2. r12.52 SP1 に関する CA SiteMinder® Federation Standalone プラットフォーム サポート マトリックスを検索します。

第 3 章: 新機能

r12.52 SP1 の新機能

このリリースに新機能はありません。

第 4 章: 変更された機能

OpenSSL のアップグレード

以下の脆弱性を修正するために、CA SiteMinder® Federation Standalone は OpenSSL 0.9.8za を使用します。

- CVE-2014-0224: An SSL/TLS MITM の脆弱性は、OpenSSL 0.9.8y 以前に存在します。 攻撃者は、注意深く作られたハンドシェイクを使用して、OpenSSL SSL/TLS クライアントおよびサーバ内の脆弱なキー材料の使用を強制できます。 これは、攻撃を受けたクライアントおよびサーバからのトラフィックを攻撃者が復号化し変更することで、MITM（Man-in-the-Middle、中間者）攻撃に悪用される場合があります。
- CVE-2014-0221： DTLS 再帰エラーは OpenSSL 0.9.8y 以前に存在します。 OpenSSL DTLS クライアントに無効な DTLS ハンドシェイクを送信してコードを再帰させることにより、DoS 攻撃のクラッシュを引き起こす場合があります。
- CVE-2014-3470： 匿名 ECDH サービス拒否エラーは OpenSSL 0.9.8y 以前に存在します。 匿名 ECDH ciphersuites を可能にする OpenSSL TLS クライアントは、サービス拒否攻撃の対象となります。
- CVE-2014-0076： 攻撃の修正については「Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack」を参照してください。

脆弱性の詳細については、OpenSSL ドキュメント セットを参照してください。

第 5 章: 12.5 で修正された問題

XML シグネチャ ラッピング攻撃に対する保護(168095)

悪意のあるユーザは、署名を無効にせずにドキュメントのコンテンツを変更することにより、XML シグネチャ ラッピング攻撃を実行できます。 デフォルトでは、ポリシー サーバおよび Web エージェント オプション パックのソフトウェア制御には、シグネチャ ラッピング攻撃に対する防御が設定されています。 ただし、サードパーティ製品は、XML 仕様に準拠しない方法で XML ドキュメントを発行できます。 その結果、デフォルトの署名確認によって署名検証が失敗する場合があります。

署名検証の失敗は、以下の理由で発生します。

- 重複した ID 要素が XML ドキュメント内にあり、署名がこの重複した ID を参照している場合。 重複した ID 属性は許可されていません。
- XML 署名が、想定された親要素を参照していない場合。シグネチャ ラッピングの脆弱性がログに記録されます。

フェデレーション トランザクションが失敗する場合は、署名検証の失敗に関する smtracedefault.log ファイルおよび fwstrace.log ファイルを確認します。 これらのエラーは、受信した XML ドキュメントが XML 標準に準拠していないことを示す場合があります。 回避策として、シグネチャ ラッピング攻撃に対するデフォルトのポリシー サーバおよび Web エージェント保護を無効にできます。

重要: 署名の脆弱性に対する保護を無効にした場合は、これらの攻撃に対する別の保護対策を決定します。

XML シグネチャ ラッピングの確認を無効にする方法

1. xsw.properties ファイルに移動します。このファイルは、ポリシー サーバと Web エージェントで別の場所に存在します。
   - ポリシー サーバの smtracedefault.log ファイルでエラー メッセージが発生した場合は、*siteminder_home*/config/properties に移動します
   - Web エージェントの fwstrace.log でエラー メッセージが発生した場合は、

     *web_agent_option_pack_ home/*affwebservices/web-INF/classes に移動します。

     注: Web エージェント オプション パックが Web エージェントと同じシステムにインストールされている場合、このファイルは *web_agent_home* ディレクトリに存在します。
2. 以下の xsw.properties 設定を true に変更します。
   - DisableXSWCheck=true （ポリシー サーバ設定のみ）
   - DisableUniqueIDCheck=true （ポリシー サーバおよび Web エージェント オプション パック設定）

     注: DisableUniqueIDCheck 設定の値は、ポリシー サーバと Web エージェント オプション パックで同じである必要があります。
3. ファイルを保存します。

STAR イシュー番号： 21321479;1

第 6 章: 12.52 で修正された問題

HTTP ヘッダを取得できない（173924）

症状:

