RSA SecurID Ready Implementation Guide

Last Modified: April 19, 2006

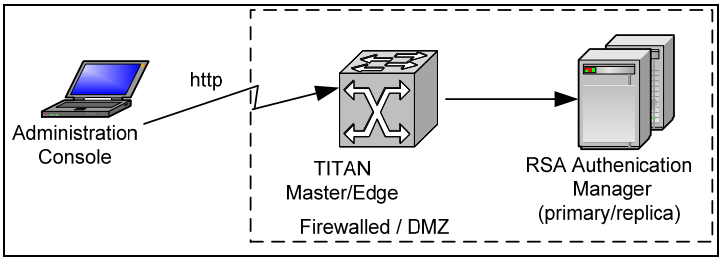
Partner Information

Product Information	
Partner Name	NetNumber Inc.
Web Site	www.netnumber.com
Product Name	TITAN – Transactional IP Telephony Addressing & Numbering
Version & Platform	5.1
Product Description	The NetNumber™ TITAN server represents the core of a communications service providers next-generation addressing infrastructure and enables the service provider to offer a variety of traditional and next generation intelligent network addressing services such as Number-Portability, Global Title Translation, SMS/MMS/IMS/VOIP routing, and Calling Name Presentation over a variety of C7/SS7 and IP protocols including AIN 0.2, PCS 1900, IS41, MAP, SCCP, as well as, SIP, ENUM/DNS and SOAP/XML.
Product Category	Networks and Communications

Solution Summary

The purpose of this guide is to show an administrator how to configure the NetNumber TITAN application to use RSA SecurID to authenticate users of the web-based TITAN Administration Console. The RSA SecurID Agent support is seamlessly integrated into the TITAN application providing a simple deployment and configuration experience. The TITAN Administration Console is used to configure the settings that are necessary for the TITAN application to communicate with the RSA Authentication Manager.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	/opt/titan/sys/rsa/secured
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and SD800 Automation	No
Use of Cached Domain Credentials	No



Product Requirements

Partner Product Requirements: NetNumber TITAN Server	
CPU	See the TITAN Installation Guide
Memory	See the TITAN Installation Guide
Storage	See the TITAN Installation Guide

Operating System	
Platform	**Required Patches**
Red Hat Enterprise Linux	RHEL 4
Solaris 10	Core OS Software Group

Additional Software Requirements:

The Java Runtime Environment, JRE, is bundled with the TITAN application distribution ensuring that the correct version is always available. Also bundled with TITAN is the MySQL database software, although the customer has a choice of databases that TITAN can interface with.

Additional Software Requirements	
Application	**Additional Patches**
Internet Explorer	5.0 or greater

Agent Host Configuration

To facilitate communication between the NetNumber TITAN and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the NetNumber TITAN server within its database and contains information about communication and encryption. Both TITAN Master and Edge systems can be configured to be RSA Agent Hosts in order to support user authentication via RSA SecurID.

To create the Agent Host record, you will need the following information.

- Hostname of platform where TITAN application is running
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the TITAN server as a Communication Server Agent. This setting is used by the RSA Authentication Manager to determine how communication with the NetNumber TITAN server will occur.

> **Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the NetNumber TITAN application 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.

Ensure that the TITAN platform has network access to the RSA Authentication Manager server by testing with ping, telnet, etc.

Configure the TITAN Server

The following steps should be taken to configure the TITAN server and test the authentication of a user using RSA SecurID.

1. Copy the RSA SecurID Agent configuration file to the TITAN server
2. Select RSA SecurID as the TITAN authentication type
3. Create a TITAN administrator
4. Test authentication of the administrator

The following sections describe each of the four steps. For detailed information about any of these steps, please see the NetNumber TITAN Administration Guide.

Copy the RSA SecurID Agent configuration file to the TITAN server

Once the Agent Host configuration is complete (see previous section, Agent Host Configuration), you must save the configuration to a file named sdconf.rec using the RSA Authentication Manager Administration interface and then transfer the file to the TITAN platform using FTP, SFTP, etc. The sdconf.rec file must be placed in the following TITAN application directory (where <root_dir> is the directory that the TITAN application is installed):

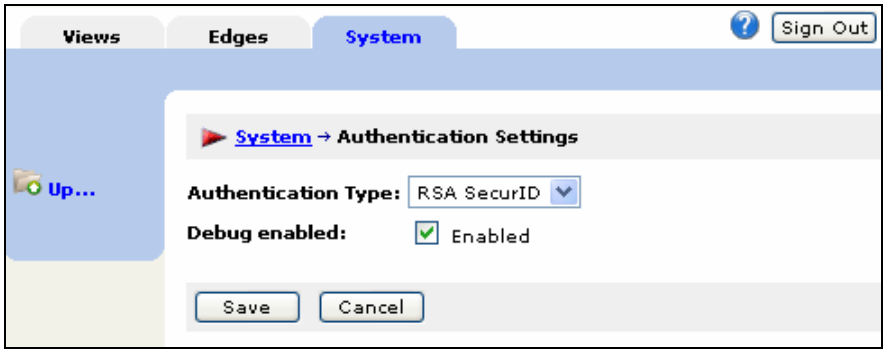
```
<root_dir>/sys/rsa/
```

The file permissions on the sdconf.rec file should be the same as those given to the TITAN application during installation/setup.

