



RSA SecurID Ready Implementation Guide

Last Modified: March 27, 2008

Partner Information

Product Information	
Partner Name	Juniper Networks
Web Site	www.juniper.net
Product Name	Unified Access Control (UAC)
Version & Platform	2.0
Product Description	<p>Juniper Networks Unified Access Control solution combines user identity and device security state information with network location information, to create a unique access control policy for each user. The solution can be enabled at Layer 2, using 802.1X, or at Layer 3 using an overlay deployment. UAC 2.0 can also be provisioned in mixed mode, using 802.1X for network admission control and Layer 3 for resource access control.</p> <ul style="list-style-type: none"> • Ties user identity, device integrity, and location information with session-specific policy, enforced throughout the network, enables access control for guests, contractors and employees • Provides enforcement using any vendor's 802.1X-enabled infrastructure, existing Juniper firewalls or both • Support for access control open standards through Trusted Network Connect
Product Category	Networks and Communication

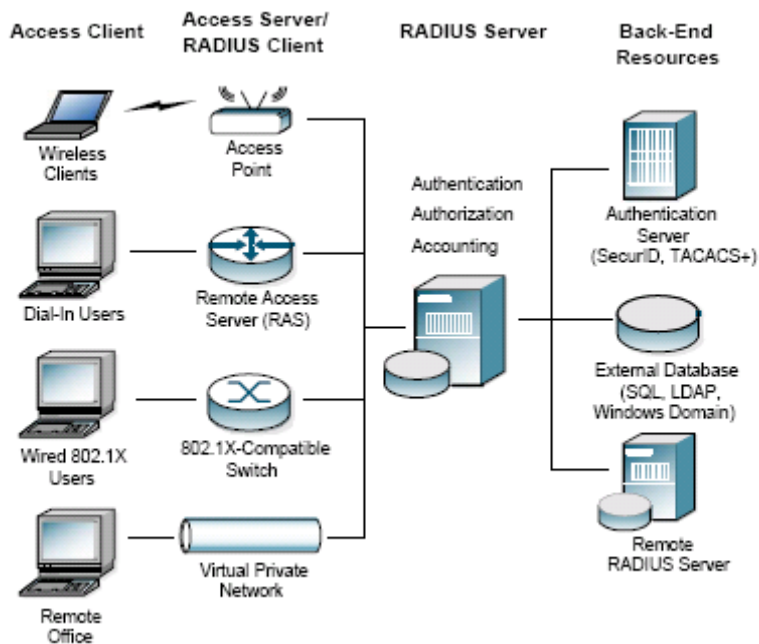




Solution Summary

The scope of this guide is to show how to setup and configure Juniper's Unified Access Control (UAC) solution to authenticate users to an RSA Authentication Manager. For a more in depth explanation of how to configure your switch/wireless hardware, please refer to the documentation provided by your hardware vendor.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication and RADIUS
List Library Version Used	5.03
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	Yes (2)
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No





Product Requirements

Unified Access Control (UAC) is a self-contained hardware appliance and therefore there are no hardware requirements.

Minimum software and patch requirements used in this certification include the following:

Partner Product Requirements: Unified Access Control (self contained appliance)	
Version	
Infranet Controller 4000	2.0 UAC2.0R2 (build 49383)
Infranet Controller 6000	2.0 UAC2.0R2 (build 49383)

Operating System	
Platform	Required Patches
Proprietary	

Please contact Juniper Technical Support in obtaining updated software and recent patches.

Additional Software Requirements	
Application	Additional Patches
Web browser with optional Windows plug-in	Tested with Internet Explorer v6.0, Service Pack 1
Odyssey Access Client v4.6 or higher	

Odyssey Access Client Configuration

Please refer to the Odyssey Access Client Implementation Guide and Juniper Odyssey Administrator Guide for additional information.



Agent Host Configuration

To facilitate communication between the Unified Access Control (UAC) 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 UAC device within its database and contains information about communication and encryption.

