Cisco ACS 5.X と RSA SecurID トークン サーバの統合

目次

概要

このドキュメントでは、RSA SecurID 認証技術と Cisco Access Control System（ACS）バージョン 5.x を統合する方法について説明します。

背景説明

Cisco Secure ACS は、外部データベースとして RSA SecurID サーバをサポートします。

RSA SecurID の 2 要素認証は、ユーザの個人識別番号（PIN）と、タイム コード アルゴリズムに基づいて使い捨てのトークン コードを生成する個別に登録された RSA SecurID トークンで構成されます。

異なるトークン コードが固定間隔（通常は 30 または 60 秒ごと）で生成されます。 RSA SecurID サーバでは、この動的な認証コードが検証されます。 各 RSA SecurID トークンは固有であり、過去のトークンに基づいて将来のトークンの値を予測することはできません。

そのため、正しいトークン コードが PIN とともに提示された場合、その人が有効なユーザである確実性が高くなります。 したがって、RSA SecurID サーバでは、従来の再利用可能なパスワード

よりも信頼性の高い認証メカニズムが提供されます。

次の方法で RSA SecurID 認証技術と Cisco ACS 5.x を統合することができます。

- RSA SecurID エージェント：ユーザは、ネイティブ RSA プロトコル経由でユーザ名とパスコードを使って認証されます。
- RADIUS プロトコル：ユーザは、RADIUS プロトコル経由でユーザ名とパスコードを使って認証されます。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- RSA セキュリティ
- Cisco Secure Access Control System（ACS）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure Access Control System（ACS）バージョン 5.x
- RSA SecurID トークン サーバ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