Select RSA SecurID as the TITAN Authentication Type

Login to the web-based TITAN Administration Console as the root administrative user that was created during TITAN application setup. On the main page, select the *System* tab and then click on the *Authentication* link. The Authentication configuration page will display the current, system-wide authentication type followed by the configuration settings for that type. The default authentication type "Local" is displayed initially. Push the **Edit** button and, from the drop down menu, select RSA SecurID as the Authentication Type. Push the **Save** button.

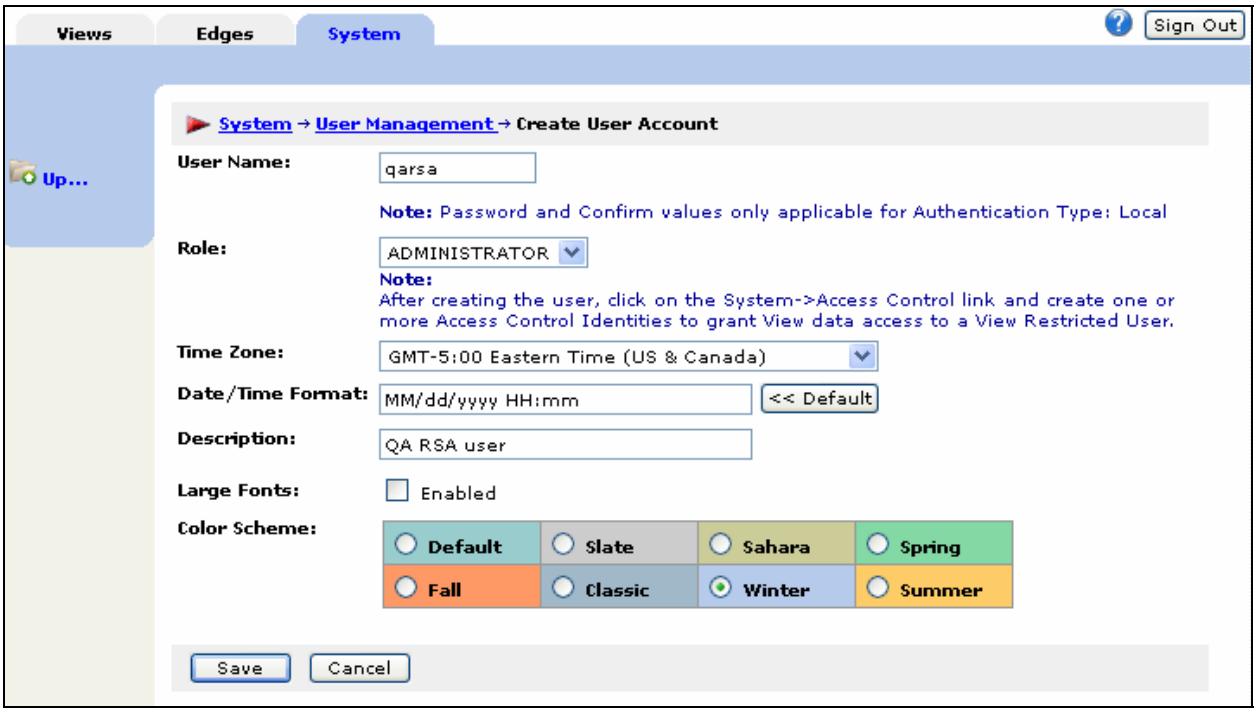
The only configurable setting for the RSA SecurID type is enabling/disabling debug. We recommend that debug be disabled on all production systems. The following figure shows the Authentication configuration web page with RSA SecurID as the selected value:



Create a TITAN Administrator

There must be a user configured in both the RSA Authentication Manager and in the TITAN server who has been given the same login user name. Use the RSA Authentication Manager Administration interface to create an RSA SecurID user. The following examples use the user name “qarsa”. See the RSA documentation for detailed information on how to do this.

