

# Technical Document

## NiagaraAX RSA SecurID® Authentication Guide

March 21, 2011



## Confidentiality Notice

The information contained in this document is confidential information of Tridium, Inc., a Delaware corporation ("Tridium"). Such information and the software described herein, is furnished under a license agreement and may be used only in accordance with that agreement.

The information contained in this document is provided solely for use by Tridium employees, licensees, and system owners; and, except as permitted under the below copyright notice, is not to be released to, or reproduced for, anyone else.

While every effort has been made to assure the accuracy of this document, Tridium is not responsible for damages of any kind, including without limitation consequential damages, arising from the application of the information contained herein. Information and specifications published here are current as of the date of this publication and are subject to change without notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia.

## Trademark Notice

BACnet and ASHRAE are registered trademarks of American Society of Heating, Refrigerating and Air-Conditioning Engineers. Microsoft and Windows are registered trademarks, and Windows NT, Windows 2000, Windows XP Professional, and Internet Explorer are trademarks of Microsoft Corporation. Java and other Java-based names are trademarks of Sun Microsystems Inc. and refer to Sun's family of Java-branded technologies. Mozilla and Firefox are trademarks of the Mozilla Foundation. Echelon, LON, LonMark, LonTalk, and LonWorks are registered trademarks of Echelon Corporation. Tridium, JACE, Niagara Framework, Niagara<sup>AX</sup> Framework, and Sedona Framework are registered trademarks, and Workbench, WorkPlace<sup>AX</sup>, and <sup>AX</sup>Supervisor, are trademarks of Tridium Inc. All other product names and services mentioned in this publication that is known to be trademarks, registered trademarks, or service marks are the property of their respective owners.

## Copyright and Patent Notice

This document may be copied by parties who are authorized to distribute Tridium products in connection with distribution of those products, subject to the contracts that authorize such distribution. It may not otherwise, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Tridium, Inc.

© Tridium, Inc. 2011.

All rights reserved. The product(s) described herein may be covered by one or more U.S or foreign patents of Tridium.

# CONTENTS

<b>Preface .....</b>	<b>iii</b>
Document change log .....	iii
Related documentation .....	iii
<b>About RSA Authentication .....</b>	<b>1-1</b>
RSA authentication overview .....	1-1
Types of authentication files .....	1-2
RSA SecurID® Authentication important terms and abbreviations .....	1-2
About the RsaUserService component .....	1-4
<b>Installing the RSA Service .....</b>	<b>2-1</b>
Configure the non-running station files .....	2-1
Configure the “default.properties” file .....	2-3
Configure the Fox Service Authentication Policy .....	2-4
Configure User Accounts for RSA Authentication .....	2-5
<b>Types of RSA Connections .....</b>	<b>3-1</b>
RSA station connection (Workbench using tokencode) .....	3-2
RSA station connection (browser using tokencode) .....	3-2
RSA station connection (Workbench using passcode) .....	3-3
RSA station connection (browser using passcode) .....	3-4
<b>RSA Frequently Asked Questions .....</b>	<b>4-1</b>
What are the requirements for using RSA Authentication in Niagara? .....	4-1
What files do I need to get from the RSA Authentication Server? .....	4-1
What are the “configuration files” and where should I install them? .....	4-1
What is the “node secret”? .....	4-2
Why do I get an “access denied” message? .....	4-2
Can I change the name or location of my configuration files? .....	4-2
Can I change the name or location of my <i>default.properties</i> file? .....	4-2
Where do I get the rsa module ( <i>rsa.jar</i> )? .....	4-3
In the Edit User dialog box, what is the Password field used for? .....	4-3
Does the “Remember these credentials” option work with RSA authentication? .....	4-3



# PREFACE

## Preface

---

### Document change log

Following are a list of document changes

- March 21, 2011, Initial release document.

### Related documentation

The following documents are related to the content in this document and may provide additional information on the topics it covers:

- *NiagaraAX-3.x User Guide*
- *NiagaraAX-3.x Platform Guide*





# CHAPTER 1

## About RSA Authentication

Integrating the RSA User Service with a NiagaraAX Supervisor station provides RSA SecurID® security when authenticating users against the NiagaraAX Framework. With the RSA User Service, you have the option to enable RSA Authentication using an RSA Authentication Manager.

This guide is written for users who are certified for RSA authentication. Users must have an understanding of RSA authentication concepts in order to employ RSA authentication in a NiagaraAX environment.

*NOTE: The RSA module is not included with the standard CD image and must be downloaded separately from "Niagara-Central.com".*

Starting in NiagaraAX-3.6, RSA SecurID integration is available for Supervisor stations using the RSA User Service component  RsaUserService provided in the RSA module. When the *rsa.jar* module  is installed, the RsaUserService component is available on the rsa palette in Workbench.

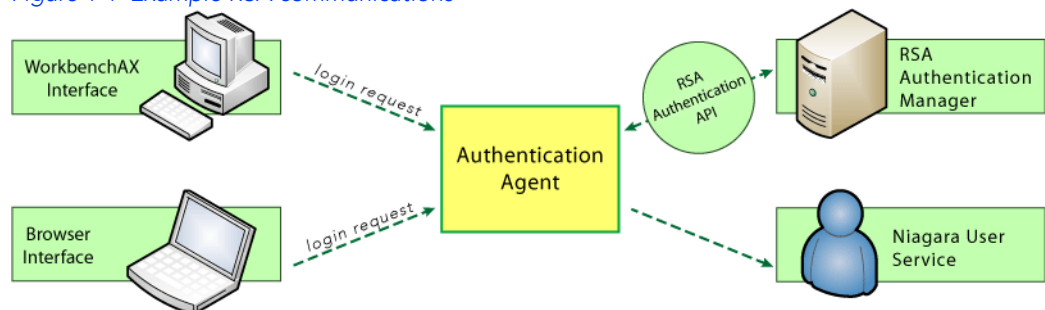
## RSA authentication overview

NiagaraAX integrates RSA SecurID Authentication within Niagara Stations through the RSA User Service provided within the Niagara Framework. When you configure a station to use the RSA User Service, you can then configure users under that service so that they can use RSA Authentication. The RSA Authentication Manager is specified in the service's associated \*.properties file.