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

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret (When using RADIUS Authentication Protocol)

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

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	In Memory
Node Secret	In Memory
sdstatus.12	In Memory
sdopts.rec	Not implemented

Go to the appendix of this document to get detailed information regarding these files.



Partner Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product 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.

Documenting the Solution

Native RSA SecurID Authentication Support

1. Copy the `sdconf.rec` file from the RSA Authentication Manager server to the machine that you will be using to administer the Unified Access Control (UAC) device.
2. Log into the Juniper Networks Administrator Console of UAC device. This can be reached via a web browser by entering <https://hostname/admin> or <https://ipaddress/admin>.
3. On the left hand pane, click on **Authentication** and then **Auth.Servers**.
4. On the right hand pane from the **New** pull down menu, select **Ace Server** then click on **New Server**.

The screenshot shows the Juniper Networks Administrator Console interface. The left sidebar contains a navigation menu with categories like System, Authentication, and Maintenance. The main content area is titled 'Authentication Servers' and features a 'New' dropdown menu with a list of server types. The 'ACE Server' option is selected and highlighted. Below the dropdown is a table with columns for 'Name' and 'Type'. The table contains several entries, including 'Local Authentication', 'Certificate Server', 'ACE Server', 'Certificate Server', 'Radius Server', and 'Local Authentication'.

Name	Type
Local Authentication	Local Authentication
Certificate Server	Certificate Server
ACE Server	ACE Server
Certificate Server	Certificate Server
Radius Server	Radius Server
Local Authentication	Local Authentication

5. Under the **Settings** tab, on the **Name**: field; enter a name that will refer to the Authentication Manager server.
6. Ace Port should be 5500 (default)
7. Make sure **Users authenticate using tokens or one-time passwords** is checked.
8. Under the **Configuration File** section, click **Browse** to locate the `sdconf.rec` file you copied in step one of this section.
9. Click **Import** to import the file once the path is defined.
10. Click **Save Changes**.



Juniper NETWORKS

Infranet Controller Help | Guidance | Sign Out

System

- Status
- Configuration
- Network
- Clustering
- Log/Monitoring

Authentication

- Signing In
- Endpoint Security
- Auth. Servers

Administrators

- Admin Realms
- Admin Roles

Users

- User Realms
- User Roles
- Resource Policies

Maintenance

- System
- Import/Export
- Push Config
- Archiving
- Troubleshooting

Auth Servers >
Native-RSA

Settings Users

Name: Label to reference this server.

ACE Port:

Users authenticate using tokens or one-time passwords

Configuration File

Current config file:
Imported on: Wed Aug 8 01:23:02 2007

Import new config file: Specify new configuration file and click Save Changes

Node Verification File

Node	Creation Time
<input type="checkbox"/> this node	Wed Aug 8 01:34:57 2007

Save Changes ?

Creating a User Role

1. On the left hand pane, select **User Roles**.



The screenshot shows the Juniper Infranet Controller web interface. The top navigation bar includes the Juniper logo and the text "Infranet Controller" on the left, and "Help | Guidance | Sign Out" on the right. A left-hand sidebar menu lists various system and authentication options. The main content area is titled "Roles" and "RSA-Role". It features two tabs: "General" (selected) and "Agent". Under the "General" tab, there are sub-tabs for "Overview", "Restrictions", "Session Options", and "UI Options". The "Overview" sub-tab is active, showing a form with the following fields: "Name" (containing "RSA-Role"), "Description" (empty), and a "Save Changes" button. Below the form is an "Options" section with a note: "If these settings are not specified by any roles assigned to the user, the settings specified in [Default Options](#) will be used." This section contains two checked checkboxes: "Session Options" and "UI Options", each with an "Edit" link. At the bottom of the page, there is a "Save changes?" prompt with a "Save Changes" button.

2. On the right hand pane under the **General – Overview** tab, enter a name for the user role.
3. Enter a description in the **Description** field. (optional)
4. Click **Save Changes**.




