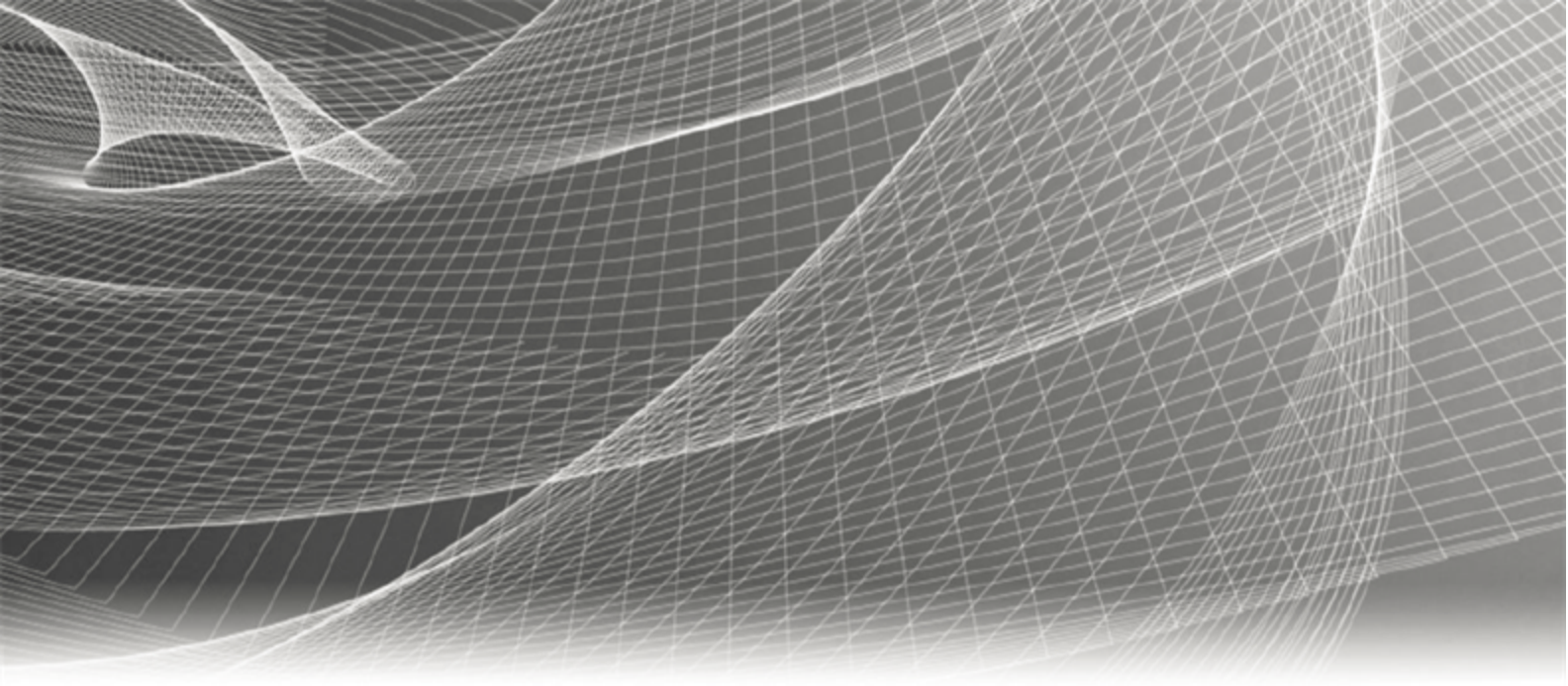

RSA® Authentication Agent 8.1 for PAM

Installation and Configuration Guide for SUSE

Revision 7

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license. RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

October 2018

Revised: January 2021

Contents

Revision History

Revision Number	Date	Revision
1	February 2018	Added a configuration procedure for xdm.
2	June 2018	Added more details about the REST server URL and the client key for the two REST Protocol authentication modes.
3	August 2018	Added "Replace the Server Trusted Root CA Certificate" and link to knowledgebase article for exporting trusted root CA certificate.
4	August 2019	Added a note about file permissions for non-privileged users.
5	November 2019	Added a statement that the PAM agent in REST mode uses the TCP protocol for deployments that require authentication agents to use IPv4 or IPv6.
6	October 2020	Added instructions for obtaining the RSA SecurID Authentication API REST URL from the Cloud Administration Console.
7	December 2020	Added information on supported authentication methods. Added configuration details for using RSA Authentication Manager 8.5 as a secure proxy server for the Cloud Authentication Service.

Preface

Audience

This guide is for network and system administrators who install, upgrade, and troubleshoot RSA® Authentication Agent for PAM (pluggable authentication module).

Support and Service

You can access community and support information on RSA Link at https://community.rsa.com. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

RSA Ready Partner Program

The RSA Ready Partner Program website at www.rsaready.com provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Chapter 1: Installing the PAM Agent

Overview of the RSA Authentication Agent 8.1 for PAM

The RSA Authentication Agent 8.1 for PAM (pluggable authentication module) supports authentication on UNIX systems with standard or OpenSSH connection tools. The PAM agent uses RSA customized shared libraries, and supports access to UNIX servers and workstations with the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

You can choose whether the PAM agent authenticates to the Cloud Authentication Service or Authentication Manager. The RSA SecurID Access Enterprise Edition license and the Premium Edition license include both of these components of RSA SecurID Access. Authentication Manager is not required to use the PAM agent.

Version 8.1 of the PAM agent offers the following new benefits:

- Support for the Cloud Authentication Service. The Cloud Authentication Service uses multifactor authentication methods, such as Approve (mobile-optimized push notification), Authenticate Tokencode, Device Biometrics, SMS Tokencode, Voice Tokencode, and RSA SecurID tokens to help secure access to software as a service (SaaS) and on-premises web applications for users.
- Ability to access Authentication Manager with the REST protocol, instead of the UDP protocol.
- Continued support for the UDP protocol used by earlier versions of the PAM agent.
- Authentication Manager has agent reports that help you to manage your installed REST protocol PAM agents. In REST mode, the PAM agent can send additional information to the Authentication Manager server, such as a unique software ID number for each installed PAM agent and information on the operating system used by the agent.

Using the PAM agent in REST mode offers additional advantages over using the UDP protocol:

- Makes it easy for your Authentication Manager deployment to integrate the Cloud Authentication Service.
- You can add and maintain one authentication agent record in Authentication Manager and use it to represent multiple installed agents.
- You can run multiple authentication agents on the same hardware more easily than you can using the UDP protocol.
- Uses the TCP protocol for deployments that require authentication agents to use IPv4 or IPv6 network settings or the IPv4 or IPv6 protocol.
- In the REST protocol authentication modes, version 8.1 of the PAM agent uses the FIPS-compliant cryptographic library module **fips-2.0.16** with OpenSSL version 1.0.2l. For more information, see *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* at https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf.
- Requires fewer authentication agent updates for new features and enhancements than authentication agents that do not use the REST protocol. Authentication agents that use the REST protocol are more likely to take advantage of changes in Authentication Manager, thus reducing the number of updates required on multiple agents.

Authentication Modes

You can install the PAM agent in one of three authentication modes. All modes provide RSA SecurID authentication. You can change the mode after installation as needed. For instructions, see Changing the PAM Agent Authentication Mode on page 37.

Authentication Mode	Description
RSA Authentication Manager with the UDP Protocol	RSA SecurID hardware and software authenticators generate RSA SecurID tokencodes. The agent verifies that the user-entered data matches the data stored in Authentication Manager and allows or denies access based on the result. By default, the PAM agent upgrade configures the agent to use the UDP protocol. You can easily switch to a different authentication mode that uses the REST protocol.
RSA Authentication Manager with the REST Protocol	Support for all types of authentication supported by Authentication Manager over the REST protocol, such as RSA SecurID software and hardware tokens and Authenticate Tokencode through an integration with the Cloud Authentication Service component.
Cloud Authentication Service with the REST Protocol	Supports Approve (mobile-optimized push notification), Authenticate Tokencode, Device Biometrics, SMS Tokencode, Voice Tokencode, and RSA SecurID tokens. FIDO, and authentication conditions requiring combinations of methods (such as Approve AND RSA SecurID token) are not supported.

RSA Authentication Agent 8.1 for PAM supports RSA Authentication Manager trusted realms. Authentication Manager risk-based authentication (RBA) is not supported.

PAM Agent Workflow

The PAM agent is installed on a UNIX server. It acts as an intermediary between authenticating users and either the RSA Authentication Manager server or the Cloud Authentication Service.

The PAM agent supports Authentication Manager security features. For example, if Authentication Manager determines that the user associated with a particular token requires a new PIN, then the agent requests the PIN, which has characteristics defined in Authentication Manager, and sends the information to Authentication Manager. If Authentication Manager requests the next tokencode displayed on the user's token, then the PAM agent prompts the user. If the correct next tokencode is not sent to Authentication Manager, authentication fails.

These steps describe the authentication flow for the PAM agent, in all three authentication modes:

1. A user attempts to access a machine protected by the PAM agent, either locally, with login, or remotely, with tools such as rlogin, telnet, SSH, and FTP.

