RSA Ready Implementation Guide for

RSA SecurID

GlobalSCAPE EFT Server 7.3

FAL, RSA Partner Engineering
Last Modified: 5/19/2016

Solution Summary

GlobalSCAPE Enhanced File Transfer (EFT) server can be configured to use RSA Authentication Manager as an authentication source. The EFT server passes user login information to and from the EFT user login page and the RSA Authentication Manager Server. When the RSA Authentication Manager server authenticates the user, the user is granted access to the EFT server resources.

GlobalSCAPE EFT server can be configured to communicate with RSA Authentication Manager via native SecurID protocol or RADIUS protocol

RSA Authentication Manager supported features <Partner Product Name and version>	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

Agent Host Configuration

To facilitate communication between the EFT Server 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 EFT Server and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Important: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

> **Important: The RSA agent name is specified in the rsa_api.properties file.**

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with EFT Server will occur.

If EFT Server will be communicating with RSA Authentication Manager via RADIUS, then a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

> **Important: The RADIUS client's hostname must resolve to the IP address specified.**

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

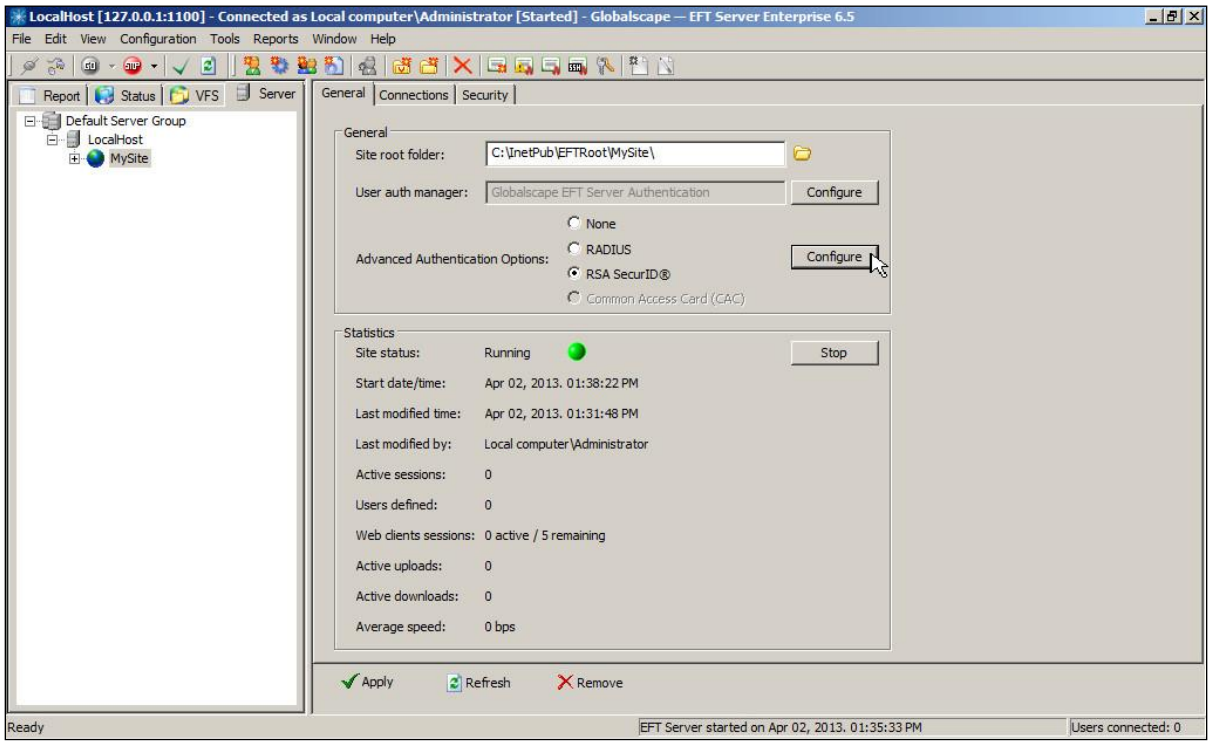
This section provides instructions for configuring the EFT Server with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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.

