CA Advanced Authentication

リリース ノート

8.0

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

CA Advanced Authentication 8.0 リリース ノートへようこそ。 このドキュメントでは、CA Advanced Authentication の一般的なリリース情報、新機能と変更された機能、既知の問題、修正された問題、および制限について説明します。

第 2 章: 新機能と変更された機能

このセクションでは、このリリースの新機能および拡張機能について説明します。

- このリリースでは、OpenSSL 1.0.1h バージョンがサポートされています。また、DataDirect ドライバのバージョンは 7.1.4 です。
- **サイレント モード インストール**は、Windows と Unix 両方の Risk Authentication と Strong Authentication でサポートされています。Strong Authentication または Risk Authentication コンポーネントをインストールした後に、サイレント モードのインストールを使用して、コンポーネントを再度インストールできます。 サイレント モード インストールでは、ユーザによる操作なしでインストールが完了します。
- **ユーザ行動プロファイリング**は、Risk Authentication インストーラでプラグインとして提供されています。 データが不十分な場合に、同じユーザまたはそのピア グループのユーザによる以前のアクセスと現在のトランザクションとの類似点または相違点を測定し、トランザクションを追跡してセキュリティを強化します。

第 3 章: アップグレード後の設定の変更

このセクションでは、Risk Authentication 8.0 にアップグレードした後に予想される変更を示します。

ルールのサイレント実行

スコアが 0 であるルールは、サイレント ルールと見なされます。 このようなルールはスコアリングに使用されません。この機能では、エンド ユーザに意図しない影響を及ぼすリスクなしで、トランザクション中にルールがどのように実行されるか観察できます。 以前のリリースでは、スコアが 0 であるルールは常に ALLOW アドバイスを生成します。

アクティブ セットにリスト表示される削除されたルール

ルールを削除すると、そのルールはアクティブなセットに表示されたままになります。 さらに、ルールが削除されたことを示すメッセージが、提示されたセットに表示されます。

ルール セットの削除

現在いずれの組織にも割り当てられていないルール セットを削除できます。

カスタム アクション

カスタム アクションを追加し、次にこれらのアクションを使用してルールを構築できます。

インスタンスおよびプロトコルの設定

以前は riskfortserver.ini ファイルに存在したログ ディレクトリ、ログ ファイル サイズ、ログ バックアップ ディレクトリ、ログ レベル、およびログ タイム スタンプなどのログ パラメータは、現在、管理コンソールの［インスタンス管理］ページから編集できます。

以前は riskfortserver.ini ファイルに存在した最大スレッド数および最小スレッド数などのサーバ パラメータは、現在、管理コンソールの［プロトコル設定］ページから編集できます。

モデル設定

モデル設定はグローバル レベルで実行され、ルール セットに固有ではなくなりました。 マスタ管理者だけが、モデル設定パラメータを編集できます。 グローバル管理者は、グローバル レベルおよび組織レベルでモデルを有効または無効にできます。

ユーザ作成モード

以前のリリースではルール セット レベルで利用可能だった**ユーザ作成モード**設定は、現在、組織レベルで**ユーザ登録モード**として使用できます。

マシン FingerPrint（MFP）のしきい値

以前のリリースでの MFP しきい値設定パラメータは、現在 Device MFP Not Match ルールの一部となっています。

逆引き検索設定

アップグレードの後、デバイス MFP および IP アドレスの逆引き検索設定をチャネル レベルで使用できます。 ［その他の設定］ページで、これらのパラメータ［**デバイス識別で逆引き検索を有効化**］と［**逆引き検索で IP アドレスを使用**］を設定できます。

リスク評価 API 応答での注釈

リスク評価 API 応答では、*annotation* と呼ばれるフィールドにルールの結果がすべて含まれます。Risk Authentication 1.7.0.3 では、USERDIDMATCH は管理コンソールで使用できるルールではありませんでしたが、annotation フィールドにはルール結果、USERDIDMATCH=Y、または USERDIDMATCH=N が含まれました。 この問題は、Risk Authentication 3.0 で解決されました。また、現在、annotation フィールドには、管理コンソールで設定されるルールの結果のみ含まれます。 呼び出し元アプリケーションが Risk Authentication 1.7.0.3 でこの annotation を使用していた場合で、アップグレードの後にこの機能を必要とする場合には、USERDIDMATCH ルールに相当する USERDEVICEIDASSOCIATED ルールを使用できます。

ユーザ デバイス関連付けおよび DeviceID-MFP 一致に基づくルール

Risk Authentication 1.*x* には基本の組み合わせルールがありました。 Risk Authentication 1.7 以降、管理コンソールでこれらのルールを設定できました。 これらのルールは User-DeviceID 一致ルールおよびマシン フィンガープリント一致ルールに基づいていました。また、管理コンソール内のスタンドアロン ルールとは独立していました。Risk Authentication 8.0 にアップグレードした後に、**User Associated with DeviceID**（USERDEVICEASSOCIATED）ルールおよび **Device MFP Match** （SIGMATCH）ルールを使用して、適切なルール短縮名でこれらの組み合わせルールを再作成することができます。

Risk Authentication リリース 1.5.1.6 以前での組み合わせルールのデフォルト スコアは、以下のとおりでした。

- USERDEVICEASSOCIATED AND SIGMATCH： 10
- NOT （USERDEVICEASSOCIATED） AND SIGMATCH： 65
- USERDEVICEASSOCIATED AND NOT （SIGMATCH） ： 65
- NOT （USERDEVICEASSOCIATED） AND NOT （SIGMATCH） ： 85

Risk Authentication リリース 1.5.1.7 以降 2.0 までの組み合わせルールのデフォルト スコアは、以下のとおりでした。

- USERDEVICEASSOCIATED AND SIGMATCH： 10
- NOT （USERDEVICEASSOCIATED） AND SIGMATCH： 65
- USERDEVICEASSOCIATED AND NOT （SIGMATCH） ： 65
- NOT （USERDEVICEASSOCIATED） AND NOT （SIGMATCH） ： 65

ルール セット設定

アップグレード後には、以下のルール セット設定を使用できません。

- 別のルール セットの参照による新しいルール セットの作成
- 別のルール セットを参照するためのルール設定の編集
- 別のルール セットからコピーするルールの編集

Amount Check ルール

AMOUNT エレメントを持たないチャネルに関連付けられた組織の Amount Check ルールが存在する場合、アップグレードの後に手動でこのルールを再作成する必要があります。 ルールでは別の通貨用に別のしきい値を設定する必要がある場合、チャネル エレメントとして AMOUNT を追加する必要があります。 トランザクションが単一通貨のみに基づくと想定する場合、ルール ビルダで CUSTOM エレメントを使用して、単純な数値の比較ルールを作成できます。

注: DEFAULT チャネルには AMOUNT エレメントがありません。必要に応じて、アップグレード前の Amount Check ルールの設定を記録し、アップグレード後に再作成します。

新規ルールおよび廃止されたルール

このリリースでは、4 つの事前定義済みルールが廃止されました。 廃止されたこれらのルールに対して、代替ルールが導入されました。 以下の表に、廃止されたルールと新規ルール、およびルールの短縮名を示します。

廃止されたルール名とルールの短縮名	新規ルール名とルールの短縮名
DeviceID Known （DEVICEIDCHECK）	Unknown DeviceID （UNKNOWNDEVICEID）
Device MFP Match （SIGMATCH）	Device MFP Not Match （MFPMISMATCH）
User Associated with DeviceID （USERDEVICEASSOCIATED）	User Not Associated with DeviceID （USERDEVICENOTASSOCIATED）
User Known （USERKNOWN）	Unknown User （UNKNOWNUSER）

