リリース ノート

RSA®Authentication Manager 8.0

2013 年 3 月

はじめに

本書では、RSA Authentication Manager 8.0 における新機能と変更点に加え、既知の不具合とその回避方法を記載しています。Authentication Manager 8.0 仮想アプライアンスを導入する前に、本書をお読みください。このドキュメントには、次のセクションがあります。

このリリースの最新情報

このセクションでは、本リリースにおける主要な変更について説明します。各変更点の詳細については、製品ドキュメントを参照してください。

仮想化

RSA Authentication Manager 8.0 は、VMware 環境に、RSA Authentication Appliance と呼ばれる仮想アプライアンスとして導入されます。VMware vSphere Client を使用して、仮想アプライアンスを、VMware vCenter 経由で導入するか、VMware ESXi プラットフォームに直接導入します。RSA Authentication Appliance の導入に VMware vCenter は必須ではありません。

仮想化には、次のようなメリットがあります。

- **VMware 機能サポート**。Authentication Manager は、vMotion、Storage vMotion、High Availability、DRS（Distributed Resource Scheduler）、スナップショットなどの VMware 機能をサポートしています。次の制限があります。

  VMware Fault Tolerance。Fault Tolerance と互換性があるのは、単一の仮想 CPU を持つ仮想アプライアンスだけです。デフォルトでは、各 Authentication Manager インスタンスは 2 つの仮想 CPU を持つよう導入されますが、必要に応じて仮想 CPU の数は変更できます。手順については、VMware vSphere Client のドキュメントを参照してください。

  VMware スナップショット。Authentication Manager プライマリ インスタンスまたはレプリカ インスタンスの VMware スナップショットを取ることができますが、スナップショットは、Operations Console のバックアップ機能に代わるものではありません。

  Authentication Manager インスタンスのスナップショットを取るときは、特定の設定が必要です。複雑な Authentication Manager 環境では、スナップショットを復元するために追加のタスクを実行する必要があります。詳細については、「RRSA Authentication Manager 8.0 管理者ガイド」の「災害復旧」の章を参照してください。

  VMware DRS（Distributed Resource Scheduler）。セキュリティと冗長性を実現するため、プライマリ インスタンスとレプリカ インスタンスを別々のホストにインストールできます。VMware DRS は、両方のインスタンスを同じホストに移動できます。各インスタンスを別々の物理ホストに維持するよう DRS を構成します。

- **Quick Setup の簡略化と高速化**。Quick Setup が開始する前に、仮想アプライアンスのネットワーク設定は構成されます。その結果、導入作業全体が高速になりました。Quick Setup での混乱を解消するため、Security Console、Operations Console、仮想アプライアンス オペレーティング システムの管理者アカウントを別々に作成します。Quick Setup プロセスは、以前のリリースより高速になりました。

リスク ベース認証

RBA（リスク ベース認証）。RBA は、ユーザーに気づかせることなくユーザーの行動パターンと認証に使用するデバイスを解析し、その結果から潜在的なリスクや不正な認証の試みを特定することによって、従来のパスワード ベースの認証および RSA SecurID 認証を強化します。RBA でネットワーク リソースを保護する場合、ユーザーが認証を試行するたびに、ユーザーのプロファイル、認証デバイス、認証履歴に基づいて、システムが保証レベルを決定します。

RBA/ODA ライセンス カウント。リスク ベース認証と ODA（On-Demand 認証）が組み合わされて、RBA/ODA という 1 つの機能になりました。RBA/ODA は、ライセンスで指定されているユーザー数に対して有効です。

RSA SecurID と RBA。RBA では、プライマリ認証方式としてパスワードに加えて RSA SecurID も使用できます。詳細については、「RSA Authentication Manager 8.0 管理者ガイド」の「リスクベース認証の導入」の章を参照してください。

運用コストの削減と管理の改良

ユーザー ダッシュボード。ユーザー ダッシュボードは、最近の認証アクティビティ、ユーザー グループ メンバーシップ、On-Demand トークンコードの配布方法など、ユーザー認証データに関する統合的なビューを提供します。ヘルプ デスク管理者とアカウント管理者は、ダッシュボードからエンド ユーザーの問題を特定してトラブルシューティングできます。

Web Tier。Authentication Manager には、RBA、動的シード配布、Self-Service Console のサービスが含まれます。これらのサービスには、企業ネットワーク外のユーザーからのアクセスが必要となる場合があります。ネットワークに DMZ（非武装地帯）が設置されている場合、Web Tier を使用して、これらのサービスを DMZ 内に導入することができます。DMZ 内の Web Tier 上に Authentication Manager のサービスを導入すると、次のような利点があります。

- Self-Service Console や RBA ユーザーとのやりとりによって生じる、フィルタリングされないインターネット トラフィックから内部ネットワークを保護します。Web Tier サーバで、プライベート ネットワークに入る前の着信インターネット トラフィックを受信し、管理します。
- RBA のログイン ページと Self-Service Console をカスタマイズできます。
- デフォルトの証明書を、認証機関から取得した証明書と交換できます。
- 一部のタスク処理をバックエンド サーバから切り離すことにより、システム パフォーマンスが向上します。

Operations Console 管理者の管理。スーパー管理者は、Security Console を使用して Operations Console 管理者アカウントを管理できるようになりました。

Security Console、Operations Console、Self-Service Console の URL の簡略化。各コンソールの URL が簡略化され、覚えやすくなりました。

RSA Authentication Manager 6.1 からのアップグレード。Authentication Manager 6.1 からのアップグレードでは、次の機能がサポートされています。

- **レガシーデータの移行**。RSA Authentication Manager 6.1 から円滑に移行するため、ユーザー、トークン、エージェント、グループ、管理者、RADIUS データなどのレガシーデータを維持できます。
- **テスト移行と移行レポート**。実際に移行を実行する前に、テスト移行を実行し、移行によるデータへの影響をレポートで確認できます。

詳細については、「RSA Authentication Manager 6.1 から 8.0 への移行ガイド」を参照してください。また、RSA Authentication Manager 8.0 Migration Resources ページ（**https://knowledge.rsasecurity.com/scolcms/set.aspx?id=9620**）では、「Migration Overview Data Sheet」の閲覧、RSA Authentication Manager 6.1 to 8.0 Migration Assessment Utility のダウンロード、RSA Authentication Manager 6.1 から 8.0 への移行に関する E ラーニング コースおよび動画デモンストレーションを利用できます。