To create a user account in the TITAN server for “qarsa”, select the System tab and then select the User Management link. You are presented with the User Management configuration page. Push the **Create** button to create a new user account. The following page is displayed:



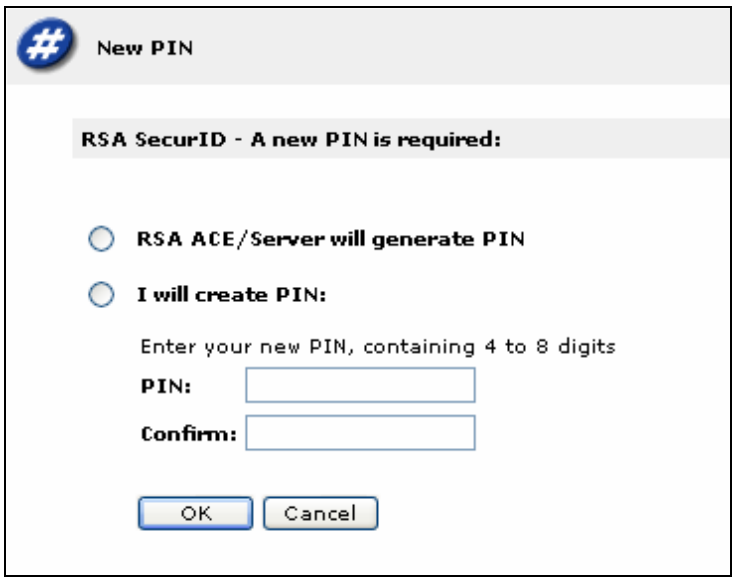
In the User Name text field, type in “qarsa” (or your user’s login name). Modify any other settings as desired for user preferences. Push the **Save** button. Now logout by pushing the **Sign Out** button.

Test Authentication of the Administrator

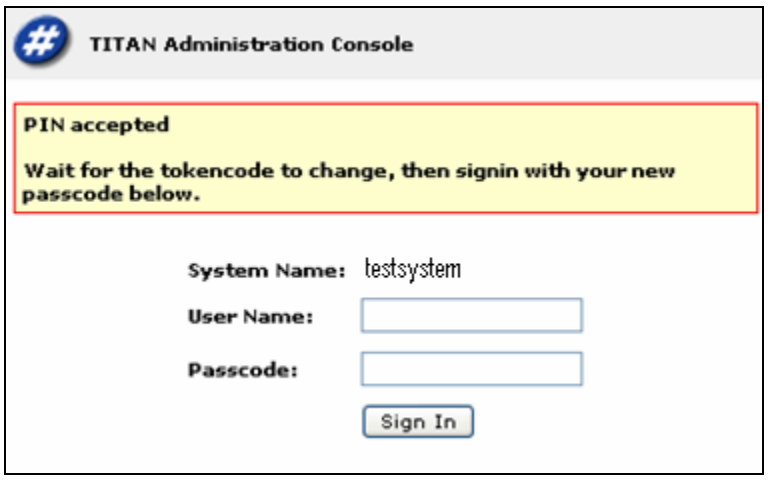
Test that RSA SecurID authentication works by attempting to login to the TITAN application with the "qarsa" login name. Enter "qarsa" in the User Name text field and enter the tokencode displayed on their RSA SecurID authenticator (ie. keyfob) in the Passcode text field and push the **Sign In** button. After the first login, the user will enter their PIN followed by their tokencode into the Passcode field. A new user does not yet have a PIN until after they go through New PIN Mode, which is described below. The following shows the main TITAN Administration console login screen:

If the user name and tokencode are accepted by the RSA Authentication Server, the user is put into New PIN mode which will walk them through the process of getting a new PIN. Depending on the configuration of your RSA Authentication Server, the user will either be:

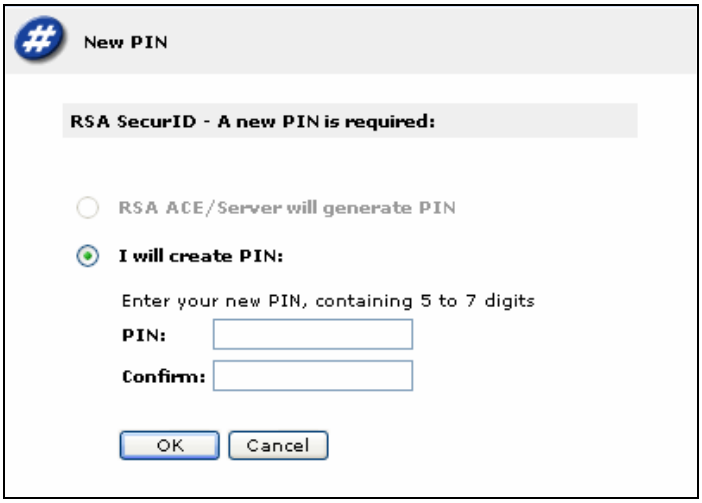
- prompted to select their own PIN
- given a system generated PIN
- or they will have to choose between the two methods of getting a new PIN, as shown in the following screen:

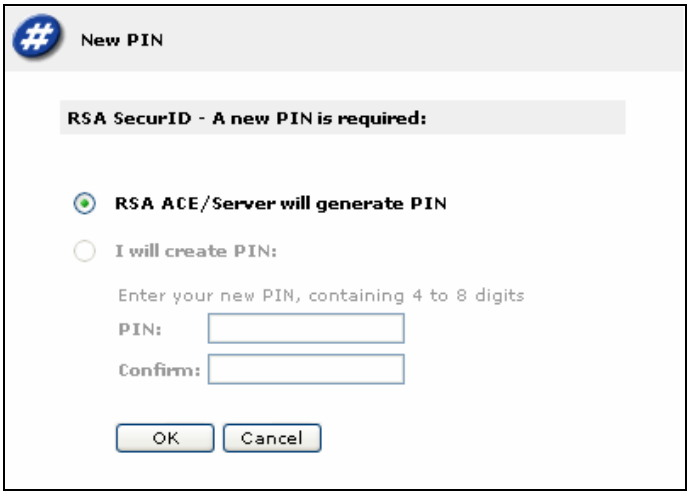


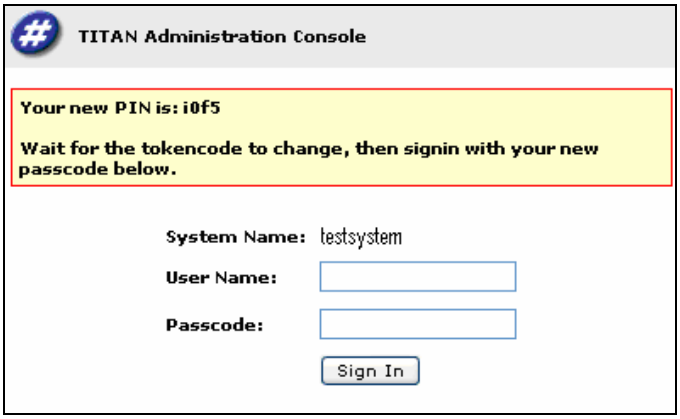
The length of the PIN is determined by the configuration settings on the RSA Authentication Manager. In the above screen, the user should make a selection by clicking on the desired button, enter a PIN if desired in the PIN and Confirm fields, and push the **Ok** button. If the PIN is valid, the following screen is displayed instructing the user to wait for the token code to change and then signing in with their new passcode (PIN + tokencode).



The screens for the other two New PIN options are shown below. The first is when the user is required to choose their PIN. The second is when the system generates the PIN for the user. Again, the New PIN Mode behavior is determined by the settings in the RSA Authentication Manager and can not be set in the TITAN application.

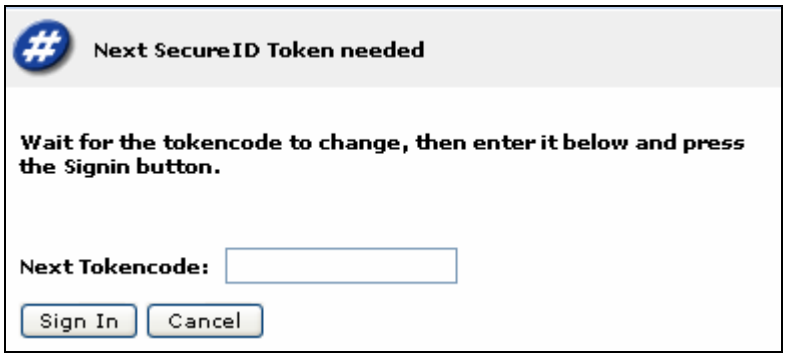






Next Tokencode Mode

If the user enters an incorrect passcode three times, the RSA Authentication Manager puts the user into "Next Tokencode Mode". This scenario exists to ensure that the keyfob has not been stolen/lost and that someone else is not trying to guess the PIN + tokencode. If the real user then enters a correct PIN + tokencode (passcode), the following screen is displayed:



The user should wait for the tokencode to change, enter the new tokencode in the Next Tokencode text field and then push the **Sign In** button. If an incorrect tokencode is entered, then the user is denied access. The next time the user tries to sign in, the user will again be prompted for the next tokencode.

Certification Checklist

Date Tested: April 17, 2006

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Red Hat Enterprise Linux 4
RSA Authentication Agent	5.3	Red Hat Enterprise Linux 4
NetNumber TITAN	5.1	Red Hat Enterprise Linux 4

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
PASSCODE			
16 Digit PASSCODE	✓	16 Digit PASSCODE	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SD800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Domain Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Domain Credential	N/A	Set Domain Credential	
Retrieve Domain Credential	N/A	Retrieve Domain Credential	

BSD / PAR

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