重要: これらのルールは廃止されましたが、引き続き使用可能であり、リリース 8.0 にアップグレード後に使用できます。 ただし、ルール式の必要な変更を加えて、廃止されたルールを、対応する新しいルールで置換することを推奨します。

廃止された 4 つのルールのいずれかに対して、ルールが No に評価される場合、ルールは一致したと考えられます。 その後、それはスコアリングに使用されます。 対照的に、その他の事前定義済みの各ルールは、Yes に評価されると一致したと考えられます。

リリース 8.0 で導入された 4 つの新規ルールのいずれかに対して、ルールが Yes に評価される場合、ルールは一致したと考えられます。このように、4 つの新しいルールはその他の事前定義済みルールと一致しています。

ルールの移行

すべてのルールは、システム内でデフォルトでサポートされているすべてのアクションに対する DEFAULT チャネルに移行されます。

ルールの実行優先度

Risk Authentication 2.*x* からアップグレードした後、実行用のルールを有効または無効にする必要はありません。 実行優先度は、システムによって自動的に決定されます。

セカンダリ認証結果

現在、[**セカンダリ認証結果**]ステータスを持つ Risk Authentication 2.2.5.11 内のトランザクションは使用できず、アップグレード後には放棄ステータスで表示されます。

アップグレードの後のアントラステッド IP タイプ設定

1.7 より前の Risk Authentication リリースでは、管理コンソールから、拒否 IP タイプをアクティブ、要注意、またはプライベートとして設定できました。 Risk Authentication 1.7 から、アクティブ、要注意、プライベート、非アクティブ、および不明の拒否タイプ カテゴリは、インテリジェント パートナーによって提供されたデータから派生します。 したがって、Risk Authentication 1.6.0.*x* または以前の展開で、いずれかの拒否 IP タイプをアクティブ、要注意、またはプライベートとして設定した場合、8.0 にアップグレードした後に、これらの IP タイプが、アントラステッド IP タイプの「拒否」カテゴリに移行されます。

キャッシュ リフレッシュ

Risk Authentication リリース 2.*x* 以降からアップグレードした後、管理コンソールからすべてのサーバ インスタンスのキャッシュをリフレッシュできます。 コマンド ライン オプションの使用を選択する場合、現在は、arrfadmin ツールの代わりに arrfclient ツールを使用して、サーバ インスタンスをリフレッシュする必要があります。

アップグレード後のケースの割り当て

Risk Authentication リリース 2.*x* 以降からアップグレードした後、以前のリリースで生成されたすべてのケースは、組織のデフォルト キューに割り当てられたままになります。

注: Risk Authentication 2.0 では、ケースは各テクニカル サポート担当者（CSR）に割り当てられました。しかし、Risk Authentication 2.2 から、ケースは個別の CSR には割り当てられません。 詳細については、「CA Risk Authentication 管理ガイド」を参照してください。

Risk Authentication 8.0 にアップグレードした後に生成されるすべての新しいケースは、Risk Authentication 8.0 のキュー マネージャによって定義されたキュー基準に従って関連するキューに割り当てられます。

呼び出し元アプリケーション コードの変更

以下に、アップグレード後の呼び出し元アプリケーション コードへの変更について説明します。

- 古い Java SDK クライアントは、Risk Authentication サーバの新しいインストールでも動作します。 古い SDK の使用を続行する場合、クライアント コードは変更を必要としません。ただし、新しい SDK は追加機能を提供しています。したがって、SDK の最新のリリースと呼び出し元アプリケーション コードを統合することを推奨します。
- 古いリスク評価 WSDL を使用して統合されたアプリケーションは、コードの変更なしで引き続き動作します。

注: Risk Authentication 1.x リリースでは、Web サービスは WAR 実装として構築されました。 クライアントは、Risk Authentication 8.0 にアップグレードした後でも、引き続き古い Web サービスを指定する必要があります。 Risk Authentication 8.0 を含めて、Risk Authentication リリース 2.0 以降では、Web サービスは WAR としてではなく Risk Authentication サービスの一部として実装されます。新しい WSDL を使用してアプリケーションを統合し、新しいアーキテクチャに従って Risk Authentication サービスに対してアプリケーションを設定することをお勧めします。

- 以前のリリースでは、発行 Java API はプログラム可能なインターフェースを提供しています。これを使用して Java クライアント（Java サーブレットや JSP ページなど）は発行に関連するリクエストを Risk Authentication サーバに送信します。 Risk Authentication 3.0 では、発行 API （Issuance）は廃止されました。 現在、この目的では、ユーザ管理 Web サービス（ArcotUserRegistrySvc）を使用する必要があります。
- 以前にリリースされた例外ユーザ Web サービスを使用していた場合、現在は、例外ユーザ API を提供する Risk Authentication サービスで実装された新しい Risk Authentication 管理 Web サービス WSDL を使用する必要があります。
- 現在、応答コードおよび理由コードを返す拡張された Risk Authentication 8.0 リスク評価 API を使用することをお勧めします。

ロール権限

Risk Authentication 2.*x* からアップグレードした後、さまざまなロールに関連付けられた権限を確認する必要があります。以下の表に、アップグレード後に削除されたマスタ管理者、グローバル管理者、および組織管理者ロールに関する権限を示します。

ロール	Scope	削除された権限
MA （マスタ管理者）	Global	■ Risk Authentication プロトコルの更新 ■ アドオン ルール タイプの追加

ロール	Scope	削除された権限
GA （グローバル管理者）	Global	■ 拒否国の管理 ■ 拒否 IP アドレスの管理 ■ ユーザ頻度設定の管理 ■ デバイス頻度設定の管理 ■ トラステッド IP/アグリゲータの管理 ■ IP 頻度設定の管理 ■ スコアリング設定の管理 ■ その他のルール設定の管理 ■ 拒否 IP タイプの管理 ■ アドオン ルールの設定 ■ GDP URL の表示 ■ トラステッド IP アドレス/アグリゲータ レポートの表示 ■ 拒否 IP アドレス レポートの表示 ■ 拒否国レポートの表示 ■ カテゴリ ベース ルール データの管理 ■ マッピング データ レポートの表示

ロール	Scope	削除された権限
	組織	■ 拒否国の管理 ■ 拒否 IP アドレスの管理 ■ ユーザ頻度設定の管理 ■ デバイス頻度設定の管理 ■ トラステッド IP/アグリゲータの管理 ■ IP 頻度設定の管理 ■ スコアリング設定の管理 ■ その他のルール設定の管理 ■ 拒否 IP タイプの管理 ■ アドオン ルールの設定 ■ カテゴリ ベース ルール データの管理
OA （組織管理者）	Global	■ キューの管理 ■ トラステッド IP アドレス/アグリゲータ レポートの表示 ■ 拒否 IP アドレス レポートの表示 ■ 拒否国レポートの表示 ■ マッピング データ レポートの表示
	組織	■ 拒否国の管理 ■ 拒否 IP アドレスの管理 ■ ユーザ頻度設定の管理 ■ デバイス頻度設定の管理 ■ トラステッド IP/アグリゲータの管理 ■ IP 頻度設定の管理 ■ スコアリング設定の管理 ■ その他のルール設定の管理 ■ 拒否 IP タイプの管理 ■ アドオン ルールの設定 ■ カテゴリ ベース ルール データの管理