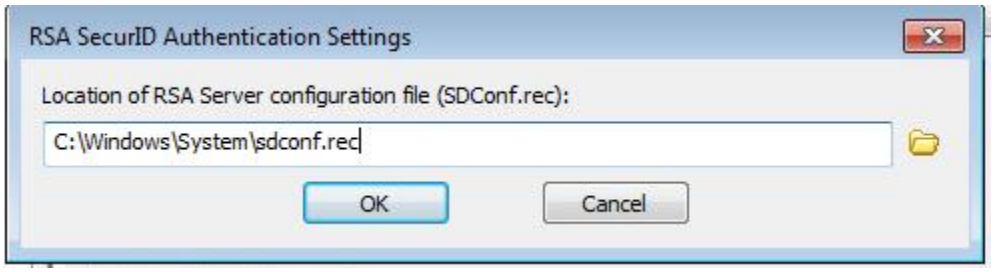
All EFT Server components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

GlobalSCAPE EFT Server Configuration

1. Use the RSA Security Console to generate the sdconf.rec configuration file. Copy the file to a location on the EFT server (typically %windir%\system).
2. Log in to the EFT Server Administrator console and browse to your **Server Group** > **Host** > **Site**.
3. Copy the Sdconf.rec file to the c:\windows\system folder
4. Select **Enable RSA SecurID support** and click **Configure**.



5. Browse from the ETF GUI to the location of RSA Server configuration file and click **OK**.



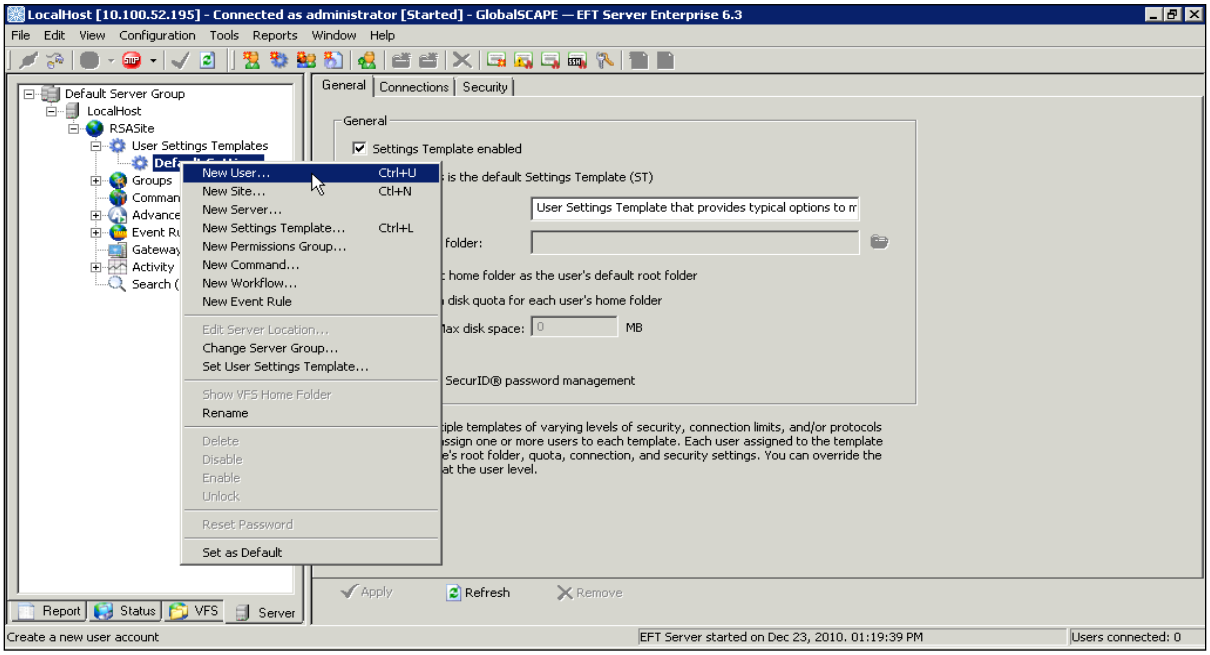
! Important: In this step you are setting the path where RSA SecurID files will reside. Node secret and sdstatus.12 files will be generated at this location. If the Sdconf.rec file does not appear move it to a different folder.

