How to integrate RSA ACE Server SecurID Authentication with Juniper Networks Secure Access SSL VPN (SA) with Single Node or Cluster (A/A or A/P)

The following document was prepared using:

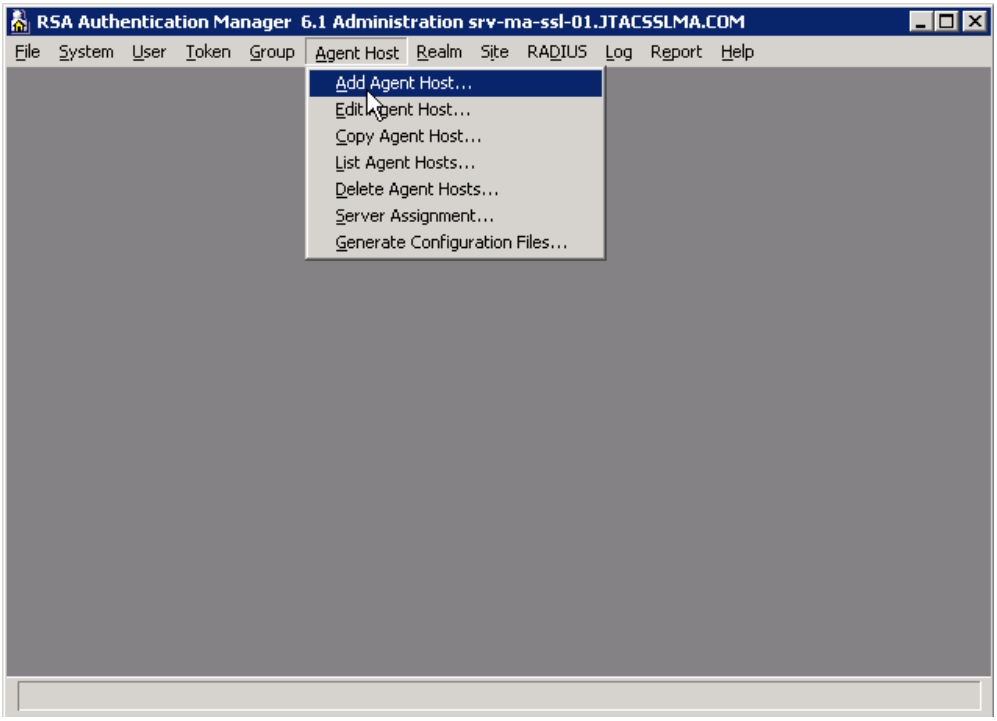
SA OS Version - 7.1R2
RSA ACE Version - 6.1

Scenario # 1: Single Node or Standalone SA

There are four configuration steps required to integrate RSA SecurID with the SA appliance.

1. Add SA as an Agent Host in the RSA Authentication Manager's database and create sdconf.rec file.
2. Add ACE server to the SA configuration and import the sdconf.rec file.
3. Bind the Ace server to an SA authentication realm
4. Configure role mapping rules

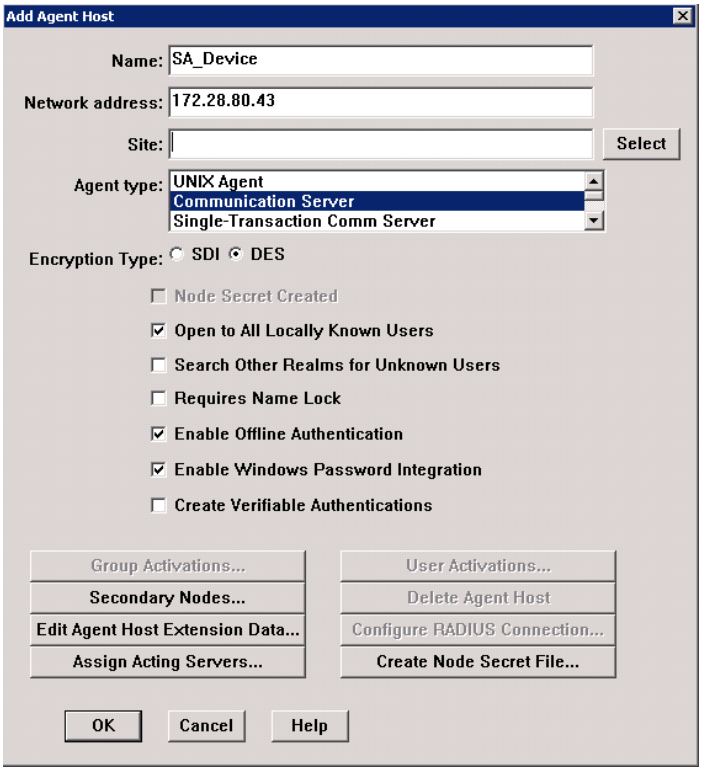
Step 1: Add the SA as an Agent Host within the RSA Authentication Manager's database and create an sdconf.rec file.



1. On the RSA Authentication Manager computer, go to **Start → All Programs → RSA Security → RSA Authentication Manager Host Mode**. On the Agent Host menu, choose "**Add Agent Host**".

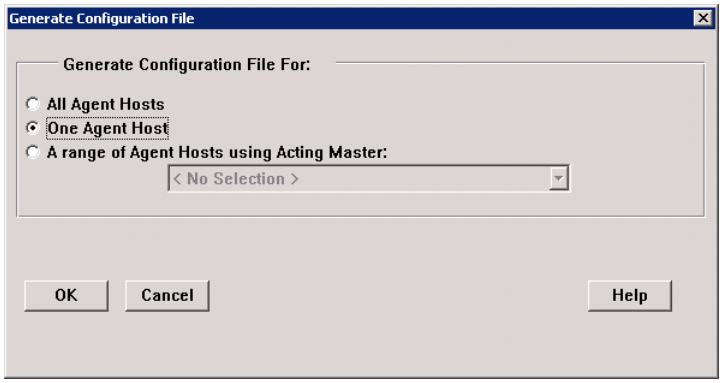
- **Name:** Type the hostname of the SA
- **Network Address:** Type the **real IP address** of the SA internal interface for **NodeA**
- **Agent Type:** Select **Communication Server**
- **Encryption Type:** Choose your encryption method. The SA supports both **SDI & DES** encryption
- Assign users to the Agent Host by choosing either **"Open to All**

- **Locally Known Users" or click "User Activations"** and assign users. In our example we choose **"Open to All Locally Known Users".**



Click** OK **to add the SA as an Agent Host to the RSA Authentication Manager's database.

