

RSA SECURID[®] ACCESS
PAM Agent
Implementation Guide

IBM Virtual I/O Server

Last Modified: September 12th, 2016



Solution Summary

The Virtual I/O Server (VIOS) facilitates the sharing of physical I/O resources among client logical partitions within the server. VIOS provides virtual SCSI target, virtual fibre channel, Shared Ethernet Adapter, PowerVM Active Memory Sharing and PowerVM Client Partition Mobility capability to client logical partitions within the system. As a result, client logical partitions can share SCSI devices, fibre channel adapters and Ethernet adapters. With VIOS, you can expand the amount of memory available to logical partitions by using paging space devices and move AIX and Linux logical partitions from one system to another.

The Virtual I/O Server is included in all PowerVM Editions.


The RSA Authentication Agent 7.0 for PAM enables RSA SecurID authentication on UNIX systems, using either standard or OpenSSH connection tools. The agent uses RSA-customized shared libraries, and it supports several forms of RSA SecurID authenticators for access to VIOS.

RSA SecurID Access Supported Features	
IBM Virtual I/O Server	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	N/A
RSA SecurID Authentication via RADIUS Protocol	N/A
RSA SecurID Authentication via IPv6	N/A
On-Demand Authentication via Native SecurID UDP Protocol	Yes
Risk-Based Authentication	N/A
RSA Authentication Manager Replica Support	Yes
RSA SecurID Software Token Automation	N/A
RSA SecurID SD800 Token Automation	N/A
RSA SecurID Protection of Administrative Interface	N/A

Partner Product Configuration

Before You Begin

This section provides instructions for enabling the RSA Authentication Agent for PAM on IBM VIOS. You should have working knowledge VIOS and RSA Authentication Manager as well as access to the appropriate end-user and administrative documentation. Ensure that both products are running properly prior to configuring the integration.

 **Note:** This document is not intended to suggest optimal installations or configurations.

Configuring the RSA PAM Authentication Agent on IBM VIOS

! > Important: The **System Requirements** section in the installation and configuration guide referenced below does not list support for IBM VIOS. However, the platform is supported.

Please refer to the [RSA Authentication Agent 7.0 for PAM—Installation and Configuration Guide for AIX](#). It contains complete instructions for installing the RSA PAM agent and enabling RSA SecurID for the following clients:

- login (console)
- su
- ssh
- sudo
- rlogin
- telnet
- ftp¹

! > Important: The *ftp* client only supports RSA SecurID passcode authentication. It doesn't support new PIN mode, next tokencode mode or on demand authentication. See the [Known Issues](#) section or the [RSA Authentication Agent 7.0 for PAM—Installation and Configuration Guide for AIX](#) for more information.

¹ The ftp client doesn't support New PIN Mode, Next Tokencode Mode or On-Demand Authentication.

Certification Checklist for RSA SecurID Access

Date Tested: September 1st, 2016

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.2	Virtual Appliance
RSA Authentication Agent	7.0 PAM Auth Agent for AIX	IBM VIOS
console login client	IBM VIOS	IBM VIOS
rlogin client	N/A	IBM VIOS
su client	N/A	IBM VIOS
ssh client	N/A	IBM VIOS
sudo client	N/A	IBM VIOS
telnet client	N/A	IBM VIOS
ftp client ²	N/A	IBM VIOS

! Important: The checklist below excludes ftp test results. See the [Known Issues](#) section for details.

RSA SecurID Authentication

Mandatory Functionality	Native UDP	Native TCP	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	✓	N/A	N/A
System Generated PIN	✓	N/A	N/A
User Defined (4-8 Alphanumeric)	✓	N/A	N/A
User Defined (5-7 Numeric)	✓	N/A	N/A
Deny 4 and 8 Digit PIN	✓	N/A	N/A
Deny Alphanumeric PIN	✓	N/A	N/A
Deny PIN Reuse	✓	N/A	N/A
Passcode			
16 Digit Passcode	✓	N/A	N/A
4 Digit Fixed Passcode	✓	N/A	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	N/A	N/A
On-Demand Authentication (ODA)			
On-Demand Authentication	✓	N/A	N/A
On-Demand New PIN	✓	N/A	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	N/A	N/A
No RSA Authentication Manager	✓	N/A	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

² The ftp client supports standard RSA SecurID authentication. It doesn't support New PIN Mode, Next Tokencode Mode or ODA.



Known Issues

The ftp client doesn't support RSA SecurID New PIN Mode, Next Tokencode Mode or On-Demand Authentication. The client uses the operating system's standard password authentication prompts. It doesn't display RSA SecurID-specific authentication prompts or error messages during the login process. For more information, see the [RSA Authentication Agent 7.0 for PAM—Installation and Configuration Guide for AIX](#).