6. Click **Apply** to apply your changes.

7. Click **Yes** to restart the site.

Browse to your **Server Group** > **Host** > **Site** > **User Settings Templates**.

8. Right click **Default Settings** and click **New User**.



9. Mark the **Enable RSA SecurID** checkbox, enter a **Username** and click **Next** to continue.

Note: The new username must correspond to a username in the RSA Authentication Manager server's database.

10. Make appropriate changes and/or click Next to continue.

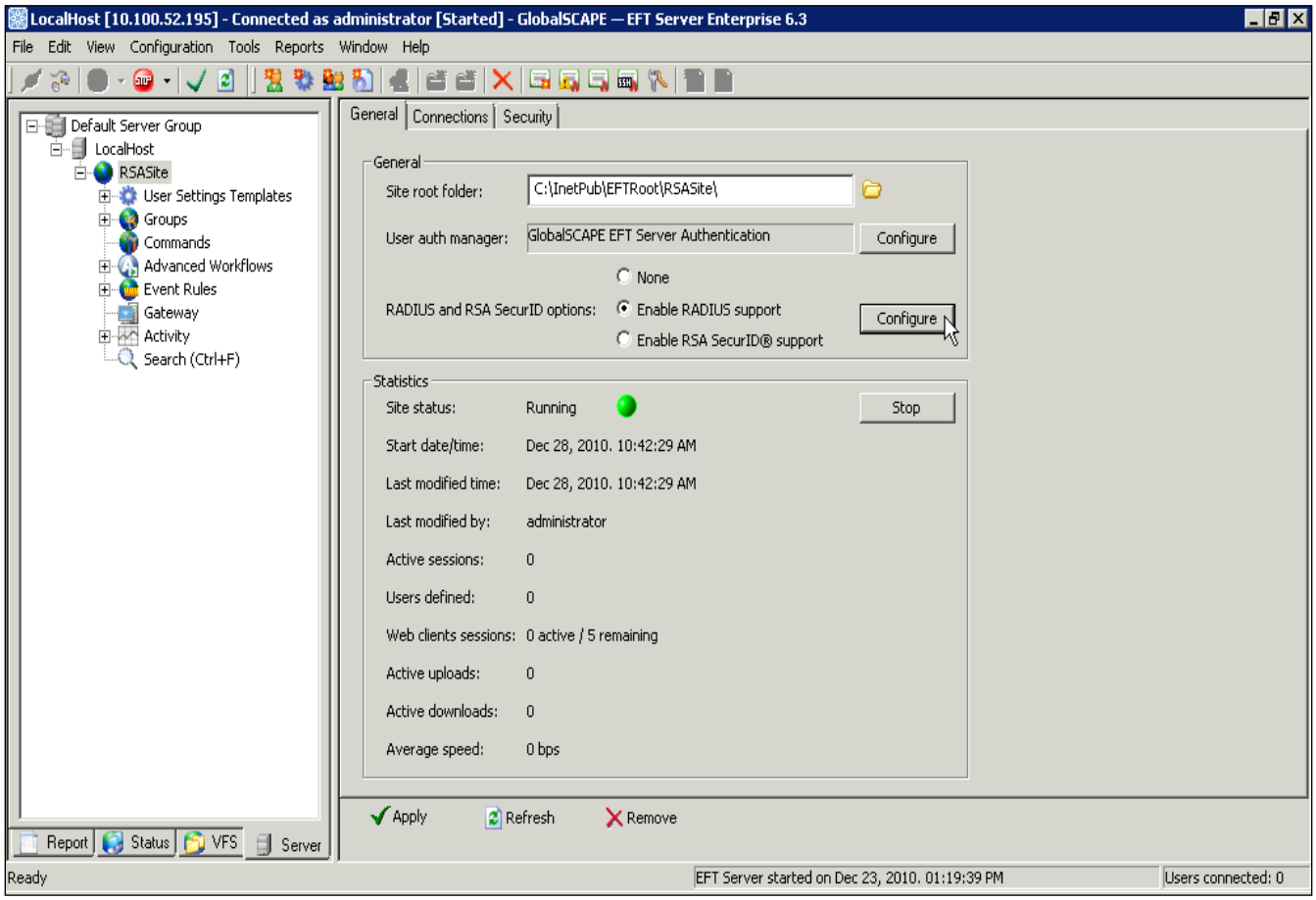
11. Make appropriate changes and/or click **Finish** to complete the wizard.