The following list describes a simplified authentication process, as illustrated in the figure below:

- An RSA user may attempt login from either Workbench or a browser.
- If the RSA Authentication Manager authenticates the user login credentials (via the Authentication Agent) the user account is accessed from the Niagara user service.

Figure 1-1 Example RSA communications



The RSA authentication process includes several modes. When properly configured, an RSA user is initially prompted to provide a username, PIN, and tokencode or passcode, using a pre-defined means of authentication (software token, hardware token, or fixed passcode). Once a user enters the required information, the login information is sent to an Authentication Manager, which responds with one of the following:

- Access Granted. The user is allowed access to system.
- Access Denied. The user is denied access to the system and an error message may be displayed.

- **New PIN Mode.** The user is prompted with a New PIN dialog box and must create a new PIN. Once the new PIN is accepted, the user must re-authenticate with the new PIN and a new token-code.
- **Next Tokencode.** The user is prompted to enter a second successive tokencode before authentication can be completed.

The following paragraphs describe some of the major RSA SecurID authentication concepts:

- **NiagaraAX client access**  
Authorized users gain access to RSA enabled applications by initiating a login request from a platform running either the Workbench application or a web browser. Depending on the configuration settings, the user enters a combination of PIN and tokencode, or a passcode in addition to a user name.
- **RSA Authentication Agent**  
All RSA SecurID-enabled Supervisor stations require corresponding “RSA Authentication Agents”. These agents are responsible for authentication login credentials between the NiagaraAX Station and the RSA Authentication Manager. An RSA Authentication Agent is comprised of records in the RSA Authentication Manager database. These records contain information about the NiagaraAX stations (including host name and IP address). Authentication Agents are managed using the RSA Security Console.
- **RSA Authentication Manager**  
The RSA Authentication Manager contains Authentication Agent records in a database and provides files that are required for RSA setup in a NiagaraAX station.  
*NOTE: This document does not describe how to work with the RSA Authentication Manager. Please refer to the appropriate RSA documentation for additional information about working with the RSA Authentication Manager.*
- **NiagaraAX RsaUserService**  
For any NiagaraAX station to interact with an RSA Authentication Manager, this component must replace the default UserService. It has most of the same properties of the default UserService component, however, several properties within the RSA User Service are unique to RSA authentication.
- **default.properties file**  
This file provides information for the RSA Agent to use in locating the *sdconf.rec* file, the *securid* file, and additional files.
- **Authentication files**  
Authentication files are required for successful RSA SecurID Integration. Refer to *Types of authentication files* for a listing of the types of authentication files.

## Types of authentication files

### **sdconf.rec**

This is a file that is generated on the Authentication Manager. The file is required to allow communication from the RSA agent (your station) to the RSA Authentication Manager. The *sdconf.rec* file is downloaded from the RSA Authentication Manager directly and may need to be obtained from your RSA system administrator. After the file is added to your host platform, you must specify the file path in the *default.properties* file.

### **securid**

This is the “node secret” file. It is downloaded on the first successful authentication of the RSA Agent with the RSA Authentication Manager. The location for this file is specified by a value in your *default.properties* file.

### **JASatus.1**

This file is automatically downloaded to the station host platform on the first successful authentication of the RSA Agent with the RSA Authentication Manager. If the location of the *JStatus.1* file is specified in the *default.properties* file, the file will be downloaded to that location.



### **sdopts.rec**

You have to manually create this file if you want to use it. See the RSA developer documentation for more information about the sdopts.rec file.

## **RSA SecurID® Authentication important terms and abbreviations**

The following terms are important for understanding RSA SecurID concepts.

### **Authentication**

The act of validating an identity by confirming authenticity. This is accomplished with RSA SecurID by presenting a passcode. The correct passcode confirms the user's identity.

### **Seed record**

A unique identifier which is generated for each RSA SecurID Token. Two copies of this identifier exist, one in the RSA Authentication Manager and the other in the RSA SecurID Token.

### **One-Time Password**

A password that may only be used once, after which the password becomes invalid.

### **RSA SecurID Token**

Either a hardware or software token.

### **Tokencode**

The Pseudo Random Number which is generated and displayed by RSA SecurID Tokens.

### **PIN**

A string of numbers and/or letters which an end-user knows.

### **Passcode**

The concatenation of the PIN and tokencode.

### **RSA Authentication Manager**

The back end server software for the RSA SecurID Tokens. Messages are sent to the server via the RSA Authentication Agent. This product was formally known as the ACE/Server.

### **RSA Authentication Agent**

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 Authentication Agent sends and receives messages from the RSA Authentication Manager Server.

### **SecurID Native Protocol**

An RSA proprietary authentication protocol used in the RSA Authentication Manager product line.

### **RSA Authentication Library**

The SecurID Native Protocol implementation. The RSA Authentication Agents use the functions exposed by this library to communicate with the RSA Authentication Manager.