   The user must exist locally on the machine on which the PAM agent is installed.

2. The UNIX pluggable authentication module (PAM) infrastructure intercepts all logon requests, and uses PAM configuration files to access the RSA PAM module:
   - If a user is not configured for RSA SecurID authentication, the RSA PAM module allows the request to succeed.
   - If the user requesting access is challenged by RSA SecurID, the PAM agent continues authentication with step 3.
3. Based upon the PAM agent authentication mode, the agent contacts either Authentication Manager or the Cloud Authentication Service.

   For Authentication Manager with a UDP connection or the REST protocol, the following steps occur:

a. The agent prompts the user for the user name and then for the passcode.
b. The agent securely sends the user name and passcode to Authentication Manager:
   - If Authentication Manager approves the request, the agent grants access to the user.
   - If Authentication Manager does not approve the request, the agent denies access.

For the Cloud Authentication Service, the following steps occur:

a. The agent prompts the user for a user name, and sends the information to the Cloud Authentication Service.
b. The Cloud Authentication Service provides the agent with the authentication methods configured for the user in the assurance level of the Cloud Authentication Serviceaccess policy.
c. The agent prompts the user to authenticate.
d. The user chooses an available authentication method and authenticates:
   - If the Cloud Authentication Service approves the request, the agent grants access to the user.
   - If an authentication method is unsuccessful, the Cloud Authentication Service prompts the user for the next authentication method.
   - If the Cloud Authentication Service does not approve the request, the agent denies access.

Supported Authentication Methods for the PAM Agent

Scenario	Authentication Methods
PAM agent connects to the Cloud Authentication Service	The following methods are supported: • RSA SecurID Token • RSA SecurID Authenticate Tokencode • Approve • Device Biometrics • SMS Tokencode • Voice Tokencode FIDO Tokens and authentication conditions requiring combinations of methods (such as Approve AND RSA SecurID token) are not supported.
PAM agent connects to RSA Authentication Manager with the UDP protocol	You can authenticate with RSA SecurID hardware and software tokens.
PAM agent connects to RSA Authentication Manager with the REST protocol	Support for all types of authentication supported by Authentication Manager over the REST protocol, such as RSA SecurID software and hardware tokens and Authenticate Tokencode through an integration with the Cloud Authentication Service.
Direct connection to the Cloud Authentication Service uses RSA Authentication Manager 8.5 as a secure proxy server.	• Cloud Authentication Service methods are supported. • Users are prompted for Authenticate Tokencode if the Cloud Authentication Service or the connection between Authentication Manager and the Cloud Authentication Service is temporarily

Scenario	Authentication Methods
	unavailable or too slow.
Direct connection to RSA Authentication Manager 8.5 with the UDP protocol or the REST protocol. Authentication Manager is connected to the Cloud Authentication Service	• Authentication Manager methods are supported, and methods , such as Authenticate Tokencode, that are supported through an integration with the Cloud Authentication Service. • Users are prompted for Authenticate Tokencode or RSA SecurID passcode if the Cloud Authentication Service or the connection between Authentication Manager and the Cloud Authentication Service is temporarily unavailable or too slow.

Software Requirements

This section describes the minimum software versions supported by the PAM agent.

Required Operating Systems

The PAM agent requires one of the following operating systems:

- SUSE Linux Enterprise Server version 11 SP4 (32-bit and 64-bit)
- SUSE Linux Enterprise Server version 12 SP3 (64-bit)
- SUSE Linux Enterprise Server version 15 (64-bit)

The corresponding 32-bit or 64-bit version of **libuuid.so** (UUID library) must be installed on the PAM agent machine.

RSA SecurID Authentication API Version Support

The RSA SecurID Authentication Agent 8.1 for PAM supports the RSA SecurID Authentication API version 1.1 , which is the current version of the REST APIs.

RSA Authentication Manager Version Support

The following table lists the RSA Authentication Manager versions that are required to support specific features.

Required RSA Authentication Manager Version	Supported Feature
8.2 SP1 or later	The PAM agent requires RSA Authentication Manager 8.2 SP1 or later.
8.2 SP1 Patch 5 or later	If the agent reporting flag is enabled on the PAM agent, RSA Authentication Manager 8.2 SP1 Patch 5 or later is required to avoid failed authentications in REST mode.
8.3 or later	RSA Authentication Manager 8.3 and later versions include agent reports that help you to manage your installed REST protocol PAM agents. These reports include the additional information that the PAM agent can send to Authentication Manager.
8.5	RSA Authentication Manager 8.5 lets you use RSA Authentication Manager as a secure proxy

Required RSA Authentication Manager Version	Supported Feature
	server that sends any authentication requests that Authentication Manager cannot validate directly to the Cloud Authentication Service. This authentication mode supports the all of the authentication methods supported by the PAM agent. It does not support certain Authentication Manager features, such as agent reporting, enabling and disabling or restricting agents, and failover to replica instances for agents.

Cloud Authentication Service Version Support

The RSA SecurID Authentication Agent 8.1 for PAM supports the RSA SecurID Authentication API version 1.1, which is the current version of the REST APIs.

Certificate Requirements

The PAM agent uses TLS 1.2 certificates for the REST protocol. The Cloud Authentication Service and RSA Authentication Manager 8.2 or later can accept these certificates. Deployments that do not use TLS 1.2 certificates must use the authentication mode that supports Authentication Manager with the UDP protocol.

In the REST protocol authentication modes, the PAM agent uses the FIPS-compliant cryptographic library module **fips-2.0.16** with OpenSSL version 1.0.2l. For more information, see *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* at https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf.

Supported Tools

The PAM agent supports the following tools:

- telnet
- login
- rlogin
- su
- ssh (ssh, sftp and scp)
- sudo

  Download and install the supported sudo version from https://www.sudo.ws.

- ftp (limited to a single transaction)
- gdm
- xdm (limited to single transaction)

OpenSSH Support (Optional)

If you are using OpenSSH, verify that you are using the compatible version of OpenSSH for your platform. OpenSSH is not required.

The following optional OpenSSH tools are supported:

- ssh
- sftp
- scp

Install OpenSSH on the agent machine. For OpenSSH, including prerequisites and the additional software required for compiling source code, see https://www.openssh.com.

Planning to Install the PAM Agent

Before installing the PAM agent, do the following:

- On the machine where you are installing the PAM agent:
  1. Obtain root permissions.
  2. Create a **/var/ace** directory for PAM agent configuration files, if one does not already exist, and create an installation directory.
  3. Obtain the server trusted root CA certificate from RSA Authentication Manager or the Cloud Authentication Service. If you are using RSA Authentication Manager 8.5 as a secure proxy server to the Cloud Authentication Service, you require an Authentication Manager certificate. (For instructions, see the knowledgebase article How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate.) Then do the following:
     a. Verify that the certificate has not expired.
     b. Store the certificate in PEM format. If there are multiple CA certificates, they need to be concatenated into a single file in PEM format.

        The file format should be like the following:

        -----BEGIN CERTIFICATE-----

        Thawte (BASE64)

        -----END CERTIFICATE-----

        -----BEGIN CERTIFICATE-----

        Entrust (BASE64)

        -----END CERTIFICATE-----

     c. Copy ***filename*.pem** into the **/var/ace/** directory.
     d. Protect the **/var/ace/** directory containing the certificates. Use the appropriate privileges to restrict access to trusted administrators.
- To authenticate with RSA Authentication Manager, create an authentication agent record for the PAM agent in the internal database. For more information, contact your Authentication Manager Super Admin or see the Authentication Manager Help on RSA Link.
- To authenticate with the UDP protocol, you must generate the Authentication Manager configuration file, **sdconf.rec**, or obtain this file from your Authentication Manager Super Admin. This file is not needed for authentication with the REST protocol.

  The **sdconf.rec** file specifies how the agent communicates with the Authentication Manager primary instance and replica instances by IP address. Do the following:

  - Make sure the latest version of the **sdconf.rec** file is in an accessible directory on the agent machine, such as the default **/var/ace** directory.
  - You must have write permission to the directory in which the **sdconf.rec** file is stored.
- In the authentication mode that uses the Cloud Authentication Service with the REST Protocol, the PAM agent relies upon the Cloud Authentication Service for load balancing and failover.
- In the authentication mode that uses RSA Authentication Manager with the REST protocol, the PAM agent does not support load balancing. The PAM agent supports failover to a maximum of 15 Authentication Manager replica instances.
- If you are using RSA Authentication Manager 8.5 as a secure proxy server to the Cloud Authentication Service, you can use RSA Authentication Manager with REST protocol mode or Cloud Authentication Service mode, depending upon the authentication methods that are required. In each case, the PAM agent connects to Authentication Manager. Collect the required information that is listed in the Authentication Manager with the REST protocol table.
- Collect the information that you will provide while installing the PAM agent.

  Authentication Manager with the UDP protocol. You can keep the default values or specify new directories.

Description	Your Plan
Directory where **sdconf.rec** is located. The default value is **/var/ace/**.	
Root path for the PAM agent directory. The default value is **/opt**.	

