HazelTree Treasury Management Solutions
Atlas

RSA SecurID Ready Implementation Guide

Last Modified: February 17th, 2016

Partner Information

Product Information	
Partner Name	HazelTree Treasury Management Solutions
Web Site	www.hazeltree.com
Product Name	Atlas
Version & Platform	4.1 for Windows
Product Description	HazelTree is the leading Treasury Management solution provider, serving hedge funds, fund administrators, managed account providers and family offices with powerful, proactive performance enhancement and risk mitigation capabilities that generate operational alpha, reduce a range of risks and streamline operations. Its complete treasury management solution includes comprehensive cash management, securities financing, OTC collateral management, counterparty management and prime-broker margin management capabilities. While each of these modules enables improved performance and control of specific functions, HazelTree is most powerful when working as an integrated treasury management suite. All modules are delivered through a single user interface and supported by a common data management infrastructure that integrates and normalizes feeds from multiple sources, performs quality checks and provides an audit trail. For more information please visit www.hazeltree.com

Solution Summary

The Atlas web site integrates RSA SecurID Authentication into its logon screen. Users are prompted to provide their username and passcode in order to gain access into the system.

RSA Authentication Manager supported features	
Atlas 4.1	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	No
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
RSA SecurID Authentication via IPv6	Yes
On-Demand Authentication via Native SecurID UDP Protocol	No
On-Demand Authentication via Native SecurID TCP Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
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 Atlas web site 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 Atlas web site 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 TCP-based agent host record.

- RSA agent name (in the hostname field)

> **Note: 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 the Atlas web site will occur.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Atlas web site 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 Atlas web site components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring Atlas Web Site for RSA Authentication

The Atlas web site comes preconfigured for RSA authentication. Simply adjust the "Login Action" setting to turn this feature on and properly set some RSA configuration files and you'll be all set.

Setting the "Login Action"

1. Using Windows Explorer, navigate to the folder in which the web site was installed, typically, c:\Websites\Atlas
2. In that folder locate the appSettings.config file and open it in a text editor.
3. Locate the "LoginAction" and set its value to "RsaLogon", like this:

```
<add key="LoginAction" value="RsaLogon" />
```

4. Save the file and exit the text editor.

Set the Necessary RSA Configuration Files

1. Using Windows Explorer, navigate to the "\bin\UnmanagedDlls" folder under the web sites installed directory, typically, c:\Websites\Atlas\bin\UnmanagedDlls
2. In that folder locate the rsa_api.properties file and open it in a text editor.
3. Locate the "RSA_AGENT_NAME" and set its value to "HtAtlasApp", like this:

```
RSA_AGENT_NAME = HtAtlasApp
```

> **Note: Be sure to uncomment the line by removing the "#" at the beginning of it.**

4. In this same folder ("c:\Websites\Atlas\bin\UnmanagedDlls") replace the sdconf.rec file with the file that was exported from the RSA Authentication Server, Security Console web site.

Verify the Web Site Logon Page

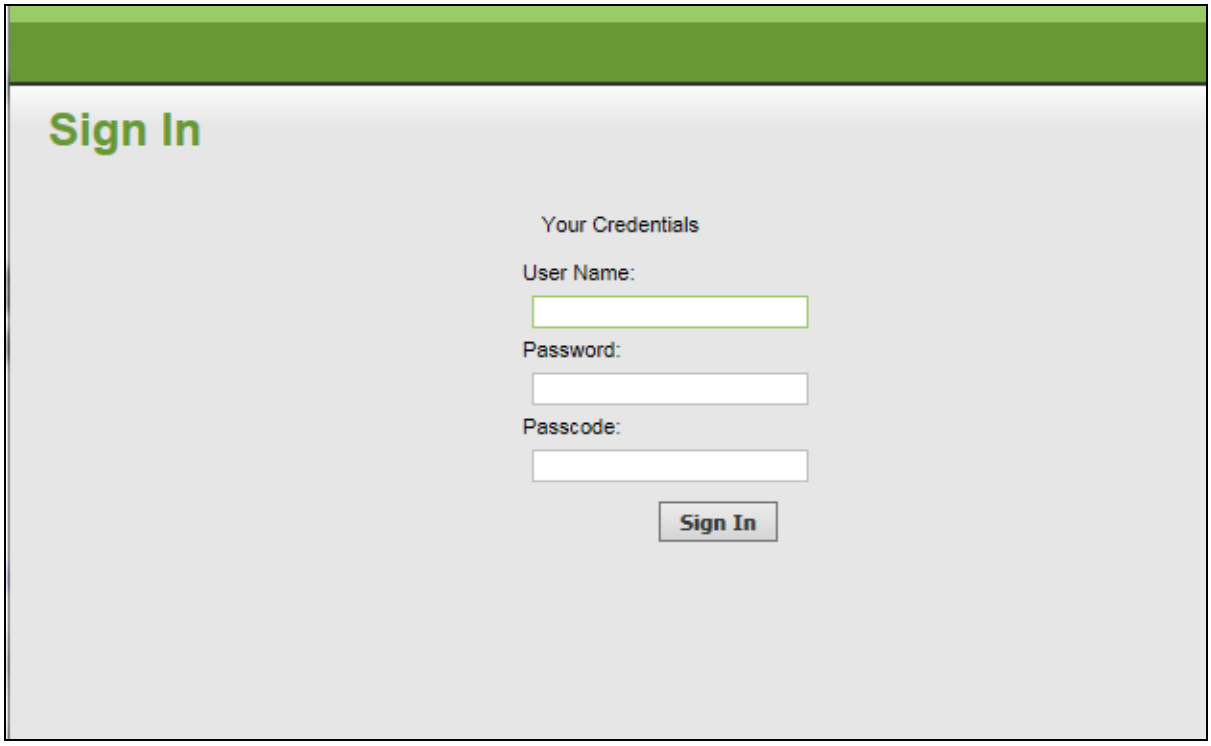
1. Using a web browser, navigate to the web site, typically located at

```
http://localhost/Account/Logon
```

2. Observe that your login page now requests a username, password and passcode.

RSA SecurID Login Screens

Login screen:



User-defined New PIN:

System-generated New PIN:

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1 SP1	Virtual Appliance
HazelTree Atlas web site	4.1	Windows 7 SP1

RSA SecurID Authentication

Date Tested: February 17th, 2016

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	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			
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

PEW / PAR

✓= Pass ✗= Fail N/A = Not Applicable to Integration

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	N/A
sdopts.rec	N/A
Node secret	N/A
sdstatus.12 / jastatus.12	N/A
TCP Agent Files	**Location**
rsa_api.properties	\bin\UnmanagedDlls
sdconf.rec	\bin\UnmanagedDlls
Node secret	\bin\UnmanagedDlls

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	N/A
RSA SecurID TCP API	8.5
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes, using rsa_api.properties

Node Secret:

Optionally, A node secret file can be manually installed into the \bin\UnmanagedDlls directory.

sdconf.rec:

The sdconf.rec file is located in the \bin\UnmanagedDlls directory. Delete or overwrite the file to clear or update the server configuration.

Agent Tracing:

Edit the rsa_api.properties file to specify the agent debug level and destination.