以下の表に、アップグレード後に追加されたマスタ管理者、グローバル管理者、組織管理者、およびユーザ管理者ロールに関する権限を示します。

ロール	ターゲット	追加された権限
MA （マスタ管理者）	Global	■ インスタンスの管理 ■ インスタンス管理レポートの表示 ■ モデル設定
	API	■ ユーザ プロファイルの取得（Web サービス） ■ 例外リストへのユーザの追加（Web サービス） ■ 例外リストからのユーザの削除（Web サービス） ■ 場所および接続情報の取得（Web サービス）
GA （グローバル管理者）	Global	■ その他の設定の管理 ■ レポート サマリ ■ ルールおよびスコアリング管理 ■ モデル設定 ■ キューの再構築
	組織	■ その他の設定の管理 ■ チャネルの割り当てとデフォルト アカウントの設定 ■ ルールおよびスコアリング管理 ■ モデル設定
	API	■ ユーザ プロファイルの取得（Web サービス） ■ 例外リストへのユーザの追加（Web サービス） ■ 例外リストからのユーザの削除（Web サービス） ■ 場所および接続情報の取得（Web サービス）
OA （組織管理者）	Global	■ レポート サマリ ■ キューの管理 ■ キューの再構築

ロール	ターゲット	追加された権限
	組織	■ その他の設定の管理 ■ ルールおよびスコアリング管理
	API	■ ユーザ プロファイルの取得（Web サービス） ■ 例外リストへのユーザの追加（Web サービス） ■ 例外リストからのユーザの削除（Web サービス） ■ 場所および接続情報の取得（Web サービス）
UA （ユーザ管理者）	Global	■ レポート サマリ
	API	■ ユーザ プロファイルの取得（Web サービス） ■ 例外リストへのユーザの追加（Web サービス） ■ 例外リストからのユーザの削除（Web サービス） ■ 場所および接続情報の取得（Web サービス）

第 4 章: 既知の問題

このセクションでは、このリリースの既知の問題を示します。

Strong Authentication の既知の問題

このセクションでは、CA Strong Authentication の既知の問題を示します。

Strong Authentication コンポーネントとデータベース サーバ間の一方向 SSL 通信に関するドキュメントがない

Strong Authentication の管理ガイドには、Strong Authentication コンポーネント(管理コンソールおよびユーザ データ サービス)とデータベース サーバ間の一方向 SSL 通信を設定する手順が含まれていません。

EAP 認証タイプが RADIUS 設定に有効でない

症状:

EAP 認証タイプが RADIUS 設定で有効になりません。

解決方法:

EAP 認証タイプは、RADIUS 設定画面でオプションとして表示されますが、現在サポートされていません。 このオプションを選択しないでください。

ユーザ アカウントのバルク アップロードがアカウント ステータスに対する値の範囲を受け入れない

症状:

ユーザ アカウントのバルク アップロードがアカウント ステータスに対する値の範囲を受け入れません。 以下の値のみを受け入れます。

- 0 （初期の場合）
- 10 （アクティブの場合）

20 （非アクティブの場合）

解決方法:

ステータス フィールドに対するすべての値を受け入れる createUserAccount UDS Web サービスを使用します。

CA Advanced Authentication を使用して LDAP 組織から削除されたユーザに関する情報を削除できない

症状:

CA Advanced Authentication を使用して、LDAP 組織から削除されたユーザのアカウント、PAM、およびカスタム属性などのユーザ情報を削除できません。

解決方法:

ユーザが LDAP 組織から削除されている場合は、Web サービスを使用してこの情報を削除できます。

逆の順序でのカスタム アンインストールの実行

症状:

カスタム アンインストールを実行する順序を教えてください。

解決方法:

カスタム インストールを実行した場合は、インストール時に実行したのとは逆の順序でアンインストールを行う必要があります。 たとえば、Strong Authentication サーバの後に CA Advanced Authentication をインストールした場合は、最初に CA Advanced Authentication をアンインストールしてから Strong Authentication サーバをアンインストールする必要があります。

複数のオプションを指定しても arwfutil コマンドが正常に動作する

複数のオプションを指定して arwfutil コマンドを実行すると、無効なオプションの理由で失敗する必要があります。 ただし、このリリースでは、複数のオプションを指定して実行した場合でも、arwfutil コマンドが正常に実行されます。

[OATH OTP トークン管理]ページで常にグローバル レベルのトークンが取得される

症状:

Strong Authentication の［OATH OTP トークン管理］ページで、［グローバル レベルで使用可能なフェッチ トークン］オプションが選択されていない場合でも、［取得］ボタンをクリックするとすべてのグローバル レベルのトークンが取得されます。

解決方法:

この問題は、組織名を指定した場合は発生しません。 トークンを検索する際に、組織名を指定していることを確認します。

CA Advanced Authentication が Internet Explorer 9 で正しく表示されない

症状:

Internet Explorer 9 にアップグレードした後、CA Advanced Authentication が正しく表示されません。

解決方法:

［インターネット オプション］-［詳細設定］に移動して［詳細設定を復元］をクリックすることにより、Internet Explorer 9 の設定を復元します。

アンインストール後に、レジストリのエントリが削除されない

症状:

アンインストール後に、製品に関連するレジストリ エントリの一部が削除されません。

解決方法:

この問題は、機能に影響を与えません。 レジストリ エントリは、次回のインストール時に上書きされます。

ログ ファイルの場所が直観的ではない

症状:

インストール プロセスの最後で、インストーラ画面に表示されるログ ファイルの場所が直観的ではありません。

解決方法:

Windows では、インストーラ画面に表示されるディレクトリ パスの Arcot Systems¥..¥ の部分を無視します。 同様に、UNIX プラットフォームでは、ディレクトリ パスの arcot/../ の部分を無視します。

arcotcommon.ini がない場合に NULL ポインタ例外がログに記録される

症状:

arcotcommon.ini がない場合に、arcotadmin.log に NULL ポインタ例外が記録されます。

解決方法:

arcotcommon.ini が常に存在していることを確認します。

複数のパラメータが arwfutill ユーティリティに渡されると、最初のパラメータのみが使用される

症状:

arwfutill ユーティリティに複数のパラメータを渡すと、最初のパラメータのみが使用されます。

解決方法:

複数のパラメータを arwfutil ユーティリティに渡さないでください。

リリース番号の表示に一貫性がない

症状:

Microsoft Windows 用のインストーラを実行すると、リリース番号として "7.1.1" が表示される場合があります。 また、インストールの最後に作成されるレジストリ エントリでも "7.1.1" が表示される可能性があります。

解決方法:

このようなリリース番号の表示は無視してください。 "7.1.1" および "7.1.01" の両方は同じリリースを指しています。

リリース番号の表示に一貫性がない

症状:

Microsoft Windows 用のインストーラを実行すると、リリース番号として 8.0 が表示される場合があります。 また、インストールの最後に作成されるレジストリ エントリでも 8.0 が表示される可能性があります。

解決方法:

このようなリリース番号の表示は無視してください。リリース 8.0 を参照します。

Java 設定の変更と CA AuthID をダウンロードするための HTTPS の有効化

シナリオ 1

症状:

Strong Authentication がインストールされているサーバで IE ブラウザを使用して CA AuthID をダウンロードすると、以下のエラーが表示されます。

Your security settings have blocked an application signed with an expired or not-yet-valid certificate from running.