  Authentication Manager with the REST protocol. Ask your Authentication Manager Super Admin for the following information:

Description	Your Plan
REST server URL for communication between the authentication agent and the Authentication Manager primary instance. Use the following format: `https://HOSTNAME:PORT/mfa/v1_1/authn` On the primary instance obtain the *HOSTNAME* value from the **Fully Qualified Domain Name** field on the **Administration > Network > Appliance Network Settings** page of the Operations Console. The default *PORT* is 5555.	
Number of Authentication Manager replica instances that can be used for failover.	
REST server URL for each replica instance. Use the following format:	

Description	Your Plan
`https://HOSTNAME:PORT/mfa/v1_1/authn` On the replica instance, obtain the *HOSTNAME* value from the **Fully Qualified Domain Name** field on the **Administration > Network > Appliance Network Settings** page of the Operations Console. The default *PORT* is 5555.	
Access Key (client key) for securely passing user authentication requests to Authentication Manager. This value is generated in the Security Console on the Authentication Manager primary instance. For instructions on how to obtain the Access Key, see the following topic on RSA Link: Configure the RSA SecurID Authentication API for Authentication Agents.	
Enter the directory and filename for the server trusted root certificate on the authentication agent. The default value is **/var/ace/cert.pem**.	
Authentication agent name (Client ID) that was created for the PAM agent in Authentication Manager.	
Root path for the PAM agent directory. The default value is **/opt**.	

Cloud Authentication Service with the REST protocol. Ask the Cloud Authentication Service Super Admin for the following information:

Description	Your Plan
REST server URL for communication between the agent and the Cloud Authentication Service. Use the following format: `https://HOSTNAME/mfa/v1_1/authn` Obtain the *hostname* from the Cloud Administration Console. Click **My Account > Company Settings > Authentication API Keys**. Copy the **RSA SecurID Authentication API REST URL**. You do not need to specify a port. The default port is 443.	
Authentication API key (client key) created in	

Description	Your Plan
the Cloud Administration Console for securely passing user authentication requests to the Cloud Authentication Service. For instructions on how to obtain the Authentication API key, see the following topic on RSA Link: Add an RSA SecurID Authentication API Key.	
Directory and filename for the server trusted certificate on the authentication agent. The default value is **/var/ace/cert.pem**.	
The Tenant ID is required. The PAM agent must provide a value for the Tenant ID in authentication requests. For example, you can set the Tenant ID to the the Company ID from the Cloud Administration Console. To find the Company ID, in the Cloud Administration Console, click **My Account > Company Settings** and select the Company Information tab.	
Access policy name for the Cloud Authentication Service. The policy name is case-sensitive. This policy is defined in the Cloud Administration Console.	
CLIENT_ID authentication agent name to display in mobile notifications. You can enter any value. For example, PAM_Agent.	
Root path for the PAM agent directory. The default value is **/opt**.	

Installing the RSA Authentication Agent 8.1 for PAM

Complete the following tasks to install the PAM agent:

1. Specify the Agent IP Address for UDP Mode on the facing page
2. Configure OpenSSH on the facing page
3. Install the PAM Agent on the facing page
4. For UDP mode, perform a test authentication. For more information, see Authentication Utilities for UDP Mode on page 45.

   For a REST protocol mode, test the connection by accessing the REST server URL with any browser or http client. For example, enter https://*HOSTNAME*:*PORT*/mfa/v1_1/authn. Because you are not currently authenticating, your browser or http client should display a "Forbidden" or "Unauthorized" HTTP response.

Specify the Agent IP Address for UDP Mode

For UDP mode, you must create the **sdopts.rec** file in the same directory that is used by the **sdconf.rec** file. This procedure does not apply to REST mode.

File	Description
sdopts.rec	Lists the IP address for the machine where you installed the agent. The agent uses the IP address in the **sdopts.rec** file to communicate with RSA Authentication Manager.
sdconf.rec	Specifies the IP addresses that are used by Authentication Manager.

Procedure

1. On the agent machine, use a text editor to create an **sdopts.rec** file in the path where the **sdconf.rec** file is saved.
2. In the file, type:

   ```
   CLIENT_IP=x.x.x.x
   ```

   where *x.x.x.x* is the IP address of the agent host.

   Note: Use only uppercase letters and do not include spaces.
3. Save the file.

Configure OpenSSH

If you are using OpenSSH, the suite of security-related network utilities based on the Secure Shell (SSH) protocol, you must configure this software to work with the PAM agent and to display passcode authentication messages to users.

Before you begin

Install OpenSSH on the agent machine. For OpenSSH, including prerequisites and the additional software required for compiling source code, see https://www.openssh.com.

Procedure

1. On the agent machine, open the **sshd_config** file.
2. Set the following parameters and save the changes:

Parameter	Setting
UsePAM	yes
PasswordAuthentication	no
ChallengeResponseAuthentication	yes

   Setting the PasswordAuthentication parameter to no disables the OpenSSH password prompt. The PAM agent is used instead. As a result, the user is prompted for SecurID authentication only.
3. Restart sshd. Type:

   ```
   service sshd restart
   ```

Install the PAM Agent

You can either manually install the PAM agent on individual machines, or you can choose silent installation to automate the process of deploying multiple copies of the PAM agent.

Install the PAM Agent on One Machine

Perform this task to install one PAM agent. To install the PAM agent on more then one machine, see Bulk Install the PAM Agent with the Silent Installation on the facing page.

Procedure

1. On the agent machine, change to the PAM agent installer directory.
2. Untar the file by typing:

   ```
   tar -xvf filename.tar
   ```

3. Run the install script by typing:

   ```
   /filename/install_pam.sh
   ```

4. Follow the prompts. Press ENTER to accept the default value, or enter the appropriate value.

   For RSA Authentication Manager UDP mode, do the following:

   - Accept the License for RSA Software.
   - Enter 0 to select the RSA Authentication Manager with the UDP Protocol authentication mode.
   - Enter the directory where **sdconf.rec** is located.
   - Enter the PAM agent installation directory.

   For RSA Authentication Manager REST mode, do the following:

   - Accept the License for RSA Software.
   - Enter 1 to select the RSA Authentication Manager with the REST Protocol authentication mode.
   - Enter the REST server URL for communication between the authentication agent and the primary instance.
   - Enter y if there are Authentication Manager replica instances for failover.
   - Specify the number of replica instances.
   - Enter the REST server URL for each replica instance.
   - Enter the client key (Access Key) for securely passing authentication requests to Authentication Manager.
   - Enter the directory and filename for the server trusted certificate on the authentication agent.
   - Enter the client ID, which is the authentication agent name in Authentication Manager.
   - Enter the PAM agent installation directory.

   For Cloud Authentication Service REST mode, do the following:

   - Accept the License for RSA Software.
   - Enter 2 to select the Cloud Authentication Service with the REST Protocol authentication mode.
   - Enter the REST server URL for communication between the authentication agent and the Cloud Authentication Service.

     If you are using RSA Authentication Manager 8.5 as a proxy server to the Cloud Authentication Service, enter the REST server URL for communication between the authentication agent and the Authentication Manager primary instance.

- Enter the client key (Authentication API key) for securely passing authentication requests to the Cloud Authentication Service.

  If you are using RSA Authentication Manager 8.5 as a proxy server, enter the client key (Access Key) for securely passing authentication requests to Authentication Manager.

- Enter the directory and filename for the server trusted certificate on the authentication agent.
- Enter the tenant ID for the Cloud Authentication Service.
- If you are using RSA Authentication Manager 8.5 as a proxy server, enter the same tenant ID that was used to connect Authentication Manager to the Cloud Authentication Service.
- Enter the access policy name for the Cloud Authentication Service.
- Enter the CLIENT_ID authentication agent name to display in mobile notifications.
- Enter the PAM agent installation directory.

5. For UDP mode only, verify that VAR_ACE in the **/etc/sd_pam.conf** file points to the correct location of the **sdconf.rec** file. This is the path to the configuration files. The entire path must have -rw------- root permission.

After you finish

- You can verify the installation by checking the **installer.log** file in the PAM agent installer directory.
- For UDP mode, perform a test authentication. For more information, see Authentication Utilities for UDP Mode on page 45.
- For a REST protocol mode, test the connection by accessing the REST server URL with any browser or http client. For example, enter https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn. Because you are not currently authenticating, your browser or http client should display a "Forbidden" or "Unauthorized" HTTP response.

Bulk Install the PAM Agent with the Silent Installation

Perform this task to deploy a large number of PAM agents with identical configuration information. For example, perform this task if you need to install a large number of agents that communication with the same RSA Authentication Manager servers or the same Cloud Authentication Service.

Before you begin

Install the PAM agent manually and record the prompts. For instructions, see Install the PAM Agent on One Machine on the previous page.

Procedure

1. Create a text-based configuration file where you will specify configuration options for the PAM agent install script. You can choose any name for the configuration file, such as **installoptions.conf**.
2. Open the file and list each configuration option you want to select on a separate line, in the same order that the prompts are presented during a manual installation of the PAM agent.

