



RSA SecurID Ready Implementation Guide

Last Modified: February 28, 2005

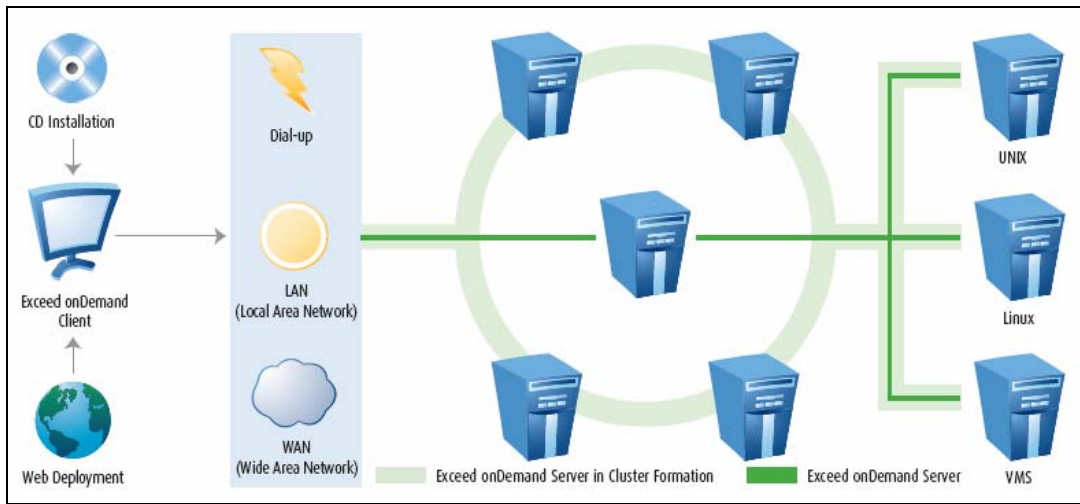
Partner Information

Product Information	
Partner Name	Hummingbird Ltd
Web Site	http://connectivity.hummingbird.com
Product Name	Exceed onDemand®
Version & Platform	5
Product Description	Exceed onDemand® is the most powerful and complete ultra-thin, server-based PC X server in the market sharing the same roots as the award-winning PC X server – Hummingbird Exceed®. Exceed onDemand offers most advanced web deployment tools and the support for the most popular security protocols, such as Secure Shell and RSA SecurID®. Exceed onDemand securely connects you to 2D and 3D X applications over any type of network connection making it a suitable solution for mobile workers. Exceed onDemand delivers unprecedented value in scalability, manageability, security and productivity providing you with the mobile functionality and performance you expect and desire.
Product Category	Remote Access



Solution Summary

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking *	Yes
RSA Authentication Manager Replica Support *	Yes
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	All Users
RSA Authentication Agent Host Type	UNIX
RSA SecurID User Specification	Designated Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	N/A
Use of Cached Domain Credentials	No
* = Mandatory Function when using Native SecurID Protocols	



Product Requirements

Partner Product Requirements: Exceed onDemand Server		
CPU make	Sun SPARC	Intel/AMD x86
Memory	256MB+	256MB+
HD space	140MB	140MB

Component Name: Exceed onDemand Clients	
CPU make	Intel/AMD x86
Memory	128MB
HD space	10MB

Operating System: Exceed onDemand Server	
Platform	Required Patches
Sun SPARC Solaris	2.6 or higher
Red Hat Linux	7.3 or higher