Creating a User Realm

1. On the left hand pane select **User Realms**.
2. On the right hand pane, click **New** to create new Authentication Realm.
3. Name the new Realm and optionally enter a description.
4. Under the **Servers** section, select the Authentication Manager Server previously created in step 5 under the **Native RSA SecurID Authentication Support** section of this document.

The screenshot shows the Juniper Infranet Controller web interface. The left navigation pane is expanded to 'User Realms'. The main content area shows the configuration for a new realm named 'AuthMan-Native'. The 'Name' field is filled with 'AuthMan-Native' and has a 'Label to reference this realm' note. The 'Description' field is empty. There is a checkbox for 'When editing, start on the Role Mapping page' which is unchecked. The 'Servers' section is expanded, showing three dropdown menus: 'Authentication' set to 'Native-RSA', 'Directory/Attribute' set to 'None', and 'Accounting' set to 'None'. Below this is a checkbox for 'Dynamic policy evaluation' which is unchecked. The 'Other Settings' section shows 'Authentication Policy' set to 'Password restrictions' and 'Role Mapping' set to '1 Rule'. At the bottom, there is a 'Save changes?' section with a 'Save Changes' button.

5. Click **Save Changes**.

 **Note:** You will automatically be directed to the **Role Mapping** page. Please continue to Step 10 of this section.



6. Click **New Rule**.

The screenshot shows the Juniper Infranet Controller interface. The left sidebar contains a navigation menu with categories like System, Authentication, Administrators, and Maintenance. The main content area is titled 'AuthMan-Native' and has tabs for 'General', 'Authentication Policy', and 'Role Mapping'. Below the tabs, there is a description: 'Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.' There are buttons for 'New Rule...', 'Duplicate', 'Delete', and 'Save Changes'. A table shows a rule with the condition 'When users meet these conditions' and the action 'assign these roles'. Below the table, there are radio button options for role assignment: 'Merge settings for all assigned roles' (selected), 'User must select from among assigned roles', and 'User must select the sets of merged roles assigned by each rule'. A note at the bottom states: 'Note: Users that do not meet any of the above rules will not be able to sign into this realm.'

7. Verify **Rules based on:** on the following screen is **Username**.

8. Enter a name in the **Name:** field.

9. Under the **Rule: If Username...** section, verify the pull down menu is set to **is** enter the wild card variable ***.***

The screenshot shows the 'Role Mapping Rule' configuration page. The 'Rule based on:' dropdown is set to 'Username'. The 'Name:' field contains 'SecurID'. The 'Rule: If username...' section has a dropdown set to 'is' and a text input field containing '*.*'. Below this, the '...then assign these roles' section shows 'Available Roles' with 'Cert-Role Users' and 'Selected Roles' with 'RSA-Role'. There are 'Add ->' and 'Remove' buttons between the two lists. At the bottom, there is a checkbox for 'Stop processing rules when this rule matches' and 'Save changes?' buttons for 'Save Changes' and 'Save + New'.


10. Under the **...then assign these roles** section, select the Role previously created in Step 2 under the **Creating a User Role** section of this document.