   The following example describes the corresponding prompt for each option specified in the UDP configuration:

Example Value	Option
y	Continue silent installation? (y) This prompt is always included first.
Accept	Accept license terms and conditions? (Accept)
0	Authentication mode? (numerical value for desired mode) 0: RSA Authentication Manager with the UDP Protocol 1: RSA Authentication Manager with the REST Protocol 2: Cloud Authentication Service with the REST Protocol
/var/ace	Directory containing sdconf.rec? (directory path)
/opt	Installation path for PAM agent directory? (directory path)
y	Upgrade/overwrite existing installation? (y/n)

In this case, the text-based configuration file would contain:

```
y
Accept
0
/var/ace
/opt
y
```

As another example, for Authentication Manager REST mode, the configuration file might contain data that is similar to the following:

```
y
Accept
1
https://am821.example.com:5555/mfa_v1_1/authn
0i78x21rih887gb48126ufxh4g63orh3a3rt28k5416a2b3jxh05h86i7gntjfh3
/var/ace/cert.pem
sp7-dp33.network.com
/opt
y
```

Note: The number and order of the install prompts vary depending on the PAM agent mode and platform you are installing.

3. Change to the PAM agent installer directory.
4. Untar the file by typing:

   ```
   tar -xvf filename.tar
   ```

5. Run the install script by typing:

   ```
   /filename/install_pam.sh -s < installoptions.conf
   ```

where ***installoptions.conf*** is the configuration file you created in Step 1. if the configuration file is in different location than current directory, specify the full path to the ***installoptions.conf*** file.

Upgrade to the RSA Authentication Agent 8.1 for PAM

You can upgrade to RSA Authentication Agent 8.1 for PAM from version 7.1 Patch 2 (7.1.0.2) or from version 8.0.

When upgraded from 7.1.0.2, the upgraded agent uses RSA Authentication Manager and UDP protocol for authentication. You can change the authentication mode to take advantage of the Cloud Authentication Service or Authentication Manager and the REST protocol. For instructions, see Changing the PAM Agent Authentication Mode on page 37.

When upgraded from 8.0, the upgraded agent retains the same authentication mode that was configured for the previous version.

Before you begin

- You must have root permissions on the agent host and write permission to the directory in which the **sdconf.rec** file is stored. This file is usually stored in the default **/var/ace** directory.
- Back up the configuration files before overwriting to save the configuration settings. For more information, see Critical Configuration Files on page 54.
- Configure the RSA SecurID protected tools to use the standard PAM module provided with your operating system, and not the RSA PAM module. Any active sessions using the RSA PAM modules must be closed before you proceed with the upgrade.

Procedure

1. On the agent machine, change to the PAM agent installer directory.
2. Untar the file by typing:

   ```
   tar -xvf filename.tar
   ```

3. Run the install script by typing:

   /<filename>/install_pam.sh

4. Overwrite the existing installation files. Type **y** when the installer prompts you to overwrite your current installation.
5. Obtain the agent version number to determine if the upgrade succeeded. Type:

   strings pam_securid.so | grep "Agent"

   This returns the version number of the installed agent.

Verifying AppArmor Settings

AppArmor is a Linux kernel security module that allows you and other administrators to restrict applications. This section describes steps to verify the AppArmor module settings.

Procedure

1. Run the following command to check if AppArmor is enabled. Type:

   /boot/grub/menu.lst

2. Run the following command to verify the policies supported by AppArmor. Type:

   /usr/sbin/apparmor_status

Configuring Tools

You must configure the supported tools to prompt users with the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

Note: The number of allowed concurrent users settings on the Unix server should be set up for each tool, the operating system being used, and the expected concurrent logons to the server, especially when using the Cloud Authentication Service.

Configure telnet below

Configure login below

Configure rlogin on the facing page

Configure su on the facing page

Configure ssh and Related Tools on the facing page

Configure sudo on the facing page

Configure ftp on page 28

Configure gdm on page 28

Configure xdm on page 28

Configure telnet

Configure telnet to prompt users for the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

1. Change to the **/etc/pam.d** directory.
2. Open the **remote** file.
3. Comment any lines that begin with `auth`.
4. Add the line:

   ```
   auth required pam_securid.so
   ```

Configure login

Configure the login command to prompt users for the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

1. Change to the **/etc/pam.d** directory.
2. Open the **login** file.

3. Comment any lines that begin with `auth`.
4. Add the line:

```
auth required pam_securid.so
```

Configure rlogin

Configure the rlogin utility to prompt users for the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

Before you begin

If rlogin connections are getting closed, follow the procedure in Known Configuration Issues on page 44.

Procedure

1. Change to the **/etc/pam.d** directory.
2. Open the **rlogin** file.
3. Comment any lines that begin with `auth`.
4. Add the line:

```
auth required pam_securid.so
```

Configure su

Configure the su command to prompt users for the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

Procedure

1. Change to **/etc/pam.d** directory.
2. Open the **su** file.
3. Comment any lines that begin with `auth`.
4. Add the line:

```
auth required pam_securid.so
```

Configure ssh and Related Tools

You can configure SSH and related tools, such as scp and sftp, to prompt users for the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

Procedure

1. Change to the **/etc/pam.d** directory.
2. Open the **sshd** file.
3. Comment any lines that begin with `auth`.
4. Add the line:

```
auth required pam_securid.so
```

Configure sudo

If you require sudo, you must configure the sudo command to prompt users for the authentication methods

supported by the Cloud Authentication Service and RSA Authentication Manager.

Before you begin

Download and install the supported sudo version from https://www.sudo.ws.

Procedure

1. Change to the **/etc/pam.d** directory.
2. Open the **sudo** file.
3. Comment any lines that begin with `auth`.
4. Add the line:

```
auth required pam_securid.so
```

Configure ftp

Configure the ftp protocol to prompt users for the authentication methods supported by RSA Authentication Manager.

You cannot use the Cloud Authentication Service to protect ftp; However, you can use sftp. For instructions, see Configure ssh and Related Tools on the previous page.

Procedure

1. Change to the **/etc/pam.d** directory.
2. Open the **vsftpd** file.
3. Comment any lines that begin with `auth`.
4. Add the line:

```
auth required pam_securid.so
```

Configure gdm

You can configure gdm to prompt users for the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

Procedure

1. Change to the **/etc/pam.d** directory.
2. Modify the **gdm**,**gdm-password** and **gdm-autologin**files as follows:
    a. Open each gdm file.
    b. Comment any lines that begin with `auth`.
    c. Add the line:

```
auth required pam_securid.so
```

Configure xdm

You can configure xdm to prompt users for the authentication methods supported by the Cloud Authentication Service and RSA Authentication Manager.

Procedure

1. Change to the **/etc/pam.d** directory.
2. Open the **xdm** file.
3. Comment any lines that begin with `auth`.
4. Add the line:

```
auth required pam_securid.so
```

Chapter 2: Configuring Features

Configuring Agent and UNIX Features

You can customize the PAM agent configuration to use optional agent and UNIX features.

Note: Before customizing the agent, make backup copies of the original configuration files.

Multiple configuration files are located in the **/etc/pam.d** directory. Each file uses the name of the connection tool.

To customize the agent, see:

Enable Agent Reporting for RSA SecurID Authentication Agent 8.1 for PAM below

Enable Debug Output below

Enable SecurID Trace Logging for UDP Mode on the facing page

Configure Stackable Modules on the facing page

Use Reserve Passwords on page 34

Enable Selective SecurID Authentication on page 35

Configure Exponential Backoff Time on page 36

Enable Agent Reporting for RSA SecurID Authentication Agent 8.1 for PAM

You can configure the ENABLE_AGENT_REPORTING parameter in the **mfa_api.properties** file to send agent details, such as the hostname, agent version, and OS version, to RSA Authentication Manager. You can use RSA Authentication Manager 8.3 or later to run reports that include these details.

Before you begin

You must have root permissions on the machine where the agent is installed and write permission to the directory in which the **mfa_api.properties** file is stored. By default, this file is stored in **/var/ace/conf**.

Procedure

1. Change to the directory where **mfa_api.properties** is located. By default, the directory is **/var/ace/conf**.
2. Open **mfa_api.properties**.
3. Change the ENABLE_AGENT_REPORTING parameter to 1, which enables agent reporting. The default value is 0.
4. Save the file.

   Details of the PAM agent and the machine that it is installed on are included in PAM agent reporting details that are sent to Authentication Manager.

Enable Debug Output

For troubleshooting, you can enable debug output for specific tools that are used by the PAM agent.

You can also configure the system log to record all PAM agent authentication log messages. For more information, see Logging for the PAM Agent on page 48.

Procedure

1. Change to the **/etc/** directory, and open the **pam.d** file.
2. Edit the appropriate file by adding a debug argument for the pam_securid.so module. Type:

   ```
   auth required pam_securid.so debug
   ```

Enable SecurID Trace Logging for UDP Mode

You can enable detailed SecurID trace logging for the PAM agent and for the authentication utilities acetest and acestatus. By default, when you install the PAM agent, SecurID trace logging is disabled.