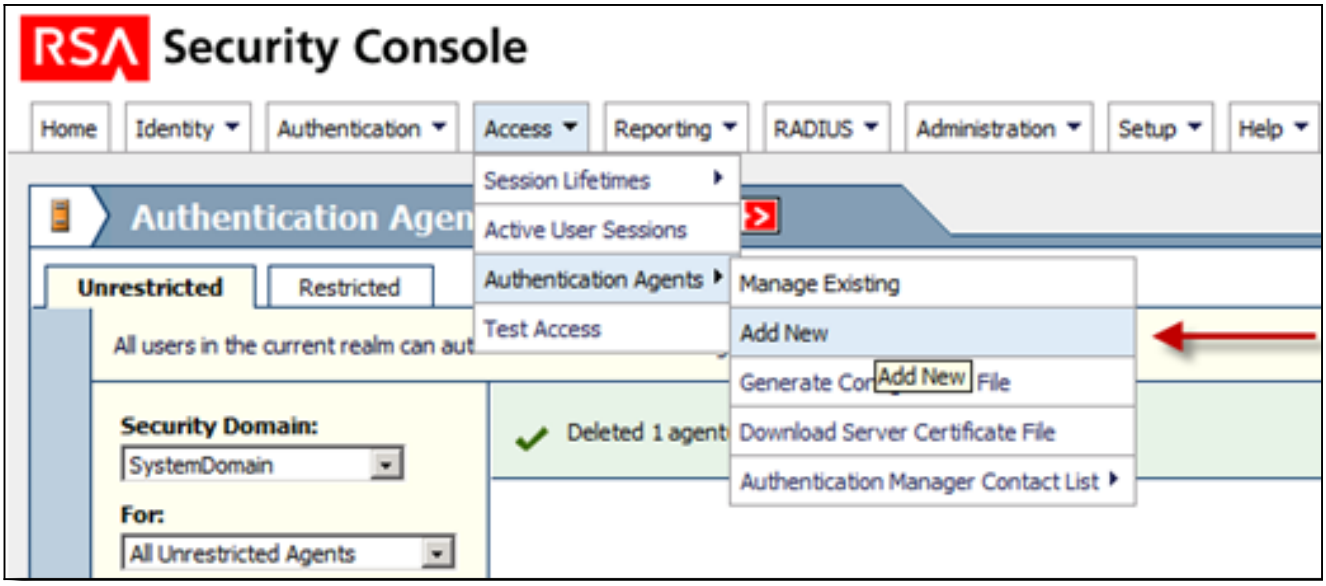
設定

RSA サーバ

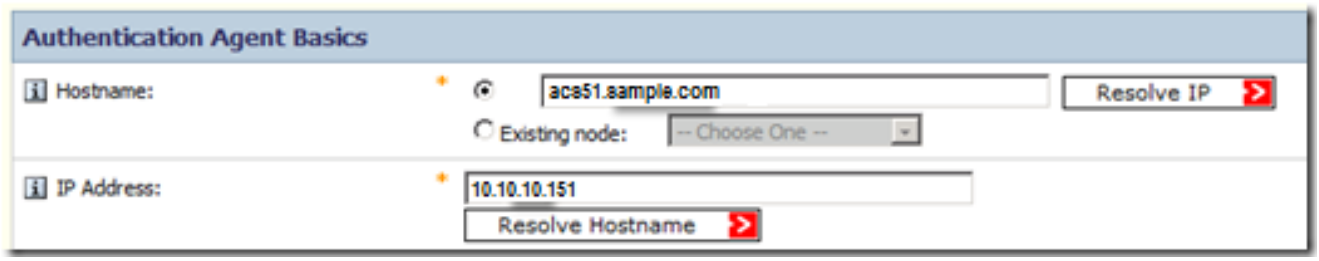
この手順では、RSA SecurID サーバ管理者が認証エージェントと設定ファイルを作成する方法について説明します。 認証エージェントは、基本的に、RSA データベースにアクセスする権限を持つデバイス、ソフトウェア、またはサービスのドメイン ネーム サーバ（DNS）の名前と IP アドレスです。 設定ファイルは、基本的に、RSA のトポロジと通信を記述したものです。