解決方法:

コントロール パネルに移動し、［Java］をクリックして Java 設定を変更します。 ［セキュリティ］オプションを（［高］ではなく）［中］に指定します。 デフォルト オプションは例外を指定する［高］です。 その後、IE、Firefox、または Chrome で「Arcot アプレット クライアント」と「Arcot Flash クライアント」を使用して CA AuthID をダウンロードします。

シナリオ 2

症状:

Strong Authentication がインストールされているサーバで Chrome ブラウザを使用して CA AuthID をダウンロードすると、以下のエラーが表示されます。

Permanent storage in the Flash player is disabled.

解決方法:

「Arcot Flash クライアント」を使用してダウンロードするために HTTP ではなく HTTPS を有効にします。 その後、IE、Firefox、または Chrome で CA AuthID をダウンロードします。

管理者とユーザが異なるタイム ゾーンにいる場合の「一時的に非アクティブ化」アクションに関する問題

症状:

管理者とユーザが異なるタイム ゾーンにいる場合、デフォルトの開始時刻および終了時刻が指定された「*一時的に非アクティブ化*」アクションでは、以下のエラーが発生します。

無効なロック期間です。開始ロック時刻は現在の時刻より前にはできません。

解決方法:

非アクティブ化のデフォルトの開始時刻を計算するときにユーザのタイム ゾーンを考慮します。 将来の非アクティブ化に対して、ユーザのタイム ゾーンに基づいて手動で開始時刻を入力します。

部分的なパスワードおよび CVM 認証情報が Strong Authentication 6.2.9 からアップグレードされた Strong Authentication 8.0 で機能しない

症状:

CVM （呼び出し元検証モード）および部分的なパスワード認証情報は、Strong Authentication 6.2.9 から 8.0 へのアップグレード セットアップに対して機能しません。

解決方法:

必須フィールドを使用して新しいプロファイルを作成し、同じプロファイルが発行フロー中に渡されることを確認します。 この手順は CVM と部分的なパスワードの両方の修正に対して適用可能です。

新しいサーバへのアップグレード後に古いサーバの Strong Authentication、Risk Authentication、ケース管理のインスタンスが[インスタンス管理]に表示される

症状:

8.0 へのアップグレード後、新しいサーバの［インスタンス管理］に古いサーバの Strong Authentication、Risk Authentication、ケース管理のインスタンスが表示されます。

解決方法:

新しいサーバの［インスタンス管理］に古いサーバのインスタンスが表示されないようにするには、以下のテーブルから古いサーバ マシンに対応するエントリを削除します。

arwfinstances

arwfprotocolconfiguration

arrfinstances

arrfprotocolregistry

Risk Authentication、Strong Authentication、ケース管理のインスタンスに固有の設定の古い値が新しいサーバ マシンへのアップグレード後に保持されない

症状:

Risk Authentication、Strong Authentication、ケース管理のインスタンスに固有の設定、転送（ssl）、およびその他のプロトコル情報が、アップグレード後に作成された新しいインスタンスではデフォルト値に設定されます。アップグレード前に設定した古い値がアップグレード後の新しいインスタンスに保持されません。

解決方法:

8.0 にアップグレードすると、新しいインスタンスはデフォルト設定の値を使用して作成されます。 Risk Authentication、Strong Authentication、ケース管理のサーバ インスタンスに固有のすべての設定、転送（ssl）、およびその他のプロトコル情報を再設定してください。

シーケンス番号が不足する

症状:

トランザクション ID は 2^32-1 に制限されています。 システムによるトランザクションの数によっては、一意の ID が使い果たされてトランザクションが失敗するおそれがあります。

解決方法:

シーケンス番号の不足を防ぐには、定期メンテナンスの一環として、トランザクション データベース内の監査ログを定期的にアーカイブまたは削除します。 トランザクション データベースに保持されるデータの量はレポートの要件によって決まります。

以下の説明に従って、定期的に監視を実行してください。

1. 以下のクエリを実行します。
   ```
   SELECT count(*)   FROM    ARWFAUTHAUDITLOG A;
   ```
   a. この数が 10 億より大きい場合は、古いレコードをアーカイブします。

   理由： この数が制限に達するとシステムで一意制約エラーが発生するため、トランザクションが失敗します。 次に監視がスケジュールされている日まで、レコード数が上限よりもかなり少なくなるようにしてください。

2. 以下のクエリを実行します。
   ```
   Select USEDVALUE FROM ARWFSEQUENCE WHERE SEQUENCENAME =
   'ARWFTXNIDSEQ';
   ```
   a. この値が 21 億よりも大きい場合は、以下の手順に従います。

   - データベースの古いレコードをアーカイブおよび削除します。手順 1 を実行していることを確認します。
   - サーバをシャットダウンします。
   - クエリを実行します。

   Update ARWFSEQUENCE SET STARTINGVALUE=1 , WHERE SEQUENCENAME = 'ARWFTXNIDSEQ';

   Update ARWFSEQUENCE SET USEDVALUE=1 , WHERE SEQUENCENAME = 'ARWFTXNIDSEQ';

   - サーバを再起動します。

理由： この数が最大値に達すると新しいシーケンス番号は制限を超えるため、トランザクションが失敗します。 次に監視がスケジュールされている日まで、使用されている値が最大値よりも少なくなるようにしてください。

データベースを監視する間隔はトランザクション レートによって決まります。上記のガイドラインで推奨されている 10 億および 21 億という数は、トランザクション量および監視頻度に応じて変更してください

Risk Authentication の既知の問題

このセクションでは、CA Risk Authentication の既知の問題を示します。

Risk Authentication コンポーネントとデータベース サーバ間の一方向 SSL 通信に関するドキュメントがない

管理ガイドには、RiskMinder コンポーネント（管理コンソールおよびユーザ データ サービス）とデータベース サーバ間の一方向 SSL 通信を設定する手順が含まれていません。

CA Advanced Authentication を使用して LDAP 組織から削除されたユーザに関する情報を削除できない

症状:

CA Advanced Authentication を使用して、LDAP 組織から削除されたユーザのアカウント、PAM、およびカスタム属性などのユーザ情報を削除できません。

解決方法:

ユーザが LDAP 組織から削除されている場合は、Web サービスを使用してこの情報を削除できます。

日付と時刻の入力値に対してローカライズ設定がサポートされない

日付と時刻の入力値に対してローカライズ設定がサポートされていません。 デフォルト ロケールは en_US です。

ユーザ アカウントのバルク アップロードがアカウント ステータスに対する値の範囲を受け入れない

ユーザ アカウントのバルク アップロードがアカウント ステータスに対する値の範囲を受け入れません。 以下の値のみを受け入れます。

- 0 （初期の場合）
- 10 （アクティブの場合）
- 20 （非アクティブの場合）

アンインストールを逆の順序で実行する必要がある

症状:

カスタム インストールのアンインストールを実行する方法

解決方法:

カスタム インストールを実行した場合は、インストール時に実行したのとは逆の順序でアンインストールを行う必要があります。 たとえば、Risk Authentication サーバの後に CA Advanced Authentication をインストールした場合は、最初に CA Advanced Authentication をアンインストールしてから Risk Authentication サーバをアンインストールする必要があります。

管理者に SYSTEM と呼ばれる組織の作成が許可される

Risk Authentication では、管理者は、SYSTEM という名前の組織を作成できます。 このような組織は、同じ名前のグローバルな Risk Authentication 組織の設定をすべて継承します。