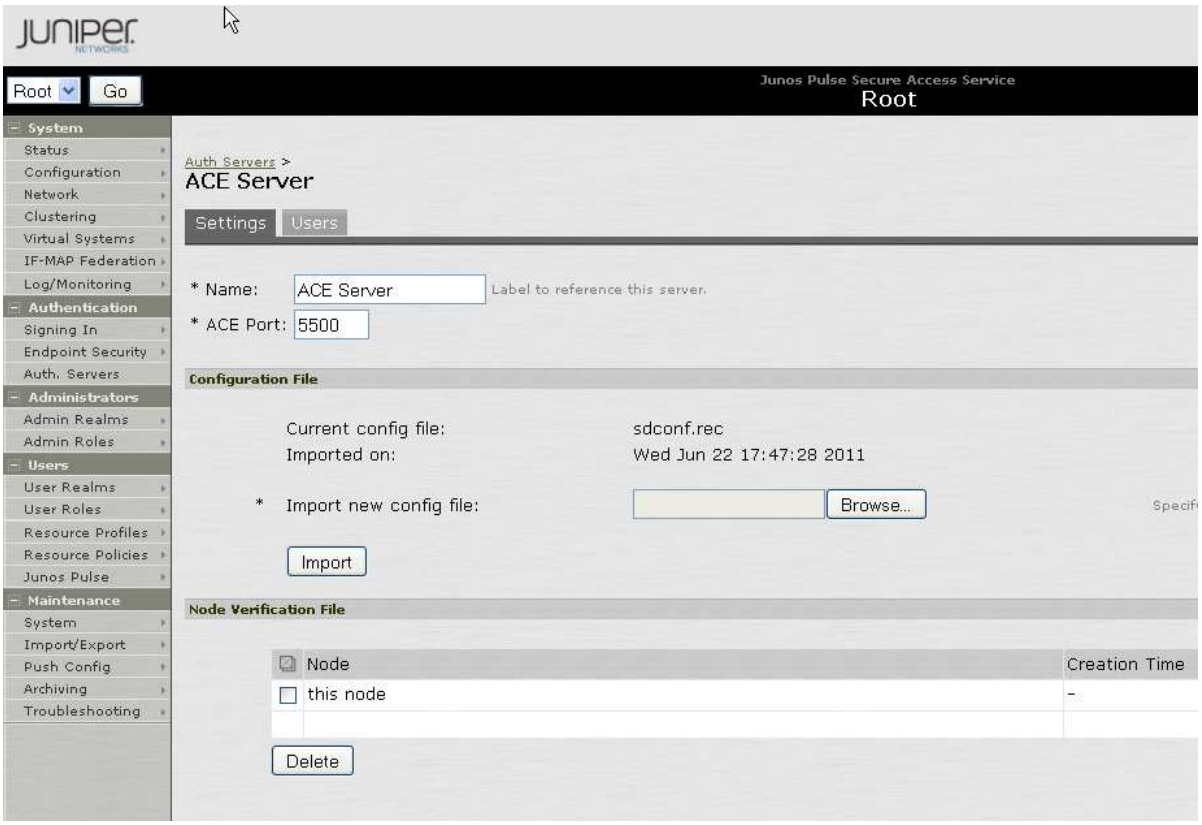
2. In **the RSA Authentication Manager** choose **Add Agent → Generate Configuration File → One Agent Host**. Select the Agent Host for the SA created in Step 2 and Click **OK** and save the sdconf.rec file in a known directory. The same sdconf.rec file will be used in subsequent steps to import on the ACE server instance created on the SA device.



Step 2: Add the ACE server as an authentication server instance on the SA by importing the sdconf.rec file

1. In the Administrator Console, choose **Authentication →Auth Servers →ACE → New Server**. The configuration page for the ACE server appears. After the sdconf.rec is imported, the ACE configuration is synchronized across all members of the cluster.

    - **Name:** Enter a name to identify the ACE Server instance
    - **Port:** Change if needed but the default is 5500
    - **Import new config file:** Click the "Browse" button and upload the sdconf.rec file.
    - Click **Save Changes**

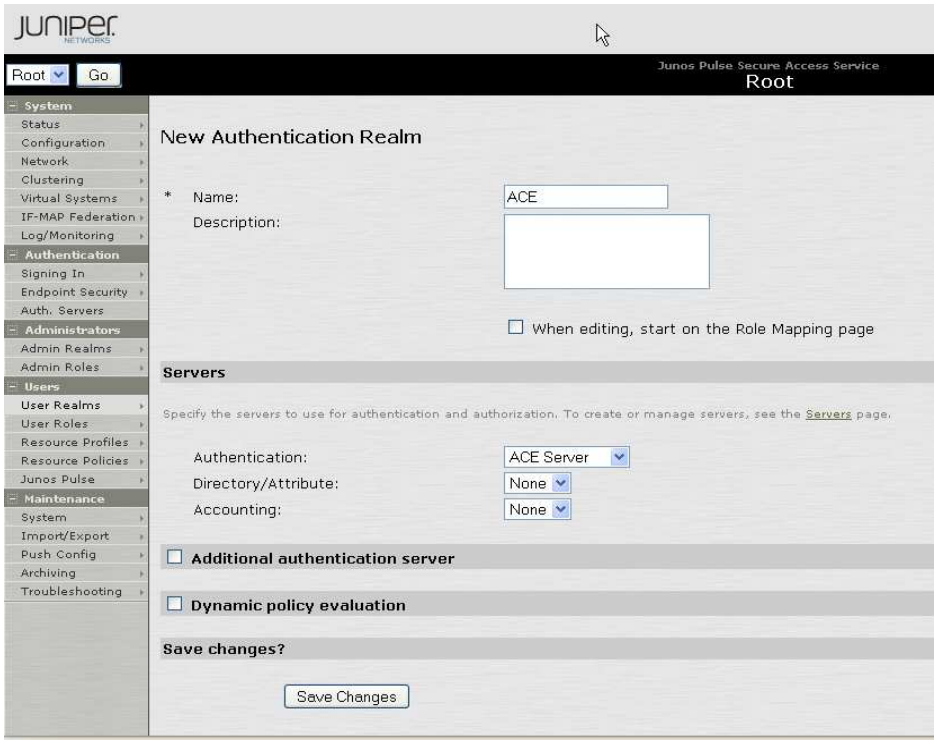


Note: Under Node Verification file, the "Creation Time" is blank. This will not be filled in until at least one user authenticates successfully to this SA device.