The GlobalSCAPE Enhanced File Transfer (EFT) server is now configured for RSA SecurID authentication via Native SecurID protocol.

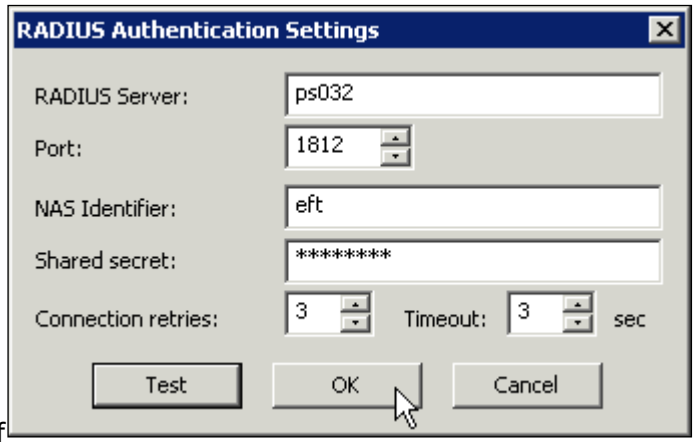
Configure GlobalSCAPE EFT server for RSA SecurID authentication via RADIUS protocol

Note: This is optional and not the typical configuration. SecurID is the preferred typical integration.

1. Log in to the EFT Server Administrator console and browse to your **Server Group** > **Host** > **Site**.
2. Select **Enable RADIUS support** and click **Configure**.



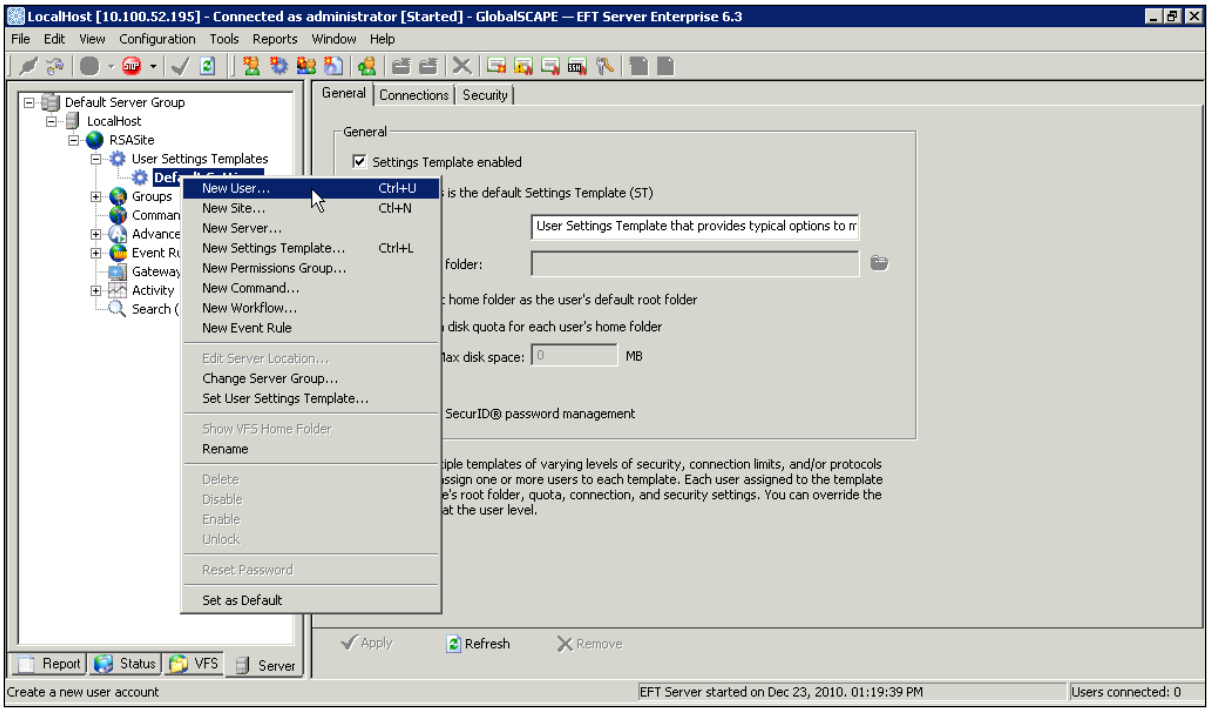
3. Enter the RADIUS Authentication Settings and click **OK**.