この例では、RSA 管理者が 2 つの ACS インスタンス用の 2 つのエージェントを作成する必要があります。

1. RSA セキュリティ コンソールで、[Access] > [Authentication Agents] > [Add New] に移動します。

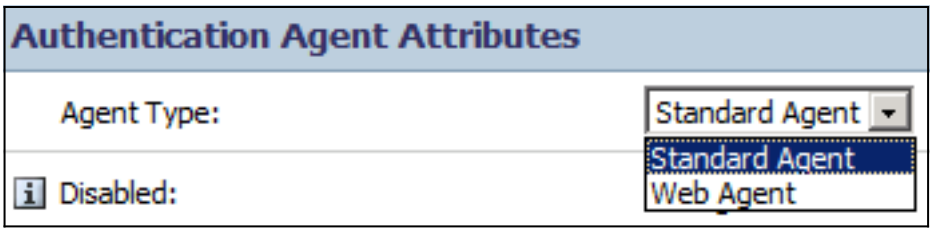


2. [Add New Authentication Agent] ウィンドウで、2 つのエージェントのそれぞれのホスト名と IP アドレスを定義します。

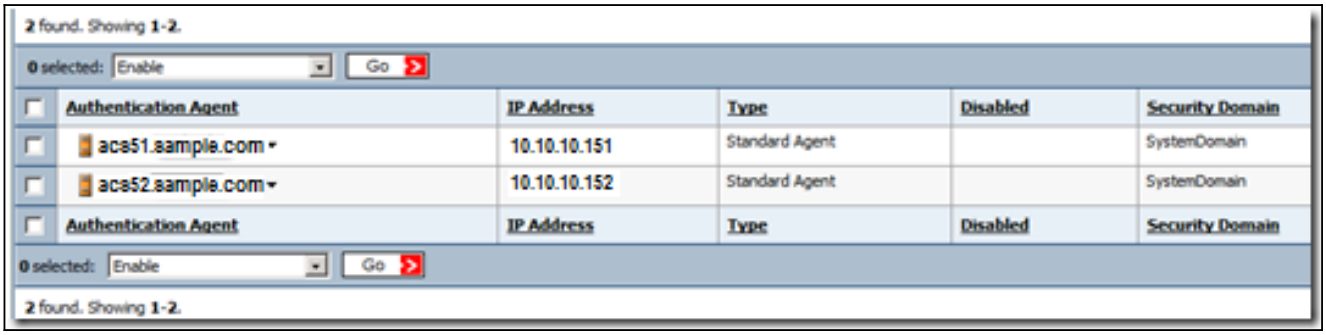


ACS エージェントの DNS の正引きと逆引きの両方が機能する必要があります。

