Ubiquiem Ltd
Tornado

RSA SecurID Ready Implementation Guide

Last Modified: May 23, 2011

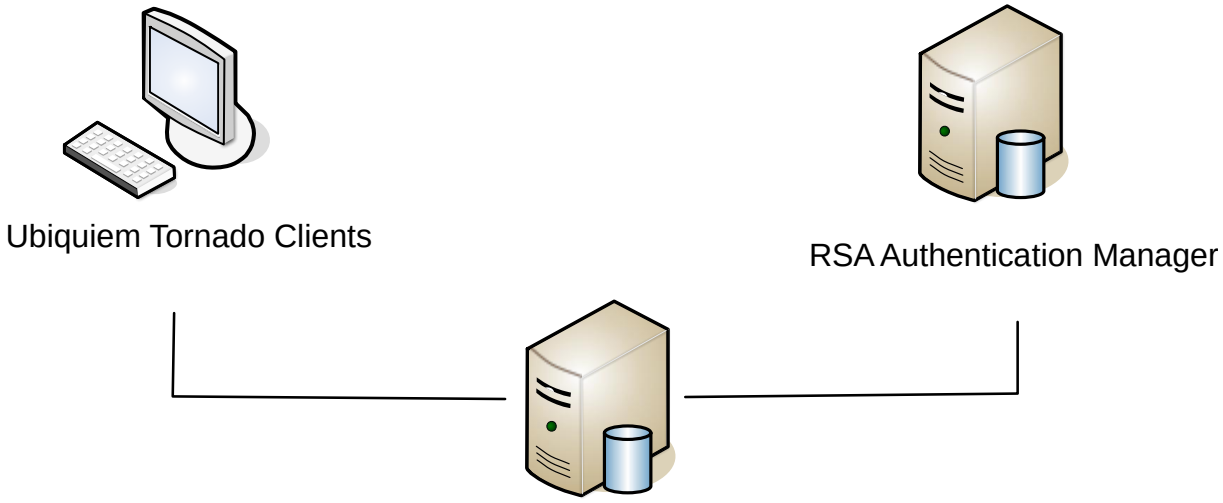
Partner Information

Product Information	
Partner Name	Ubiquiem Ltd
Web Site	www.ubiquiem.com
Product Name	Tornado
Version & Platform	1.0
Product Description	Tornado is a multi-platform, unified channel solution specifically designed for the front office.

Solution Summary

Ubiquiem Tornado provides the facility to authenticate requests to its services via an RSA Authentication Manager server using the native RSA SecurID protocol.

RSA SecurID supported features	
Ubiquiem Tornado 1.0	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
On-Demand Authentication via API	Yes
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	Yes



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

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 Tornado will occur.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	WEB-INF/conf/rsa/sdconf.rec
Node Secret	WEB-INF/conf/rsa/securid
sdstatus.12	WEB-INF/conf/rsa/sdstatus.12
sdopts.rec	Not implemented

Note: The appendix of this document contains more detailed information regarding these files.

Partner Product Configuration

Before You Begin

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

Overview

For Tornado to be able to communicate with an RSA Authentication Manager server, the following steps must be taken.

- The RSA API properties file must be configured.
- An 'sdconf.rec' file must be copied into, or made accessible to the Tornado installation.
- A path mapping must be created for the RSA SecurID login page.

Configuring the RSA API Properties

The RSA API Properties file contains configuration information for the imbedded native RSA authentication API. It is this file that determines the locations of various files the authentication API needs to communicate with the RSA Authentication manager.

The **rsa_api.properties** file is located in ***<Tornado Installation path>*/WEB-INF/classes/conf/security**.

By default the path to the sdconf.rec, node secret and the sdopts.rec are set to ***<Tornado Installation path>*/WEB-INF/conf/rsa** as per the 'RSA SecurID Files' section of this document.

The file should be edited so that every instance of ***<tornado installation path>*** is replaced with the full path of the deployed Tornado web application. Additionally, the file locations can be modified in their entirety to point to a common location accessible by multiple Tornado application servers to centralize the configuration.