SP 側でリモート プロビジョニングを使用する場合、配信モードが HTTP ヘッダとして設定されていると、HTTP ヘッダを取得できません。

解決方法:

この問題は修正されました。

STAR イシュー番号： 21493785-1

アイドルおよび最大の Cookie タイムアウト値が変更された（173107）

症状:

FEDSESSION Cookie タイムアウト設定のデフォルト値が変わりました。

解決方法:

ドキュメント内の値は更新されています。

STAR イシュー番号： 21455676-01

アサーティング パーティで認証リクエストの ACS URL が受け入れられない（170971）

症状:

CA SiteMinder® Federation Standalone では、受信した認証リクエストのアサーション コンシューマ サービス URL を受け入れず、処理していませんでした。 認証リクエストにアサーション コンシューマ サービス URL が定義されているかどうかをシステムは確認していませんでした。

解決方法:

IdP から SP へのパートナーシップの場合、Administrative UI には［Authnrequest での ACS URL の受信］という新しいチェック ボックスがあります。このチェック ボックスは、パートナーシップ設定の［SSO と SLO］手順の［SSO］セクションにあります。認証リクエスト内に URL が存在し、有効であり、メタデータにあることを確認するには、このオプションを選択します。

STAR イシュー番号： 21361990

設定をバックアップするための XPSExport コマンド構文が正しくない（173659）

症状:

「既存設定のバックアップ」の以下の行で指定された XPSExport コマンド構文が正しくありません。

```
XPSExport export_file_name -xa -passphrase passphrase
```

解決方法:

この問題は修正されました。 コマンド構文は、以下のように正しく記述されています。

```
XPSExport export_file_name -xe -xp -passphrase passphrase
```

STAR イシュー番号： 21480783-2

ユーザ データベース設定が失敗する(173170)

症状:

LDAP ユーザ ディレクトリを設定した後に ODBC ユーザ ディレクトリを設定した場合、［接続認証情報］フィールドは無効です。

解決方法:

この問題は修正されました。 UI TAG 内のバインディング パラメータは、ODBC および LDAP の接続に使用されていました。 現在は、LDAP および ODBC ユーザ ディレクトリの設定ページに、2 つの異なるバインディングがあります。

STAR イシュー番号： 21485109-1

Apache Web サーバの CSR リクエストのサイズが間違っている

症状:

組み込み Apache Web サーバに対して 2048 ビットの CSR リクエストを生成すると、1024 ビットの証明書が生成されていました。

解決方法:

この問題は修正されました。

STAR イシュー番号： 21376361

国名ドロップダウン リストに値が表示されない(171912)

症状:

Administrative UI の［証明書のリクエスト］ページの［国］ドロップダウン リストに、疑問符が表示されます。

解決方法:

この問題は修正されました。

STAR イシュー番号： 21454397-1

SAML 認証方式が認証に失敗する(170507/173913)

症状:

最初のユーザと 2 番目のユーザが同じユーザ ディレクトリの異なるブランチで認証された場合、SAML 認証方式は 2 番目のユーザを認証しません。

解決方法:

この問題は修正されました。

STAR イシュー番号： 21283896/21497645

fedmanager.sh スクリプトで ${LOGNAME} の代わりに $(logname) が使用される(170497)

症状:

fedmanager.sh スクリプトが ${LOGNAME} ではなく $(logname) を使用していました。 この代用により、ルートで 'su - fmuser' を使用してスクリプトを fmuser として起動した場合にスクリプトが失敗していました。

解決方法:

この問題は修正されました。

STAR イシュー番号： 21399266-1

12.1 SP3 から 12.5 へのアップグレードが失敗する(169579)

症状:

12.1 SP3 から 12.5 へのアップグレードが失敗していました。 以下のメッセージは、インストール ログ ファイルからの抜粋です。

```
Unable to initialize crypto subsystem Failed to open the encryption key file.
```

解決方法:

この問題は修正されました。

STAR イシュー番号： 21362417-1

オープン形式の Cookie で必要なフラグ（168080）

症状:

IWA が設定するオープン形式の Cookie に以下のフラグ セットがありません。

- Secure
- HttpOnly

その結果、JavaScript はこの Cookie を抽出できます。

解決方法:

この問題は修正されました。

STAR イシュー番号： 21308386-2

ログ設定ファイルが更新されていない（171956）

症状:

フェデレーション スタンドアロン製品では server.log ファイルへのメッセージのログ記録に log4j を使用します。 logger.properties ファイルは、server.log ファイルに記録される内容を決定するファイルの 1 つです。 ガイドにはこの変更が反映されていませんでした。

解決方法:

logger.properties ファイルの名前および場所がドキュメント内で更新されました。

STAR イシュー番号： 21454409-1

Log4j.properties ファイルが省略され SSL コマンド構文が正しくない（165412）

症状:

log4j.properties ファイルは文書化されていません。 このファイルは、Administrative UI 操作に対する追加のログ記録を制御します。

SSL でフェデレーション サービスを開始するコマンドが不正確に文書化されていました。

解決方法:

log4j.properties ファイルは、フェデレーション アクティビティを監視するログに関する情報に記述されました。

フェデレーション サービスを開始するコマンドも正しく修正されました。このコマンドは、./fedmanager.sh startssl として文書化されています。

STAR イシュー番号： 21257428-1

フェールオーバおよび負荷分散のプロセスに明確化が必要（145146）

症状:

フェールオーバおよび負荷分散に関する図で変更が必要とされていました。 また、各機能の説明が不明瞭でした。

解決方法:

フェールオーバおよび負荷分散の図の更新版が作成されました。 また、手順および説明も明確に書き換えられました。

STAR イシュー番号： 20533073;1

第 7 章: r12.52 SP1 で修正された問題

ログ ファイル（53337）の正しくないファイル名

症状:

nohup.out.log ファイルの名前に正しい形式ではなくランダムな数字が含まれています。

解決方法:

この問題は修正されました。 ファイルは以下の形式になります。

nohup.outYYYYMMDD_hhmmss.

STAR イシュー番号： 21454410-01

nohup.out ログの名前が正しく設定されない（172212）

症状:

nohup.out ログの命名規則が nohup.outxxxxxxxxxx.log （xxx はランダムな数字）でした。 予期される形式は、nohup.outYYYMMDD_hhmmss です。

この問題は、Windows プラットフォームでのみ発生します。

解決方法:

この問題は修正されました。

STAR イシュー 21454410-01

ñ 文字で SiteMinder の検索が失敗する(168418)

症状:

ñ 文字を含めると、SiteMinder の検索が失敗します。 その他の UTF 8 文字では同じ結果になりません。

解決方法:

この問題は修正されました。

STAR イシュー 21159919;1

第 8 章: マニュアル

CA SiteMinder® Federation Standalone マニュアル選択メニュー

CA SiteMinder® Federation Standalone に関する詳細情報は、ドキュメント マニュアル選択メニューから参照できます。 マニュアル選択メニューでは、以下を実行できます。

- 1 つのコンソールを使用して、すべてのドキュメントを参照する。
- アルファベット順の索引を使用して、すべてのドキュメントのトピックを検索する。
- すべてのドキュメントで 1 つ以上の単語を検索する。

CA テクニカル サポート サイトからマニュアル選択メニューを表示します。 マニュアル選択メニューにアクセスするためにサイトにログインする必要はありません。

ドキュメントをダウンロードする予定がある場合は、インストール プロセスを開始する前にダウンロードすることをお勧めします。

第 9 章: 国際化サポート

「*国際化*」製品とは、所定のローカル言語版オペレーティング システムおよびサードパーティ製品上で正常に動作し、データの入出力においてローカル言語をサポートする英語版製品です。また、国際製品は、日付、時間、通貨、および番号形式のローカル言語変換を指定できる機能をサポートしています。

「*翻訳済み*」製品（「*ローカライズ済み*」製品とも言います）とは、製品のユーザ インターフェース、オンライン ヘルプ、その他ドキュメントのローカル言語サポートに加えて、日付、時刻、通貨、数値に関してローカル言語でのデフォルトの書式設定をサポートする国際化製品です。

CA SiteMinder® Federation Standalone は、CA SiteMinder® Federation Standalone r12.52 SP1 のプラットフォーム サポート マトリックスで示されているとおりに、国際化およびローカライズが行われています。