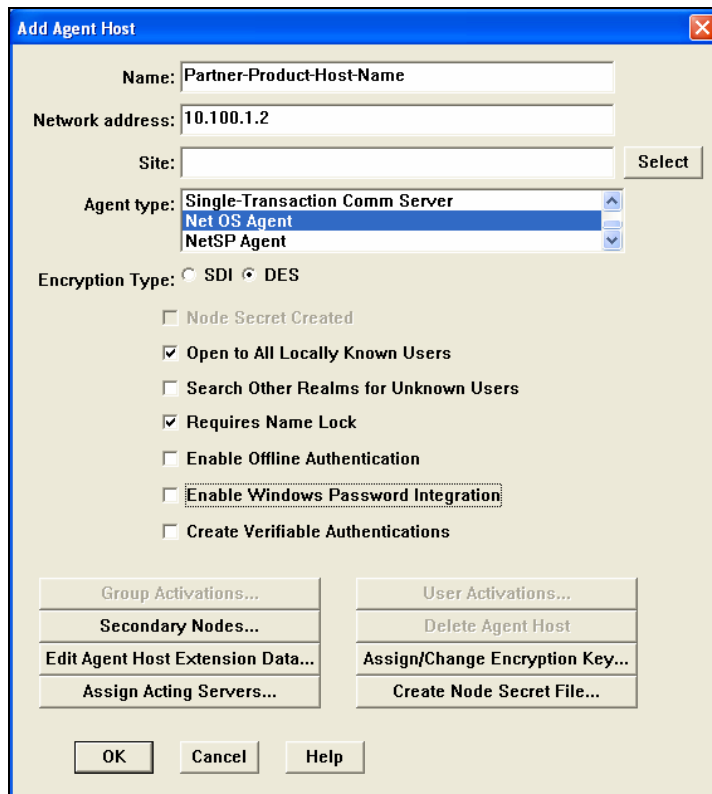
Operating System: Exceed onDemand Clients	
Platform	Required Patches
Windows 2000	
Windows XP Professional	
Windows Server 2003	

RSA Authentication Manager Configuration

Perform the following steps to set up the Exceed onDemand Server as an Agent Host within the RSA Authentication Manager's database.

On the RSA Authentication Manager computer, go to Start > Programs > RSA ACE Server, and then Database Administration - Host Mode.

1. On the Agent Host menu, choose Add Agent Host.



- In Name, type the hostname of the Exceed onDemand Server.
- In Network address, type the IP address of the Exceed onDemand Server.*
- For Agent Type, select UNIX.
- Under Secondary Nodes, define all hostname/IP addresses that resolve to the Exceed onDemand Server. (IF NEEDED)

* It is important that all hostname and IP addresses resolve to each other. Please reference the RSA Authentication Manager documentation for detailed information on this and other configuration parameters within this screen. Subsequently, you can also select the 'Help' button at the bottom of the screen.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. 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 vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Installation and configuration of RSA/ACE Agent for PAM is outlined in the RSA product manual and README.

Integration Overview

In order to complete the integration with Exceed onDemand Server, please follow the steps listed below.

- Installation of the RSA SecurID ACE/Agent 5.0 for PAM
- Configure Exceed onDemand for RSA SecurID Authentication
- Examples of Platform Specific Configuration

Installation of the RSA SecurID ACE/Agent 5.0 for PAM

In order to provide the Exceed onDemand server with the necessary libraries, the RSA SecurID ACE/Agent 5.0 for PAM must be installed on the UNIX / Linux host.

Note: For information regarding supported platforms for the RSA SecurID Agent, please refer to the RSA Security product documentation included within the RSA SecurID Agent distribution.