リスト名とカテゴリ マッピング名に対してマルチバイト文字がサポートされる

リスト名とカテゴリ マッピング名には、マルチバイト文字を許可すべきではありません。しかし、このリリースでは、許可されます。

電子メールが唯一の必須パラメータの場合に暗黙のユーザ作成が成功する

組織に対して、電子メール以外のいずれかのパラメータが必須として設定されると、暗黙のユーザ作成が失敗します。

キャッシュのリフレッシュがデータベース フェイルオーバの後に失敗する

データベース フェイルオーバが発生した後に、キャッシュのリフレッシュを実行すると、エラーが発生します。

CA Advanced Authentication がデータベース フェイルオーバ中に Risk Authentication サーバに接続しない

CA Advanced Authentication は、データベースのフェイルオーバ中に Risk Authentication サーバに接続できません。

逆引き検索機能での問題

MFPMISMATCH ルールがアドオン ルールとして含まれている場合、逆引き検索機能は動作しません。

サンプル アプリケーション 2.0 で空の MFP 値を持つリスク評価が失敗する

Risk Authentication 8.0 でサンプル アプリケーション 2.0 を展開した場合、ユーザに対する既存の MFP 値を削除し、そのユーザのリスクを評価しようとすると、評価が失敗します。

CA Advanced Authentication が Internet Explorer 9 で正しく表示されない

症状:

Internet Explorer 9 にアップグレードした後、CA Advanced Authentication が正しく表示されません。

解決方法:

［インターネット オプション］-［詳細設定］に移動して［詳細設定を復元］をクリックすることにより、Internet Explorer 9 の設定を復元します。

アンインストール後にレジストリのエントリが削除されない

症状:

アンインストール後に、製品に関連するレジストリ エントリの一部が削除されません。

解決方法:

この問題は、機能に影響を与えません。 レジストリ エントリは、次回のインストール時に上書きされます。

インストーラ画面に表示されるログ ファイルの場所が直観的ではない

症状:

インストール プロセスの最後で、インストーラ画面に表示されるログ ファイルの場所が直観的ではありません。

解決方法:

Windows では、インストーラ画面に表示されるディレクトリ パスの Arcot Systems¥..¥ の部分を無視します。 同様に、UNIX プラットフォームでは、ディレクトリ パスの arcot/../ の部分を無視します。

arcotcommon.ini がない場合に NULL ポインタ例外がログに記録される

症状:

arcotcommon.ini がない場合に、arcotadmin.log に NULL ポインタ例外が記録されます。

解決方法:

arcotcommon.ini が常に存在していることを確認します。

リリース番号の表示に一貫性がない

症状:

Microsoft Windows 用のインストーラを実行すると、リリース番号として 8.0 が表示される場合があります。 また、インストールの最後に作成されるレジストリ エントリでも 8.0 が表示される可能性があります。

解決方法:

このようなリリース番号の表示は無視してください。リリース 8.0 を参照します。

フェールオーバが、Oracle RAC で予期したように動作しない

症状:

ノードの障害によりバックアップ Oracle RAC データベースへのフェールオーバが発生し、障害のあるノードが再起動された場合、元のプライマリ データベースへのノードの自動復元が失敗します。 代わりにバックアップ データベースを参照し続けます。

解決方法:

??

管理者とユーザが異なるタイム ゾーンにいる場合の「一時的に非アクティブ化」アクションに関する問題

症状:

管理者とユーザが異なるタイム ゾーンにいる場合、デフォルトの開始時刻および終了時刻が指定された「*一時的に非アクティブ化*」アクションでは、以下のエラーが発生します。

無効なロック期間です。開始ロック時刻は現在の時刻より前にはできません。

解決方法:

非アクティブ化のデフォルトの開始時刻を計算するときにユーザのタイム ゾーンを考慮します。 将来の非アクティブ化に対して、ユーザのタイム ゾーンに基づいて手動で開始時刻を入力します。

HSM またはソフトウェアを使用してシステムが設定されている場合に Risk Authentication のアップグレードが失敗する

症状:

HSM を使用してシステムが設定されている場合に、Risk Authentication の通常のアップグレードが失敗します。 MySQL を使用している Risk Authentication 3.1.01 から 8.0 へのアップグレードが失敗します。

解決方法:

Risk Authentication アップグレード ツールは、Risk Authentication 3.1.01 から 8.0 への移行で MySQL データベースをサポートしていません。

新しいサーバへのアップグレード後に古いサーバの Strong Authentication、Risk Authentication、ケース管理のインスタンスが[インスタンス管理]に表示される

症状:

8.0 へのアップグレード後、新しいサーバの［インスタンス管理］に古いサーバの Strong Authentication、Risk Authentication、ケース管理のインスタンスが表示されます。

解決方法:

新しいサーバの［インスタンス管理］に古いサーバのインスタンスが表示されないようにするには、以下のテーブルから古いサーバ マシンに対応するエントリを削除します。

arwfinstances

arwfprotocolconfiguration

arrfinstances

arrfprotocolregistry

Risk Authentication、Strong Authentication、ケース管理のインスタンスに固有の設定の古い値が新しいサーバ マシンへのアップグレード後に保持されない

症状:

Risk Authentication、Strong Authentication、ケース管理のインスタンスに固有の設定、転送（ssl）、およびその他のプロトコル情報が、アップグレード後に作成された新しいインスタンスではデフォルト値に設定されます。アップグレード前に設定した古い値がアップグレード後の新しいインスタンスに保持されません。

解決方法:

8.0 にアップグレードすると、新しいインスタンスはデフォルト設定の値を使用して作成されます。 Risk Authentication、Strong Authentication、ケース管理のサーバ インスタンスに固有のすべての設定、転送（ssl）、およびその他のプロトコル情報を再設定してください。

8.0 へのアップグレード後の Risk Authentication インスタンスおよび新しい Risk Authentication サーバ名の問題

症状:

8.0 へのアップグレード後、Risk Authentication サーバの［Risk Authentication 接続］に、新しいサーバではなく古いシステム名が表示されます。また、Risk Authentication インスタンスの下にアクティブなインスタンスが表示されません。

解決方法:

CA Advanced Authentication から、Strong Authentication および［Risk Authentication 接続］に表示されるサーバ名を新しいサーバ名に変更します。 これにより、Risk Authentication の［インスタンス管理］に新しいサーバ インスタンスが表示されます。 保存してキャッシュをリフレッシュします。

Red Hat Linux 6 からのアンインストールで示されるログ ファイルの場所が正しくない

症状:

Red Hat Linux 6 から Risk Authentication をアンインストールする場合に示されるアンインストール ログ ファイルの場所が正しくありません。

アンインストール ディレクトリ（/tmp/arcot/Uninstall_CA Risk Authentication）から Risk Authentication のアンインストールを実行します。

注: これはアンインストールを実行するために推奨されている場所ではありません。したがって、ユーザ エラーです。

アンインストールによってアンインストール ディレクトリを削除できないため、警告が生成されます。 その後、以下のメッセージが表示されますが、示されているアンインストール ログ ファイルの場所が正しくありません。

The uninstallation of Risk Authentication 8.0.0.0 is complete, but some warnings occurred during the uninstall. Please see the uninstallation log for details in /tmp/arcot/logs.