### **Node Secret**

A secret shared between an RSA Authentication Manager and an RSA Authentication Agent which is used to encrypt messages being sent between the two.

### **Sdconf.rec**

The file which contains RSA Authentication Manager server-generated configuration information used by the RSA Authentication Library.

**Sdopts.rec**

The file which contains user-generated configuration information used by the RSA Authentication Library.

**Password**

A string of characters that is used for authentication.

**Fixed-passcode**

RSA equivalence to a password. Instead of being assigned an RSA SecurID Token, a user can have a fixed-passcode for authentication.

## About the RsaUserService component

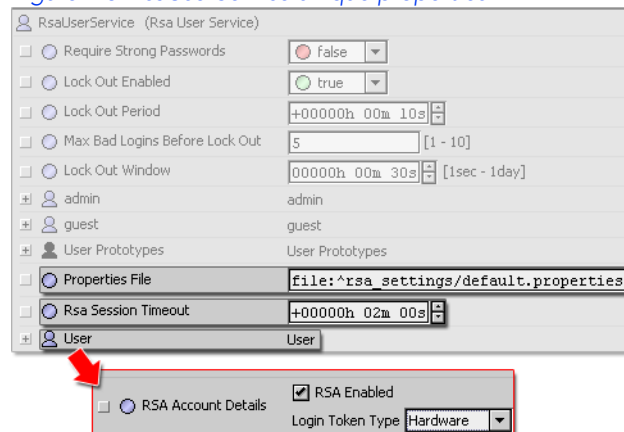
The RsaUserService authenticates RSA-defined user accounts against an RSA Authentication Manager. The RsaUserService module contains the RsaUserService component. It is available in Workbench from the RsaUserService palette.

Figure 1-2 RsaUserService in the rsa palette



The RsaUserService replaces the default UserService component when you want to setup RSA Authentication in a station. The RsaUserService has most of the same properties as the default UserService component.

Figure 1-3 RsaUserService unique properties



The following properties are unique to the RsaUserService component:

- **Properties File**  
This field points to the location of the RSA client properties file. This file specifies the location of the *sdconf.rec* file and other files needed to interface with the Authentication Manager
- **Rsa Session Timeout**  
Older RSA authentication sessions (that may be left open due to network problems) are periodically removed from the NiagaraAX system. The period at which these sessions are checked for timeout is set in this Rsa Session Timeout property and is specified as a relative time. The RsaSession field allows you to set this time.
- **User**  
Although this property is similar to the User property in the default Niagara User Service, the RsaUserService User has the following additional Rsa Account Details properties:
  - **RSA Enabled**  
This is simply a true or false option to enable or disable the RsaUserService for this user.

- **Login Token Type**

The options are “Hardware” OR “Fixed”. Hardware is for using a token generator, while Fixed is for using a fixed passcode (passcode must be set in the Authentication Manager).

RELATED LINKS:

*[Installing the RSA Service](#)*



# CHAPTER 2

## Installing the RSA Service

---

Setting up the RsaUserService in a NiagaraAX Supervisor station requires adding and configuring station files while the station is not running, then configuring files after the station is started, and adding one or more users to the newly configured RsaUserService.

To setup RSA Service in a NiagaraAX station, you need to perform the following tasks:

- *Configure the non-running station files*
- *Configure the "default.properties" file*
- *Configure the Fox Service Authentication Policy*
- *Configure User Accounts for RSA Authentication*

Note the following points before starting to perform the RSA Service integration:

- The RSA Service only runs on NiagaraAX-3.6 (and later) Supervisor stations.
- You must be familiar with NiagaraAX and specifically with Workbench.
- You must have the rsa.jar module available in your Workbench "modules" directory.

*NOTE: The RSA module is not included with the standard CD image and must be downloaded separately from Niagara-Central.com.*

- If you are modifying an existing station by adding RsaUserService, be sure to perform a station backup before stopping it.
- Save a copy of your station's "\*.bog" file so you have access to the original (non-RSA) UserService. This could be helpful for viewing any existing usernames and adding them to the new RsaUserService as necessary.

## Configure the non-running station files

The *config.bog* file is accessible and editable when the station is not running. You need to edit this file before starting the station.

### PREREQUISITE

Make sure that the target station is not running when you start this procedure. Use a platform connection to the station and stop the station if it is running.

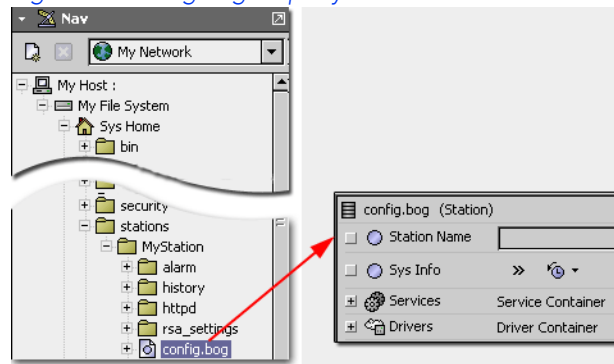
---

### TASK

1. From the Workbench nav pane, expand the My File System node and the appropriate child nodes to display the *config.bog* file under the target station folder.
2. In the nav pane, double-click on the *config.bog* file.

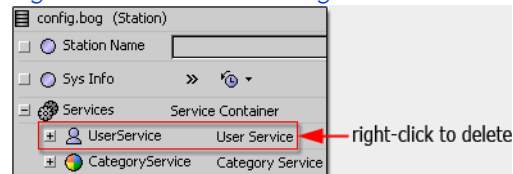
*STEP RESULT:* The *config.bog* Property Sheet view displays, as shown below.