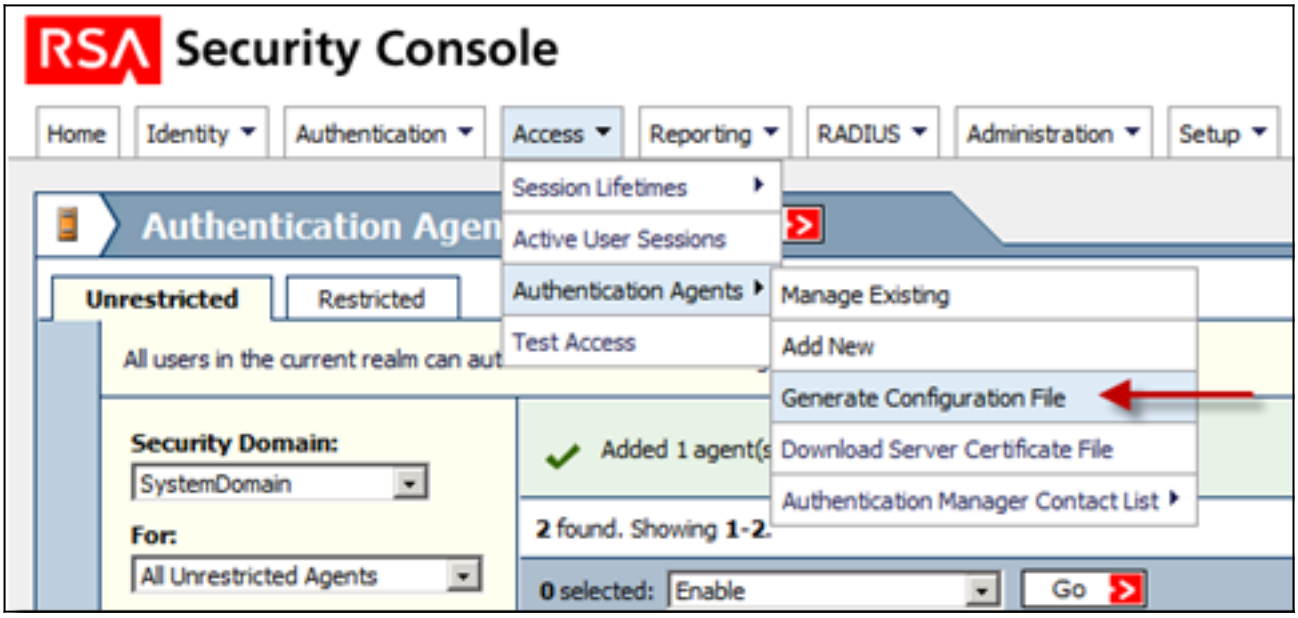
3. エージェント タイプを標準エージェントとして定義します。



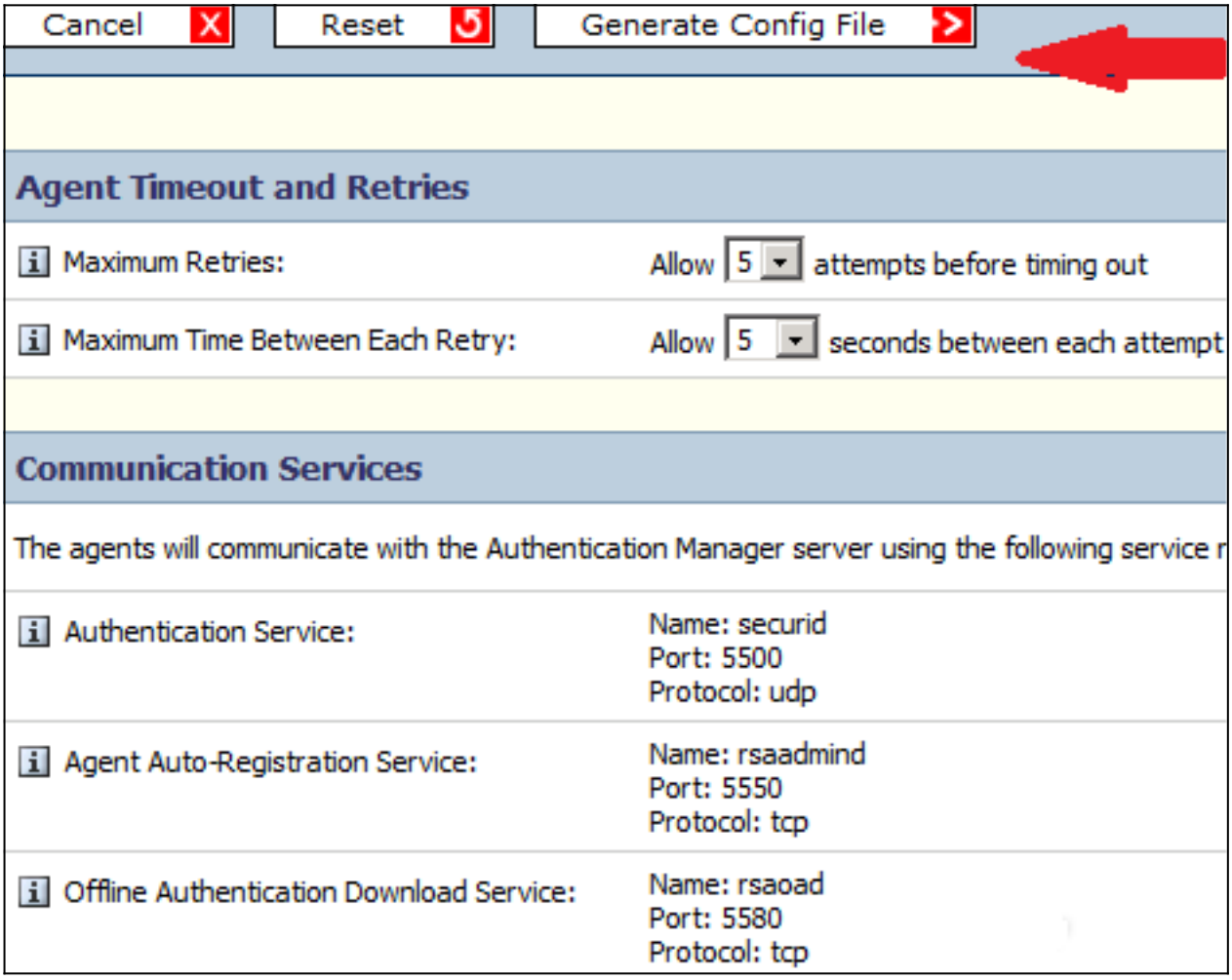
次に、エージェントを追加したときに表示される情報の例を示します。



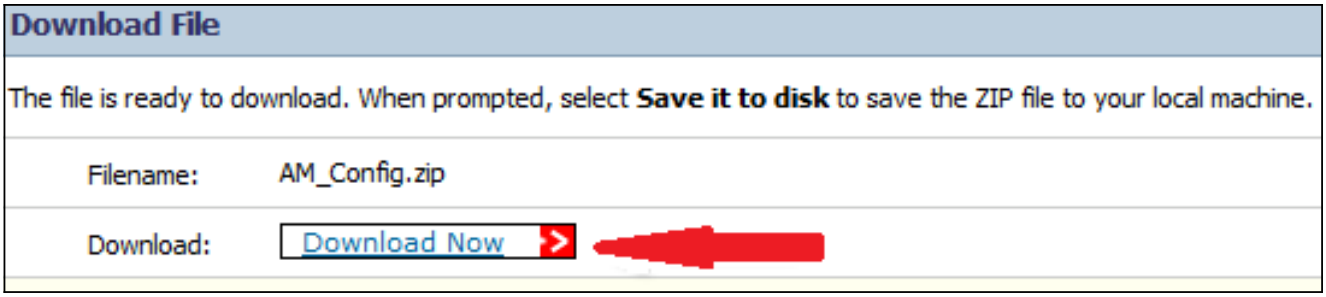
4. RSA セキュリティ コンソールで、[Access] > [Authentication Agents] > [Generate Configuration File] に移動して sdconf.rec コンフィギュレーション ファイルを生成します。