RSA Authentication Manager 7.1 からのアップグレード。RSA Authentication Manager 8.0 にアップグレードするには、RSA Authentication Manager 7.1 Migration Export Utility を使用して、データおよびログデータ（ログデータは任意）をエクスポートし、バージョン 8.0 にインポートするための暗号化された移行パッケージを作成します。Migration Export Utility には、認証のダウンタイムとデータロスの問題への対処に応じて、複数の移行シナリオのオプションがあります。

本リリースでは、テスト環境を作成して移行プロセスをテストしてから、テスト環境を本番環境に移行することもできます。詳細については、「RSA Authentication Manager 7.1 から 8.0 への移行ガイド」を参照してください。

移行の詳細については、RSA Authentication Manager 8.0 Migration Resources ページ（**https://knowledge.rsasecurity.com/scolcms/set.aspx?id=9620**）を参照してください。「Migration Overview Data Sheet」の閲覧、RSA Authentication Manager 7.1 からの移行に関する E ラーニング コースおよび動画デモンストレーションを利用できます。

Microsoft 管理コンソールのサポート。RSA Token Management スナップインは、MMC（Microsoft Management Console）の Active Directory Users and Computers スナップインのコンテキスト メニュー、プロパティ ページ、コントロール バー、ツールバーを拡張し、MMC によるトークン管理を可能にします。スナップインは、「RSA Authentication Manager 8.0 セットアップと構成ガイド」の付録「RSA Authentication Manager Token Management スナップインのインストール」にリストされているプラットフォームに加えて、Windows 8 用リモート サーバ管理ツールをインストール済みの Windows 8（32 ビットおよび 64 ビット）をサポートしています。

トークンおよびユーザーのエクスポート / インポート。1 つの Authentication Manager 8.0 環境からユーザーとトークン、またはトークンのみをエクスポートし、それらを別の Authentication Manager に安全にインポートできます。

レプリカのアタッチの機能拡張。レプリカのアタッチが、Quick Setup の一環として実行されるようになりました。セキュリティを強化するため、Operations Console のクレデンシャルを使用するようになりました。アタッチの実行中、［Progress Monitor（進行状況）］画面に、プロセスの各ステップのステータスが表示されるようになりました。レプリカのアタッチを停止することなく、問題を解決できるようになりました。

証明書の管理。外部の証明機関が発行するセキュリティ証明書の要求、ダウンロード、アクティブ化の一連のプロセスを、Operations Console を使用して実行できるようになりました。

パスワード管理の向上。Authentication Manager 8.0 では、マスター パスワードはなくなりました。これにより、管理者が覚える必要があるパスワードは減り、すべての管理アクティビティは特定の管理者アカウントに関連づけられるようになります。

ソフトウェア トークン プロファイルおよび配布。Self-Service Console でソフトウェア トークン プロファイルを使用して、ソフトウェア トークンを配布できるようになりました。ソフトウェア トークン プロファイルは、ソフトウェア トークン構成および配布プロセスを指定します。ソフトウェア トークン パラメータを、ソフトウェア トークンを配布するたびに入力するのではなく一度入力するだけで済むため、ソフトウェア トークンの配布プロセスを合理化できます。また、初期構成の後に、パラメータを変更できます。ソフトウェア トークンを配布する予定のプラットフォームごとに、1 つのソフトウェア トークン プロファイルが必要です。

CTF（Compressed Token Format）サポート。Authentication Manager では、Security Console を使用した CTF 形式のソフトウェア トークンの配布がサポートされるようになりました。CTF 形式はすべての Android デバイスでサポートされているため、コンバータ CLU（コマンド ライン ユーティリティ）を実行して SDTID ファイルを CTF 形式に手動で変換する必要がなくなります。

ホーム ページでのクイック検索。クイック ユーザー検索では、姓またはユーザー ID（どちらか一方を設定により選択）によってユーザーを検索できます。1 つのアイデンティティ ソース、または権限適用範囲内のすべてのアイデンティティ ソースでユーザーを検索できます。

SecurID ソフトウェア トークン検索オプションの増加。ソフトウェア トークンの一括配布を実行するときに、トークン シリアル番号の範囲を指定して SecurID ソフトウェア トークンを検索できます。

アプリケーション信頼関係に関するドキュメント。Operations Console を使用してアプリケーション信頼関係を作成するための手順が、「Developer's Guide」に追加されました。アプリケーション信頼証明書は、カスタム アプリケーションと Authentication Manager 間の通信のセキュリティを保護します。

セルフサービスのユーザー登録。内部データベースまたは他の任意のアイデンティティ ソースにアカウントを持つユーザーは、セルフサービスに登録する必要はありません。そのようなユーザーは、デフォルトで、Self-Service Console を使用してセルフサービス機能を利用できます。すべての外部アイデンティティ ソースは読み取り専用のため、登録を要求する新規ユーザーのユーザー レコードは、すべて内部データベースに作成されます。

RADIUS

RSA RADIUS の機能向上：

- **RADIUS サーバの自動構成および有効化**。RSA RADIUS サーバは、Authentication Manager のセットアップと構成時に、自動的に構成および有効化されます。
- **RSA RADIUS サーバの管理**。Operations Console の RADIUS ページが改良され、使いやすくなりました。
- **RADIUS データのバックアップとリストア**。RADIUS データが、導入環境の他のデータのバックアップに統合されました。プライマリ インスタンスをバックアップからリストアすると、導入環境の他のデータとともに RADIUS データもリストアされます。
- **RADIUS の昇格**。Authentication Manager レプリカ インスタンスが昇格されると、その上に存在する RSA RADIUS レプリカ インスタンスも昇格されます。これにより、RADIUS プライマリ インスタンスは常に Authentication Manager プライマリ インスタンス上に存在することになります。
- **自動 RADIUS レプリケーション**。定期レプリケーションが有効な場合、RADIUS データは、15 分ごとに RADIUS レプリカ サーバに自動的に複製されます。RADIUS 定期レプリケーションは、Security Console の［System Settings（システム設定）］ページから構成します。RADIUS レプリケーションはデフォルトで有効になっています。

レポート作成

複数のアイデンティティ ソースを対象にしたレポートの実行。レポートを実行する際、1 つのアイデンティティ ソースを指定するか、アイデンティティ ソースを指定しないままにしてすべてのアイデンティティ ソースのレポートを生成することができます。次のレポートは、複数アイデンティティ ソースに対応しています。