Figure 2-1 config.bog Property Sheet view.



3. In the Property Sheet view, expand the Services node, right-click the “UserService” property and select Delete from the popup menu.

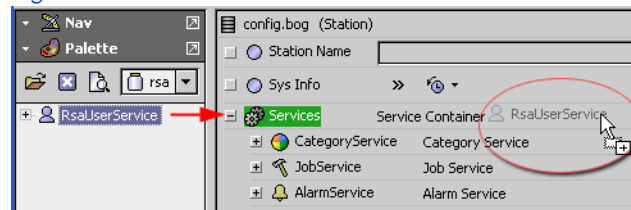
Figure 2-2 Delete the existing UserService



The UserService is deleted and removed from the view.

4. From the Palette Side Bar (**Window > Side Bars > Palette**) open the rsa palette and drag the RsaUserService component directly onto the Services container in the Property Sheet view.

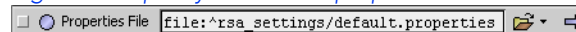
Figure 2-3 Add the RsaUserService



STEP RESULT: The RsaUserService is added and displays in the view.

5. In the Property Sheet view, expand the RsaUserService container and notice the “Properties File” field.

Figure 2-4 Specify the default.properties file location



The file path value that is in this field, by default, specifies the location of the *default.properties* file. The RsaUserService automatically creates this folder and file the first time you start the configured station. If you rename or move the location of the *default.properties* file you must edit this property to match the new name and location.

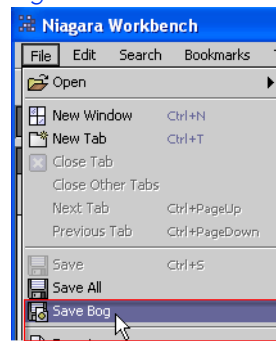
*NOTE: The default.properties file and the "rsa\_settings" folder are created automatically when the RSA User service is added to the station and the station is restarted. However, if you have your own \*.properties file already, you can use it instead. Just make sure that the location is specified in your RsaUserService property sheet.*

6. In the RsaSession Timeout property field, set the time, as desired.

*ADDITIONAL INFORMATION: Older RSA Auth Sessions (that may be left open due to network problems) are periodically removed from the NiagaraAX system. The period at which these sessions are checked for timeout is set in this Rsa Session Timeout property and is specified as a relative time. The RsaSession field allows you to set this time.*

7. From the Workbench main menu, select **File > Save Bog**.

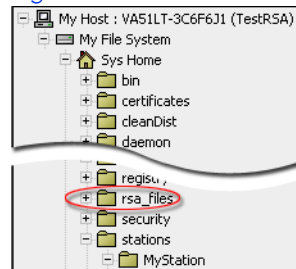
Figure 2-5 Save the config.bog file



*STEP RESULT:* Your changes are saved to the *config.bog* file.

8. In the nav tree, right-click on the Sys Home node and select **New > New Folder** to create an "rsa\_files" (name is optional) folder under the Sys Home directory.

Figure 2-6 Add a folder for your files



*NOTE:* You may want to put this folder under a higher directory - above the current Workbench installation so you don't have to create the folder again for newer installations of Workbench. This folder can be located in any "writable" location.

*STEP RESULT:* This folder is now available as a container for the following files: *sdconf.rec*, *JAStatus.1*, *securid*, *sdopts.rec*. The path to their location must be specified in the *default.properties* file.

---

*RESULT:*

The offline station configuration is complete.

## Configure the “default.properties” file

The “default.properties” file specifies the location of the *sdconf.rec*, *JAStatus.1*, *sdopts.rec*, and *securid* files. Edit this file to specify the location for each file.

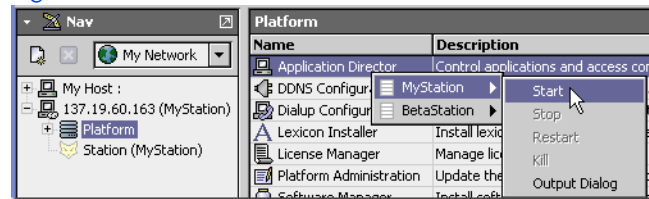
*NOTE:* If your station is already running, you can skip steps 1 and 2 in the following task. However, you should verify the name and location of the *rsa\_files* folder and make adjustments to the following steps, as needed.

---

### TASK

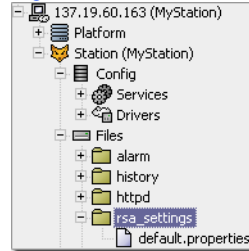
1. Connect to your station's host platform from Workbench (**File > Open Platform (http)**).  
*STEP RESULT:* The Platform Nav Container View displays.
2. In the Nav Container View, right-click on the “Application Director” entry and select **Station Name > Start**.

Figure 2-7 Start the station



**STEP RESULT:** When the station starts, if the RsaUserService has been added, it automatically creates an “rsa\_settings” folder under the **Stations > Files** node, as shown below.

Figure 2-8 The rsa\_settings folder contains the “default.properties” file



- From Workbench, open the station using **File > Open > Open Station (fox)** and login with the default “admin” user and password credentials.
- Expand the **Station > Files > rsa\_settings** node and double-click on the “default.properties” file.  
**STEP RESULT:** The “default.properties” file displays in the Text File Editor view.
- Edit the following lines in the “default.properties” file so that they define a path to the appropriate “rsa\_files” folder, including the appropriate file name:

**Example:** The following example file paths assume that Workbench is installed under the D:\Niagara\NiagaraAX-3.6.24 directory. The “rsa\_files” folder was added in the previous task.