Step 3: Bind the ACE Server to an SA Authentication Realm:

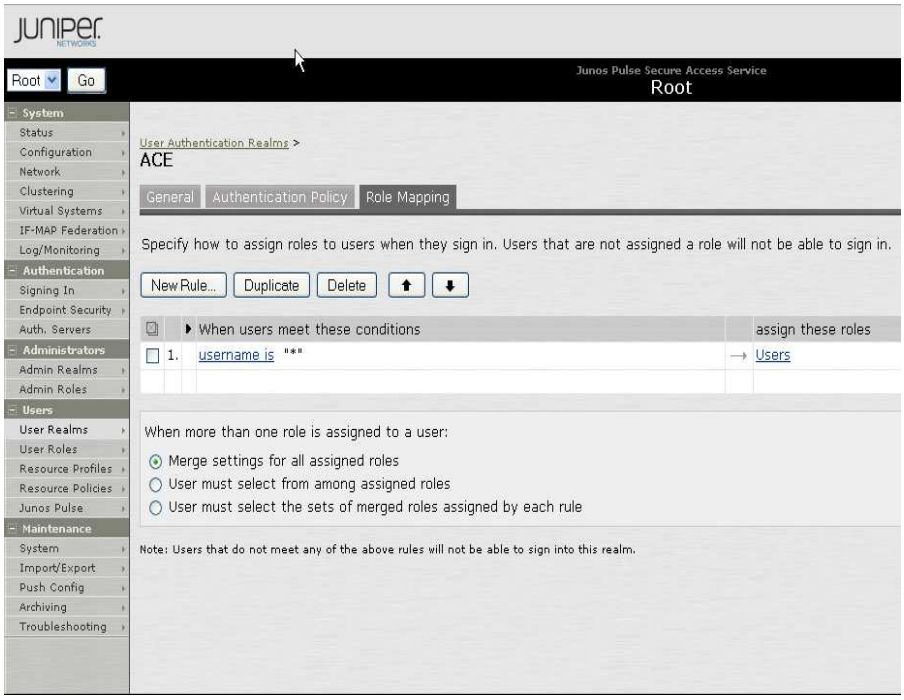
1. Go to **Users** → **Roles** and create a role for your SecurID users based on your secure access policies.
2. Go to **Users** → **Realm** → **New** and enter the appropriate information for the Authentication Realm

    - **Name:** Give the Realm a Name
    - **Authentication Server:** Select the ACE server defined step above and save changes



Step 4: Configure Role-Mapping rules.

1. Click “New Rule” and create a role mapping rule.



After successfully configuring the server, SecurID authentication is enabled on the SA. Users who are configured to use SecurID authentication can sign in with their username and their SecurID Passcode.

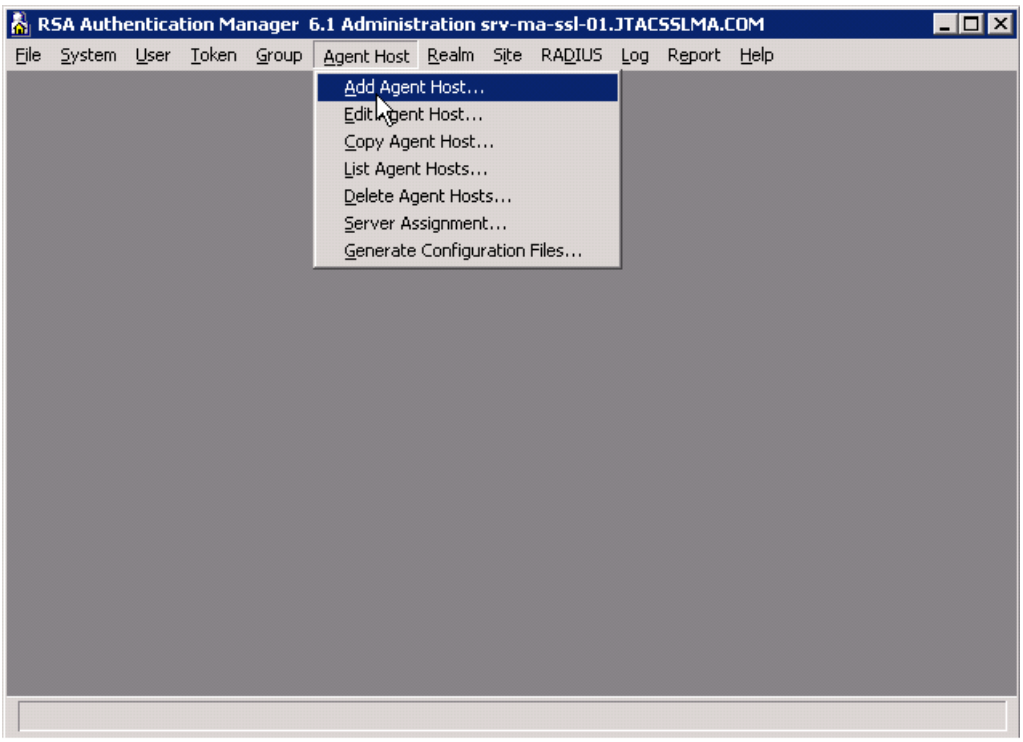
Scenario # 2: Active/Active or Active/Passive SA Cluster

There are four configuration steps required to integrate RSA SecurID with the SA appliance.