Installation of sdconf.rec

The **sdconf.rec** file contains the information required for Tornado to communicate with the RSA Authentication Manager. This file is obtained from the RSA Security Console of your Authentication Manager deployment.

The sdconf.rec file is created by the Authentication Manager host and then copied into the path defined in the 'SDCONF_LOC' field within the RSA API properties file. By default this would be ***<Tornado Installation path>*/WEB-INF/conf/rsa**.

SecurID Login Path Mapping

For the SecurID enabled login page to be accessible a URL mapping must be configured within the Tornado Access Control file.

The 'tornado_access_control.xml' is located in ***<Tornado Installation path>*/WEB-INF/classes/conf/security/**

To enable the SecurID login page, uncomment the following line from the 'mapping' section of the document.

```
<mapping id="rsa" page='/site/rsa_login.html' name='RSASecurID'></mapping>
```

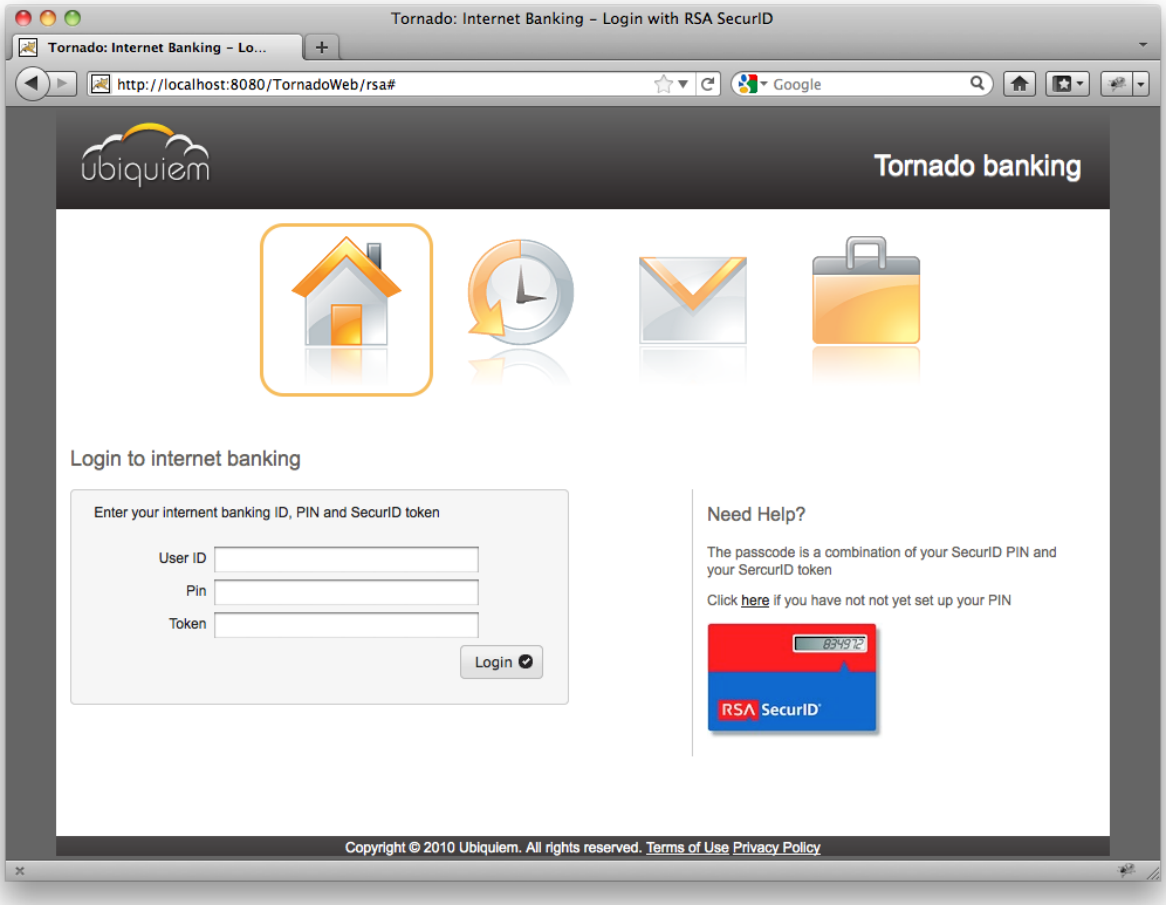
The login page would then be accessible locally at the following URL.

```
http://127.0.0.1/TornadoWeb/rsa
```