- SDCONF\_LOC=/D:/rsa\_files/sdconf.rec
- SDSTATUS\_LOC=/D:/rsa\_files/JAStatus.1
- SDOPTS\_LOC=/D:/rsa\_files/sdopts.rec
- SDNDSCRT\_LOC=/D:/rsa\_files/securid

Figure 2-9 Example “default.properties” file

Example file syntax

```
# [This section is for Data Repository configuration.]
# Type of the Server configuration.
SDCONF_TYPE=FILE
# Path of the Server configuration.
#SDCONF_LOC=sdconf.rec
SDCONF_LOC=/D:/rsa_files/sdconf.rec
# Type of the Server statuses.
SDSTATUS_TYPE=FILE
# Path of the Server statuses.
#SDSTATUS_LOC=JAStatus.1
SDSTATUS_LOC=/D:/rsa_files/JAStatus.1
# Type of the Server options.
SDOPTS_TYPE=FILE
# Path of the Server options.
#SDOPTS_LOC=sdopts.rec
SDOPTS_LOC=/D:/rsa_files/sdopts.rec
# Type of the Node Secret.
SDNDSCRT_TYPE=FILE
# Path of the Node Secret.
SDNDSCRT_LOC=/D:/rsa_files/securid
```

*Note: If the target location is not specified in default.properties, the location of the files will be as follows: .../Niagara/Niagara-3.6.xx/daemon/*

- After finishing your edits, click **File > Save** from the main menu.  
**STEP RESULT:** Changes to the default.properties file are saved.

**RESULT:**

The default.properties file is configured.



## Configure the Fox Service Authentication Policy

Authentication policy options are available in the Fox Service component. For RSA authentication to work, the Fox Service must be configured to use “Transactional” authentication policy.

### PREREQUISITE

This task requires that the station you want to configure is running and that you are logged into the station with admin privileges.

### TASK

1. In the nav tree, expand nodes under your station to display the NiagaraNetwork node (**Station > Config > Drivers > NiagaraNetwork**). Right-click on the NiagaraNetwork component and select **Views > Property Sheet** from the popup menu.

*STEP RESULT:* The NiagaraNetwork Property Sheet view displays.

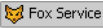
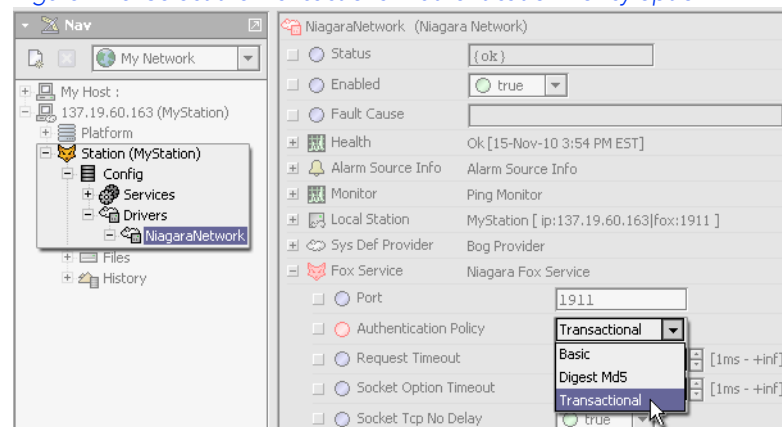
2. From the NiagaraNetwork Property Sheet view, expand the Fox Service property  and set the Authentication Policy property to “Transactional”.

Figure 2-10 Select the Transactional Authentication Policy option



3. At the bottom of the view, click the **Save** button.

*STEP RESULT:* Changes to the Fox Service are saved.

### RESULT:

The Fox Service configuration is completed.

## Configure User Accounts for RSA Authentication

You can configure an RSA User Account (RsaUserAccount) using the standard User Manager view in Workbench. The properties in the RsaUserAccount component are similar to those in the standard UserAccount, with the exception a few additional properties that are unique to RSA authentication. Only users that are listed in the RSA User Service may authenticate with RSA authentication.

### PREREQUISITE

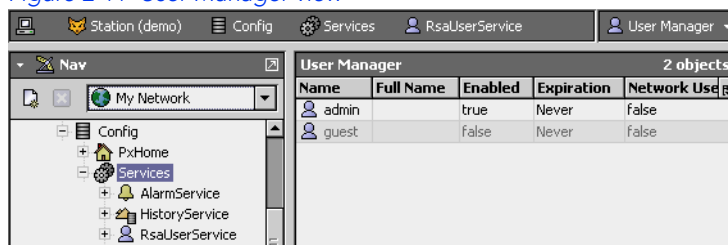
This procedure requires the following prerequisites

- The RSAUserService is in the Services container.
- The Supervisor station that you want to configure is running
- you are logged into the station with admin privileges

### TASK

1. In the nav tree, under your station, expand the Services node and double-click on the RsaUserService node.

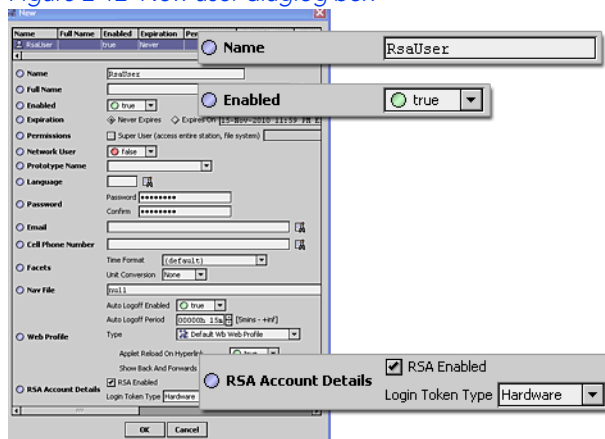
Figure 2-11 User Manager view



**STEP RESULT:** The User Manager view displays.

- In the User Manager view, click the **New** button to open a succession of two New dialog boxes.