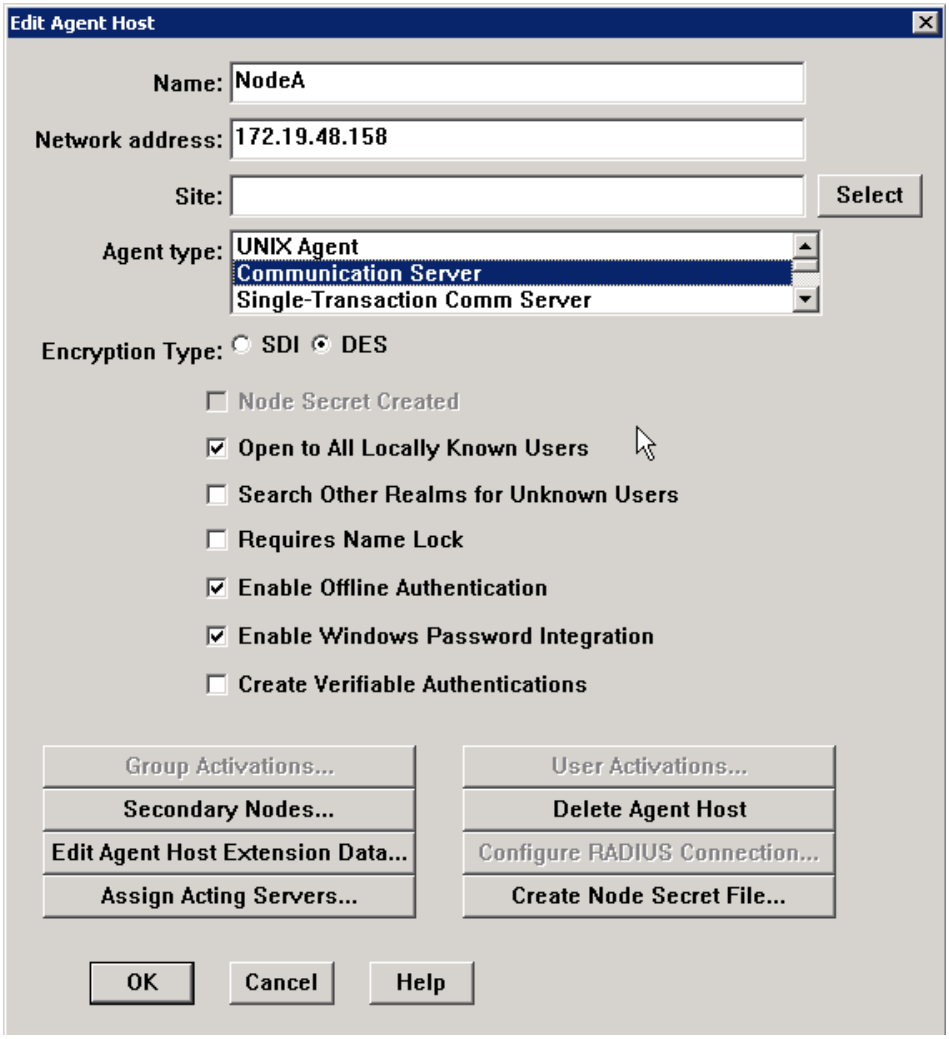
1. Add **each SA node** of the cluster as an Agent Host in the RSA Authentication Manager's database and create sdconf.rec file.
2. Add ACE server to the SA configuration and import the sdconf.rec file.
3. Bind the Ace server to an SA authentication realm
4. Configure role mapping rules

Step 1: Create an Agent Host within RSA Authentication Manager, one for each member in the SA Cluster with its corresponding IP address.

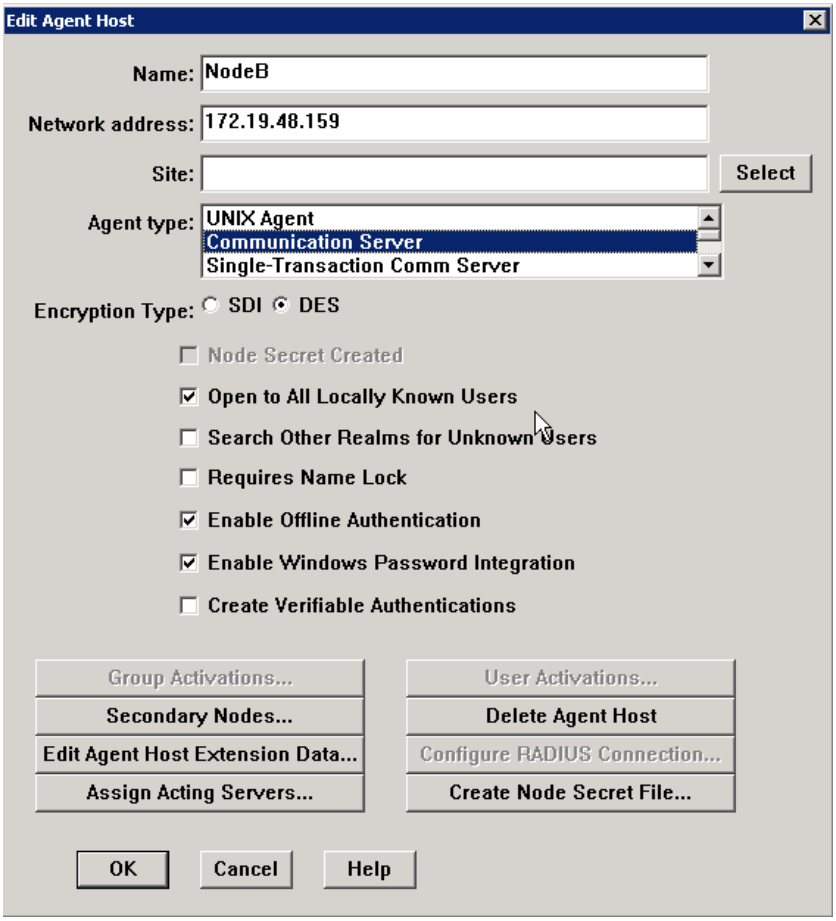
1. On the RSA Authentication Manager computer, go to **Start> All → Programs → RSA Security → RSA Authentication Manager Host Mode**. On the Agent Host menu, choose **"Add Agent Host".**



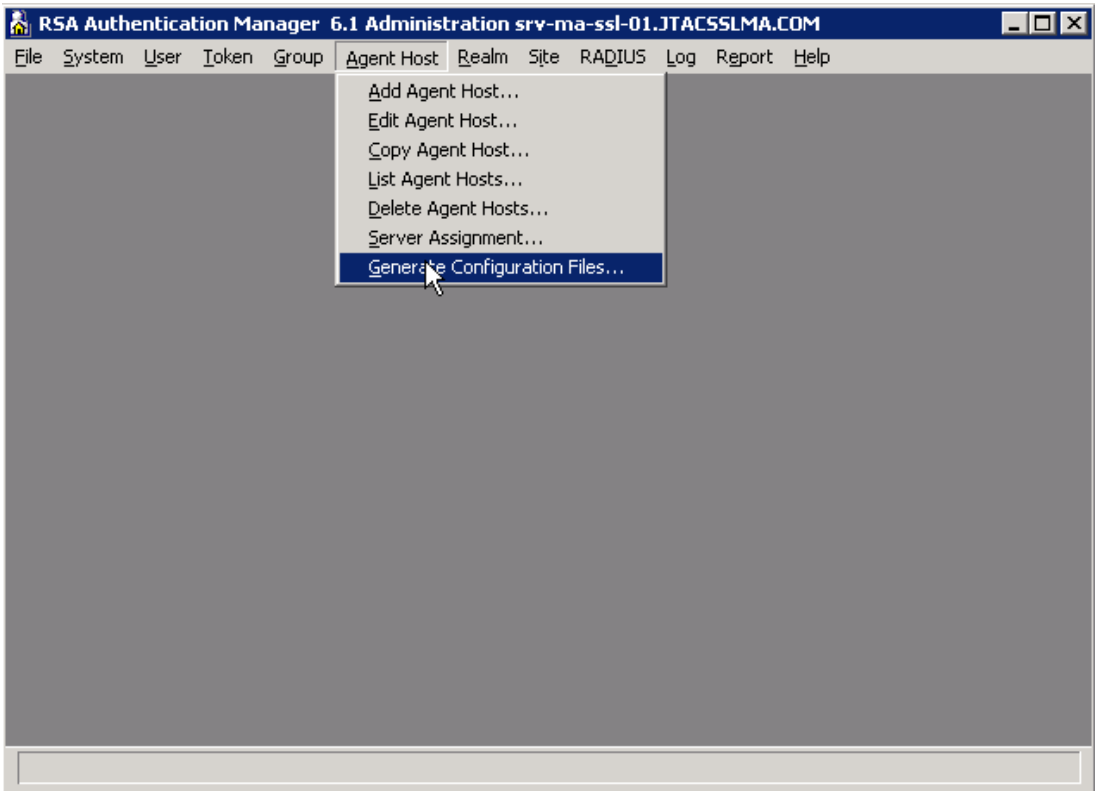
- **Name:** Type the hostname of the SA
- **Network Address:** Type the **real IP address** of the SA internal interface for **NodeA**
- **Agent Type:** Select **Communication Server**
- **Encryption Type:** Choose your encryption method. The SA supports both **SDI & DES** encryption
- Assign users to the Agent Host by choosing either **"Open to All Locally Known Users" or click "User Activations"** and assign users. In our example we choose **"Open to All Locally Known Users".**
- Click **OK** to add the SA as an Agent Host to the RSA Authentication Manager's database.