5. [Maximum Retries] と [Maximum Time Between Each Retry] のデフォルト値を使用します。



6. コンフィギュレーション ファイルをダウンロードします。

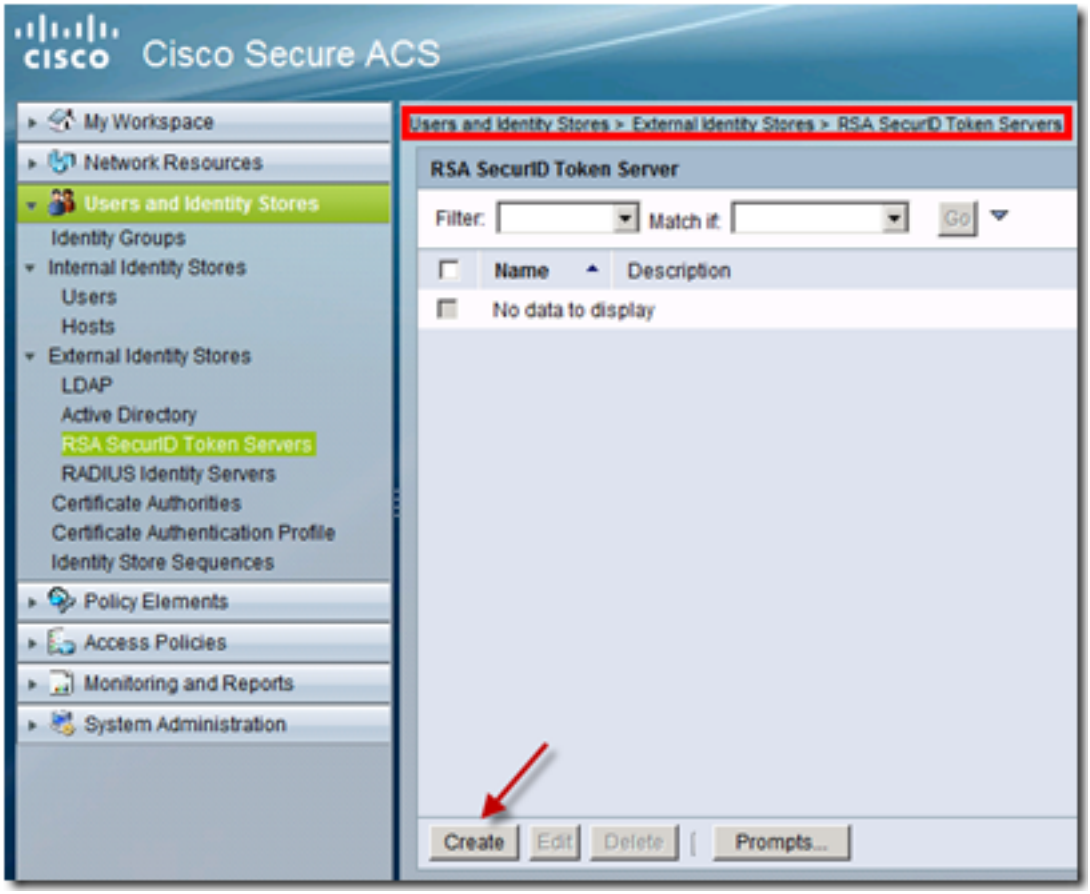


.Zip ファイルには、ACS 管理者が設定タスクを実行するために必要な実際のコンフィギュレーション sdconf.rec ファイルが含まれています。

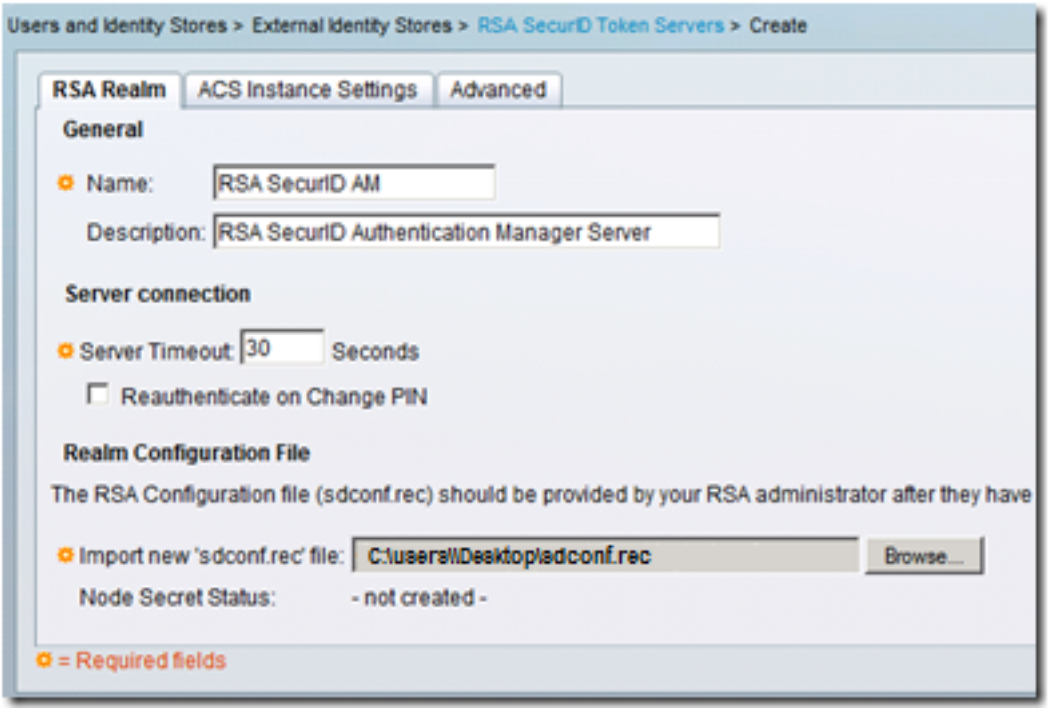
ACS バージョン 5.x サーバ

この手順では、ACS 管理者がコンフィギュレーション ファイルを取得して送信する方法について説明します。

