



SECURITY®

Readme

RSA Authentication Manager 6.1

2006 年 1 月

はじめに

このドキュメントでは、RSA Authentication Manager 6.1 の新機能と更新された機能、報告されている問題点、その他の重要な情報について説明します。このドキュメントはソフトウェアをインストールする前にお読みください。

このドキュメントの内容は次のとおりです。

- [報告されている問題点](#)
- [サポートとサービス](#)

この Readme は、更新されることがあります。最新情報が記載された Readme は、RSA SecurCare Online <https://knowledge.rsasecurity.com> において閲覧できます。

報告されている問題点

RSA RADIUS Server のサポートについて

RSA RADIUS Server 6.1 は、HP または IBM AIX オペレーティング システムではサポートされていません。RSA RADIUS がサポートしているオペレーティング システムについては、『RSA RADIUS Server 6.1 Administrator's Guide』を参照してください。

RSA RADIUS Server 6.1 は、クロス レalm 認証をサポートしていません。**cross-realm authentication**.

トラッキング番号 : 19263

RSA RADIUS Server インストーラの -p オプションは動作しません。管理通信ポートとして TCP ポート 1813 (デフォルト) を使用してください。

トラッキング番号 : 20188

レプリカ RADIUS Server が新しいプライマリとなるように指定されると同時に管理者がプライマリ RADIUS Server 上で変更を行った場合、変更した設定は元のプライマリで失われます。

対処法：レルム内でレプリカを新しいプライマリ RADIUS Server にすることと、元のプライマリでのすべての管理セッションは中断する必要があることを、すべての管理者に通知してください。

RSA Authentication Manager をアンインストールしているとき、RADIUS Server がアンインストールできない。

トラッキング番号：19095

問題点：UNIX と LINUX プラットフォームで、プライマリ RADIUS Server が Replica Authentication Manager と同じマシンにある場合、プライマリ RADIUS Server は Replica Authentication Manager をアンインストールする際にアンインストールされません。さらに、ユーザは Replica Authentication Manager をアンインストールした後、プライマリ RADIUS Server に認証されなくなります。

対処法：Replica Authentication Manager をアンインストールする前に、次のいずれかの操作を行ってください。

- レルムの一部としてレプリカ RADIUS Server がある場合、Replica Authentication Manager をアンインストールする前に、レプリカ RADIUS Server を元のプライマリ RADIUS Server の代わりに指定します。詳しくは、『RSA RADIUS Server 6.1 Administrator's Guide.』を参照してください。
- 指定できるレプリカ RADIUS Server がない場合、Replica Authentication Manager をアンインストールする前に、異なるマシンにプライマリ RADIUS Server を再インストールします。

RSA RADIUS Server Administration Data Field が更新されない。

トラッキング番号：20143

問題点：レプリカ RADIUS Server を追加する場合、サーバの情報は RSA RADIUS Server Administration インターフェイスで更新されません。

対処法：レプリカ **RADIUS Server** を追加した後に [Refresh] をクリックします。

コマンド ラインでインストールした場合、自動的に RSA RADIUS Server が開始する。

トラッキング番号：20104

問題点：コマンド ライン ユーティリティを使用して RSA RADIUS Server をインストールすると、インストールが完了した時点で自動的に開始します。

対処法：RSA RADIUS Server スタートアップ タイプを “Automatic” から “Manual” に変更してください。

オフライン認証が無効の場合、Windows パスワード情報が更新されない。

トラッキング番号 16941

問題点：[Enable Offline Authentication at system level] チェックボックスがオフのとき、ユーザがローカル認証を実行すると、ユーザのパスワードが Windows エージェント上で更新されない場合があります。

対処法：ローカルの **Authentication Client** コンピュータを再起動してください。

オフラインの認証サービスポートを手動で変更する必要がある。

トラッキング番号 : tst00041788

問題点 : システム レベルでオフライン認証を有効にした場合、データベース ロード ユーティリティはデフォルトでポート 5580 を使用します。プライマリの認証サービス ポート番号を変更すると、新しいレプリカ パッケージを作成してレプリカに送信され、レプリカ上のポート番号は変更されません。

対処法 : サードパーティ サービスとの競合を避けるためにサービスのポート番号を変更するには、プライマリとすべてのレプリカ上で **Configuration Management** アプリケーションを使用します。

Windows XP SP2 更新すると、オフライン データをダウンロードするために必要なポートが閉じる。

トラッキング番号 : 13413

問題点 : RSA Authentication Agent for Microsoft Windows を実行しているマシンを Windows XP SP2 にアップグレードすると、Windows ファイアウォール が有効になり、オフライン ログオン データをドメイン コントローラとドメイン クライアントにダウンロードする際に使用するポート番号 2334 と 2335 が閉じます。