- Users Enabled for On-Demand Authentication（On-Demand 認証が有効なユーザー）
- Users Enabled for On-Demand Tokencode Service Who Have Never Logged In（On-Demand トークンコード サービスが有効な未ログイン ユーザー）
- Users Never Logged In with Token（トークンを使用してログインしたことがないユーザー）
- Users with Days Since Last Login Using Specific Token（特定のトークンタイプの最終ログイン日が指定期間内にあるユーザー）
- Users with Tokens（トークン所有ユーザー）
- Token Expiration Report（トークン有効期限レポート）
- Distributed Token Requests（配布済みのトークン リクエスト）

カスタム属性のサポート。次のレポートでは、カスタム属性がサポートされるようになりました。

- すべてのユーザー
- Users with Tokens（トークン所有ユーザー）
- Users Enabled for On-Demand Authentication（On-Demand 認証が有効なユーザー）
- List all Users with Assigned RADIUS Profile（RADIUS プロファイルが割り当てられた全ユーザーのリスト）
- RBA（リスク ベース認証）ユーザー

レポートにカスタム属性の列を含めたり、特定のカスタム ユーザー属性入力パラメータに基づいてレポートを生成したりできます。

メンテナンスとトラブルシューティングの向上

Operations Console の機能拡張：

- **トラブルシューティング用ログ ファイル**。ログ ファイルを、パスワードで保護された .zip ファイルでダウンロードできます。
- **hosts ファイルの編集**。RSA Authentication Manager アプライアンスの hosts ファイルを表示し、エントリーを編集できます。
- **ネットワーク診断ツール**。ping や traceroute などのコマンドを使用して、ネットワーク接続性の問題を診断できます。

災害復旧の機能拡張。バックアップやリストアなどの災害復旧操作が、Operations Console から実行できるようになりました。バックアップは暗号化されています。スケジュール機能が簡略化されました。バックアップ処理はログに記録されるようになり、Operations Console Progress Monitor を使用してリアルタイムで進捗を表示できるようになりました。ユーザーは、バックアップを格納する場所として、Authentication Manager のローカルディスク、Windows 共有フォルダ、NFS（Network File System）共有フォルダを選択できます。また、レプリカ インスタンスの昇格プロセスが簡略化されました。既存のレプリカ インスタンスは、同期プロセスを使用して新しいプライマリ インスタンスに簡単に接続できます。RADIUS レプリカから RADIUS プライマリへの昇格は、Authentication Manager の昇格プロセスに統合されました。

重大なシステム イベント通知。Authentication Manager は、重大なシステム イベントが発生するとメールで管理者に通知できるようになりました。重大なシステム イベントには、ディスク空き領域の低下、アイデンティティ ソースの障害、レプリケーション ステータスの変更などがあります。管理者は、解決が必要な問題が発生したことを直ちに知ることができます。

Operations Console での日付と時間の変更。Quick Setup で NTP（Network Time Protocol）サーバを指定しなかった場合は、Operations Console から指定することができます。Operations Console を使用すると、各インスタンスの日付と時間の設定を同期および検証できます。

製品ドキュメント

本リリースでは、次のドキュメントが提供されます。

タイトル	ファイル名
RSA Authentication Manager 8.0 管理者ガイド	**am_administrators_guide.pdf**
RSA Authentication Manager 8.0 Getting Started	**am_getting_started.pdf**
RSA Authentication Manager 8.0 設計ガイド	**am_planning_guide.pdf**
RSA Authentication Manager 8.0 セットアップと構成ガイド	**am_setup_config_guide.pdf**
RSA Authentication Manager 6.1 から 8.0 への移行ガイド	**am_migration_guide_6.1.pdf**
RSA Authentication Manager 8.0 SNMP Reference Guide	**am_snmp_ reference_guide.pdf**
RSA Authentication Manager 7.1 から 8.0 への移行ガイド	**am_migration_guide_7.1.pdf**
RSA Authentication Manager 8.0 Help Desk Administrator’s Guide	**am_help_desk_administrator_guide.pdf**
RSA Authentication Manager 8.0 トラブルシューティング ガイド	**am_troubleshooting_guide.pdf**

タイトル	ファイル名
RSA Authentication Manager 8.0 Developer’s Guide	
RSA Authentication Manager 8.0 Security Configuration Guide	**am_security_config_guide.pdf**
RSA RADIUS リファレンス ガイド	**am_radius_reference_guide.pdf**
Security Console ヘルプ	
Operations Console ヘルプ	
Self-Service Console ヘルプ	
RSA Token Management Snap-In for the Microsoft Management Console ヘルプ	

既知の問題

このセクションでは、本リリースで未解決の問題について説明します。回避策や修正が利用可能な場合、その内容、または詳細の参照先が記載されています。このセクションの多くの回避策では、管理権限が必要です。必要な権限がない場合は、管理者に問い合わせてください。

移行

バージョン 6.1 から移行すると、アクセス時間の制限なしでグループにアクセスを許可していた無制限エージェントは、制限付きエージェントに変換されます。

追跡番号：AM-11452

問題：バージョン 6.1 では、無制限エージェントが、アクセス時間の制限なしでグループにアクセスを許可できます。バージョン 8.0 への移行中、特定のユーザー グループにアクセスを許可するすべての無制限エージェントは、関連づけられているユーザー グループにのみアクセスを許可する制限付きエージェントに自動的に変換されます。その結果、バージョン 6.1 で無制限エージェントで認証できていた一部のユーザーは、バージョン 8.0 ではそのエージェントで認証できなくなります。

回避策：このエージェントへのアクセスをすべてのユーザーに許可するには、次の手順を実行します。

手順

1. バージョン 8.0 プライマリ インスタンスの Security Console で、**［Access（アクセス）］**＞**［Authentication Agents（認証エージェント）］**＞**［Manage Existing（既存項目の管理）］**の順にクリックします。
2. **［Restricted Agents（制限付きエージェント）］**タブをクリックし、検索フィールドを使用して、編集するエージェントを検索します。
3. エージェントの名前をクリックして、コンテキスト メニューから **［Edit（編集）］**を選択します。
4. ［Authentication Agent Attributes（認証エージェントの属性）］で、**［Allow access only to members of user groups who are granted access to this agent（このエージェントへのアクセスが許可されているユーザー グループのメンバーにのみアクセスを許可する）］**チェックボックスをオフにします。
5. **［Save（保存）］**をクリックします。