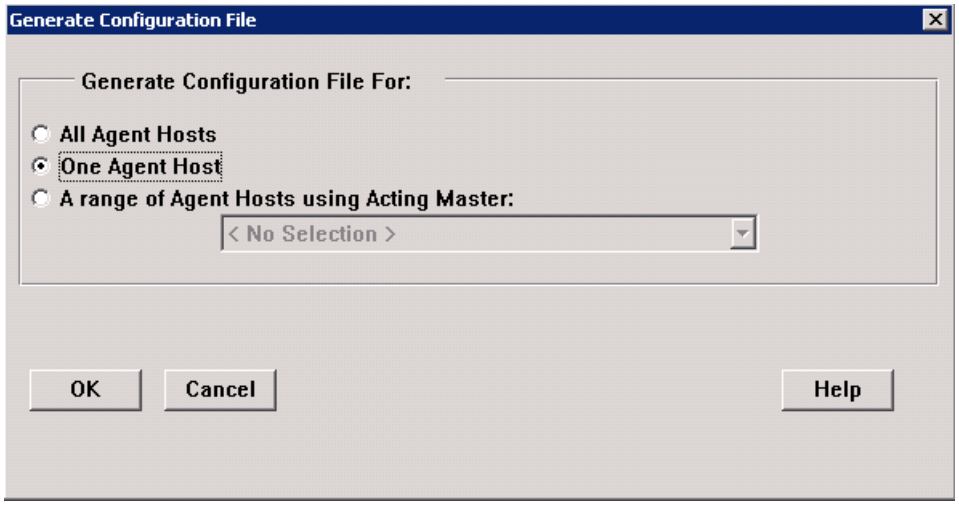


- **Go back and repeat step one for "Node B" as shown in the screenshots below.**

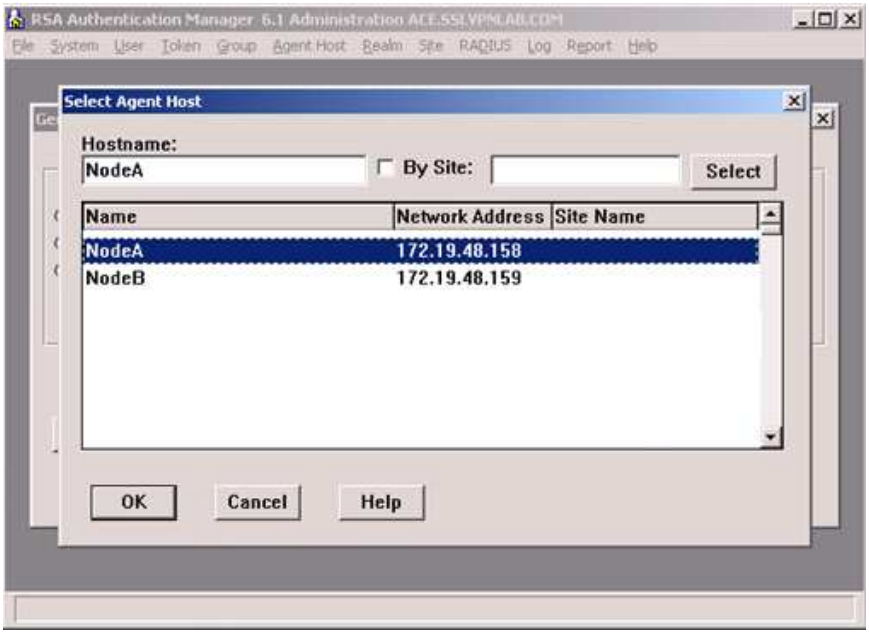


2. In the **RSA Authentication** choose **Generate Configuration File>One Agent**





3. Select any one of the above two Agent Hosts that were created as above in Step 1 and Click **OK** to save the sdconf.rec file in a known directory.