etf 

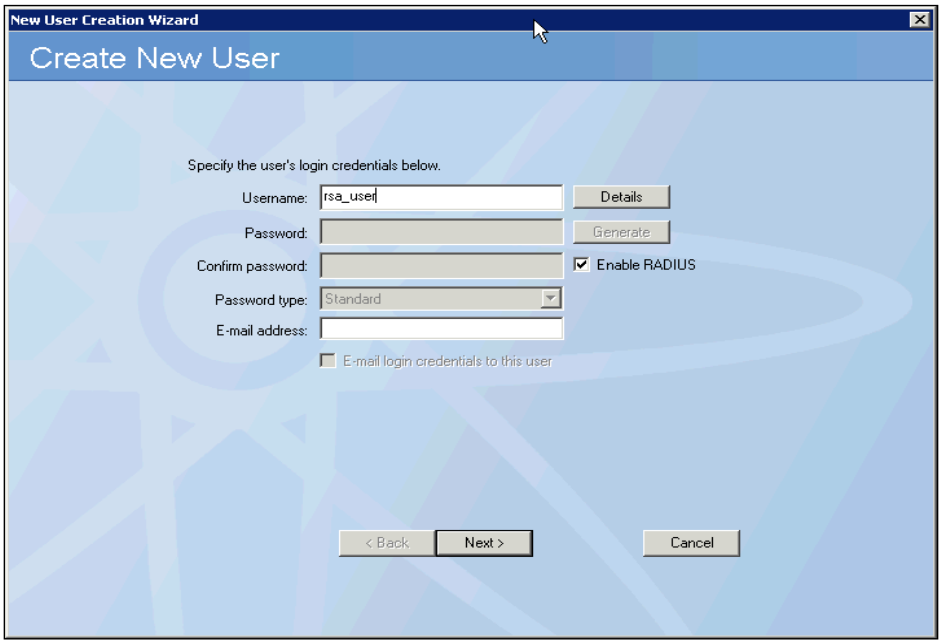
4. Click **Apply** to apply your changes.

5. Click **Yes** to restart the site.

6. Browse to your **Server Group** > **Host** > **Site** > **User Settings Templates**.
7. Right click **Default Settings** and click **New User**.