1. Cisco Secure ACS バージョン 5.x コンソールで、[Users and Identity Stores] > [External Identity Stores] > [RSA SecurID Token Servers] に移動して、[Create] をクリックします。



2. RSA サーバの名前を入力して、RSA サーバからダウンロードした sdconf.rec ファイルを参照します。



3. ファイルを選択して、[Submit] をクリックします。

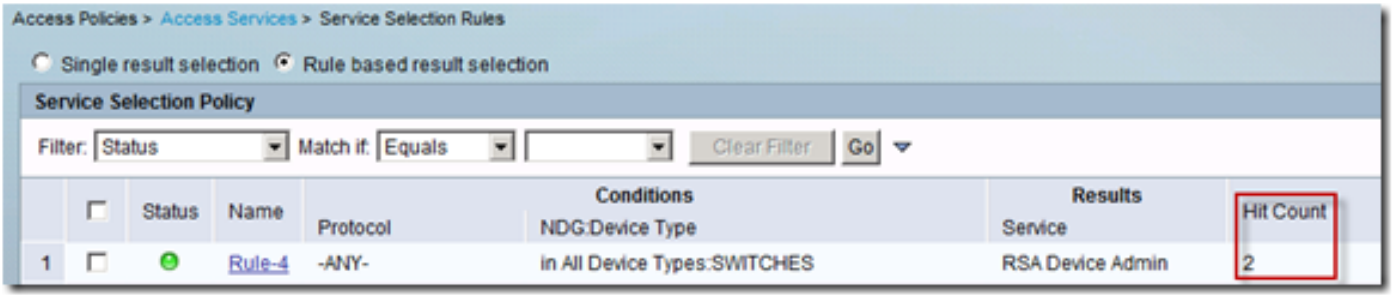
   注: ACS がトークン サーバに初めて接続した場合は、ノード シークレット ファイルと呼ばれる別のファイルが RSA Authentication Manager の ACS エージェント用に作成され、ACS にダウンロードされます。 このファイルは暗号化通信に使用されます。