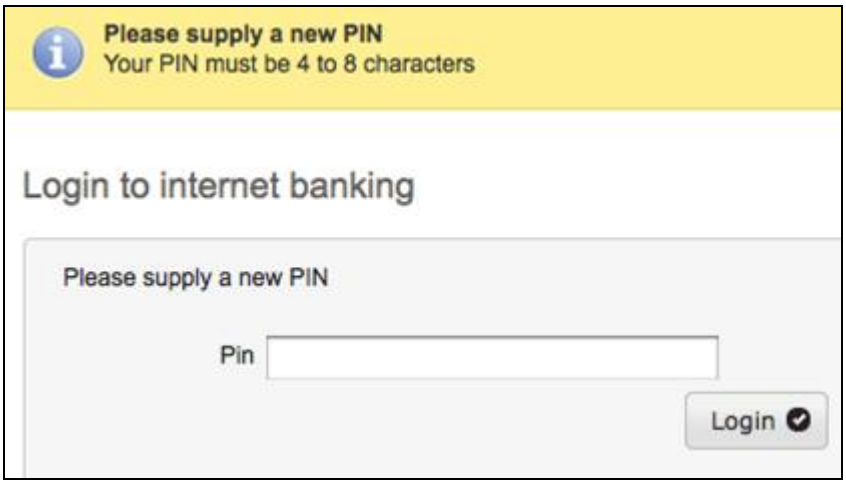
Note: After making these configuration changes, you may have to restart the web server on the Tornado device before these changes will take effect.

Screens

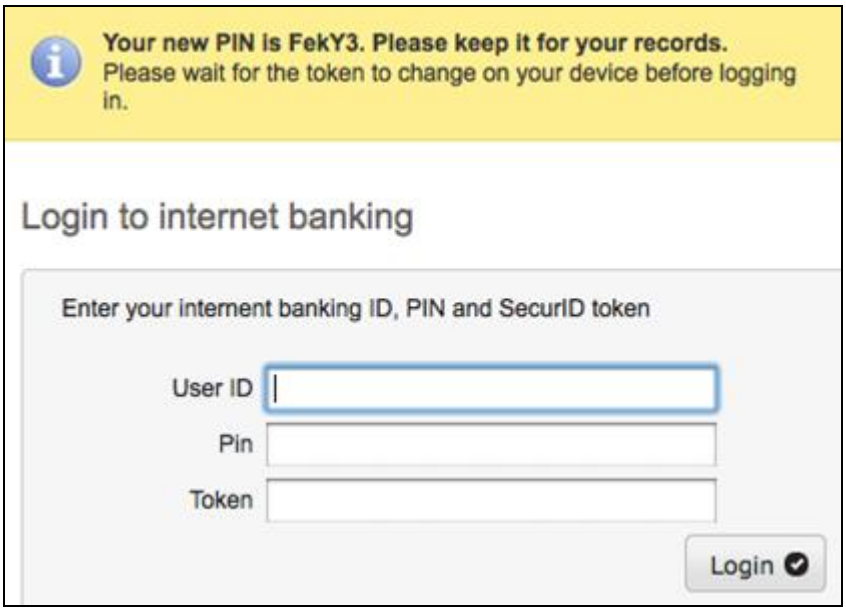
Login Screen:



User-generated New PIN:



System-generated New PIN:



Next Tokencode:

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: May 23, 2011

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows Server 2003
Ubiquiem Tornado	1.0	RedHat Enterprise Linux 5