バージョン 7.1 から、バージョン 8.0 の昇格されたレプリカ インスタンスへの移行が失敗する

追跡番号：AM-24674

問題：バージョン 8.0 のレプリカ インスタンスをプライマリ インスタンスに昇格してから、昇格されたレプリカ インスタンスにバージョン 7.1 のデータを移行しようとすると、移行が失敗します。

回避策：最初の移行パッケージをインポートしていない場合、またはシステム設定や導入環境トポロジーを保持しなで追加のインポートを実行したい場合は、昇格したレプリカ インスタンスを削除し、バージョン 8.0 のプライマリ インスタンスを再セットアップし、新しいプライマリ インスタンスにデータをインポートする必要があります。最初のインポートを実行済みで、システム設定や導入環境トポロジーを保持したまま追加のインポートを実行する場合、昇格したレプリカ インスタンスに移行することができます。

Authentication Manager 6.x の大量のユーザー拡張データの移行が失敗する

追跡番号：AM-25754

問題：一意の拡張キーを大量に移行しようとすると（たとえば 1,000）、移行が遅くなり失敗します。

回避策：拡張キーを整理して、同じデータに対して複数のフィールドがないことを確認します。

バージョン 6.1.3 と 6.1.4 の PIN 管理データは、バージョン 8.0 導入環境には移行されません。

追跡番号：AM-25968

問題：バージョン 6.1.3 と 6.1.4 は、導入環境の PIN ポリシーを管理するため、システム拡張データ属性の使用をサポートしています。サポートされるシステム拡張データ キーは次のとおりです。RSA_PIN_HISTORY、RSA_PIN_EXPIRATION、RSA_MIN_NUM_ALPHA、RSA_MIN_NUM_NUMERIC。これらの設定はバージョン 8.0 には移行されません。

回避策：バージョン 8.0 のトークン ポリシーを手動で構成して、バージョン 6.1.x PIN 管理設定の動作と一致するようにします。

手順

1. バージョン 6.1.x にログオンします。
2. Database Administration アプリケーションで、**［System（システム）］** > **［Edit System Extension Data（システム拡張データの編集）］**の順にクリックします。
3. **［Key（キー）］**フィールドで、次のキーを探して**［Data（データ）］**値を記録します。
   - RSA_PIN_HISTORY
   - RSA_PIN_EXPIRATION
   - RSA_MIN_NUM_ALPHA
   - RSA_MIN_NUM_NUMERIC
4. Authentication Manager 8.0 Security Console にログオンして、**［Authentication（認証）］** > **［Policies（ポリシー）］** > **［Token Policies（トークン ポリシー）］** > **［Manage Existing（既存項目の管理）］**の順にクリックします。
5. 検索フィールドを使用して、編集するトークン ポリシーを検索します。
6. 編集するトークン ポリシーをクリックして、コンテキスト メニューから**［Edit（編集）］**を選択します。
7. ステップ 3 のデータを次のように入力します。
   - RSA_PIN_HISTORY の値が存在する場合、**［SecurID PIN Lifetime（SecurID PIN の有効期間）］**で、**［Restrict Reuse（再使用の制限）］**オプションの**［Users cannot reuse their last value SecurID PINs（ユーザーは過去の SecurID PIN を再使用できない）］**を選択して、テキスト フィールドに RSA_PIN_HISTORY の値を入力します。
   - RSA_PIN_EXPIRATION の値が存在する場合、**［SecurID PIN Lifetime（SecurID PIN の有効期間）］**の**［Periodic Expiration（定期的な変更を要求）］**フィールドで、**［Require periodic SecurID PIN changes（SecurID PIN の定期的な変更を要求）］**チェックボックスをクリックします。**［Maximum Lifetime（最大有効期間）］**テキスト フィールドに RSA_PIN_EXPIRATION の値を入力します。ドロップダウン メニューから**［days（日数）］**を選択します。
   - RSA_MIN_NUM_ALPHA の値が存在する場合、**［SecurID PIN Format（SecurID PIN 形式）］**の**［Character Requirements（文字要件）］**フィールドで、**［Allow alphanumeric PINs（英数字 PIN の許可）］**を選択します。**［Require at least value alphabetic characters（最低限必要な英字の文字数）］**ドロップダウン メニューから RSA_MIN_NUM_ALPHA の値を選択します。
   - RSA_MIN_NUM_NUMERIC の値が存在する場合、**［SecurID PIN Format（SecurID PIN 形式）］**の**［Character Requirements（文字要件）］**フィールドで、**［Allow alphanumeric PINs（英数字 PIN の許可）］**を選択します。**［Require at least value alphabetic characters（最低限必要な数字の文字数）］**ドロップダウン メニューから RSA_MIN_NUM_NUMERIC の値を選択します。
8. **［Save（保存）］**をクリックします。

バージョン 8.0 のトークン ポリシーの詳細については、「Security Console ヘルプ」の「トークン ポリシー」のトピックを参照してください。

スペイン語の Windows ホストで動作するバージョン 6.1 環境で RADIUS エクスポート ユーティリティを実行後、RADIUS 管理機能を回復できない

追跡番号：AM-25969

問題：スペイン語の Windows ホストで動作するバージョン 6.1 環境で、RADIUS データをエクスポートした後、RADIUS 管理機能を回復できません。コマンド プロンプトを使用して RADIUS 管理機能の回復と、RADIUS エクスポート ユーティリティの削除を実施した後、バージョン 6.1 Database Administration アプリケーションから **[RADIUS] > [Manage RADIUS Server（RADIUS サーバの管理）]** を選択すると、RADIUS エクスポート ユーティリティが表示され、RADIUS サーバを管理できません。

回避策：バージョン 6.1 RADIUS 管理機能へのアクセスを回復するには、次の処理手順を実行します。

手順

1. バージョン 6.1 環境で、***RSA_HOME*/prog/radius/Admin/** にアクセスします。
2. ファイル **sbradmin.exe** の名前を **rsa_patch_sbradmin.exe** に変更します。
3. ファイル **sbradmin.exe.orig** の名前を **sbradmin.exe** に変更します。

バージョン 6.1 から移行した後、ユーザー グループにアクセスを許可する無制限エージェントは、制限付きエージェントに変換されます。

追跡番号：AM-26168

問題：バージョン 6.1 では、無制限エージェントが特定のユーザー グループにアクセスを許可でき、そのグループのメンバーに対するログオン エイリアスを設定することができます。バージョン 8.0 への移行時、特定のユーザー グループにアクセスを許可する無制限エージェントは、制限付きエージェントに自動的に変換されます。この制限付きエージェントは、特定のユーザー グループのユーザーのみアクセスできます。Security Console を使用してエージェントを無制限エージェントに変更できますが、バージョン 8.0 の無制限エージェントはログオン エイリアスの設定をサポートしていません。