第 10 章: サード パーティ製ソフトウェアの使用許諾契約書

CA SiteMinder® Federation Standalone には、サードパーティ社製のソフトウェアが組み込まれています。 サード パーティ製ソフトウェアの使用許諾契約書の詳細については、CA SiteMinder® Federation Standalone マニュアル選択メニューのメインページを参照してください。

付録 A: アクセシビリティ機能

CA Technologies では、さまざまな利用環境のすべてのお客様が、当社の製品およびサポート ドキュメントを正しく使用して重要なビジネス業務を遂行できるよう、全力を尽くしています。 このセクションでは、CA SiteMinder® Federation Standalone に含まれているアクセシビリティ機能について説明します。

製品拡張機能

CA SiteMinder® Federation Standalone では、以下の領域でアクセシビリティが機能拡張されています。

- 表示
- 音
- キーボード
- マウス

注: 以下の情報は Windows ベースおよび Macintosh ベースのアプリケーションに適用されます。 Java アプリケーションは多数のホスト オペレーティング システムで実行されており、これらのシステムの一部にはすでに Java アプリケーションで使用可能な支援テクノロジがあります。 これらの既存の支援テクノロジで、JPL で記述されたプログラムへのアクセスを提供するには、ネイティブ環境における支援テクノロジ自体と、Java 仮想マシン（Java VM）内から使用可能な Java Accessibility サポートとの間のブリッジが必要です。 このブリッジは、両端が Java VM とネイティブ プラットフォームであるため、ブリッジ先のプラットフォームごとに若干異なります。 Sun では現在、このブリッジの JPL 側と Win32 側の両方を開発しています。

表示

コンピュータ ディスプレイでの可視性を向上させるために、以下のオプションを調整できます。

アイテムのフォント スタイル、色、およびサイズ

フォントの色、サイズ、その他の表示の組み合わせを選択できます。

画面解像度

ピクセル数を変更して、画面上でオブジェクトを拡大できます。

カーソルの幅と点滅の速さ

カーソルを見つけやすくしたり、点滅速度を最小化したりできます。

アイコン サイズ

アイコンを大きくして見やすくしたり、アイコンを小さくして画面のスペースを増やしたりできます。

ハイコントラスト スキーム

見やすい色の組み合わせを選択できます。

音

視覚に代わるものとして音を使用します。以下のオプションを調整してコンピュータの音を聞き取りやすくするか、または聞き分けやすくします。

音量

コンピュータ サウンドの音量を上げたり下げたりできます。

音声合成

音声で読み上げたコマンド オプションやテキストを聞くことができます。

警告

目に見える警告を表示できます。

通知

アクセシビリティ機能がオンまたはオフになったときに、聴覚的または視覚的な合図を出します。

スキーム

コンピュータのサウンドと特定のシステム イベントを関連付けることができます。

キャプション

スピーチおよびサウンドのキャプションを表示できます。

キーボード

以下のキーボード調整を行うことができます。

表示の間隔

キーを押したときにどのくらいの速度で文字を繰り返すかを設定できます。

トーン

特定のキーを押したときに音が鳴るようにできます。

固定キー機能

片手または 1 本の指で入力するユーザは、別のキーボード レイアウトを選択できます。

マウス

マウスをより速く、より使いやすくするために以下のオプションを使用できます。

クリックの速度

選択するときのマウス ボタンのクリック速度を選択できます。

クリック ロック

マウス ボタンを押したままにしなくても強調表示したりドラッグしたりできます。

リーバス アクション

マウスの左ボタンで制御される機能と右ボタンで制御される機能を入れ替えることができます。

点滅の速さ

カーソルの点滅速度を選択したり、点滅させるかどうかを選択したりできます。

ポインタ オプション

以下の操作を実行できます。

- タイプ入力中にポインタの表示を非表示にする
- ポインタの場所を表示する
- 画面でポインタが移動する速度を設定する
- 可視性を高めるためにポインタのサイズおよび色を選択する
- ダイアログ ボックス内でデフォルトの場所へポインタを移動する

キーボード ショートカット

以下の表に、CA SiteMinder® Federation Standalone がサポートするキーボード ショートカットを示します。

キーボード	説明
Ctrl + X	切り取り
Ctrl + C	コピー
Ctrl + V	貼り付け
Ctrl + 右方向キー	次の語句
Ctrl + 下方向キー	下にスクロール

キーボード	説明
終端	行の終わり