Figure 2-12 New user dialog box



Use these dialog boxes for adding one or more new users, as desired. Set properties for each new user, as needed, taking note of the following properties that are particularly important for the RsaUserService:

- Name**  
 Enter a user name in this field that matches EXACTLY your user name as it is stored in the Authentication Manager database.
- Enabled**  
 Set this property to true.

*NOTE: Setting the Enabled property value to false prevents the user from having station access using the RSA Authentication Manager.*

- RSA Account Details**  
 The options are “Hardware” OR “Fixed”. Hardware is for using a token generator, while Fixed is for using a fixed passcode (passcode must be set in the Authentication Manager).

- Click the **OK** button.

**STEP RESULT:** The user configuration settings are saved.

---

**RESULT:** The new RSA User Account is added.

# CHAPTER 3

## Types of RSA Connections

If you have configured a Supervisor station with the RsaUserService, you can connect to the station from either Workbench or from a web browser.

Using either a web browser or the Workbench application interface, your options for connecting to a Supervisor station include one of the following, depending on the way the RsaUserService is configured:

- **RSA Authentication using a tokencode at login**

*Figure 3-1 Logging in using a tokencode*

The screenshot shows the 'MyStation' login page. It features a key icon on the left. To the right of the icon are three input fields: 'Username', 'PIN', and 'Tokencode'. Below these fields is a checkbox labeled 'Fixed Passcode Enabled' and a 'Login' button.

This method requires that you use a Hardware generated Tokencode and a PIN entry for the Credentials fields in the Open Station RSA dialog box. For this login option, "Hardware" must be designated in the RSA Account Details "Login Token Type" options (as shown below).

*Figure 3-2 Choose "Hardware" in the User properties Edit dialog box*

The screenshot shows the 'RSA Account Details' dialog box. The 'RSA Enabled' checkbox is checked. The 'Login Token Type' dropdown menu is open, showing 'Hardware' selected and 'Fixed' as an option below it.

Refer to the following tasks for details about connecting to a station using a tokencode at login.

- “RSA station connection (Workbench using tokencode)” on page 3-2
- “RSA station connection (browser using tokencode)” on page 3-3

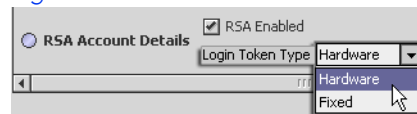
- **RSA Authentication using a passcode at login**

*Figure 3-3 Logging in using a passcode*

The screenshot shows the 'MyStation' login page. It features a key icon on the left. To the right of the icon are three input fields: 'Username', 'PIN', and 'Tokencode'. Below these fields is a checkbox labeled 'Fixed Passcode Enabled' and a 'Login' button.

This method requires that you use a Username and Passcode (no separate PIN required). These credentials must match your User credentials in the Authentication Manager database. For this login option, "Fixed" must be designated in the RSA Account Details "Login Token Type" options.

Figure 3-4 Choose “Fixed” in the User properties Edit dialog box



Refer to the following tasks for details about connecting to a station using a passcode at login.

- “RSA station connection (Workbench using passcode)” on page 3-3
- “RSA station connection (browser using passcode)” on page 3-4

## RSA station connection (Workbench using tokencode)

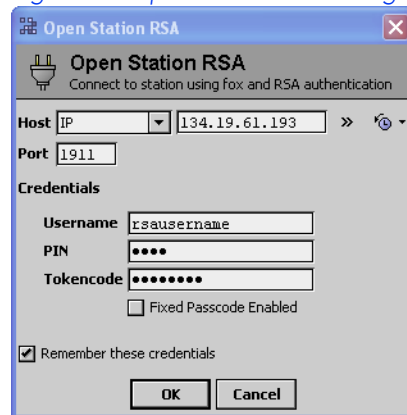
You can perform a tokencode login to a station using Workbench.

### TASK

1. In Workbench, select **File > Open > Open Station (for RSA)** from the main menu.

*STEP RESULT:* The Open Station RSA dialog box displays.

Figure 3-5 Open Station RSA dialog box



2. In the Open Station RSA dialog box, enter the station's IP address and Port number (1911 is the default port).

*ADDITIONAL INFORMATION:* In the Credentials fields, note the following:

- **Username:**  
This name must be in your RsaUserService and must match exactly the name in the Authentication Manager.
- **PIN**  
This field is available only if the **Fixed Passcode Enabled** box is cleared. The PIN value is a user-controlled value that must already be set in the RSA Authentication Manager.
- **Tokencode**  
Read this value from your appropriate RSA SecurID Token.

3. With the proper values entered, click the **OK** button.
  - If authentication is successful, the station connection completes and the Station Summary view displays. You are logged in with the access permissions that are defined for your user credentials in the RsaUserService.
  - If authentication is not successful, an error message may appear.

## RSA station connection (browser using tokencode)

You can perform a tokencode login to a station using a web browser.