回避策：すべてのユーザーにエージェントへのアクセスを許可するには、次の処理手順を実行します。この処理手順を実行すると、構成済みのログオン エイリアスの設定がこのエージェントには適用されなくなります。

手順

1. バージョン 8.0 プライマリ インスタンスの Security Console で、**[Access（アクセス）] > [Authentication Agents（認証エージェント）] > [Manage Existing（既存項目の管理）]** の順にクリックします。
2. **[Restricted Agents（制限付きエージェント）]** タブをクリックし、検索フィールドを使用して、編集するエージェントを検索します。
3. エージェントの名前をクリックして、コンテキスト メニューから **[Edit（編集）]** を選択します。
4. [Authentication Agent Attributes（認証エージェントの属性）] で、**[Allow access only to members of user groups who are granted access to this agent（このエージェントへのアクセスを許可したユーザー グループのメンバーにのみアクセスを許可する）]** チェックボックスをオフにします。
5. **[Save（保存）]** をクリックします。

バージョン 6.1 データベース ダンプ ファイルまたはバージョン 7.1 移行パッケージをアップロードできない

追跡番号：AM-26224

問題：ブラウザでは、2 GB を超える移行データ ファイルのアップロードをサポートしていません。Internet Explorer 8.0 では、2 GB 未満の移行データ ファイルのアップロードも行えない場合があります。

回避策：以下のいずれかの操作を実行します。

- バージョン 6.1 データベース ダンプ ファイルまたはバージョン 7.1 移行パッケージが 2 GB を超える場合、RSA カスタマー サポートにご連絡ください。
- Internet Explorer 8.0 で 2 GB 未満の移行データ ファイルのアップロードが行えない場合、サポート対象の次のいずれかのブラウザをお試しください。
  - Firefox 10.0 以降
  - Google Chrome 18 以降
  - Apple Safari 5.1 以降

バージョン 7.1 からの移行時、無効な Windows または NFS 共有フォルダのパスを指定すると、[Import Migration Package（移行パッケージのインポート）] ページでシステム内部エラーが発生する

追跡番号：AM-26632

問題：Operations Console を通してバージョン 7.1 移行パッケージをインポートする際に、Windows または NFS（Network File System）共有フォルダへの無効なパスを入力すると、[System Internal Error（システム内部エラー）] メッセージが表示されます。

回避策：エラー メッセージで [home（ホーム）] をクリックし、バージョン 7.1 からの移行のインポート ページに戻ります。Windows または NFS 共有フォルダから移行パッケージをインポートする場合、Windows 共有フォルダまたは NFS サーバおよびディレクトリへの有効なパスを入力します。たとえば、有効なパスは次のようになります。

- Windows 共有フォルダの場合：**\\example.com\migration_folder**
- NFS 共有フォルダの場合：**fileserver.example.net:/migration_directory**

バージョン 7.1 から移行した導入環境にアイデンティティ ソースを追加した後、拡張ユーザー属性が表示されない

追跡番号：AM-26671

問題：バージョン 7.1 から移行した Authentication Manager 8.0 導入環境にアイデンティティ ソースを追加すると、携帯電話属性などの拡張ユーザー属性が表示されません。ユーザー ID、姓名といった基本的なユーザー属性は表示されます。

回避策：新しいアイデンティティ ソースの属性を編集して保存します。

1. Security Console で **[Identity（アイデンティティ）] > [Identity Attribute Definitions（アイデンティティ属性定義）] > [Manage Existing（既存項目の管理）]** の順にクリックします。
2. 編集するアイデンティティ属性定義をクリックして、コンテキスト メニューから **[Edit（編集）]** を選択します。
3. アイデンティティ属性定義に必要な変更を行います。

   注：管理者権限に応じてユーザーの属性を指定できるか決まります。[Add New User and Edit Users（ユーザーの新規追加と編集）] ページでは、必須属性であっても、ロールによって編集が許可されていない属性の値を入力することはできません。

4. **[Save（保存）]** をクリックします。

バージョン 6.1 からの移行では、LDAP ディレクトリ上のユーザー グループが移行時に使用できない場合、制限付きエージェントの設定が保持されない

追跡番号：AM-26715

問題：バージョン 6.1 データベース ダンプ ファイルに含まれるユーザー グループが、移行時に LDAP ディレクトリ上で使用できない場合、そのユーザー グループは制限付きエージェントへのアクセスを許可されません。

回避策：バージョン 6.1 からの移行前に、外部 LDAP ディレクトリでユーザー グループを正しく構成するか、移行完了後にユーザー グループに対して制限付きエージェントへのアクセスを許可します。

Security Console を使用して、プライマリ インスタンスとレプリカ インスタンスの Self-Service Console のヘッダ テキストを変更できない

追跡番号：AM-26726

問題：Authentication Manager 8.0 では、Security Console を使用して、プライマリ インスタンスとレプリカ インスタンスの Self-Service Console のヘッダ テキストを変更することはできません。バージョン 8.0 では、Web Tier の Self-Service Console のヘッダ テキストのみ Operations Console から変更できます。

回避策：

Authentication Manager 7.1 を 8.0 に移行する場合、次の点に注意します。

- Authentication Manager 7.1 環境で、プライマリ インスタンスとレプリカ インスタンスの Self-Service Console のヘッダ テキストがカスタマイズされている場合、移行後もカスタマイズが保持されます。7.1 のカスタマイズが、8.0 導入環境のプライマリ インスタンス、レプリカ インスタンス、Web Tier に適用されます。
- 本番移行前のテスト移行環境で、Web Tier の Self-Service Console のヘッダ テキストをカスタマイズした場合、本番移行時の移行シナリオの選択により、システム設定と導入環境トポロジーを維持することができます。本番移行時の移行シナリオで、システム設定と導入環境トポロジーを上書きするよう選択した場合、移行後に Self-Service Console のヘッダ テキストを再度カスタマイズする必要があります。

バージョン 8.0 の導入環境では、新規か移行したかにかかわらず、次のいずれかを行います。

- Web Tier の Self-Service Console のヘッダ テキストをカスタマイズするだけの場合、Operations Console を使用します。作業手順については、「Operations Console ヘルプ」で「Self-Service Console Web ページのカスタマイズ」のトピックを参照してください。
- Self-Service Console のヘッダ テキストをすべてのコンポーネント（プライマリ インスタンス、レプリカ インスタンス、Web Tier を含む）でカスタマイズする場合、次の処理を実行してリソース バンドル ファイルを更新します。