Procedure

1. Change to the **/etc/** directory, and open the **sd_pam.conf** file.
2. To enable detailed agent logging and set the level of logging, set the following variable:

   RSATRACELEVEL=*value*

   Where *value* is a setting from the following table.

Value	Description
0	Disables logging (default)
1	Logs regular messages
2	Logs function entry points
4	Logs function exit points
8	All logic flow controls use this (ifs)

   For combinations, add the corresponding values. For example, to log regular messages and function entry points, set the value to 3.

3. Specify the file path where the logs are redirected. Set the following variable:

   RSATRACEDEST=*filepath*

   Where *filepath* is the file path.

   By default this variable is blank. If you do not set this variable, the logs go to standard error for authentication utilities acetest and acestatus, and no logs are generated for authentication tools, even if the RSATRACELEVEL value has been specified.

4. Save your changes.

Configure Stackable Modules

In a stacked configuration, you use the agent to integrate the RSA SecurID PAM authentication module with other PAM authentication modules in your environment. The password or passcode is passed from the one authentication module to the next one. You can configure the priority of authentication challenges by editing the appropriate **/etc/pam.d/*tool name*** configuration file.

Note: The arguments use_first_pass and try_first_pass are not supported when a stacked configuration is used with the Cloud Authentication Service.

The agent works with these arguments:

- **use_first_pass.** The agent uses only the password or passcode passed from the previous module, and denies access if the credentials do not match. The user is not prompted for authentication again.
- **try_first_pass.** The agent uses the password or passcode passed from the previous module. If the credentials do not match, the user is prompted for authentication.
- **not_set_pass.** The agent does not send the password or passcode to the stacked password module.

Note: When users excluded from SecurID authentication make failed login attempts to access the RSA PAM module, the exponential backoff feature ensures that RSA PAM module retains control until login is successful or the authentication session ends. For more information on configuring exponential backoff time, see Configure Exponential Backoff Time on page 36.

The following section provides an example of how to configure a connection tool (login tool) in a stacked environment.

Procedure

1. Change to **/etc/pam.d/** and open the **login** file.
   The following lines are displayed:
   ```
   auth required pam_securetty.so
   auth include common-auth
   auth required pam_nologin.so
   account include common-account
   password include common-password
   session include common-session
   session required pam_lastlog.so nowtmp
   session required pam_resmgr.so
   session optional pam_mail.so standard
   session required pam_limits.so
   ```
2. Comment the following lines:
   ```
   auth required pam_securetty.so
   auth include common-auth
   auth required pam_nologin.so
   ```
3. Add the following lines. Type:
   ```
   auth required pam_securid.so
   ```

Use Reserve Passwords

The reserve password feature is an emergency access method that enables you, the administrator, to authenticate to the protected machine on which the agent is installed without entering an RSA SecurID passcode. The PAM agent allows only root administrators to use reserve passwords during unforeseen circumstances, such as loss of communication between the agent and RSA SecurID Authentication Agent 8.1 for PAM. In these situations, administrators can temporarily disable the agent, if users require immediate access to the hosted resources.

Note: The UNIX password is the reserve password.

Procedure

1. Open the appropriate file in **/etc/pam.d.**
2. Add a reserve argument to the pam_securid.so module. Type:

```
auth required pam_securid.so reserve
```

Enable Selective SecurID Authentication

You can configure the agent to selectively always or never prompt specific UNIX users or groups for SecurID authentication:

Enable Selective SecurID Authentication for UNIX Groups below

Enable Selective SecurID Authentication for UNIX Users on the next page

Note: When both selective group support and selective user support are enabled, only selective user support is enabled, and selective group support is ignored.

The following table lists the possible values which can be set in the **sd_pam.conf** file.

ENABLE_ GROUPS_ SUPPORT	ENABLE_ USERS_ SUPPORT	Result
0	0	Neither feature is enabled. Every user and user group gets challenged.
0	1	Selected user support is enabled. The PAM agent always prompts specific UNIX users to authenticate with SecurID, or never prompts specific users to authenticate with SecurID.
1	0	Selected group support is enabled. The PAM agent always prompts specific UNIX groups to authenticate with RSA SecurID, or never prompts specific groups to authenticate with SecurID.
1	1	Selected user support is enabled. The PAM agent always prompts specific UNIX users to authenticate with SecurID, or never prompts specific users to authenticate with SecurID.

Enable Selective SecurID Authentication for UNIX Groups

You can configure the PAM agent to always or never prompt specific UNIX groups to authenticate with RSA SecurID. When the PAM agent is installed, this feature is not enabled.

Group members excluded from SecurID authentication can be authenticated either with UNIX credentials or through another PAM module in the stack. To do this, configure the PAM_IGNORE_SUPPORT parameter.

Note: Do not specify RSA Authentication Manager groups. This feature is for UNIX groups only.

Procedure

1. Change to the **/etc** directory, and open the **sd_pam.conf** file.
2. Set the ENABLE_GROUP_SUPPORT parameter to 1. The default value is 0.
3. Populate the LIST_OF_GROUPS parameter.
4. Set the value for the INCL_EXCL_GROUPS parameter.
   Valid values are:

0—Disable SecurID authentication for the listed groups (default).
1—Enable SecurID authentication only for the listed groups.

5. (Optional) Set the PAM_IGNORE_SUPPORT parameter.
   Valid values are:
   0—Enable UNIX password authentication (default).
   1—Disable UNIX password authentication.
   This parameter applies only to groups excluded from SecurID authentication.
6. Save the file.

Enable Selective SecurID Authentication for UNIX Users

You can configure the PAM agent to always or never prompt specific UNIX users to authenticate with SecurID. When the PAM agent is installed, this feature is not enabled.

Users excluded from SecurID authentication can be authenticated either with UNIX credentials or through another PAM module in the stack. To do this, configure the PAM_IGNORE_SUPPORT_FOR_USERS parameter.

Procedure

1. Change to the **/etc** directory, and open the **sd_pam.conf** file.
2. Set the ENABLE_USERS_SUPPORT parameter to 1. The default value is 0.
3. Populate the LIST_OF_USERS parameter.
4. Set the value for the INCL_EXCL_USERS parameter.
   Valid values are:
   0—Disable SecurID authentication for the listed users (default).
   1—Enable SecurID authentication only for the listed users.
5. (Optional) Set the PAM_IGNORE_SUPPORT_FOR_USERS parameter.
   Valid values are:
   0—Enable UNIX password authentication (default).
   1—Disable UNIX password authentication.
   This parameter applies only to users excluded from SecurID authentication.
6. Save the file.

Configure Exponential Backoff Time

You can configure the time that a user who is excluded from RSA SecurID authentication is required to wait before authenticating after each successive failed login attempt. By default, users can retry UNIX authentication after a failed login attempt with a pow(4, failattempts) second delay. For example, three failed login attempts result in a 64-second delay (four to the power of three, or 4 X 4 X 4 = 64).

Note: The ftp protocol does not support Exponential Backoff Delay.

Procedure

1. Change to the **/etc** directory, and open the **sd_pam.conf** file.
2. Set the BACKOFF_TIME_FOR_RSA_EXCLUDED_UNIX_USERS parameter to *N*, as follows:

N	**Authentication Behavior**
0	Disable retry UNIX authentication after a failed login attempt. There is no authentication delay for login attempts that follow a failed login attempt.

N	Authentication Behavior
1,2,3	Enable retry UNIX authentication after a failed login attempt with a pow(3, failattempts) second delay.
4	Enable retry UNIX authentication after a failed login attempt with a pow(4, failattempts) second delay.
5/Above	Enable retry UNIX authentication after a failed login attempt with a pow(5/Above, failattempts) second delay.

Replace the Server Trusted Root CA Certificate

You might need to replace the server trusted root CA certificate, for example, if the current RSA Authentication Manager or Cloud Authentication Service certificate is updated.

For instructions on obtaining this certificate, see the knowledgebase article How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate.

Before you begin

- You must have root permissions to the **/var/ace** directory on the machine where the PAM agent is installed.
- Confirm that the new certificate is in PEM format. If there are multiple CA certificates, they need to be concatenated into a single file in PEM format.

  The file format should be like the following:

  -----BEGIN CERTIFICATE-----

  Thawte (BASE64)

  -----END CERTIFICATE-----

  -----BEGIN CERTIFICATE-----

  Entrust (BASE64)

  -----END CERTIFICATE-----

Procedure

1. Rename the new root certificate so it has the same name as the certificate you are replacing.
2. On the machine where the PAM agent is installed, copy and replace ***new_cert_file*.pem** into the **/var/ace/** directory.

Changing the PAM Agent Authentication Mode

You can change the authentication mode for the PAM agent. For example, you can change the mode if you want to use the expanded authentication options that are provided by the Cloud Authentication Service. By default, an upgraded PAM agent uses RSA Authentication Manager with the UDP protocol.

Change from the UDP Protocol to the REST Protocol

You can change the UDP protocol authentication mode to the REST protocol for RSA SecurID Authentication Agent 8.1 for PAM or the Cloud Authentication Service.