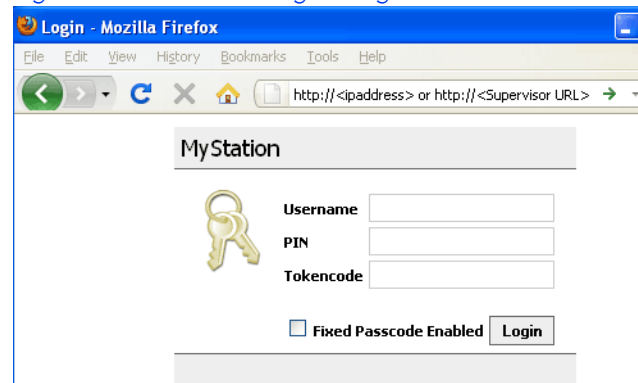
---

### TASK

1. In the browser address bar, enter the URL (or IP address) of the station that you want to connect to and press the **Enter** key.

*STEP RESULT:* The Login view displays.

Figure 3-6 RSA browser login using tokencode



2. In the browser Login view, select the **Fixed Passcode Enabled** check box and enter your credentials.

*ADDITIONAL INFORMATION:* Note the following:

- **Username:**  
This name must be in your RsaUserService and must match exactly the name in the Authentication Manager.
  - **PIN**  
This field is available only when the **Fixed Passcode Enabled** box is cleared. The PIN value is a user-controlled value that must already be set in the RSA Authentication Manager.
  - **Tokencode**  
Read this value from your appropriate RSA SecurID Token.
3. With the proper values entered, click the **Login** button.
    - If authentication is successful, the station connection completes and the Station Summary view (or Home view) displays. You are logged in with the access permissions that are defined for your user credentials in the RsaUserService.
    - If authentication is not successful, an error message may appear.

## RSA station connection (Workbench using passcode)

You can perform an RSA passcode login to a station using the Workbench application interface.

---

### TASK

1. In Workbench, select **File > Open > Open Station (for RSA)** from the main menu.  
*STEP RESULT:* The **Open Station RSA** dialog box displays.
2. In the **Open Station RSA** dialog box, enter the station's IP address, Port number (1911 is the default port) and select the **Fixed Passcode Enabled** check box.

*NOTE:* The PIN field is not available after the **Fixed Passcode Enabled** check box is selected.

3. In the **Open Station RSA** dialog box, enter the appropriate credentials:

*ADDITIONAL INFORMATION:* In the Credentials fields, note the following:

- **Username**  
This name must be in your RsaUserService and must match exactly the name in the Authentication Manager.
  - **PIN**  
This field is not available when the **Fixed Passcode Enabled** check box is selected.
  - **Passcode**  
Enter your passcode for authentication.
4. With the proper values entered, click the **OK** button.
    - If authentication is successful, the station connection completes and the Station Summary view displays. You are logged in with the access permissions that are defined for your user credentials in the RsaUserService.
    - If authentication is not successful, an error message may appear.

## RSA station connection (browser using passcode)

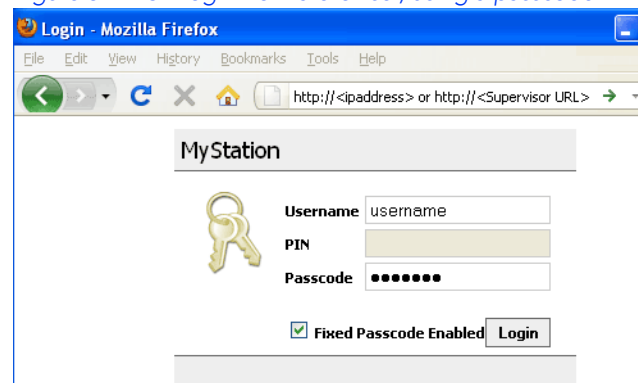
You can perform an RSA passcode login to a station using the a web browser.

### TASK

1. In the browser address bar, enter the URL of the station that you want to connect to and press the Enter key.

*STEP RESULT:* The Login view displays.

Figure 3-7 RSA login from a browser, using a passcode



2. In the browser Login view, select the **Fixed Passcode Enabled** check box and enter your credentials.

*ADDITIONAL INFORMATION:* In the Credentials fields, note the following:

- **Username**  
This name must be in your RsaUserService and must match exactly the name in the Authentication Manager.
  - **PIN**  
This field is not available when the **Fixed Passcode Enabled** check box is selected.
  - **Passcode**  
Enter your passcode for authentication.
3. With the proper values entered, click the **OK** button.
    - If authentication is successful, the station connection completes and the Station Summary view (or Home view) displays. You are logged in with the access permissions that are defined for your user credentials in the RsaUserService.
    - If authentication is not successful, an error message may appear.

# CHAPTER 4

## RSA Frequently Asked Questions

This topic includes a list of Frequently Asked Questions related to the integration and use of RSA Authentication with the NiagaraAX Framework:

### What are the requirements for using RSA Authentication in Niagara?

RSA is available in NiagaraAX-3.6 and later on Supervisor station's only. Other requirements include:

- RSA module installed in the modules directory
- Network connection to a properly configured Authentication Management Server
- RSA requires certification of persons using RSA Authentication Managers

### What files do I need to get from the RSA Authentication Server?

The *sdconf.rec* file must be generated on the RSA Authentication Server and then *manually copied* to a location on your host platform. All other required files are automatically generated on station startup (if RsaUserService is enabled) or downloaded to your host platform on initial user authentication. The path to the *sdconf.rec* file and any auto-downloaded files is noted in the *default.properties* file. You can edit this file in your Workbench Text Editor view.