手順

この手順では、Authentication Manager 8.0 リソース バンドル ファイルに含まれる Self-Service Console ヘッダ テキストを変更し、ヘッダ テキストを表示するプライマリ インスタンス、レプリカ インスタンス、Web Tier に保存します。

1. **am-i18n-resources-8.0.0.0.0-full.jar** ファイルは以下の場所に存在します。
   - プライマリ インスタンスとレプリカ インスタンスでは、**/opt/rsa/am/utils/resources/am-i18n-resources-8.0.0.0.0-full.jar** に存在します。
   - Web Tier では、**[RSA_HOME]/utils/resources/am-i18n-resources-8.0.0.0.0-full.jar** に存在します。
2. **am-i18n-resources-8.0.0.0.0-full.jar** をバックアップします。
3. **am-i18n-resources-8.0.0.0.0-full.jar** を解凍します。
4. **com/rsa/ucm/web/selfservice/i18n** にアクセスします。
5. 次のプロパティ ファイルを見つけてください。
   - **UCMSelfService.properties**
   - **UCMSelfService_en.properties**
   - **UCMSelfService_en_US.properties**
6. 各プロパティ ファイルで、次の行を見つけます。
   ```
   #UCM.Home.Welcome=Welcome to the RSA Self-Service Console
   ```
7. 各プロパティ ファイルで、# を削除して、「`Welcome to the RSA Self-Service Console`」の部分を任意のテキストに置き換えます。

   例：`UCM.Home.Welcome=Welcome to the <企業名> Self-Service Console`

8. 3 つのプロパティ ファイルをすべて保存し、**am-i18n-resources-8.0.0.0.0-full.jar** を再度圧縮します。
9. カスタマイズした Self-Service Console のヘッダ テキストを表示するプライマリ インスタンス、レプリカ インスタンス、Web Tier で、**am-i18n-resources-8.0.0.0.0-full.jar** を次のディレクトリに配置します。
   - プライマリ インスタンスとレプリカ インスタンスでは、**/opt/rsa/am/utils/resources/am-i18n-resources-8.0.0.0.0-full.jar** に配置します。
   - Web Tier では、**[RSA_HOME]/utils/resources/am-i18n-resources-8.0.0.0.0-full.jar** に配置します。
10. すべてのインスタンスと Web Tier を再起動します。

管理

［Trusted Realms（トラステッド レルム）］ページのコンテキスト メニューで［Trusted Users（トラステッド ユーザー）］を選択すると、空白のページが表示される

追跡番号：AM-26723

問題：管理者が次のステップを実行すると、Security Console には空白のページが表示されます。

1. Authentication Manager 8.0 の管理者が別の Authentication Manager 8.0 のインスタンスとの信頼関係を作成する。
2. 管理者が Security Console にログオンして、**［Administration（管理）］＞［Trusted Realms（トラステッド レルム）］＞［Manage Existing（既存項目の管理）］**にアクセスする。
3. 管理者が［Trusted Realms（トラステッド レルム）］ページで、トラステッド レルムの名前をクリックして、コンテキスト メニューから**［Trusted Users（トラステッド ユーザー）］**を選択する。

回避策：Security Console で、**［Administration（管理）］＞［Trusted Realms（トラステッド レルム）］＞［Trusted Users（トラステッド ユーザー）］＞［Manage Existing（既存項目の管理）］**にアクセスして、トラステッド ユーザーを表示します。

プライマリ インスタンスに変更を加えた後、複数のレプリカ インスタンスを同期できない

追跡番号：AM-26689

問題：複数のレプリカ インスタンスがある導入環境では、次のいずれかのイベントが生じるとレプリカ インスタンスとの同期が失われます。

- スナップショットを使用してプライマリ インスタンスを復元する
- バックアップを使用してプライマリ インスタンスをリストアする
- レプリカ インスタンスをプライマリ インスタンスに昇格する

これらのいずれかのイベントの後、同期が失われたレプリカ インスタンスがあまりに早いタイミングでプライマリ インスタンスと同期しようとすると、同期が成功しない可能性があります。

回避策：これらのいずれかのイベントの後、Authentication Manager のサービスがプライマリ インスタンスにリストアされてから 15 分待って、レプリカ インスタンスを同期します。

Authentication Manager 7.1 のインスタンスとリストアした Authentication Manager 8.0 のインスタンスとの新しい信頼関係のテストが失敗する

追跡番号：AM-26391

問題：この問題は次のイベントが生じた後に発生します。

1. Authentication Manager 7.1 のインスタンスが複数の Authentication Manager 8.0 のインスタンスとの信頼関係を作成する。
2. Authentication Manager 8.0 のいずれかのインスタンスが応答しなくなり、Authentication Manager 7.1 のインスタンスで信頼関係を削除する。

3. 応答しなくなった Authentication Manager 8.0 のインスタンスを、同じホスト名を使用した新しい Authentication Manager 8.0 のインスタンスとしてリストアする。
4. Authentication Manager 7.1 のインスタンスがこの新しい Authentication Manager 8.0 のインスタンスとの信頼関係を作成する。

回避策：Authentication Manager 7.1 のインスタンスで、Authentication Manager のサービスを再起動します。

トークンの検索結果をすべての列でソートできない

追跡番号：AM-24776

問題：［SecurID Tokens（SecurID トークン）］ページでトークンを検索します（**［Authentication（認証）］＞［SecurID Tokens（SecurID トークン）］＞［Manage Existing（既存項目の管理）］**）。**［Assigned（割り当て済み）］**タブでは、**［Serial Number（シリアル番号）］**列と［**Token Type（トークン タイプ）**］列でソートできますが、他の列ではソートできません。［**Unassigned（未割り当て）**］タブでは、［**Expires On（有効期限）**］列と**［Security Domain（セキュリティ ドメイン）］**列ではソートできません。

回避策：なし。

日付と時間のフォーマットが一貫して適用されない

追跡番号：AM-23733

問題：ブラウザの言語選択に応じて、Authentication Manager に表示される日付と時間のフォーマットが決まります。中国語、ドイツ語、日本語などの一部の言語では、日付と時間のフォーマットがすべての Web ページやレポートにおいて一貫していません。