Before you begin

- You must have root permissions on the machine where the agent is installed.
- You must have write permission to the directory in which the **sdconf.rec** file is stored. By default, this file is stored in **/etc**.
- You must have write permission to the directory in which the **mfa_api.properties** file is stored. By default, this file is stored in **/var/ace/conf**.
- Collect the required information.

  For Authentication Manager authentication with the REST protocol, ask your Authentication Manager Super Admin for the following information.

Parameter	Description
REST_URL	REST server URL for communication between the authentication agent and the Authentication Manager primary instance. Use the following format: `https://HOSTNAME:PORT/mfa/v1_1/authn` On the primary instance obtain the *HOSTNAME* value from the **Fully Qualified Domain Name** field on the **Administration > Network > Appliance Network Settings** page of the Operations Console. The default *PORT* is 5555.
REPLICA_*number* Where *number* is from 1 to 15.	A REST server URL for each replica instance that can be used for failover. Use the following format: `https://HOSTNAME:PORT/mfa/v1_1/authn` On the replica instance, obtain the *HOSTNAME* value from the **Fully Qualified Domain Name** field on the **Administration > Network > Appliance Network Settings** page of the Operations Console. The default *PORT* is 5555.
CLIENT_KEY	Access Key (client key) for securely passing user authentication requests to Authentication Manager.This value is generated in the Security Console on the Authentication Manager primary instance. For instructions on how to obtain the Access Key, see the following topic on RSA Link: Configure the RSA SecurID Authentication API for Authentication Agents.
CA_CERT_FILE_PATH	Directory and filename for the server trusted certificate on the authentication agent. The default value is **/var/ace/cert.pem**.
CLIENT_ID	Authentication agent name (Client ID) that was created for the PAM agent in Authentication Manager.

For authentication with the Cloud Authentication Service, ask the Cloud Authentication Service Super Admin for the following information.

Parameter	Description
REST_URL	REST server URL for communication between the agent and the Cloud Authentication Service. Use the following format: `https://HOSTNAME/mfa/v1_1/authn`

Parameter	Description
	For the Cloud Authentication Service, obtain the *HOSTNAME* value. In the Cloud Administration Console, click **My Account > Company Settings > Authentication API Keys**. Copy the **RSA SecurID Authentication API REST URL**.The default *PORT* is 443.
CLIENT_KEY	Authentication API key (client key) created in the Cloud Administration Console for securely passing user authentication requests to the Cloud Authentication Service. For instructions on how to obtain the Authentication API key, see the following topic on RSA Link: Add an RSA SecurID Authentication API Key.
CA_CERT_FILE_ PATH	Enter the directory and filename for the server trusted certificate on the authentication agent. The default value is **/var/ace/cert.pem**.
TENANT_ID	The Tenant ID is required. The PAM agent must provide a value for the Tenant ID in authentication requests. For example, you can set the Tenant ID to the the Company ID from the Cloud Administration Console. To find the Company ID, in the Cloud Administration Console, click **My Account > Company Settings** and select the Company Information tab.
ASSURANCE_ POLICY_ID	Access policy name for the Cloud Authentication Service. The policy name is case-sensitive. This policy is defined in the Cloud Administration Console.
CLIENT_ID	CLIENT_ID authentication agent name to display in mobile notifications. You can enter any value. For example, PAM_Agent.

Procedure

1. Change to the directory where **sd_pam.conf** is located. The default location is **/etc**.
2. Open **sd_pam.conf**.
3. Change the OPERATION_MODE parameter:
   - For Authentication Manager with the REST protocol, enter 1.
   - For the Cloud Authentication Service with the REST protocol, enter 2.

   If the OPERATION_MODE parameter is 0, not specified or commented out, then the PAM agent defaults to UDP mode.
4. Change to the directory **/var/ace/conf**. You need to update the **mfa_api.properties** file.
5. Open **mfa_api.properties**.
6. Remove comments to enable the required parameters.
7. Enter a value for each required parameter.
8. Save the file.

   You can now use the REST protocol.

Change from the REST Protocol to the UDP Protocol

After installing the PAM agent to use the REST protocol, you can change the authentication mode to use RSA SecurID Authentication Agent 8.1 for PAM with the UDP Protocol.

After you change the authentication mode to use the UDP protocol, the REST protocol configuration settings in the **mfa_api.properties** file no longer applies.

Before you begin

- The Authentication Manager configuration file, **sdconf.rec**, is required. You can generate this file in Authentication Manager or obtain this file from your Authentication Manager Super Admin. For more information, see Planning to Install the PAM Agent on page 17.
- You must have root permissions on the machine on which the agent is installed and write permission to the directory in which the **sd_pam.conf** file is stored. By default, this file is stored in the **/etc** directory.

Procedure

1. Change to the directory where **sd_pam.conf** is located. The default location is **/etc**.
2. Open **sd_pam.conf**.
3. Change the OPERATION_MODE parameter to 0 for the UDP protocol:

   ```
   OPERATION_MODE=0
   ```

   If the OPERATION_MODE parameter is 0, not specified or commented out, then the PAM agent defaults to UDP mode.

4. Copy **sdconf.rec** to the **/var/ace** directory.

   You can now use the UDP protocol.

Change Between RSA Authentication Manager and the Cloud Authentication Service

You can change whether the PAM agent uses the REST protocol with Authentication Manager or the Cloud Authentication Service.

If you are using RSA Authentication Manager 8.5 as a secure proxy server to the Cloud Authentication Service, you might want to use all of the authentication methods supported by the Cloud Authentication Service. To do so, select Cloud Authentication Service mode. If you want RSA Authentication Manager 8.5 to handle authentication and only send authentication requests that it cannot validate to the Cloud Authentication Service, select Authentication Manager mode. In both cases, you must use the REST server URL and the Authentication API key (client key) for RSA Authentication Manager.

Before you begin

- You must have root permissions on the machine on which the agent is installed.
- You must have write permission to the directory in which the **sdconf.rec** file is stored. By default, this file is stored in **/var/ace**.
- You must have write permission to the directory in which the **mfa_api.properties** file is stored. By default, this file is stored in **/var/ace/conf**.
- The parameter CA_CERT_FILE_PATH for the server trusted certificate can remain the same. For the other parameters, collect the required information:
  For Authentication Manager authentication with the REST protocol, ask your Authentication Manager Super Admin for the following information:

Parameter	Description
REST_URL	REST server URL for communication between the authentication agent and the Authentication Manager primary instance. Use the following format: `https://HOSTNAME:PORT/mfa/v1_1/authn`

Parameter	Description
	On the primary instance obtain the *HOSTNAME* value from the **Fully Qualified Domain Name** field on the **Administration > Network > Appliance Network Settings** page of the Operations Console. The default *PORT* is 5555.
REPLICA_*number* Where *number* is from 1 to 15.	REST server URL for each replica instance. Use the following format: `https://HOSTNAME:PORT/mfa/v1_1/authn` On the replica instance, obtain the *HOSTNAME* value from the **Fully Qualified Domain Name** field on the **Administration > Network > Appliance Network Settings** page of the Operations Console. The default *PORT* is 5555.
CLIENT_KEY	Access Key (client key) for securely passing user authentication requests to Authentication Manager. This value is generated in the Security Console on the Authentication Manager primary instance. For instructions on how to obtain the Access Key, see the following topic on RSA Link: Configure the RSA SecurID Authentication API for Authentication Agents.
CLIENT_ID	Authentication agent name (Client ID) that was created for the PAM agent in Authentication Manager.

For authentication with the Cloud Authentication Service, ask the Cloud Authentication Service Super Admin for the following information:

Parameter	Description
REST_URL	REST server URL for communication between the agent and the Cloud Authentication Service. Use the following format: `https://HOSTNAME/mfa/v1_1/authn` Obtain the hostname from the Cloud Administration Console. Click **My Account > Company Settings > Authentication API Keys**. Copy the **RSA SecurID Authentication API REST URL**. You do not need to specify a port. The default port is 443.
CLIENT_KEY	Authentication API key (client key) created in the Cloud Administration Console for securely passing user authentication requests to the Cloud Authentication Service. For instructions on how to obtain the Authentication API key, see the following topic on RSA Link: Add an RSA SecurID Authentication API Key.
TENANT_ID	The Tenant ID is required. The PAM agent must provide a value for the Tenant ID in authentication requests. For example, you can set the Tenant ID to the the Company ID from the Cloud Administration Console. To find the Company ID, in the Cloud Administration Console, click **My Account > Company Settings** and select the Company Information tab.
ASSURANCE_POLICY_ID	Access policy name for the Cloud Authentication Service. The policy name is case-sensitive. This policy is defined in the Cloud Administration Console.
CLIENT_ID	CLIENT_ID authentication agent name to display in mobile notifications. You can enter any value. For example, PAM_Agent.

Procedure

1. Change to the directory where **sd_pam.conf** is located. The default location is **/etc**.
2. Open **sd_pam.conf**.
3. Change the OPERATION_MODE parameter:
   - For Authentication Manager with the REST protocol, enter 1.
   - For the Cloud Authentication Service with the REST protocol, enter 2.