### What are the “configuration files” and where should I install them?

Configuration files are listed in the Data Repository Configuration section of the *default.properties* file. You can install them in any “writable” file system location by specifying their target location in the *default.properties* file. With the exception of the *sdconf.rec* file, the first time that a User logs into an RSA configured station and is successfully authenticated, these files are automatically transferred to the specified location.

*NOTE: If the target location is not specified in the default.properties file, the location of the files will be as follows: “.../Niagara/Niagara-3.6.xx/daemon/”. This is true also for event log and debug files: rsa\_api.log and rsa\_api\_debug.log.*

The following files are included:

File	Description
<i>sdconf.rec</i>	This is a file that is generated on the Authentication Manager. The file is required to allow communication from the RSA agent (your station) to the RSA Authentication Manager. The <i>sdconf.rec</i> file is downloaded from the RSA Authentication Manager directly and may need to be obtained from your RSA system administrator. After the file is added to your host platform, you must specify the file path in the <i>default.properties</i> file.

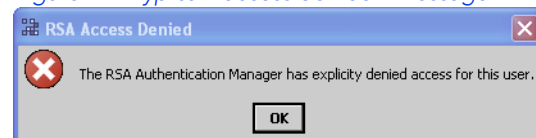
File	Description
<i>securid</i>	This is the “node secret” file. It is automatically downloaded on the first successful authentication of the NiagaraAX client with the RSA Authentication Manager. The location for this file is specified by a value in your <i>default.properties</i> file
<i>JASatus.1</i>	This file is automatically downloaded to the station host platform on the first successful authentication of the NiagaraAX client with the RSA Authentication Manager. If the location of the <i>JASatus.1</i> file is specified in the <i>default.properties</i> file, the file will be downloaded to that location.
<i>sdopts.rec</i>	You have to manually create this file if you want to use it. See the RSA developer documentation for more information about the <i>sdopts.rec</i> file.

## What is the “node secret”?

After the first successful authentication, a secret value is generated on the RSA Authentication Manager and downloaded to the agent automatically as the *securid* file. You can specify the download location for this file in your *default.properties* file. If the *securid* file is not downloaded to the agent, or cannot be found, then authentication requests result in failures. After an authentication request failure, the node secret must be cleared at the Authentication Manager before attempting another login.

## Why do I get an “access denied” message?

Figure 4-1 Typical “access denied” message



This response lets you know that your authentication request has failed. Possible reasons include:

- The RSA SecurID Card or RSA SecurID Key Fob user entered a valid PIN followed by an invalid Tokencode. The code could have been invalid because it was used previously, because it was mis-typed, or because an unauthorized user guessed it that did not have the token.
- When using an RSA SecurID PINPAD Card, the user entered an invalid Passcode. The code could have been invalid because it was used previously, because it was mis-typed, or because an unauthorized user guessed it that did not have the token.
- The RSA SecurID Card or RSA SecurID Key Fob user entered an invalid PIN followed by a valid Tokencode. The PIN could have been invalid because it was mis-typed, guessed, or the authenticator was in New PIN mode and its previous PIN had been cleared.
- When using an RSA SecurID PINPAD Card, the user entered an invalid PIN into the card, and therefore, an invalid Passcode was generated.
- The user’s RSA SecurID authenticator is disabled. Tokens can be disabled either automatically to evade a system attack or by an administrator.
- A person attempting to gain unauthorized access is guessing Passcodes.
- The user is not activated on the client directly or via group membership.
- The client was not found in the RSA Authentication Manager database.
- Mismatch of node secret or encryption type.
- Authenticator has expired or the user’s temporary access period has expired.

## Can I change the name or location of my configuration files?

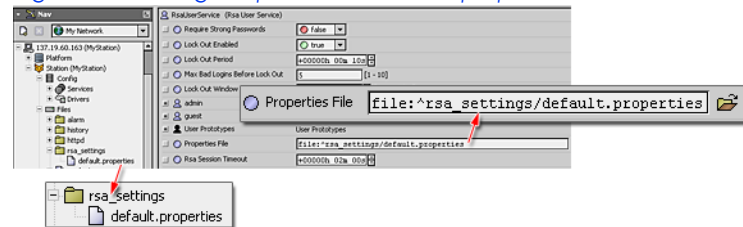
Yes, but any file location changes must be matched by an equivalent change in the *default.properties* file that points to them. You must also restart your station after the change.



## Can I change the name or location of my *default.properties* file?

The *default.properties* file and the "rsa\_settings" folder are created automatically when the RSA User service is added to the station and the station is restarted. However, if you have your own \*.properties file already, you can use it instead. Just make sure that the location is specified in your RsaUserService property sheet (see the following image).

Figure 4-2 Setting the path to the *default.properties* file



## Where do I get the rsa module (rsa.jar)?

Similar to other NiagaraAX modules, the rsa.jar module is located on the Niagara-Central portal. You can login and go to the following link and download the latest version of the module file:

<http://www.niagara-central.com/ord?portal:/software/SoftwareModule/680>

## In the Edit User dialog box, what is the Password field used for?

The Password field is used for Niagara-authenticated users only (when the RSA Enabled value is "false"). Non-RSA authentication does not require any RSA Authentication PIN or Passcode and is not authenticated through the RSA Authentication Manager.

## Does the "Remember these credentials" option work with RSA authentication?

No. This check box does not work with RSA authentication. It only applies to non-RSA Authenticated users.