回避策：表示の問題は、諸機能の使用の妨げにはなりません。

デフォルトのユーザー検索では不完全な結果が返される

追跡番号：AM-24836

問題：1 つのアイデンティティ ソース内に複数の下位レベル セキュリティ ドメインが存在しそれぞれが組織単位（OU）にマッピングされている場合、そのアイデンティティ ソースでデフォルト検索（フィルタを適用しない検索）を実行し、10,000 人を超えるユーザーが該当する場合、結果が 1 件も返されません。

回避策：ユーザーの検索には、ユーザー ID やユーザーの姓名など、特定の条件を使用します。

［Select Identity Source（アイデンティティ ソースの選択）］ページにある［Help On This Page（このページのヘルプ）］リンクからは、登録するアイデンティティ ソースを選択するためのヘルプ トピックにアクセスできません。

追跡番号：AM-26636

問題：［Select Identity Sources（アイデンティティ ソースの選択）］ページで［Help on this page（このページのヘルプ）］をクリックすると、［Help（ヘルプ）］ウィンドウに空白ページが表示されます。

回避策：このトピックにはヘルプの目次からアクセスできます。

1. **［Setup（構成）］＞［Self-Service Settings（Self-Service 設定）］**タブをクリックします。
2. **［Select Identity Sources（アイデンティティ ソースの選択）］**をクリックします。
3. **［Help（ヘルプ）］＞［All Help topics（すべてのヘルプ トピック）］**をクリックします。
4. ［Security Console Help（Security Console ヘルプ）］ウィンドウの［Contents（目次）］パネルで、［Security Console］の下にある**［Security Console Help（Security Console ヘルプ）］**を展開します。
5. **［Self-Service］**を展開します。
6. **［Enable Enrollment by Selecting Identity Sources（アイデンティティ ソースを選択して登録を有効化）］**をクリックします。

Security Console と Self-Service Console における低速のメモリ リーク

追跡番号：AM-26760

問題：24,000 回を超える管理認証を行った後、Security Console や Self-Service Console でメモリ不足エラーが表示されることがあります。

回避策：RSA Console Server サービスを再起動します。手順については、「RSA Authentication Manager 8.0 管理者ガイド」の「RSA Authentication Manager サービスの手動管理」を参照してください。

認証

アイデンティティ ソース内のユーザーが、ユーザー グループから削除された後も認証可能

追跡番号：AM-22035

問題：アイデンティティ ソースでグループ フィルタを使用してアイデンティティ ソース内のユーザーを判定している場合、グループからユーザーを削除しても、そのユーザーは依然として無制限エージェントで認証できます。このユーザーは Security Console には表示されず、［Users and User Groups Missing from Identity Source（アイデンティティ ソースから消えたユーザーおよびユーザー グループ）］レポートに表示されますが、依然として認証できます。

回避策：制限付きエージェントを使用するか、クリーンアップ ジョブを頻繁に実行します。クリーンアップ ジョブが実行されるまでユーザーは引き続き認証可能なため、RSA では制限付きエージェントの使用を推奨しています。

リスク ベース認証ユーザーの認証がタイムアウトする

追跡番号：AM-26660

問題：ユーザー確認方法として On-Demand 認証を使用するリスク ベース認証ユーザーの認証がタイムアウトする場合、ログオン セッション タイムアウト値が短すぎる可能性があります。

回避策：値を 5 分に増やしてみます。この値は、特定のニーズに合わせて増減できます。手順については、RSA Security Console ヘルプのトピック「セッション有効期間の編集」を参照してください。

RADIUS

RADIUS レプリケーション ステータス チェックで同期失敗がレポートされる

追跡番号：AM-26591

問題：レプリカ インスタンスを導入環境に追加した後、RADIUS レプリケーション レポートには、新しいレプリカ インスタンスがプライマリ インスタンスと同期していないことが示されます。

回避策：新しいレプリカ インスタンスが同期されるまで待ちます。新しいレプリカ インスタンスが同期によって更新されれば、この RADIUS 障害メッセージは表示されなくなります。

バックアップからデータをリストアする際、RADIUS EAP の信頼できるルート証明書がリストアされない

追跡番号：AM-26637

問題：リストアするバックアップ ファイルに含まれる RADIUS EAP の信頼できるルート証明書が Internet Explorer によってインスタンスに追加されたか、ファイル名に Windows のファイル パスに関連する文字（: や \ など）を含んでいる場合、この証明書はリストアされません。

回避策：RADIUS EAP の信頼できるルート証明書を追加する際、Internet Explorer を使用しません。Windows ファイル パスに関連する文字が証明書のファイル名に含まれていないことを確認します。

プライマリ インスタンス上で停止した RADIUS サーバを、Operations Console から再起動できない

追跡番号：AM-26738

問題：プライマリ インスタンス上で停止した RADIUS サーバを Operations Console から再起動しようとすると、「RADIUS Server not found（RADIUS サーバが見つかりません）」というメッセージが表示されます。

回避策：次の手順を実行します。

手順

1. SSH（セキュア シェル）クライアントか VMware vSphere Client を使用し、ユーザー ID **rsaadmin** と現在のオペレーティング システム パスワードを指定してプライマリ インスタンス アプライアンスにログオンします。
2. ディレクトリを変更します。次のように入力します。
   cd /opt/rsa/am/server

   Enter キーを押します。
3. RADIUS サーバを再起動します。次のように入力します。
   ./rsaserv restart radius

   Enter キーを押します。
4. プライマリ インスタンスを再起動します。

その他

「RSA Authentication Manager 8.0 Developer's Guide」の Java サンプルコードを使用するには JDK（Java Development Kit）1.6 が必要である

追跡番号：AM-26824

問題：「Developer's Guide」では、API 開発環境をセット アップする際に「JDK 1.5 以降」をインストールする必要があると述べられていますが、Java サンプルコードを使用するには JDK 1.6 が必要です。

回避策：JDK 1.6 を使用して API 開発環境をセット アップします。

メール通知がセルフ サービス ユーザーに送信されない

追跡番号：AM-26579

問題：セルフ サービス ユーザーやワークフロー参加者にメール通知が送信されません。

回避策：Authentication Manager サーバでサービスを再起動すると、セルフ サービス ユーザーやワークフロー参加者にメール通知が送信されます。

ワークフロー参加者が、応答しないアイデンティティ ソースに存在する場合、ワークフロー通知が失敗する

追跡番号：AM-26589

問題：［Waiting for Approval（承認待ち）］ワークフロー通知のいずれかの参加者が、応答しないアイデンティティ ソース内に存在する場合、通知は送信されません。ワークフロー参加者は通知を受信しないため、承認待ちのユーザーがいることに気づきません。System Activity Monitor には「Error connecting to IS（IS 接続エラー）」と表示されます。