   If the OPERATION_MODE parameter is 0, not specified or commented out, then the PAM agent defaults to UDP mode.
4. Change to the directory **/var/ace/conf**. You must update the required values for the parameters in the **mfa_api.properties** file.
5. Open **mfa_api.properties**.
6. Remove comments to enable the required parameters, and comment out any parameters that are no longer needed.
7. Enter a value for each required parameter.
8. Save the file.

   You can now use the REST protocol with the new authentication mode.

Appendix A: Troubleshooting

Known Configuration Issues

This section describes known issues.

Issues With Supported Tools

Tool	Known Issue
dtlogin	**Problem:** Display limitations can cause two problems for users: • Authenticating users cannot see the entire message about available authentication methods. • Reserve password users can see a partial text entry field on screens where it is not needed. **Solution:** Authenticating users can press ENTER, as instructed on the screen, to see the full message. Reserve password users can ignore the unnecessary field.
ftp	• **Problem:** When you use SecurID to protect ftp, the SecurID authentication prompts and error messages are not displayed to users. Only standard operating system (OS) prompts and error messages are displayed. **Solution:** Instruct users to enter their user names at the OS user name prompt, and their SecurID passcodes at the OS password prompt. If a user doesn't know the token status (for example, if the token is in the Next Tokencode mode, or the New PIN mode), the user must to authenticate with another connection tool, such as rlogin to verify that the PIN or tokencode is still valid. • FTP does not support Exponential Backoff Delay. • You cannot use the Cloud Authentication Service to protect ftp; however, sftp is supported.
ssh	**Problem:** After a user makes three unsuccessful SecurID authentication attempts in a single session, the connection is closed. **Solution:** The user can terminate the session and start another session.
rlogin	**Problem:** Before rlogin is configured to work with the PAM agent, rlogin connections are getting closed. **Solution:** Make sure that rlogin works before configuring the PAM agent. Follow these steps: 1. Open the **/etc/xinet,d/rlogin** file. 2. Add **nice = 5** at the end of the rlogin configuration. 3. Restart xinetd services: `service xinetd restart`
rlogin	**Problem:** If the first attempt to process an rlogin request fails, the session is handed off to the login daemon. **Solution:** If you configure Linux to use rlogin, you must configure the remote login file in **/etc/pam.d**.
rlogin	**Problem:** When a user tries to access the system using rlogin tool and enters wrong credentials, the system redirects the authentication process to the telnet tool, and the system may prompt for password or passcode as per the telnet configuration. **Solution:** When rlogin is protected with SecurID, telnet must also be protected with SecurID and vice versa.
rlogin	**Problem:** If the PAM agent is the only authentication module used to protect rlogin (in other words, rlogin is used in a non-stacked configuration) and the incorrect passcode is entered, the system

Tool	Known Issue
	prompts the user for the UNIX password and allows access if this is entered correctly. **Solution:** Use a stacked configuration.

Upgrade and Uninstall Issues

Problem: If you try to upgrade or uninstall the PAM agent without disabling the RSA PAM module, you may receive the error message: 'pam_securid.so is busy, not able to remove/replace'.
Solution: To resolve this issue, you must log on with tools other than ssh and remove **pam_securid.so**.

Authentication Utilities for UDP Mode

Authentication utilities are located in the following directories:

- 32-bit operating system: ***pam agent installation directory*/bin/32bit**
- 64-bit operating system: ***pam agent installation directory*/bin/64bit**

Use these utilities to:

- Perform a test authentication. For more information, see Run the acetest Utility below.
- Verify communication between the PAM agent and RSA Authentication Manager. For more information, see Run the acestatus Utility below

You can enable logging for these utilities. For more information, see Enable SecurID Trace Logging for UDP Mode on page 33

Run the acetest Utility

This utility checks that the agent is functioning properly by performing a test authentication.

Procedure

1. Change to the PAM agent authentication utilities directory:
   - 32-bit operating system: ***pam agent installation directory*/bin/32bit**
   - 64-bit operating system: ***pam agent installation directory*/bin/64bit**
2. Type:

   ```
   ./acetest
   ```

3. Enter a valid user name and passcode.

If you are repeatedly denied access, test the connectivity to the Authentication Manager server with the Run the acestatus Utility below utility or contact your Authentication Manager administrator.

Run the acestatus Utility

This utility checks the status of each Authentication Manager where the PAM agent is registered as an agent host. If you have questions concerning the displayed information, contact your Authentication Manager administrator.

Procedure

1. Change to the PAM agent utilities directory.
2. Type:

```
./acestatus
```

The following table lists the information displayed in the Authentication Manager section.

Returned Information	Description
Configuration Version	Version of the **sdconf.rec** file that is in use. For RSA Authentication Manager 8.0 or later, this number is 14.
DES Enabled	If your configuration environment supports legacy protocols, YES is displayed.
Client Retries	Number of times the PAM agent sends authentication data to Authentication Manager before a timeout occurs.
Client Timeout	Time (in seconds) that the PAM agent waits before resending authentication data to Authentication Manager.
Server Release	Version number of Authentication Manager.
Communication	Protocol version used by Authentication Manager and the PAM agent.

The following table lists the status information displayed in the Authentication Manager section.

Status Information	Description
Server Active Address	The IP address that the PAM agent uses to communicate with the server. This address could be the actual IP address of the server you have selected, or it could be an alias IP address assigned to the server. An IP address of 0.0.0.0 indicates that the agent has not yet received communication from the server.

The following table lists the server status information displayed in the Authentication Manager section.

Server Status	Description
Available for Authentications	This server is available to handle authentication requests.
Unused	The server has not yet received an authentication request.
For Failover only	The server is reserved for failover use only.
Default Server During initial requests	Only this server is available to handle requests at this time.

Conversion Utility for UDP Mode

The conversion utility is used when a UDP-based PAM agent co-exists with other SecurID agents.

The conversion utility ns_conv_util is located in the following directories:

- 32-bit operating system: ***pam agent home*/bin/32bit**
- 64-bit operating system: ***pam agent home*/bin/64bit**

Procedure

1. Change to the PAM agent utilities directory.
2. Type:

   ```
   ./ns_conv_util <Existing_Securid_file_path> <New_Securid_dir_path>
   ```

   where <Existing_Securid_file_path> is the path where the current SecurID file exists,

   and <New_Securid_dir_path> is the directory where the newly generated SecurID file should be stored.

   For example:

   ```
   ./ns_conv_util /var/ace/securid /var/ace_pam/
   ```

3. If the new destination location is not the same as the location specified by VAR_ACE, copy the new SecurID file to this location.

Node Secrets for UDP Mode

The node secret is a symmetric encryption key that RSA Authentication Manager and the PAM agent use to encrypt and decrypt packets of data as they travel across the network. Node secrets are required for agents that use the UDP protocol. The shared node secret is stored in both the Authentication Manager database and in a file on the machine where the PAM agent is installed. For agents that use the REST protocol, a node secret file is not used. Instead of a node secret, a dynamically negotiated key is used to encrypt the channel along with a strong encryption algorithm.

For UDP-based agents, if the node secret is missing on either the Authentication Manager server or the machine where the PAM agent is installed, clear the node secret in the other location. If the node secret files on the Authentication Manager and the PAM agent machine do not match, clear the node secret in both locations. After you clear the node secret, you must generate a new node secret.

Clear the Node Secret From RSA SecurID Authentication Agent 8.1 for PAM

If the node secret does not match on the RSA SecurID Authentication Agent 8.1 for PAM and the machine where the PAM agent is installed, or if the node secret is missing from the PAM agent machine, you must clear the node secret from Authentication Manager. For example, if you reinstall the PAM agent, the node secret is missing from the PAM agent machine.

Procedure

1. In the Authentication Manager Security Console, click **Access > Authentication Agents > Manage Existing**.
2. Locate the affected agent machine and select **Manage Node Secret** from the drop-down menu.
3. Select the **Clear the node secret** checkbox, and then click **Save**.

After you finish

- If there is a node secret on the PAM agent machine, see Clear the Node Secret on the PAM Agent Machine on the next page.
- If the PAM agent machine does not have a node secret, follow the procedure Generate a New Node Secret on the next page.

Clear the Node Secret on the PAM Agent Machine

If the node secret does not match on the RSA Authentication Manager instance and the PAM agent machine, or if the node secret is missing from the Authentication Manager, you must clear the node secret from the PAM agent machine. For example, if you install a new Authentication Manager instance and add an existing PAM agent, the node secret is missing from Authentication Manager.

Before you begin

If there is a node secret on the Authentication Manager, see Clear the Node Secret From RSA SecurID Authentication Agent 8.1 for PAM on the previous page.

Procedure

1. Log on to the machine on which the PAM agent is installed and locate the node secret file, **securid**, in the **/var/ace** directory.
2. Rename or delete the node secret file.
3. The node secret is also stored in the server cache. Restart the machine to clear the node secret from the cache.