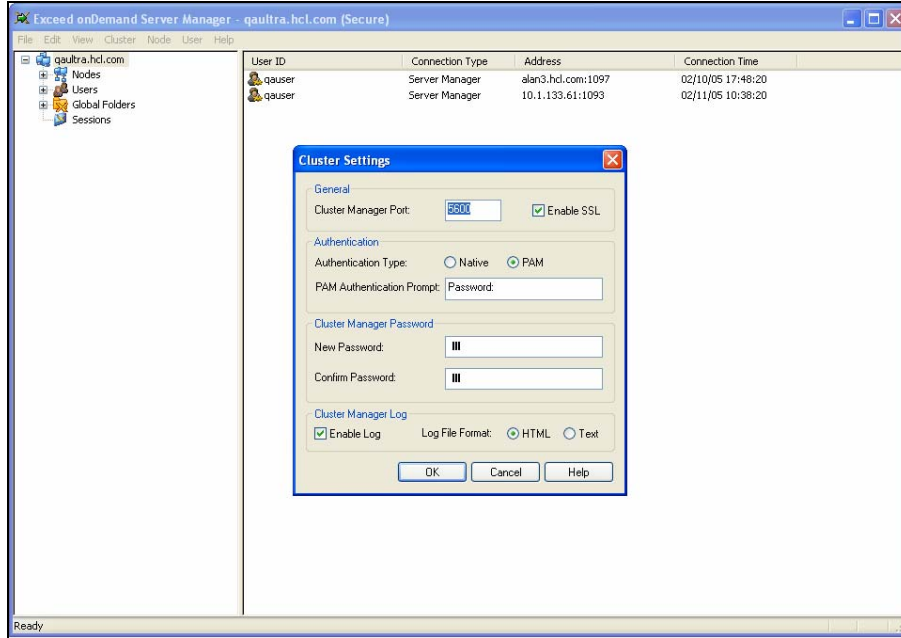
To complete the installation of the RSA SecurID Agent, please refer to procedures in the product documentation for your chosen platform.

When installing the Agent software, it is important to know that the Node Secret will be located in the same directory as the sdconf.rec file. Be sure that the user whom is responsible for installation and execution of the Exceed onDemand has the appropriate read permissions for these files.

Configure Exceed onDemand for RSA SecurID Authentication

Follow these five steps to configure Exceed onDemand Server to authenticate users through RSA ACE/Agent for PAM:

1. Connect to Exceed onDemand Server using Exceed onDemand Server Manager.
2. Right click on the root node of the tree on the left panel and select the **Cluster Settings** option
3. Switch the **Authentication Type:** from **Native** to **PAM**
4. Change the PAM **Authentication Prompt** from “Password” to “Enter PASSCODE:”
5. Click OK button and restart Cluster Manager.



Follow the instruction supplied by the vendor to add a new service for Exceed onDemand authentication, there will be different steps based on the chosen platform of your Exceed onDemand Server.

Examples of Platform Specific Configuration

Please review the information below as an example of settings for the Solaris and Linux platforms. Additional information is available in the RSA SecurID ACE/Agent 5.0 for PAM product documentation.

Configuration example for Red Hat 7.3 / Enterprise Advanced Server 3.0

1. Change to the `/etc/pam.d` directory.
2. Open the `pam.conf` file with a text editor.
3. Verify the path to your `'pam_secuid.so'` file.
4. To enable Exceed onDemand, add the following entry within the Authentication Management section in order to add reference to the RSA SecurID ACE/Agent PAM module.

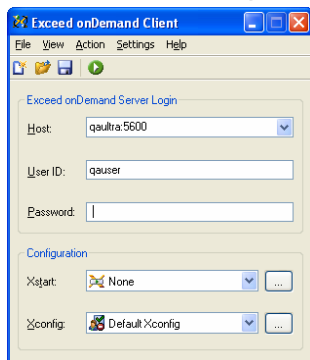
```
exceedondemand      auth required      <path>/pam_secuid.so
```

Configuration example for Solaris 8 / 9

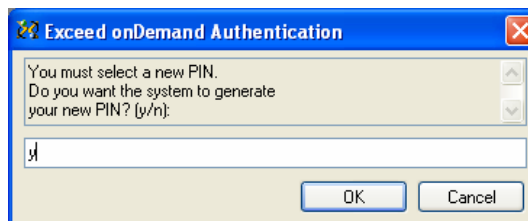
1. Change to the `/etc` directory.
2. Open the file `pam.conf` with a text editor.
3. Verify the path to your `'pam_secuid.so'` file.
4. To enable Exceed onDemand, add the following entry within the Authentication Management section in order to add reference to the RSA SecurID ACE/Agent PAM module.

```
exceedondemand      auth required      <path>/pam_secuid.so
```