回避策：応答しないアイデンティティ ソースに関する接続の問題を解決します。

SNMP GET カウントが増加しない

追跡番号：AM-25985

問題：Self-Service Console および On-Demand 認証リクエスト、トークン割り当て、PIN イベント、セルフ サービス登録、オフライン認証ポリシーの発生回数を計算する際に、SNMP カウンタが増分されません。

回避策：なし。

Security Console でキーボード ショートカットが機能しない

追跡番号：AM-25511

問題：Security Console の［My Preferences（環境設定）］ページに表示されるキーボード ショートカットが機能しません。

回避策：Security Console ではキーボード ショートカットを使用しないでください。

On-Demand 認証 PIN を Self-Service Console で設定した場合、SNMP の PIN 合計が更新されない

番号：AM-24672

問題：ユーザーが Self-Service Console を使用して On-Demand 認証 PIN を設定した際に、関連する SNMP カウンタが更新されません。

回避策：なし。

サイズの大きい完了済みレポートを XML または HTML 形式でダウンロードした後、ブラウザで開くことができない

追跡番号：AM-26593

問題：大量のデータが含まれる完了済みレポートを XML または HTML 形式でダウンロードした後、ブラウザで開くと、ブラウザが応答しなくなるか終了します。

回避策：レポート出力ファイルを CSV、HTML、XML 形式でダウンロードした後、ブラウザ以外のアプリケーションで開きます。たとえば、HTML や XML のレポート ファイルはテキスト エディタで、CSV のレポート ファイルはスプレッドシート アプリケーションで開くことができます。

トークン検索を同時に 500 人以上の管理者が実行すると、内部サーバ エラーが発生する

追跡番号：AM-26669

問題：500 人を超える管理者が同時にトークンを検索すると、Security Console に内部サーバ エラーが表示されることがあります。

回避策：管理者セッションを同時に最大 1,000 個サポートするには、仮想アプライアンスに含まれるスクリプトを実行します。

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を右クリックし、コンテキスト メニューから **［Open Console（コンソールを開く）］** を選択します。
3. **rsaadmin** というユーザー名とオペレーティング システム パスワードを指定して、仮想アプライアンスにログオンします。
4. 次のように入力します。
   /opt/rsa/am/config/config.sh WeblogicSoftware:enableConcurrentQueue
5. このスクリプトによる構成が完了した後、Authentication Manager サービスを再起動します。次のように入力します。
   /opt/rsa/am/server/rsaserv restart all

Jython スクリプトでクラス検索にパッケージ スキャンを使用できない

追跡番号：AM-26750

問題：Authentication Manager プロセスを自動化する Jython スクリプトを作成した場合、Authentication Manager 8.0 では、Authentication Manager 7.1 で提供されていたパッケージ スキャン機能が自動的にスクリプトで使用されません。

回避策：パッケージ スキャン機能を有効化するには、*RSA_HOME*/utils/bin/ ディレクトリにある **jython.sh** ファイルを編集する必要があります。

次の行を見つけます。

```
JYTHON_OPTS="$JYTHON_OPTS -Dpython.cachedir=$UTILS_DIR/jython/cacheDir"
```

この行の下に次の行を追加します。

```
JYTHON_OPTS="$JYTHON_OPTS -Dpython.cachedir.skip=false"
```

特殊文字のサポート

Authentication Manager では、サポート対象の LDAP ディレクトリで使用可能な一部の文字がサポートされません。ユーザーやユーザー グループの識別名に特定の文字の組み合わせが含まれる場合、Security Console を使用してユーザーやユーザー グループを管理する機能が影響を受ける可能性があります。次の表に、これらの特殊文字に関する問題を示します。

追跡番号	説明	現象	機能に影響する文字
AM-18884	登録しようとしたときに、次のユーザー エラー メッセージが表示されます。「There was a problem processing your request.（要求を処理しているときに問題が発生しました。）」	外部アイデンティティ ソースのユーザーの DN にバックスラッシュ（\）または円記号が含まれ、その前か後にスペースがある場合、そのユーザーを管理することはできません。	DN にバックスラッシュ（\）または円記号が含まれ、その前か後にスペースがある
AM-18391	名前に <> が含まれる場合、そのユーザーまたはユーザー グループを Security Console から管理することはできません。	Security Console では、ユーザーまたはユーザー グループを含むアイデンティティ ソースの User Base DN または User Group Base DN に左山括弧（<）と右山括弧（>）が順番に含まれている場合、そのユーザーまたはユーザー グループを管理することができません。いずれかの山括弧を DN 内で単独で使用することはできます。	次のいずれかの場所で、左山括弧と右山括弧（<>）が連続するか、他の文字を囲む形で使用されている • ユーザーまたはユーザー グループの DN • アイデンティティ ソースの設定に使用された LDAP ディレクトリ内の組織単位（OU）
AM-18450	Security Console では、特殊文字を含むユーザーまたはユーザー グループを外部アイデンティティ ソース内に作成することはできません。	読み取り / 書き込みアイデンティティ ソースでは、Security Console を使用して、識別名に特殊文字が含まれるユーザーやユーザー グループを作成することはできません。LDAP 管理ツールを使用すると、Base DN に特殊文字を含むユーザーやユーザー グループを作成できますが、この表で示されているその他の制限に注意してください。	読み取り / 書き込みアイデンティティ ソース内のユーザー グループ名に次のいずれかの文字が含まれている。 • スペース（ ） • バックスラッシュ（\）または円記号 • スラッシュ（/） • アンパサンド（&） • プラス記号（+）
AM-18452	OU 名にバックスラッシュ（\）または円記号と特殊文字の組み合わせが含まれる OU にマップされたアイデンティティ ソースで、ユーザーとユーザー グループが表示されません。	そのアイデンティティ ソース内のユーザーやユーザー グループを Security Console で検索すると、結果が返されません。	OU 名が次に該当する場合 : • バックスラッシュ（\）または円記号の直後に特殊文字を含んでいる。 • 等号（=）を含んでいる。

サポートとサービス

RSA SecurCare Online	https://knowledge.rsasecurity.com
RSA Solution Directory	https://gallery.emc.com/community/marketplace/rsa?view=overview