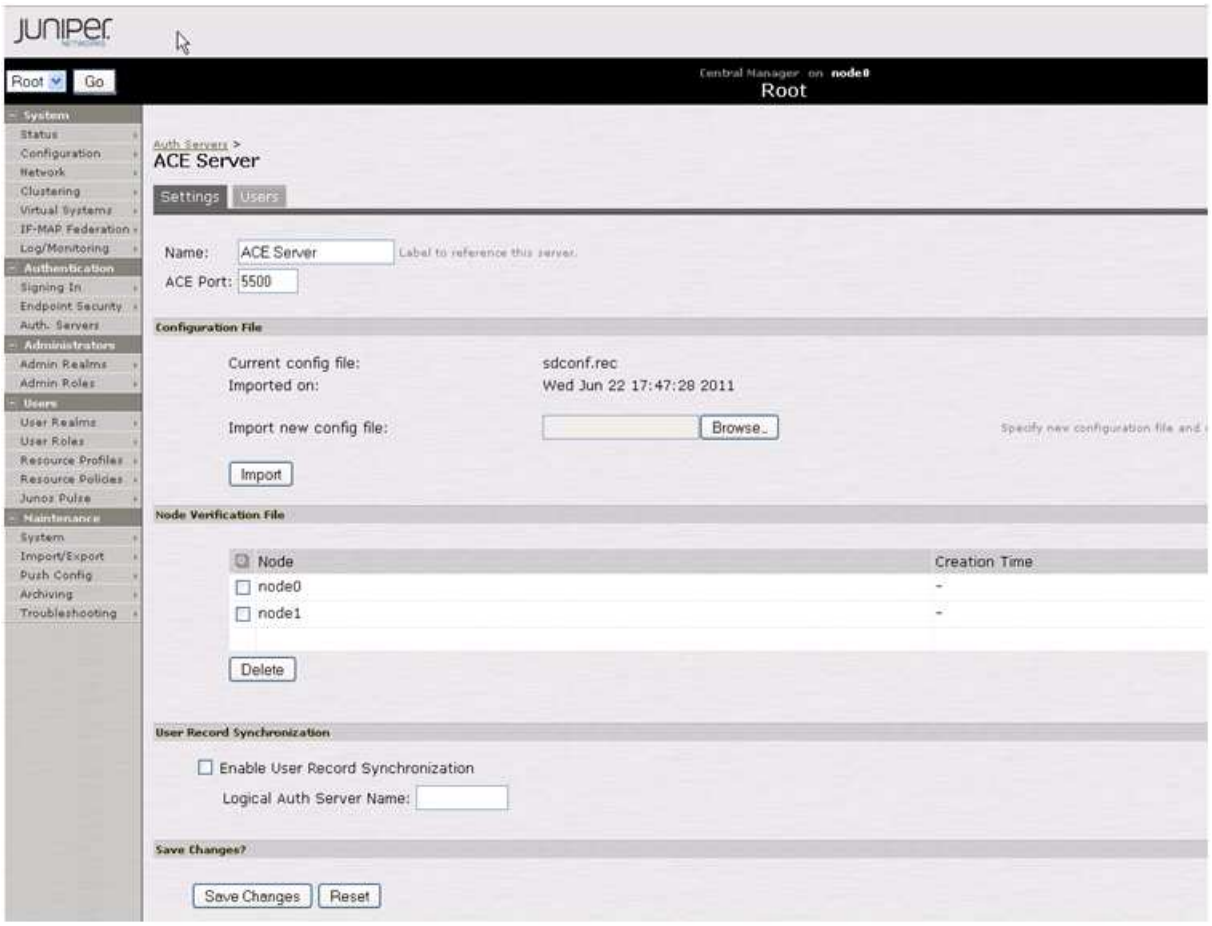
4. In the above screenshot we have saved sdconf.rec file of Agent host ‘NodeA’. The same sdconf.rec file will be used in subsequent steps to import on the ACE server instance created on the SA device.

Step 2: Add the ACE server as an authentication server instance on the SA by importing the sdconf.rec file

In the Administrator Console, choose **Authentication → Auth Servers → ACE → New Server**.

The configuration page for the ACE server appears. After the sdconf.rec is imported, the ACE configuration is synchronized across all members of the cluster.

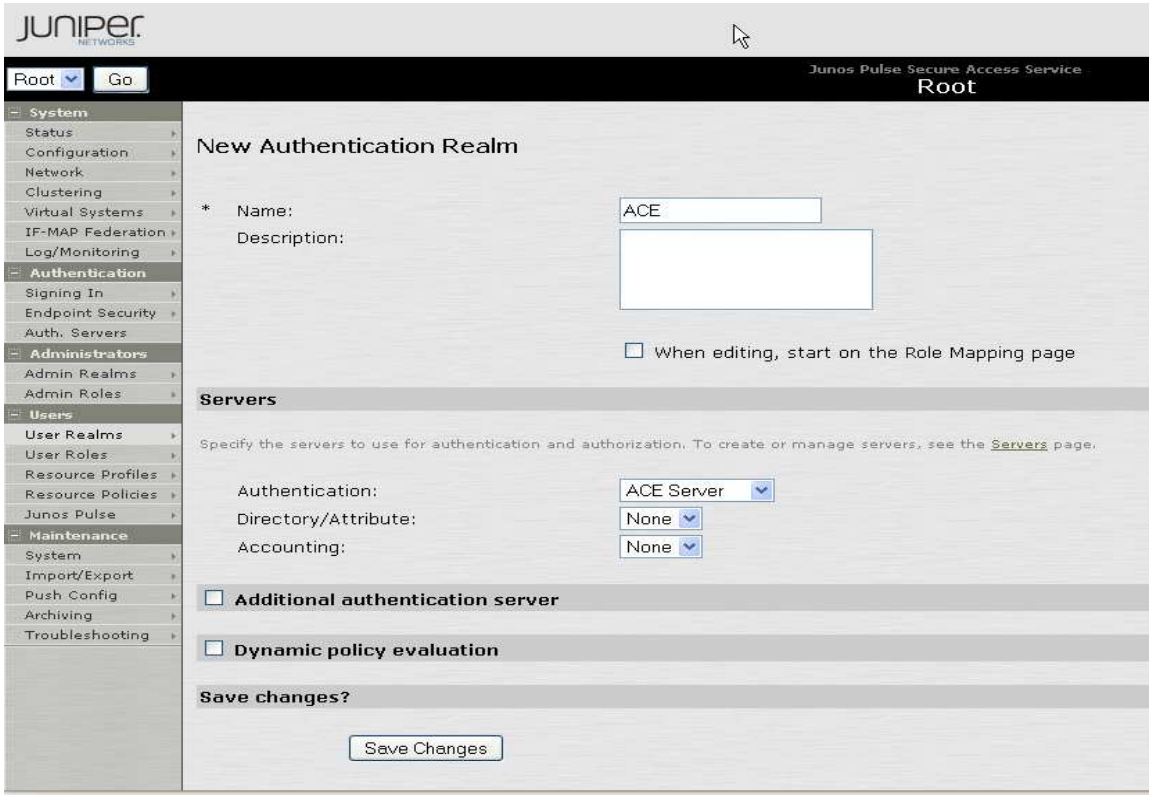
- **Name:** Enter a name to identify the ACE Server instance
- **Port:** Change if needed but the default is 5500
- **Import new config file:** Click the "Browse" button and upload the sdconf.rec file.
- **In this case upload sdconf.**rec file saved as shown in above step1.
- Click **Save Changes**



Note: Under Node Verification file, the "Creation Time" is blank. This will not be filled in until at least one user authenticates successfully to each of the nodes. You will need to log into the physical IP of each node to allow the SA and the ACE server to negotiate a node secret on first successful login.