確認

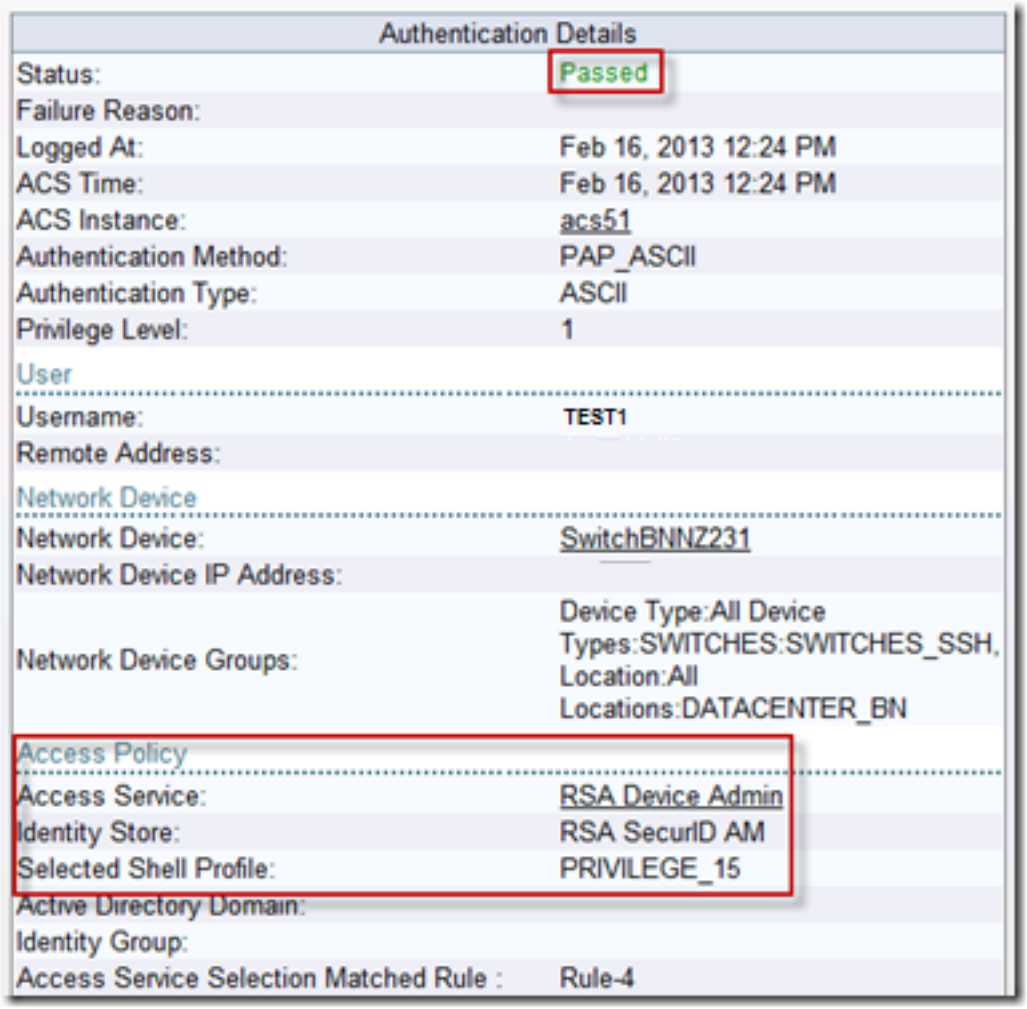
このセクションでは、設定が正常に機能していることを確認します。

ACS バージョン 5.x サーバ

ログインの成功を検証するには、ACS コンソールに移動して、[Hit Count] を確認します。



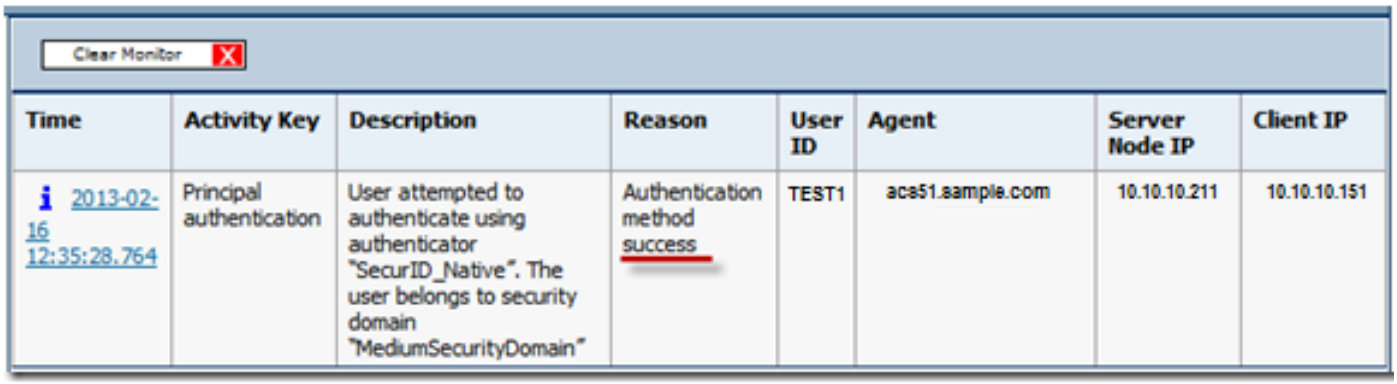
また、ACS ログで認証詳細情報を確認することもできます。



Authentication Details	
Status:	Passed
Failure Reason:	
Logged At:	Feb 16, 2013 12:24 PM
ACS Time:	Feb 16, 2013 12:24 PM
ACS Instance:	acs51
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
User	
Username:	TEST1
Remote Address:	
Network Device	
Network Device:	SwitchBNNZ231
Network Device IP Address:	
Network Device Groups:	Device Type:All Device Types:SWITCHES:SWITCHES_SSH, Location:All Locations:DATACENTER_BN
Access Policy	
Access Service:	RSA Device Admin
Identity Store:	RSA SecurID AM
Selected Shell Profile:	PRIVILEGE_15
Active Directory Domain:	
Identity Group:	
Access Service Selection Matched Rule :	Rule-4

RSA サーバ

認証の成功を検証するには、RSA コンソールに移動して、ログを確認します。



Clear Monitor

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
2013-02-16 12:35:28.764	Principal authentication	User attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "MediumSecurityDomain"	Authentication method success	TEST1	acs51.sample.com	10.10.10.211	10.10.10.151