対処法 : 次の操作を行ってください。

1. [スタート] > [コントロールパネル] の順に選択します。
2. [Windows ファイアウォール] をクリックします。
3. [例外] タブをクリックします。
4. [ポートの追加] をクリックします。
5. [ポートの追加] ダイアログボックスで、[名前] ボックスに「sdoad」と入力し、ポート番号ボックスに「2334」（ドメイン クライアント）または「2335」（ドメイン コントローラ）を入力します。
6. [TCP] をクリックします。
7. [OK] をクリックします。
8. もう一度 [OK] をクリックします。

Automated Log Maintenance によってアーカイブ ファイルの作成に失敗する。

トラッキング番号 : 14472

問題点 : Automated Audit Log Maintenance を設定する際、ログ アーカイブ ファイル名には文字と番号のみが使用できます。ファイル名に次の記号が含まれていないかどうかを確認してください :

* “ < > |

RSA Authentication Manager は、これらの記号も使用できますが、アーカイブ ファイルを作成することはできません。

対処法 : 名前には文字と数字のみを使用してください。

プライマリ名または IP アドレスを変更した後にデータベースをレプリケートできない。

トラッキング番号 : 14994

問題点 : プライマリの名前または IP アドレスを変更し、Push DB-Assisted Recovery が有効になっている場合、レプリカはプライマリからの変更を受け付けません。

対処法：レプリカ パッケージを生成してレプリカに手動で配信するか、各レプリカ システムに「ACE_ALLOW_TAKEOVER」という環境変数を追加して値を「1」に設定します。この環境変数により、プライマリ名または IP アドレスを変更した後にもレプリカはプライマリと通信することができます。

アップグレードを行うと **apidemon.ini** ファイルが削除される。

トラッキング番号：19805

問題点：Windows マシンで Authentication Manager 6.0 を Authentication Manager 6.1 にアップグレードすると、Administration Toolkit と Quick Admin の環境設定を含む **apidemon.ini** ファイルが削除されます。

対処法：アップグレードを実行する前に、**apidemon.ini** をプライマリまたはレプリカの %SystemRoot%\system32\ にバックアップします。アップグレードが完了した後、%SystemRoot%\system32\ にバックアップした **apidemon.ini** ファイルを戻します。

ダンプ ファイルがすでにある場合、**sddump** エラーが発生する。

トラッキング番号：21358

問題点：Linux プラットフォームで ACEPROG に sdserv.dmp または sdlog.dmp がすでにある場合、**sddump** エラーが発生します。

対処法：**sddump** を実行する前に、ACEPROG から既存の **sdserv.dmp** または **sdlog.dmp** を削除します。

一度発行したソフトウェア トークンの割り当てを解除した後に、再度ソフトウェア トークンを発行することができない。

問題点：一度 [Issue Software Token] を使用してユーザに割り当てたソフトウェア トークンに対し、割り当てを解除すると、その後別のユーザにソフトウェア トークンを発行しようとしても、トークン レコードの「Issued」フラグが「Yes」となっているため、発行できません。

対処法：[Token] メニューの [Revoke Software Tokens] を実行して、割り当てが解除されたソフトウェア トークンの「Issued」フラグを外してください。

マニュアルとヘルプについて

RSA Authentication Manager 6.1 Administration Toolkit Reference Guide

トラッキング番号：19533

209 ページの **Sd_SetAgentHostRADIUSInfo** の説明において「default RADIUS Server Agent Host connection port is 1830」とあります。正しいデフォルト ポートは 1813 です。

RSA Authentication Manager 6.1 Administration ヘルプ

トラッキング番号：19900

ヘルプ トピック「Getting Started with RSA Authentication Manager」の「Starting and Stopping the RSA Authentication Manager」リンクは間違ったトピックとリンクしています。また、この際開かれる「Starting and Stopping the RSA RADIUS Server」には古い情報が含まれています。次が正しい手順です。

To start or stop RSA RADIUS Server processes on the Primary:

1. Click **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.
2. In the Control Panel menu, click **Start & Stop RSA Authentication Manager Services**.
3. To automatically start RSA RADIUS Server when you start the authentication engine, under Service Management, select **Start and stop RADIUS Server together with authentication engine**. Then, under **Start Services**
 - To start all services, click **Start All**.
 - To stop all services, click **Stop All**.
4. To start and stop just RSA RADIUS Server, under Service Management, make sure **Start and stop RADIUS Server together with authentication engine** is not selected. Then, under **Start Services**
 - To start RSA RADIUS Server, click **Start RADIUS**.
 - To stop RSA RADIUS Server, click **Stop RADIUS**.

サポート と サービス

RSA SecurCare Online: <https://knowledge.rsasecurity.com>

© 2006 RSA Security Inc. All rights reserved.

商標

ACE/Agent, ACE/Server, Because Knowledge is Security, BSAFE, ClearTrust, Confidence Inspired, e-Titlement, IntelliAccess, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, the RSA Secured logo, RSA Security, SecurCare, SecurID, SecurWorld, Smart Rules, The Most Trusted Name in e-Security, Transaction Authority, and Virtual Business Units are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other goods and/or services mentioned are trademarks of their respective companies.