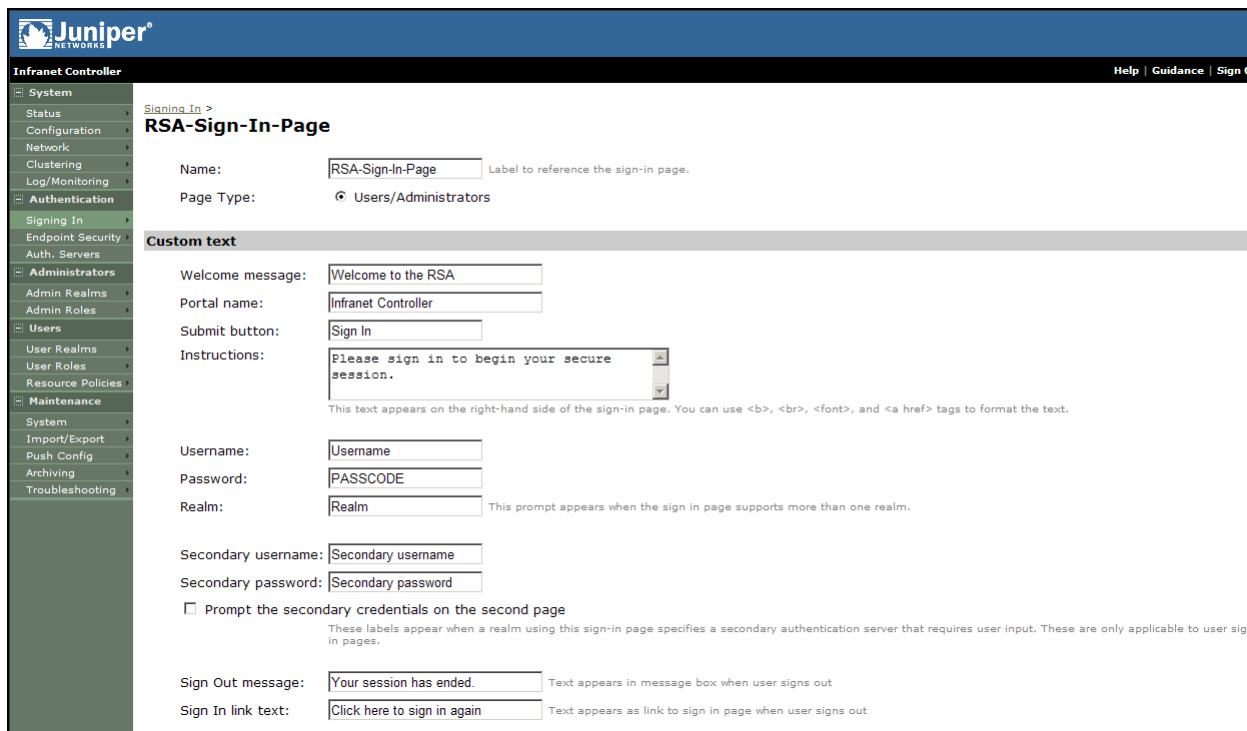
11. Click **Save Changes**.



Creating a Sign-In Page

1. Click on **Signing-In** on the left hand pane.
2. Enter a name in the **Name:** field.
3. Under the Custom text section, customize the first five fields as desired.
4. Under the **Password:** field, change the verbiage to **PASSCODE**.

 **Note:** Changing the Password field to “PASSCODE” is recommended so the user is aware on what type of credentials to enter when logging on, however, this may or may not violate specific security policies adopted by your organization.



The screenshot shows the Juniper Infranet Controller configuration interface. The left sidebar contains a navigation menu with categories like System, Authentication, and Maintenance. The main content area is titled 'RSA-Sign-In-Page' and contains several configuration fields:

- Name:** RSA-Sign-In-Page (Label to reference the sign-in page.)
- Page Type:** Users/Administrators
- Custom text** section:
 - Welcome message:** Welcome to the RSA
 - Portal name:** Infranet Controller
 - Submit button:** Sign In
 - Instructions:** Please sign in to begin your secure session. (This text appears on the right-hand side of the sign-in page. You can use ,
, , and <a href> tags to format the text.)
 - Username:** Username
 - Password:** PASSCODE
 - Realm:** Realm (This prompt appears when the sign in page supports more than one realm.)
 - Secondary username:** Secondary username
 - Secondary password:** Secondary password
 - Prompt the secondary credentials on the second page (These labels appear when a realm using this sign-in page specifies a secondary authentication server that requires user input. These are only applicable to user sign in pages.)
 - Sign Out message:** Your session has ended. (Text appears in message box when user signs out)
 - Sign In link text:** Click here to sign in again (Text appears as link to sign in page when user signs out)

5. Click **Save Changes**.



6. Click on Sign in Policy near top of page.
7. Click on New URL.
8. Enter */ for default page or <host/path> for customer URL page. (ie:www.companyname.com/uacusers)
9. Select the **Sign-in page** previously created in step 2 of this section above.