After you finish

Generate a New Node Secret below

Generate a New Node Secret

Procedure

1. Run the acetest utility from the PAM agent machine to generate the node secret file. For more information, see Authentication Utilities for UDP Mode on page 45.
2. Check your authentication logs and ensure a new node secret has been sent.
3. Restart your PAM agent machine so that the agent can read the node secret file.

Logging for the PAM Agent

If logging is enabled, by default, PAM agent authentication messages are recorded in the system log. For tracing purposes, you can configure your system log to record PAM agent authentication log messages for specific tools. See Enable Debug Output on page 32.

For information on making changes to the logging, refer to the syslog-ng documentation available with the SUSE 11 and SUSE 12 operating system.

PAM Agent Authentication Log Messages

The following table lists the authentication log messages.

Message	Description
Cannot locate **sd_pam.conf** file	The configuration file **sd_pam.conf** is not in the **/etc** directory; **/etc** must contain the correct configuration file so that the VAR_ACE can be set properly.
AceInitialize failed	AceInitialize is an API function call that initializes worker threads, and loads configuration settings from **sdconf.rec**. Verify that you have the latest copy of **sdconf.rec** from your Authentication Manager administrator and that the VAR_ACE is set properly.

Message	Description
Cannot communicate with RSA ACE/Server	Either the Authentication Manager brokers are not started, or there has been a network failure. Contact your Authentication Manager administrator or your network administrator.
Reserve password exceeds character limit	The maximum character limit is 256 characters.
Invalid reserve password	The reserve password is the same as the system password for the host. You must know this password if Authentication Manager is unable to process authentication requests.
User name exceeds character limit	The user name must not exceed 31 characters.
Reserve password not allowed. User is not root.	Verify that you are a root user. Only root users can use the reserve password.

Logging for REST Mode

The REST mode supports additional logging implemented with the **log4cxx** library. Logging for the REST layer is separate from the PAM agent logs. RollingFileAppender and SyslogAppender are supported. By default, RollingFileAppender is enabled. Logs go to **/var/ace/log/mfa_rest.log** with the log level set to INFO. Size-based rotation is enabled with a rotation size of 10 MB.

Time-based log rotation is not supported. Supported tools, such as ssh and su, load the authentication agent for every request, and so the PAM agent cannot rotate the logs based upon time. The PAM agent supports size-based log rotation.

You can change the default log settings for REST mode.

Procedure

1. Change to the **/var/ace/conf** directory.
2. Open the **log.properties** file.
3. Configure the following entries for size-based rotation:

```
log4j.rootLogger=INFO, RestLogger

log4j.appender.RestLogger=org.apache.log4j.RollingFileAppender

log4j.appender.RestLogger.File=/var/ace/log/mfa_rest.log

log4j.appender.RestLogger.MaxFileSize=10MB

log4j.appender.RestLogger.MaxBackupIndex=10

log4j.appender.RestLogger.layout=org.apache.log4j.PatternLayout
```

```
log4j.appender.RestLogger.layout.ConversionPattern=%d [%t] %-5p
(%F:%L) - %m%n

log4j.appender.RestLogger.Append=true

log4j.appender.RestLogger.ImmediateFlush=true
```

4. Configure the following entries to support local and remote logging to the syslog:

```
log4j.rootLogger=INFO,Syslog

log4j.appender.Syslog=org.apache.log4j.net.SyslogAppender

log4j.appender.Syslog.syslogHost=localhost

log4j.appender.Syslog.Facility=DAEMON

log4j.appender.Syslog.layout=org.apache.log4j.PatternLayout

log4j.appender.Syslog.layout.ConversionPattern=%d{yyyy-MM-dd
HH:mm:ss:SSS}%p [%c] %m%n
```

5. Save your changes.
6. Restart the syslog daemon.

Configure Timeout and Retry Values for REST Authentication

You can configure how long the PAM agent can take to connect to RSA Authentication Manager or the Cloud Authentication Service, and how long the PAM agent waits for a response. You can also configure the number of times that the PAM agent tries to contact an Authentication Manager primary or replica instance or the Cloud Authentication Service. These parameters are only used by the REST protocol.

Make sure to account for the speed of your network. Setting high timeout values on a slower network allows authentication to succeed.

Before you begin

You must have root permissions on the machine on which the agent is installed and write permission to the directory in which the **mfa_api.properties** file is stored. By default, this file is stored in **/var/ace/conf**.

Procedure

1. Change to the directory where **mfa_api.properties** is located. By default, the directory is **/var/ace/conf**.
2. Open **mfa_api.properties**.
3. You can change the following parameters:
   - CONNECT_TIMEOUT. The maximum number of seconds allowed for the agent to connect to the server. The default is 60 seconds.
   - READ_TIMEOUT. The maximum number of seconds allowed to connect to the server and read the response. The READ_TIMEOUT value must equal the sum of the CONNECT_TIMEOUT value and the maximum time allowed for reading the response. The default is 120 seconds.

- MAX_RETRIES. The number of times that the PAM agent tries to connect to Authentication Manager or the Cloud Authentication Service. The default value is 3.
- For the Authentication Manager REST interface Initialize phase, when the PAM agent starts an authentication attempt, the MAX_RETRIES is the number of times that the agent tries to contact the same server before failover to another server. During the Verification phase, when the PAM agent is providing authentication credentials, failover is not supported, and the MAX_RETRIES is the number of times that the agent tries to contact the same server before authentication fails.
- The Cloud Authentication Service does not support failover. For both the Initialize and Verify phases, the MAX_RETRIES is the number of times that the agent tries to contact the same server before authentication fails.

4. Save the file.

Uninstall the RSA Authentication Agent 8.1 for PAM

You can either manually uninstall the PAM agent on individual machines, or you can choose to silently and automatically uninstall multiple copies of the PAM agent.

Before you begin

- Configure the RSA SecurID protected tools to use the standard PAM module provided with your operating system, and not the RSA PAM module. Any active sessions using the RSA PAM modules must be closed before you proceed with the uninstall. You must undo the procedures that you followed in Configuring Tools on page 26.

  Note: If you uninstall the RSA module while there are references to the RSA module in **/etc/pam.d** directory, you will be locked out of your system.

- Verify that you have root permissions on the host.

Uninstall the PAM Agent from One Machine

Perform this task to uninstall one PAM agent.

Procedure

1. Change to the PAM agent home directory. For example, **/opt/pam**.
2. Run the uninstall script. Type:

   ```
   ./uninstall_pam.sh
   ```

3. Verify that the installation directory has been removed. If the directory still exists, you must remove it manually.
4. To verify that the PAM agent was successfully removed, check the **/var/pam_uninstaller/uninstaller.log** file.

Bulk Uninstall the PAM Agent in Silent Mode

Perform this task to uninstall a large number of PAM agents.

Procedure

1. Create a text-based configuration file with the name **unconfig**. The file must contain the following information:

   ```
   y
   y
   y
   ```

   Each y is a response to a prompt:

   - Are you sure that you would like to uninstall the RSA Authentication Agent 8.1.0 [101] for PAM?
   - The RSA Authentication Agent for PAM will be deleted from the <*install_path*> directory. Ok?
   - If you uninstall the RSA module while there are references to the RSA module in the PAM configuration file (file **pam.conf** or inside the directory **pam.d**), you will be locked out of your system. Proceed with uninstall? Ok?
2. Change to the PAM agent home directory. For example, **/opt/pam**.
3. Run the uninstall script. Type:

   ```
   ./uninstall_pam.sh < unconfig
   ```

Appendix B: Critical Configuration Files

Critical Configuration Files

The default PAM agent installation directory is **/opt/pam**, and this can be changed during installation. By default, the **/var/ace** directory includes REST-related libraries and files. This directory location cannot be changed.

In addition to the binaries (**pam_securid.so**, **acetest**, **acestatus**, and **ns_conv_util**), the PAM agent maintains the critical configuration files listed in the following table.

Note: As with all applications, you, the administrator, may need to modify the default file permissions when non-privileged users access the PAM agent.

File	Description
log.properties	PAM agent logging configuration file for the REST protocol. PAM agent uses the library **log4cxx** for REST-mode logging.
mfa_ api.properties	Contains the settings used by the REST protocol for authentication to Authentication Manager and the Cloud Authentication Service.
sdconf.rec	This file is generated by RSA Authentication Manager, and contains configuration information that controls the behavior of the PAM agent. This file permission should be -rw------- root root. This file is only used in UDP mode.
sdopts.rec	This file is used for manual load balancing. It contains a list of IP addresses for Authentication Manager instances. This file permission should be -rw------- root root. This file is only used in UDP mode.
sdstatus.12	This file is generated by the PAM agent authentication API to track the last known status of the Authentication Manager servers. This file permission should be -rw------- root root.
sd_pam.conf	Contains configuration settings that control behavior of the PAM agent. This file permission should be -rw-r--r-- root root.
securid	This file contains a shared secret key used to protect the UDP protocol communication between the local machine and Authentication Manager. The name of this file is derived from the local system's configured protocol name for the port over which the agent communicates with Authentication Manager, usually through the "services" file. This file permission should be -r-------- root root. However, it also depends on the OS Umask setting. The UDP protocol requires this file. This file optional for authentication with the REST protocol.