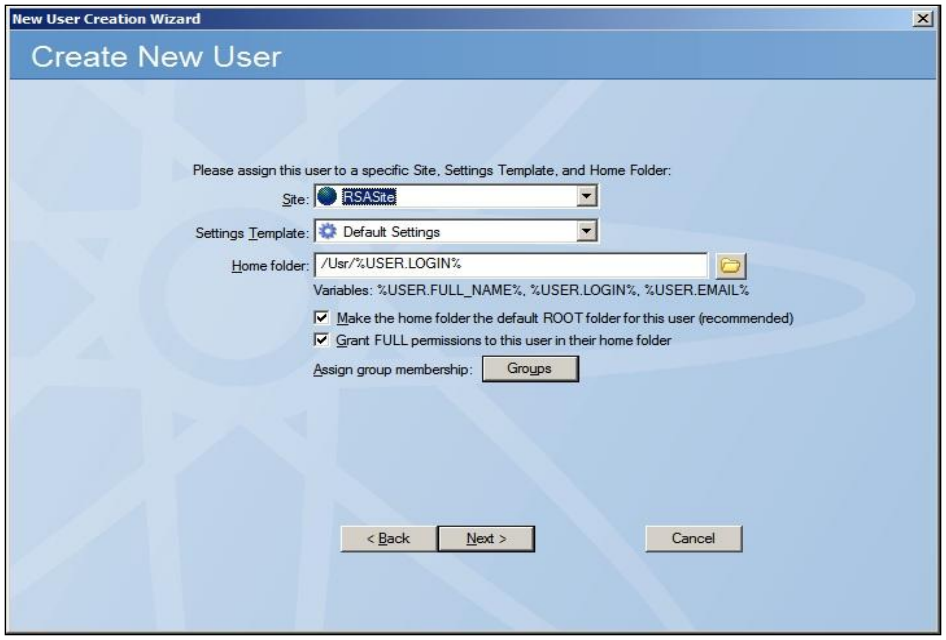

LocalHost [10.100.52.195] - Connected as administrator [Started] - GlobalSCAPE — EFT Server Enterprise 6.3
File Edit View Configuration Tools Reports Window Help
Default Server Group
LocalHost
RSASite
User Settings Templates
Groups
Advance
Gateway
Activity
Search
New User... Ctrl+U
New Site... Ctrl+N
New Server...
New Settings Template... Ctrl+L
New Permissions Group...
New Command...
New Workflow...
New Event Rule
Edit Server Location...
Change Server Group...
Set User Settings Template...
Show VFS Home Folder
Rename
Delete
Disable
Enable
Unlock
Reset Password
Set as Default
General
Connections
Security
General
Settings Template enabled
is the default Settings Template (ST)
User Settings Template that provides typical options to m
folder:
home folder as the user's default root folder
disk quota for each user's home folder
lax disk space: 0 MB
SecurID® password management
iple templates of varying levels of security, connection limits, and/or protocols
ssign one or more users to each template. Each user assigned to the template
e's root folder, quota, connection, and security settings. You can override the
at the user level.
Apply
Refresh
Remove
Report
Status
VFS
Server
Create a new user account
EFT Server started on Dec 23, 2010. 01:19:39 PM
Users connected: 0

8. Mark the **Enable RADIUS** checkbox, enter a **Username** and click **Next** to continue.



Note: The new username must correspond to a username in the RSA Authentication Manager server's database.

9. Make appropriate changes and/or click **Next** to continue.



10. Make appropriate changes and/or click **Finish** to complete the wizard.

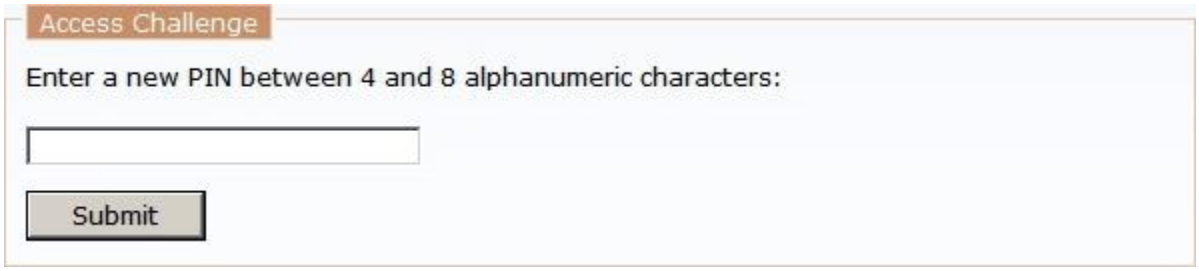
The GlobalSCAPE Enhanced File Transfer (EFT) server is now configured for RSA SecurID authentication via RADIUS protocol.