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
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Deny Numeric PIN	✓	Deny Numeric PIN	N/A
Deny PIN Reuse	✓	Deny PIN Reuse	N/A
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	N/A
4 Digit Fixed Passcode	✓	4 Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	N/A
On-Demand New PIN	✓	On-Demand New PIN	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

MRQ

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

Appendix

Partner Integration Details	
RSA SecurID API	Java 8.1
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes

Node Secret:

The node secret is contained in a file called **securid** in the **WEB-INF/conf/rsa** directory. To clear the node secret on the Tornado device, delete this file.

sdconf.rec:

This file is stored in the **WEB-INF/conf/rsa** directory. If your Authentication Manager deployment configuration information (replicas, IP addresses, etc.) changes, replace this file with an updated copy obtained from the RSA Security Console.

Agent Tracing:

Agent tracing can be enabled by editing the **rsa_api.properties** file located in ***<Tornado Installation path>*/WEB-INF/classes/conf/security**.

Configure agent tracing by setting the following values in rsa_api.properties. The log will be written to the path you specify on the Tornado device.

Event Log		
Key	**Description**	**Acceptable Values**
RSA_LOG_TO_CONSOLE	If set to YES, event logs are sent to the console. If set to NO, event logs are not sent. Valid only if RSA_LOG_LEVEL is not set to OFF.	YES or NO The default value is NO.
RSA_LOG_TO_FILE	If set to YES, event logs are sent to the log file specified by RSA_LOG_FILE. If set to No, event logs are not sent. Valid only if RSA_LOG_LEVEL is not set to OFF.	YES or NO The default value is YES.
RSA_LOG_FILE	Indicates the path to the log file. Valid only if RSA_LOG_TO_FILE is set to YES.	The applicable path. For example: /var/ace/api/my_api_events.log or C:\\WINDOWS\\system32\\my_api_events.log
RSA_LOG_LEVEL	Indicates the minimum log level. Events below this level are not logged.	OFF, DEBUG, INFO, WARN, ERROR, or FATAL The default value is INFO.

Debug Trace		
Key	**Description**	**Acceptable Values**
RSA_ENABLE_DEBUG	If set to YES, debug tracing is enabled. If set to NO, debug tracing is disabled.	YES or NO The default value is NO.
RSA_ DEBUG _TO_CONSOLE	If set to YES, debug traces are sent to the console. If set to NO, debug traces are not sent. Valid only if RSA_ENABLE_DEBUG is set to YES.	YES or NO The default value is NO.
RSA_ DEBUG _TO_FILE	If set to YES, debug traces are sent to the file specified by RSA_DEBUG_FILE. If set to NO, debug traces are not sent. Valid only if RSA_ENABLE_DEBUG is set to YES.	YES or NO The default value is YES.
RSA_ DEBUG _FILE	Indicates the path to the debug trace file. Valid only if RSA_ENABLE_DEBUG is set to YES.	The applicable path. For example: /usr/ace/api/my_api_debug.log or C:\\WINDOWS\\system32\\my_api_debug.log
RSA_ DEBUG _ENTRY	If set to YES, function entries are traced. If set to NO, function entries are not traced. Valid only if RSA_ENABLE_DEBUG is set to YES.	YES or NO The default value is NO.
RSA_ DEBUG _EXIT	If set to YES, function exits are traced. If set to NO, function exits are not traced. Valid only if RSA_ENABLE_DEBUG is set to YES.	YES or NO The default value is NO.
RSA_ DEBUG _FLOW	If set to YES, flow statements are traced. If set to NO, flow statements are not traced. Valid only if RSA_ENABLE_DEBUG is set to YES.	YES or NO The default value is NO.
RSA_ DEBUG _NORMAL	If set to YES, regular statements are traced. If set to NO, regular statements are not traced. Valid only if RSA_ENABLE_DEBUG is set to YES.	YES or NO The default value is NO.
RSA_ DEBUG _LOCATION	If set to YES, class name and line number are displayed in the trace. If set to NO, class name and line number are not displayed in the trace. Valid only if RSA_ENABLE_DEBUG is set to YES.	YES or NO The default value is NO.