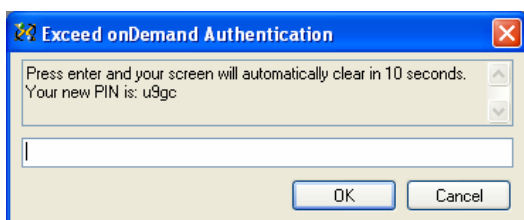
Example of SecurID login



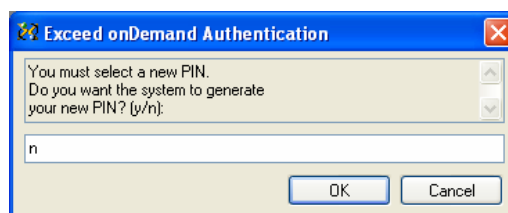
Connect using Exceed onDemand Client using the PASSCODE as the password



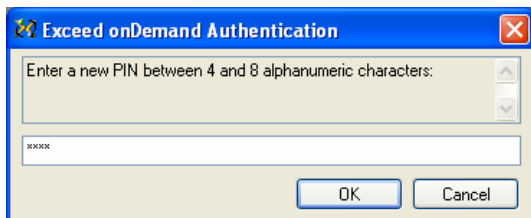
Step 2a: Allow system to generate PIN



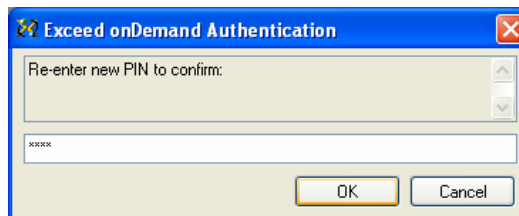
Step 2b: System generated a PIN



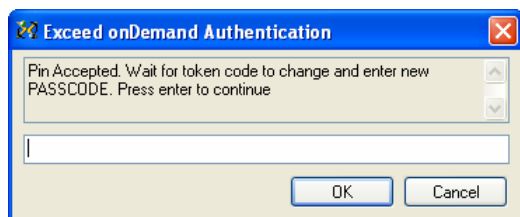
Step 2c : Allow user to generate PIN



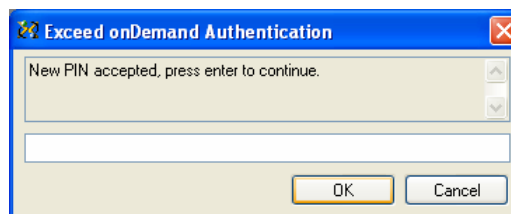
Step 2d: User created a PIN



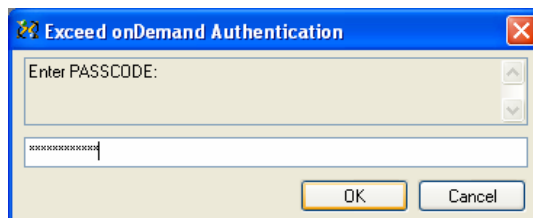
Step 3: PIN accepted



Step 4: PIN accepted



Step 5: New PIN Accepted



Step 6: Enter PASSCODE

Certification Checklist

Date Tested: February 8, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.0	Windows 2003 Server
RSA Authentication Agent	5.0 for PAM	Solaris 8 (SPARC)
Exceed onDemand Server	5.0	Solaris 8 (SPARC)
Exceed onDemand Client	5.0	Windows XP Professional (SP1)

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input type="checkbox"/> N/A
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Domain Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Domain Credential	<input type="checkbox"/> N/A	Set Domain Credential	<input type="checkbox"/>
Retrieve Domain Credential	<input type="checkbox"/> N/A	Retrieve Domain Credential	<input type="checkbox"/>

PAR / EF

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