Step 3: Bind the ACE Server to an SA Authentication Realm:

1. Go to **Users>Roles** and create a role for your SecurID users based on your secure access policies.
2. Go to **Users>Realm>New** and enter the appropriate information for the Authentication Realm



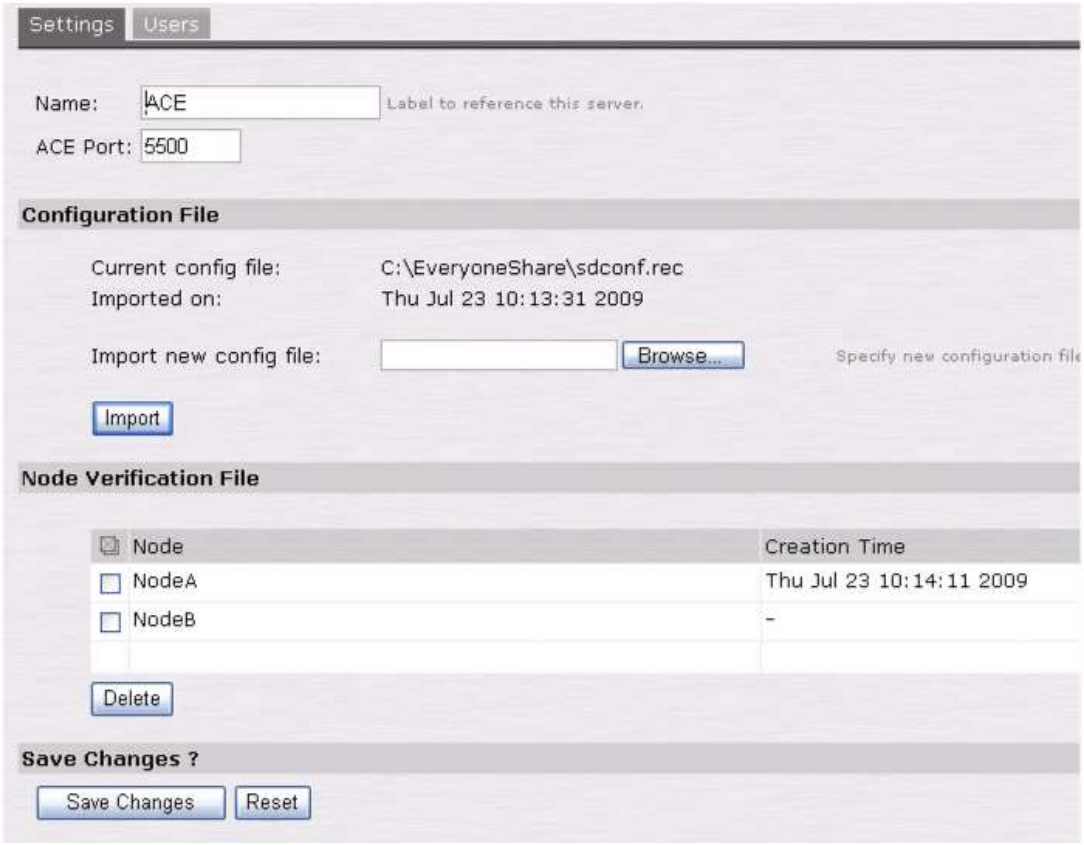
- **Name:** Give the Realm a Name
- **Authentication Server:** Select the ACE server defined step above and save changes

Step 4: Configure Role-Mapping rules.

Click “New Rule” and create a role mapping rule.

After successfully configuring the server, SecurID authentication is enabled on the SA. Users who are configured to use SecurID authentication can sign in with their username and their SecurID Passcode.

Log directly into Node A Physical IP, and you will now see node secret file created for NodeA



Log directly into Node B Physical IP, and you will now see node secret file created for Node B as well.

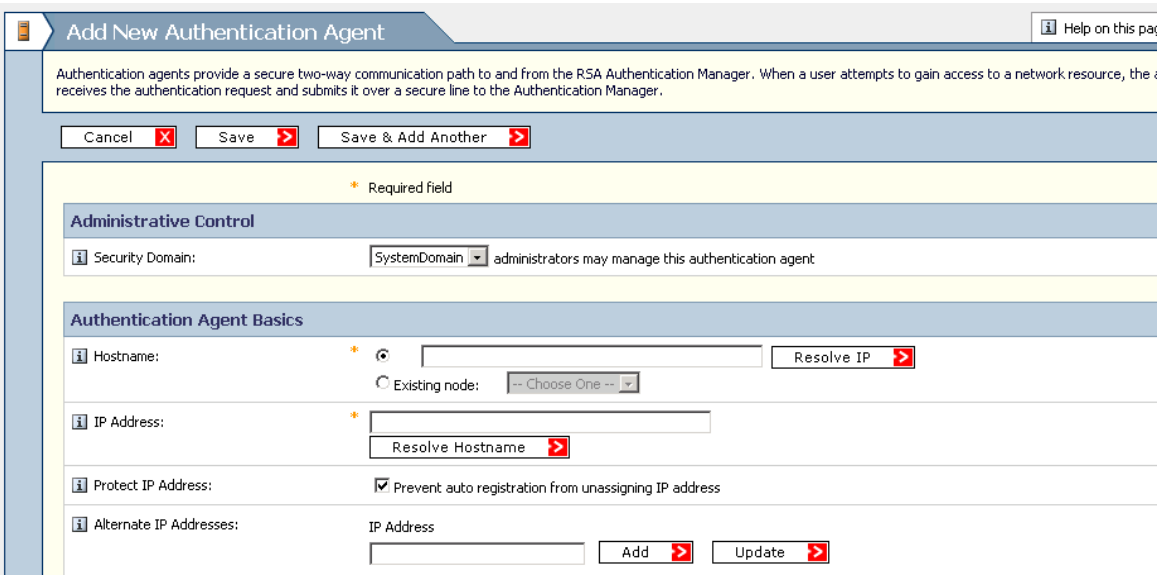
How to add an Authentication agent in ACE 7.1 Authentication Manager

1. Click **Access > Authentication Agents > Add New**.
2. From the **Security Domain** drop-down menu, select the security domain to which you want to add the new agent.
3. Use the **Hostname** buttons to specify whether you want to enter a new name for the agent or use an existing server name.

   If you choose to enter a new name, the name must be unique.

   If you choose to use an existing server node, the IP Address and Alternate IP Address fields are automatically populated with information for the host and are read-only.
4. In the **IP Address** field, enter the IP address of the agent.