RSA SecurID Login Screens

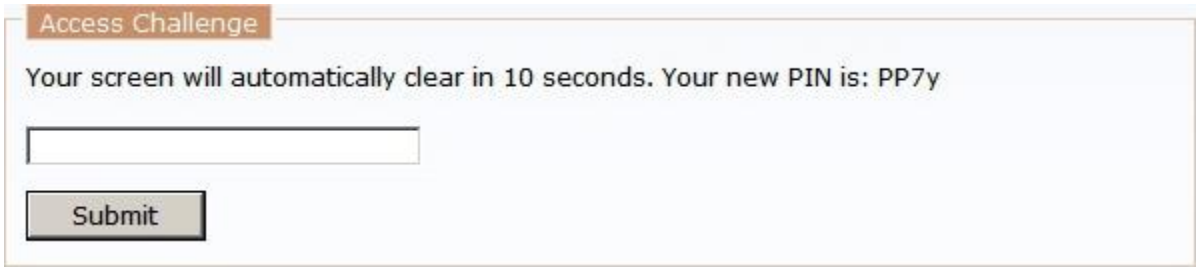
Point your browser to the host name or IP and log into the system

Login screen:

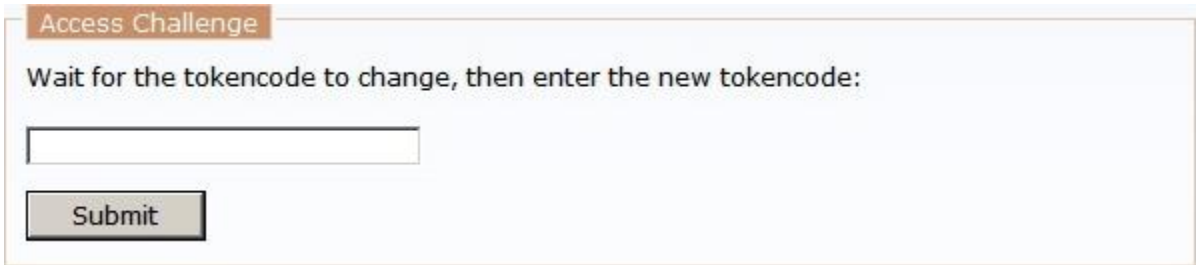
User-generated New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: May 10 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
RSA Authentication Agent	3.6	Windows Server 2008 R2
RSA Software Token		
RSA Remote Authentication Client		
GlobalSCAPE EFT Server	7.3	Windows Server 2008 R2

RSA SecurID Authentication

Date Tested: <Month, Day, Year>

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

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

FAL

RSA READY

Certification Checklist for RSA Authentication Manager

Software Token Automation

Date Tested: <Month, Day, Year>

Mandatory Functionality	Native UDP	Native TCP	RADIUS Client
PINless Token			
Next Tokencode Mode	✓		
PINpad-style Token			
Deny Alphabetic PIN	✓		
Next Tokencode Mode	✓		
Fob-style Token			
16 Digit Passcode	✓		
Alphanumeric PIN	✓		
Next Tokencode Mode	✓		
Other			
System Generated PIN	✓		
Password Protected PIN	✓		

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

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	'None stored',' In Memory' or path to sdconf.rec file
sdopts.rec	'Not implemented', 'Not tested' or path to sdopts.rec file
Node secret	'None stored', 'In Memory' or path to node secret file
sdstatus.12 / jastatus.12	'None stored', 'In Memory' or path to sdstatus.12 file
TCP Agent Files	**Location**
rsa_api.properties	'In Memory' or path to rsa_api.properties file
sdconf.rec	'None stored',' In Memory' or path to sdconf.rec file
sdopts.rec	'Not implemented', 'Not tested' or path to sdopts.rec file
Node secret	'None stored', 'In Memory' or path to node secret file

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	Version or Custom Build; API details below
RSA SecurID TCP API	Version or Custom Build; API details below
RSA Authentication Agent Type	Standard Agent, Web Agent
RSA SecurID User Specification	Designated Users, All Users, Default Method
Display RSA Server Info	Yes or No
Perform Test Authentication	Yes or No
Agent Tracing	Yes or No

API Details:

The Sdconf.rec file is loaded into a user defined folder with C:/windows/system32 being the recommended folder.

Node Secret:

User defined

sdconf.rec:

User defined

sdopts.rec:

User defined

sdstatus.12:

User defined