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

エージェント レコード（sdconf.rec）の作成

ACS バージョン 5.3 で RSA SecurID トークン サーバを設定するには、ACS 管理者が sdconf.rec ファイルを作成する必要があります。 sdconf.rec ファイルは、RSA エージェントと RSA SecurID サーバ領域との通信方法を指定する設定レコード ファイルです。

sdconf.rec ファイルを作成するために、RSA 管理者は、RSA SecurID サーバ上のエージェント ホストとして ACS ホストを追加し、このエージェント ホストのコンフィギュレーション ファイルを生成する必要があります。

ノード シークレット (securid) のリセット

エージェントが最初に RSA SecurID サーバと通信したあと、サーバは securid というノード秘密ファイルをエージェントに提供します。 サーバとエージェント間のその後の通信は、ノード シークレットの交換による相手の信頼性の検証によって行われます。

管理者がノード シークレットをリセットしなければならない場合があります。

1. RSA 管理者は、RSA SecurID サーバの Agent Host レコードの [Node Secret Created] チェックボックスをオフにする必要があります。
2. ACS 管理者は、ACS から securid ファイルを削除する必要があります。

自動ロード バランシングのオーバーライド

RSA SecurID エージェントは、領域内の RSA SecurID サーバ上の要求された負荷を自動的に分散します。 ただし、負荷を手動で分散するオプションもあります。 エージェント ホストごとに使用されるサーバを指定できます。 エージェント ホストが認証要求を一部のサーバにだけ優先的に転送できるように、サーバごとに優先度を割り当てることができます。

優先度設定をテキスト ファイルで指定して、そのファイルを sdopts.rec として保存し、ACS にアップロードする必要があります。

手動介入によるダウンした RSA SecurID サーバの削除

RSA SecurID サーバがダウンした場合、自動除外メカニズムが迅速に機能しないことがあります。 ACS から sdstatus.12 ファイルを削除すると、このプロセスが高速化します。