The screenshot shows the Juniper Infranet Controller web interface. The left sidebar contains a navigation menu with categories like System, Authentication, Administrators, Users, and Maintenance. The main content area is titled 'Sign-In Policy' and 'Odyssey Configuration'. It includes a 'Save Changes' button and several configuration fields: 'User type' (radio buttons for Users and Administrators), 'Sign-in URL' (text input with format instructions), 'Description' (text input), 'Sign-in page' (dropdown menu), and 'Install Agent' (checkbox). Below these fields is the 'Authentication realm' section, which has two radio button options: 'User types the realm name' and 'User picks from a list of authentication realms'. The second option is selected. Under this option, there are two lists: 'Available realms' (Users, Steel Belted Radi, Cert-Realm) and 'Selected realms' (AuthMan-Native). Buttons for 'Add ->', 'Remove', 'Move Up', and 'Move Down' are provided to manage these lists.

10. Under the Authentication realm section select either option. For the purposes of the documents, **Users picks from a list of authentication realms** has been selected so the user does not have to type in the realm.
11. Click **Save Changes**.

Certification Checklist For RSA Authentication Manager 6.1

Date Tested: March 8, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.2	Windows 2003
Unified Access Control (UAC)	2.1 R3 (build 10945)	Proprietary
Steel Belted RADIUS	V6.10.4280	Windows 2003 (SP2)

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Credential	<input type="checkbox"/> N/A	Set Credential	<input type="checkbox"/>
Retrieve Credential	<input type="checkbox"/> N/A	Retrieve Credential	<input type="checkbox"/>

CMY

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



Certification Checklist For RSA Authentication Manager 7.1

Date Tested: March 27, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003
Unified Access Control (UAC)	2.1 R3 (build 10945)	Proprietary
Steel Belted RADIUS	V6.10.4280	Windows 2003 (SP2)

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

CMY

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



Known Issues

12. When authenticating via the RSA Native protocol for the first time and selecting a **System Generated PIN**, the PIN does get set on the Authentication Manager Server, however, the user experience is that the authentication fails. To remediate the issue, the user can simply reauthenticate using the System Generated PIN plus Tokencode (PASSCODE). This behavior does not apply when a user defines the PIN.

Appendix

Removing the Node Secret

1. On the left hand pane, click on **Authentication** and then **Auth.Servers**.
2. On the right hand pane, click the **Settings** tab.
3. Under the **Node Verification File** section, select the **this node** box.
4. Click the **Delete** button directly below the box.
5. Click **Save Changes**.

The screenshot shows the Juniper Infranet Controller web interface. The left sidebar contains a navigation menu with categories like System, Authentication, Administrators, Users, Maintenance, and Troubleshooting. The main content area is titled 'Native-RSA' under the 'Auth Servers' section. It has tabs for 'Settings' and 'Users'. The 'Settings' tab is active, showing fields for 'Name' (Native-RSA), 'ACE Port' (5500), and a checked option for 'Users authenticate using tokens or one-time passwords'. Below this is the 'Configuration File' section with 'Current config file' and 'Imported on' (Wed Aug 8 01:23:02 2007) information, and an 'Import new config file' section with a 'Browse...' button. The 'Node Verification File' section contains a table with columns 'Node' and 'Creation Time'. The 'Node' column has a checked box for 'this node' and a 'Delete' button below it. The 'Creation Time' column shows 'Wed Aug 8 01:34:57 2007'. At the bottom, there is a 'Save Changes ?' section with 'Save Changes' and 'Reset' buttons.

Node	Creation Time
<input checked="" type="checkbox"/> this node	Wed Aug 8 01:34:57 2007