RSA SECURID® ACCESS
Implementation Guide

One Identity
Safeguard for Privileged Sessions 5.7

Peter Waranowski, RSA Partner Engineering
Last Modified: September 11th 2018

RSA READY

Solution Summary

One Identity Safeguard for Privileged Sessions (SPS) is a solution which can audit and control remote access to servers over several protocols (like SSH, RDP, etc). In these sessions SPS can integrate with RSA SecurID Access using RADIUS to enforce an additional layer of authentication.

RSA SecurID Access Features	One Identity Safeguard for Privileged Sessions 5.7
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	-
SSO	
SAML SSO	-
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	-

Supported Authentication Methods by Integration Point

This section indicates which authentication methods are supported by integration point. The next section (Configuration Summary) contains links to the appropriate configuration sections for each integration point.

One Identity Safeguard for Privileged Sessions integration with RSA Cloud Authentication Service

Authentication Methods	REST	IDR SAML	Cloud SAML	HFED	RADIUS
RSA SecurID	-	-	-	-	✓
LDAP Password	-	-	-	-	✓
Authenticate Approve	-	-	-	-	✓
Authenticate Tokencode	-	-	-	-	✓
Device Biometrics	-	-	-	-	✓
SMS Tokencode	-	-	-	-	✓
Voice Tokencode	-	-	-	-	✓
FIDO Token		-	-	-	

One Identity Safeguard for Privileged Sessions integration with RSA Authentication Manager

Authentication Methods	REST	RADIUS	UDP Agent	TCP Agent
RSA SecurID	-	✓	-	-
AM RBA		-	-	

✓ Supported
- Not supported
n/t Not yet tested or documented, but may be possible

RSA SecurID Access Configuration

RSA Cloud Authentication Service Configuration

RADIUS

To configure RADIUS for Cloud Authentication Service for use with a RADIUS client, you must first configure a RADIUS client in the RSA SecurID Access Console.

Logon to the RSA SecurID Access console and browse to **Authentication Clients** > **RADIUS** > **Add RADIUS Client** and enter the **Name**, **IP Address** and **Shared Secret**. Click **Publish** to push your configuration change to the RADIUS server.

RSA Cloud Authentication RADIUS server listens on port UDP 1812.

RSA Authentication Manager Configuration

RADIUS

To configure your RSA Authentication Manager for use with a RADIUS Agent, you must configure a RADIUS client and a corresponding agent host record in the Authentication Manager Security Console.

The relationship of agent host record to RADIUS client in the Authentication Manager can 1 to 1, 1 to many or 1 to all (global).

RSA Authentication Manager RADIUS server listens on ports UDP 1645 and UDP 1812.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the One Identity Safeguard for Privileged Sessions with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All One Identity Safeguard for Privileged Sessions components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Download the **RSA SecurID plugin** from One Identity Safeguard for Privileged Sessions – Download Software page.

One Identity SPS RADIUS Client Configuration

Complete the steps in this section to integrate with RSA SecurID Access using RADIUS authentication protocol.

Before you begin:

1. Login to One Identity SPS administrative page and navigate to **Basic Settings** > **Plugins**.
2. Browse for the **RSA SecurID plugin** zip file and click **Upload**.
3. Navigate to **Policies** > **AA Plugin Configurations** and select the **RSA SecurID Plugin** from the list.
4. Specify the necessary configuration parameters in the standard INI config file format.

The **[radius]** section has the following options:

- **server**: you can specify the name or the IP address of the RSA server. You can provide more than one server separated with comma. In this case if the authentication times out then it tries to access the next server on the list
- **port**: the UDP port where the RSA server should be accessed (default: 1812)
- **nas_identifier**: this identifier is sent in the authentication request to the RSA server
- **auth_type**: the authentication type used in RADIUS (pap, chap)

The **[plugin]** section has the following options:

- **loglevel**: how verbose the plugin should be
- **timeout**: the maximum length of waiting for an answer from the RSA server in second
- **retries**: In case of timeout this specifies how many times should be retried the same server before the authentication fails

Example:

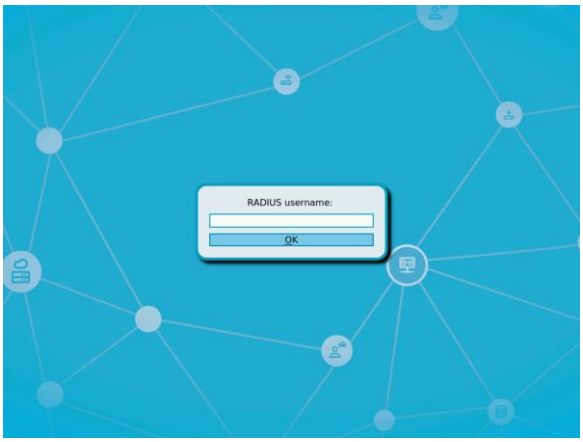
```
[radius]
server=pe081.pe-lab.com,pe082.pe-lab.com,pe083.pe-lab.com
port=1812
nas_identifier=psm.oneditentity.com
auth_type=pap

[plugin]
loglevel=debug
timeout=60
retries=5
```

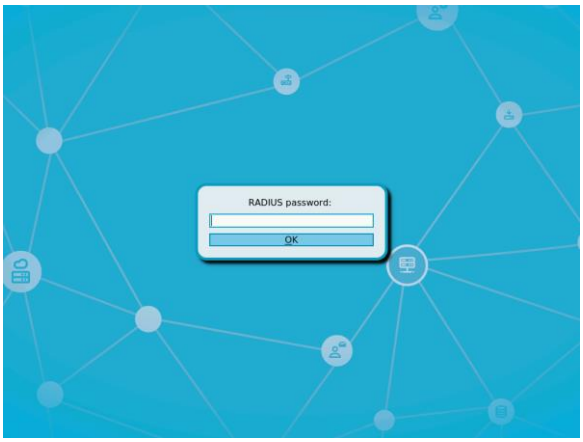
One Identity Connection Policy Configuration

1. Navigate to the Connection policy where you want to use the plugin (e.g. RDP Control > Connections), select the plugin configuration instance to use in the **AA plugin** field and click **OK**.
2. If the plugin sets or overrides the gateway username of the connection, configure a Usermapping policy and use it in the Connection policy.
3. Verify that the configuration works properly: try to establish a test connection.

Login Screenshots

Login screen:





User-defined New PIN:

System-generated New PIN:

Certification Checklist for RSA SecurID Access

Certification Environment Details:

RSA Authentication Manager 8.2 SP1, Virtual Appliance

One Identity Safeguard for Privileged Sessions 5.7.0

RSA Cloud Authentication Service

Date Tested: June 27th, 2018

Authentication Method	REST Client	RADIUS Client
RSA SecurID	-	✓
LDAP Password	-	✓
Authenticate Approve	-	✓
Authenticate Tokencode	-	✓
Device Biometrics	-	✓
SMS Tokencode	-	✓
Voice Tokencode	-	✓
FIDO Token	-	

RSA Authentication Manager

Date Tested: June 18th, 2018

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	-	-	-	✓
RSA SecurID Software Token Automation	-	-	-	-
On Demand Authentication	-	-	-	✓
Risk-Based Authentication		-		-

✓ = Passed, **X** = Failed, **-** = N/A