ログ ファイルはこの場所ではなく、:/tmp にあります。

解決方法:

アンインストール ログ ファイルは、<インストール ディレクトリ>/arcot/logs ではなく、<インストール ディレクトリ> にあります。

CA Adapter の既知の問題

このセクションでは、CA Adapter の既知の問題を示します。

IBM WebSphere でログ ファイルがバックアップ ファイルにロールオーバされない

症状:

IBM WebSphere で、State Manager および AFM アプリケーションのログ ファイルが、バックアップ ファイルに自動的にロールオーバされません。

解決方法:

AFM および State Manager のログ プロパティ ファイルを以下のように編集します。

1. *AFM_HOME*¥conf¥afm ディレクトリに移動し、arcotafm-log4j.properties および arcotsm-log4j.properties ファイルをテキスト エディタで開きます。
2. ファイル内の以下のエントリを検索し、その前にハッシュ記号（#）を挿入して、その行をコメントアウトします。
   - AFM ログ プロパティ ファイル内：
     log4j.appender.afmout=org.apache.log4j.DailyRollingFileAppender
   - State Manager ログ プロパティ ファイル内：
     log4j.appender.smlog=org.apache.log4j.DailyRollingFileAppender
3. 前の手順でコメントアウトした行の後に以下のエントリを追加します。

   AFM ログ プロパティ ファイル内：

   log4j.appender.afmout=com.arcot.logger.log4j.appender.ArcotDailyRollingFileAppender

   State Manager ログ プロパティ ファイル内：

   log4j.appender.smlog=com.arcot.logger.log4j.appender.ArcotDailyRollingFileAppender
4. ファイルを保存して閉じます。
5. WebSphere アプリケーション サーバを再起動します。

ActiveX クライアントを使用する場合に CA AuthID 認証および登録が失敗する

症状:

CA AuthID ActiveX クライアントを認証および登録に使用しており、エンドユーザのシステムにこのクライアントがインストールされていない場合、実行時には ActiveX クライアントがエンドユーザのシステムにダウンロードされますが、認証および登録の操作は失敗します。

解決方法:

エンドユーザは、ブラウザを再起動して再度認証を行う必要があります。

Internet Explorer 8 を使用した認証で警告が表示される

症状:

CA AuthID キー サイズを 2048 に設定した場合、エンドユーザが Internet Explorer 8 を使用して認証を行おうとすると、以下の警告メッセージが表示されます。

このページのスクリプトが、Internet Explorer の実行速度を遅くしています。スクリプトを実行し続けると、コンピューターが反応しなくなる可能性があります。

解決方法:

CA AuthID キー サイズに 1024 を使用します。

ArcotID PKI のダウンロード中に空白ページが表示される

症状:

エンドユーザが Windows 7 システム上で Internet Explorer 9 を使用し、Internet Explorer で特定の詳細設定を有効にしていて、かつ ArcotID PKI 認証が使用されている場合に、ArcotID PKI 認証情報のダウンロード時に空白ページが表示されることがあります。

解決方法:

エンドユーザは Internet Explorer の詳細設定をリセットする必要があります（［ツール］-［インターネット オプション］-［詳細設定］に移動して、［リセット］をクリック）。

Internet Explorer の詳細設定を使用している場合に CA AuthID をダウンロードすると空白ページが表示される

症状:

エンドユーザが Windows 7 システム上で Internet Explorer 9 を使用し、Internet Explorer で特定の詳細設定を有効にしていて、かつ CA AuthID 認証が使用されている場合に、CA AuthID 認証情報のダウンロード時に空白ページが表示されることがあります。

解決方法:

エンドユーザは Internet Explorer の詳細設定をリセットする必要があります（［ツール］-［インターネット オプション］-［詳細設定］に移動して、［リセット］をクリック）。

ネットワークの速度が遅い場合にリスク ベースのワークフローが失敗する

症状:

ネットワークの速度が非常に遅い場合に、リスク ベース認証が失敗することがあります。

解決方法:

ネットワーク設定を確認し、必要であれば adaptershim.ini ファイルで ArcotSMResponseWait パラメータにより大きい値を指定します。

組織名にスペースが含まれている場合に CA AuthID OTP 認証が失敗する

症状:

組織名にスペースが含まれている場合に、CA AuthID OTP を使用したプライマリ認証フローが機能しません。

解決方法:

組織名にスペースが含まれていないことを確認します。

JBoss ですべてのアプリケーション ログが AFM のログ ファイルにリダイレクトされる

症状:

JBoss アプリケーション サーバで、AFM、State Manager、およびサンプル アプリケーション固有の WAR ファイルを展開した後、アプリケーション サーバのすべてのログが AFM のログ ファイル（arcotafm.log）をリダイレクトされます。

解決方法:

jboss-web.xml という名前の新しいファイルを作成し、以下の手順に従います。

1. 以下の行を jboss-web.xml ファイルにコピーします。

```
<jboss-web>
  <class-loading java2ClassLoadingCompliance="false">
    <loader-repository>
      com.arcot:loader=<UniquenameforClassLoader>
      <loader-repository-config>
        java2ParentDelegation=false
      </loader-repository-config>
    </loader-repository>
  </class-loading>
</jboss-web>
```

   UniquenameforClassloader は各アプリケーションに対して一意である必要があります。たとえば、AFM に対して ArcotAFMClassloader を使用し、State Manager に対して ArcotSMClassloader を使用できます。

2. jboss-web.xml ファイルを *App_Exploded_Location*¥*App_Name*¥WEB-INF にコピーします。

   説明

   App_Exploded_Location は、JBoss がアプリケーションを抽出した場所です。

   App_Name はアプリケーションの名前です（たとえば、arcotafm や arcotsm）。

   この場所に jboss-classloading.xml ファイルが存在する場合は、そのファイルを削除します。

3. アプリケーション サーバを再起動します。

AFM、State Manager、および SAML サンプル アプリケーションに対して、この手順を繰り返します。

State Manager のリスク評価がクラス ロードの問題のために失敗する

症状:

JBoss アプリケーション サーバで、AFM、State Manager、およびサンプル アプリケーション固有の WAR ファイルを展開した後、アプリケーションの展開形態に応じた WAR ファイルの内容の抽出が行われません。 これによって、クラス ロードの問題が原因で、State Manager のリスク評価が失敗することがあります。

解決方法:

以下の手順に従います。

1. WAR ファイルの内容をローカル ディレクトリに抽出します。
2. *App_Exploded_Location*¥*App_Name*¥WEB-INF 内に jboss-web.xml という新しいファイルを作成します。

   説明

   App_Exploded_Location は、JBoss がアプリケーションを抽出した場所です。

   App_Name はアプリケーションの名前です（たとえば、arcotafm や arcotsm）。
3. 以下の行を jboss-web.xml ファイルにコピーします。

```
<jboss-web>
  <class-loading java2ClassLoadingCompliance="false">
    <loader-repository>
      com.arcot:loader=<UniquenameforClassLoader>
      <loader-repository-config>
        java2ParentDelegation=false
      </loader-repository-config>
    </loader-repository>
  </class-loading>
</jboss-web>
```

   UniquenameforClassloader は各アプリケーションに対して一意である必要があります。たとえば、AFM に対して ArcotAFMClassloader を使用し、State Manager に対して ArcotSMClassloader を使用できます。
4. *App_Exploded_Location*¥*App_Name*¥WEB-INF ディレクトリに jboss-classloading.xml ファイルが存在する場合は、そのファイルを削除します。
5. アプリケーション サーバを再起動します。

AFM、State Manager、および SAML サンプル アプリケーションに対して、この手順を繰り返します。

アプリケーションが JBoss の使用可能なバックアップ データ ソースを検出しない

症状:

JBoss アプリケーション サーバでプライマリとバックアップの両方のデータ ソースが設定されていて、両方のデータベースが停止している場合、アプリケーションはエラーをスローします。 しかし、バックアップ データベースが稼働中になった後も、アプリケーションは使用可能なバックアップ データ ソースを検出しないため、アプリケーションが動作しません。

解決方法:

バックアップ データ ソースをリフレッシュします。 アプリケーションが動作し始めます。

adaptershim.ini ファイルの時間ベース ロールオーバのセクションに不正なパラメータが追加される

症状:

ウィザードを使用して CA Adapter を設定した後、adaptershim.ini 設定ファイルで、ログ ファイルの時間ベース ロールオーバーのセクションに、以下の例のように誤ったパラメータ名および値が含まれます。

```
# "LOG_FILE_ROLLOVER_INTERVAL" property specifies how often you want
the log file to
# rollover to the backup file. The values recognized are HOURLY, DAILY,
# WEEKLY, and MONTHLY. DAILY results in the file rolling over when the
first
# log message is received after midnight. The time check is
# based on the logged time. By default, the local time zone is used
for
# logging.
Param2=MAX_LOG_FILE_SIZE=10000000
```

Param2 の値は、MAX_LOG_FILE_SIZE ではなく、
LOG_FILE_ROLLOVER_INTERVAL である必要があります。

解決方法:

adaptershim.ini ファイル内の LOG_FILE_ROLLOVER_INTERVAL プロパティ セクションで、以下の行を、

```
Param2=MAX_LOG_FILE_SIZE= 10000000
```

以下のように変更します。

```
Param2=LOG_FILE_ROLLOVER_INTERVAL=DAILY
```

CA Adapter のカスタム アンインストールでの問題

症状:

アンインストールするコンポーネントが選択されていない場合でも、インストーラはコンポーネントが正常にアンインストールされた旨のメッセージを表示します。

解決方法:

この問題は、機能に影響を与えません。 アンインストールを実行する際に、アンインストールするコンポーネントを選択します。

第 5 章: 修正された問題

このセクションでは、このリリースで修正された問題を示します。

Strong Authentication で修正された問題

Strong Authentication で双方向から一方向への SSL により、ハンドシェイクが失敗する

症状:

以前のリリースでは、双方向から一方向への SSL により、接続が失われるハンドシェイクの失敗が発生していました。一方向 SSL が動作を停止していました。

解決方法:

この問題は修正されており、SSL の双方向から一方向へのハンドシェイクの設定は、正常に行われます。

あるユーザに対して生成された OTT が RADIUS を介して別のユーザの認証に使用される問題

症状:

あるユーザに対して生成された OTT（ワンタイム トークン）は、RADIUS を介して別のユーザを認証するために使用できました。

解決方法:

この問題は修正されています。

Strong Authentication が RADIUS プロキシとして使用される場合にファイルの説明が漏洩する

症状:

Strong Authentication が RADIUS プロキシとして使用される場合、ファイル記述子が漏洩し、以下のエラーメッセージが表示されます。

There is no further connection available.

解決方法:

この問題は修正されています。

Strong Authentication サーバで自動ロック解除が機能しない

症状:

Strong Authentication サーバで自動ロック解除が正常に機能しません。ロック解除されると、arcotid パスワードを何回も試行できてしまいます。

解決方法:

この問題は修正されています。

AAC のユーザ名に一重引用符が含まれているユーザを選択できない

症状:

AAC のユーザ名に一重引用符が含まれているユーザを Strong Authentication で選択できません。

解決方法:

この問題は修正されています。

Strong Authentication と 6.2.11 SDK の下位互換性が機能しない

症状:

Strong Authentication 7.1.1 と 6.2.11 SDK との下位互換性が機能しません

解決方法:

Strong Authentication 8.0 では修正プログラムが追加され、Strong Authentication 8.0 と 6.2.11 SDK との下位互換性が機能するようになりました。

LDAP リフェラル設定の問題

症状:

LDAP リフェラルがデフォルトで有効な場合に、LDAP 組織からのユーザの取得に通常よりも時間がかかります。

解決方法:

このリフェラルはコードで無効にされており、それぞれの例外が処理されます。この問題は修正されています。

珍しい姓を持つユーザに対するエラー

症状:

珍しい姓を持つユーザに対して、Strong Authentication で問題が発生します。

解決方法:

この問題は修正されています。［名］、［ミドル ネーム］、［姓］の最大長は、32 から 64 に拡張されています。

Risk Authentication で修正された問題

TCP が無効で SSL が有効な場合に Risk Authentication がクラッシュする

症状:

TCP が無効で SSL が有効な場合、Risk Authentication がクラッシュします。

解決方法:

この問題は修正されています。

arrfclient によるキャッシュのリフレッシュが Risk Authentication に対して失敗する

症状:

以前のリリースでは、arrfclient は Risk Authentication サーバが SSL モードの場合にキャッシュをリフレッシュできませんでした。

解決方法:

この問題は修正されています。

Risk Authentication サービスが停止する

症状:

USERCONTEXT の USERCONTEXTINFO 列のデータ切り捨てのために Risk Authentication サービスが停止します。

解決方法:

この問題は修正されています。

CA Adapter で修正された問題

認証 Shim から SiteMinder ポリシー サーバに渡される値が RFC に準拠していない

症状:

SMUSRMSG Cookie の値を設定するために認証 Shim から SiteMinder ポリシー サーバに渡される値が RFC に準拠していません。

解決方法:

この問題は修正されています。

パスワードの変更後に新しいパスワードがパスしなかった場合の問題

症状:

ユーザがパスワードを変更し、新しいパスワードが複雑さのテストに 1 回でパスしなかった場合、フォームへのその後のパスワードの入力は複雑さのルールを満たしていても拒否されます。

解決方法:

この問題は修正されています。

クロス サイト スクリプティングによって shimerror.unauth.html に脆弱性が発生する

症状:

クロス サイト スクリプティングによって、CA Adapter の shimerror.unauth.html に脆弱性が発生します。

解決方法:

この問題は修正されています。

CA AuthID 認証ポリシーで定義されている[認証情報の自動ロック解除を有効化]および[ロック解除までの時間]の設定が AFM に適用されない

症状:

CA AuthID 認証ポリシーで定義されている［認証情報の自動ロック解除を有効化］および［ロック解除までの時間］の設定が Arcot Authentication Flow Manager （AFM）に適用されません。

解決方法:

この問題は修正されています。

クライアント IP アドレスが Risk Authentication サーバに渡される場合の元の IP アドレスの問題

症状:

AFM をホストしているアプリケーション サーバがロード バランサまたはプロキシ サーバの背後にある場合、AFM から Risk Authentication サーバに渡されるクライアント IP アドレスがロード バランサの IP アドレスまたは最後のプロキシ サーバの IP アドレスになります。これは、クライアントの元の IP アドレスである必要があります。

解決方法:

この問題は修正されています。

ArcotSM からのタイムスタンプの取得が失敗する

症状:

バックアップ DB が定義されている場合に、ArcotSM からのタイムスタンプの取得が失敗します。

解決方法:

この問題は修正されています。

Adapter 2.2.9 が古い DeviceDNA を使用する

症状:

Adapter 2.2.9 がパラメータの少ない古い DeviceDNA を使用しています。

解決方法:

この問題は修正され、現在のリリースでは動作が確認されています。

AFM が MFP で特殊文字を許可していないため、AFM RISK Flows がエラーで終了する

症状:

MFP に &、<、>、¥ などの文字が含まれている場合、AFM は MFP でこれらの特殊文字を許可していないため、AFM RISK Flows がエラーで終了します。

解決方法:

この問題は修正されています。

バックエンドのプロファイルで設定されている ArcotOTP のローミングの有効性および OTP 長が適用されない

症状:

バックエンドのプロファイルで設定されている ArcotOTP のローミングの有効性および OTP 長が適用されません。

解決方法:

この問題は修正されています。

デスクトップ クライアントの OTP が AOTP プロファイルと同期されない

症状:

デスクトップ クライアントの OTP が AOTP プロファイルと同期されません。

解決方法:

この問題は修正されています。

いずれかのデータベースが停止している場合に ArcotSM からのタイムスタンプの取得が失敗する

症状:

いずれかのデータベース（プライマリまたはバックアップ）が停止している場合に、ArcotSM からのタイムスタンプの取得が失敗します。

解決方法:

この問題は修正されています。

jspStrings_fr.properties で設定されているロケールが arctoafm EMAIL に適用されない

症状:

jspStrings_fr.properties で設定されているロケールが arctoafm EMAIL に適用されません（電子メールは英語で送信されます）。 AFM のページにはローカル言語が適用されますが、電子メールは英語で送信されます。

解決方法:

この問題は修正されています。

CallerID が Risk Authentication に反映されない

症状:

CallerID が Risk Authentication に反映されません。 AR_RF_CALLER_ID に追加で入力しても、ARRFSYSAUDITLOG テーブルの CALLERID フィールドに反映されません。

解決方法:

この問題は修正されています。

第 6 章: 製品の制限

このセクションでは、このリリースでの製品の制限を示します。

Strong Authentication の制限

このリリースでの Strong Authentication の既知の制限は、以下のとおりです。

- Oracle データベースおよび Apache Tomcat アプリケーション サーバを使用している場合に、プライマリ データベースのネットワーク ケーブルが接続されていないと、データベース フェイルオーバに 15 分を超える時間がかかります。
- 管理コンソールおよび UDS Web サービスは、Solaris 上の 64 ビットのアプリケーション サーバではサポートされません。
- Strong Authentication の複数インスタンスを、同じシステム上の別のフォルダにインストールすることはできません。複数のインスタンスをインストールしようとすると、インストールが正常に完了しません。
- Strong Authentication プラグインと IE11 エッジ モードの間に互換性がないため、エッジ モードが有効な場合、このブラウザはプラグインをロードできません。ブラウザが確実にプラグインをロードできるように、ArcotID OTP JavaScript ライブラリ API を使用する HTML ページに <meta http-equiv="x-ua-compatible" content="IE=8,9,10"> というメタ タグを追加することをお勧めします。

Risk Authentication の制限

このリリースでの Risk Authentication の既知の制限は、以下のとおりです。

- IBM WebSphere で、アドオン ルールの名前および説明に特定のマルチバイト文字を使用すると、すべての基本ルールが削除されます。
- プライマリ データベースのネットワーク ケーブルが接続されていない場合、Risk Authentication またはケース管理サーバ、および管理コンソールがバックアップ データベースに接続するのに長い時間がかかります。
- 3.x より前のリリースで作成されたカスタム アドオン ルール タイプの移行は、デフォルトのアップグレード スクリプトを使用した 3.1.01 へのアップグレードではサポートされません。そのようなルールの移行には、別途アップグレード スクリプトを記述する必要があります。詳細については、CA サポートにお問い合わせください。
- 管理コンソールおよび UDS Web サービスは、Solaris 上の 64 ビットのアプリケーション サーバではサポートされません。
- Risk Authentication の複数インスタンスを、同じシステム上の別のフォルダにインストールすることはできません。複数のインスタンスをインストールしようとすると、インストールが正常に完了しません。

CA Adapter の制限

ArcotID PKI のダウンロード時に接続していた USB デバイスが関連付けられる

ArcotID PKI のダウンロード時に USB デバイスをシステムに接続している場合、その USB デバイスも ArcotID PKI と関連付けられます。ArcotID PKI 認証時に、その USB デバイスがシステムに接続されていない場合は、ユーザ認証が失敗します。

ブラウザにプロビジョニングされた ArcotID OTP 認証情報が ArcotID OTP アプリケーションで使用できない

ArcotID OTP 認証情報のアルゴリズムが HOTP であり、その認証情報がブラウザにプロビジョニングされている場合、エンドユーザは、モバイル デバイスまたはデスクトップ コンピュータにインストールされている ArcotID OTP アプリケーションでその認証情報を使用できません。

CA Adapter ではドメインにわたって一意のログイン ID のみがサポートされる

同じログイン ID が LDAP 内の別のドメイン名にマップされている場合であっても、一意でないログイン ID は CA Adapter では現在サポートされません。

LDAP パスワードで特殊文字を使用すると AFM 認証エラーが発生する

LDAP ベースの認証が使用されていて、LDAP パスワードに「¥」または「"」の文字が含まれている場合、これらの文字が LDAP でサポートされていても、認証エラーが発生します。

以前にリスク評価で使用されたパブリック デバイスにエンド ユーザが関連付けられる

エンドユーザのリスク評価ワークフローで、ログインに使用するデバイスにすでにデバイス ID Cookie があり、そのユーザがそのデバイスと関連付けられていない場合に、ユーザが認証時に［Public Compute］オプションを選択しても、そのユーザはそのデバイスと関連付けられます。 その後のトランザクションでは、ユーザはセカンダリ認証を求められません。

ArcotID OTP のブラウザ ベースのコントローラでは「European Union Cookie Legislation」が適用されない

ArcotID OTP のブラウザ ベースのコントローラでは、エンドユーザが「European Union Cookie Legislation」を選択しなかった場合でも、ArcotID OTP 認証情報がエンドユーザのシステムにダウンロードされます。

CA Adapter のアンインストール後にレジストリ ファイルが削除されない

CA Adapter をアンインストールした場合、zerog レジストリ XML ファイル（.com.zerog.registry.xml）は削除されません。 この XML ファイルでは、Adapter に関連するエントリのみが削除されます。 インストールされていた製品が Adapter のみの場合、アンインストール後のこの XML ファイルの内容は高レベル要素のみで空です。

アンインストール後にレジストリのエントリが削除されない

症状:

アンインストール後に、製品に関連するレジストリ エントリの一部が削除されません。

解決方法:

この問題は、機能に影響を与えません。 レジストリ エントリは、次回のインストール時に上書きされます。

サイレント モードのインストールがサポートされない

サイレント モードのインストールはサポートされません。

CA VPN Client の制限

ユーザ プロファイルをネットワーク上の場所に配置できない

CA VPN Client では、ネットワーク上の場所へのユーザ プロファイルの保存はサポートされていません。 ユーザ プロファイル ディレクトリは、クライアントを実行しているシステムのローカルにある必要があります。

ユーザ名の重複による認証の問題

同じ名前の 2 人のユーザが 2 つの別の組織に存在し、その組織の 1 つがデフォルトの組織（DEFAULTORG）である場合、以下の条件を満たすときに ArcotID PKI 認証は失敗します。

- 組織名を指定せずに認証プロファイルが作成された場合。
- 別のユーザの ArcotID PKI がシステムにすでに存在する場合。

CA VPN Client でマルチバイト データがサポートされない

CA VPN Client の国際化（マルチバイト データ）はサポートされていません。