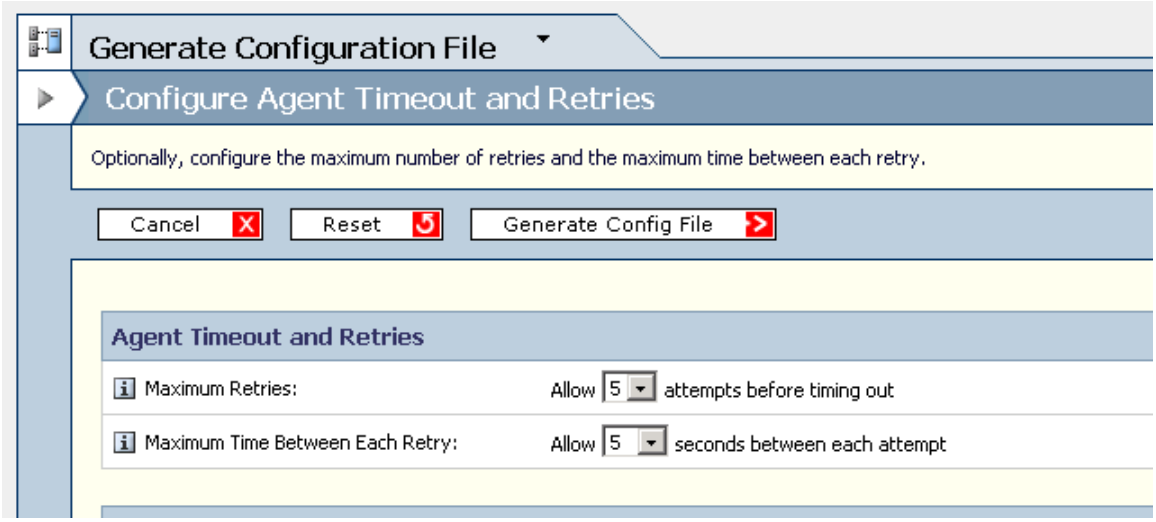
   If you choose to use an existing server name, this field is automatically populated and read-only.
5. From the **Agent Type** drop-down menu, select the type of agent you want to add. The default choice is **Standard Agent**.
6. Configure rest of the options as per your requirements.
7. Click **Save**.



This procedure configures communication between the authentication agent and RSA Authentication Manager, and generates the Authentication Manager configuration
file, sdconf.rec. Before an authentication agent can communicate with the
Authentication Manager, you must copy this file to the agent host.

To configure communication options and generate the configuration file:

1. Click **Access > Authentication Agents > Generate Configuration File**.
2. From the **Maximum Retries** drop-down menu, enter the number of times you want the authentication agent to attempt to establish communication with Authentication Manager before returning the message "Cannot initialize
   agent - server communications."
3. From the **Maximum Time Between Each Retry** drop-down menu, enter the number of seconds you want to set between attempts by the authentication
   agent to establish communications with Authentication Manager.
4. Click **Generate Config File**.
5. Click **Download Now** to download the configuration file.



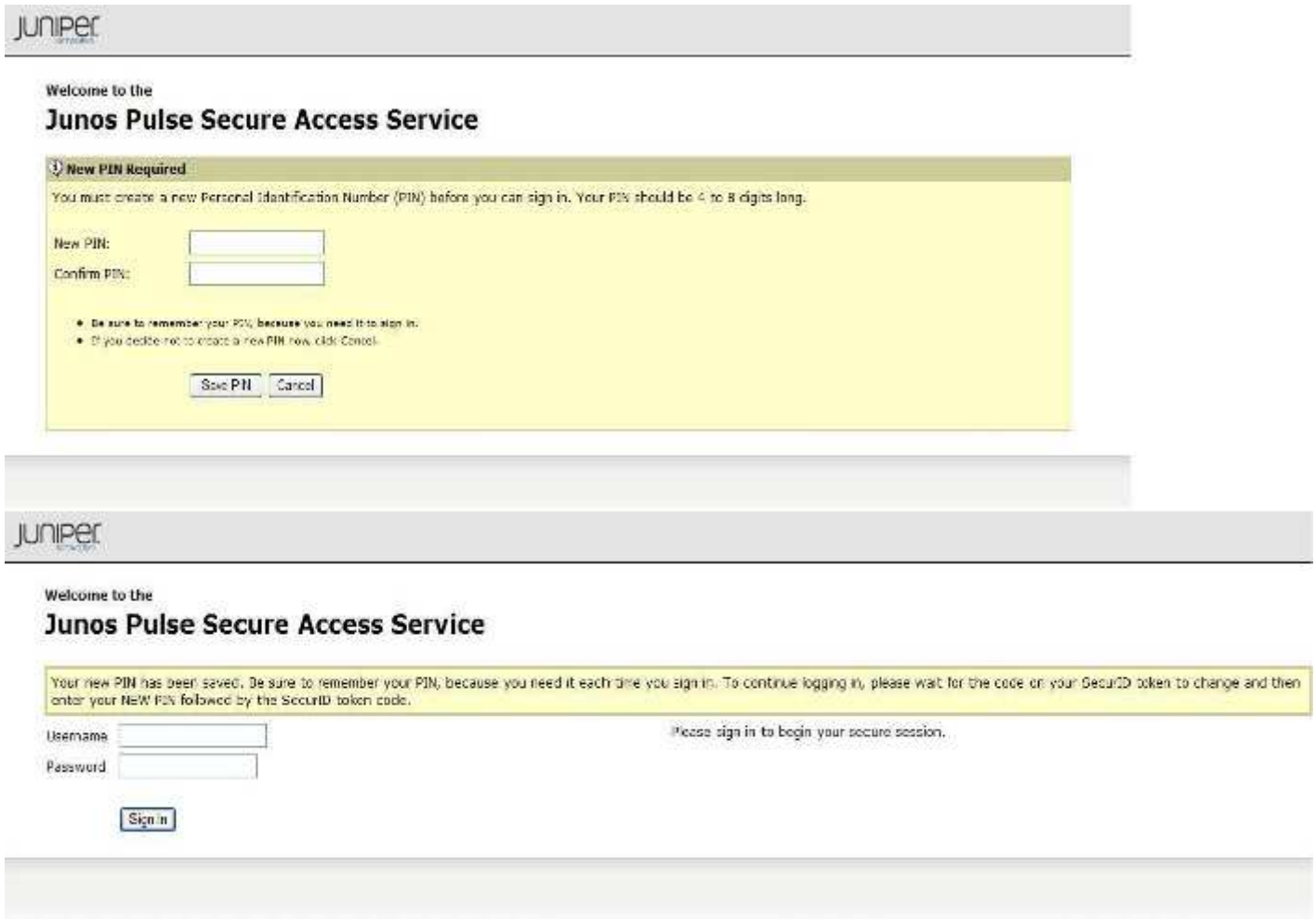
Additional ACE features:

SA ACE-ChallengeIntermediationPages

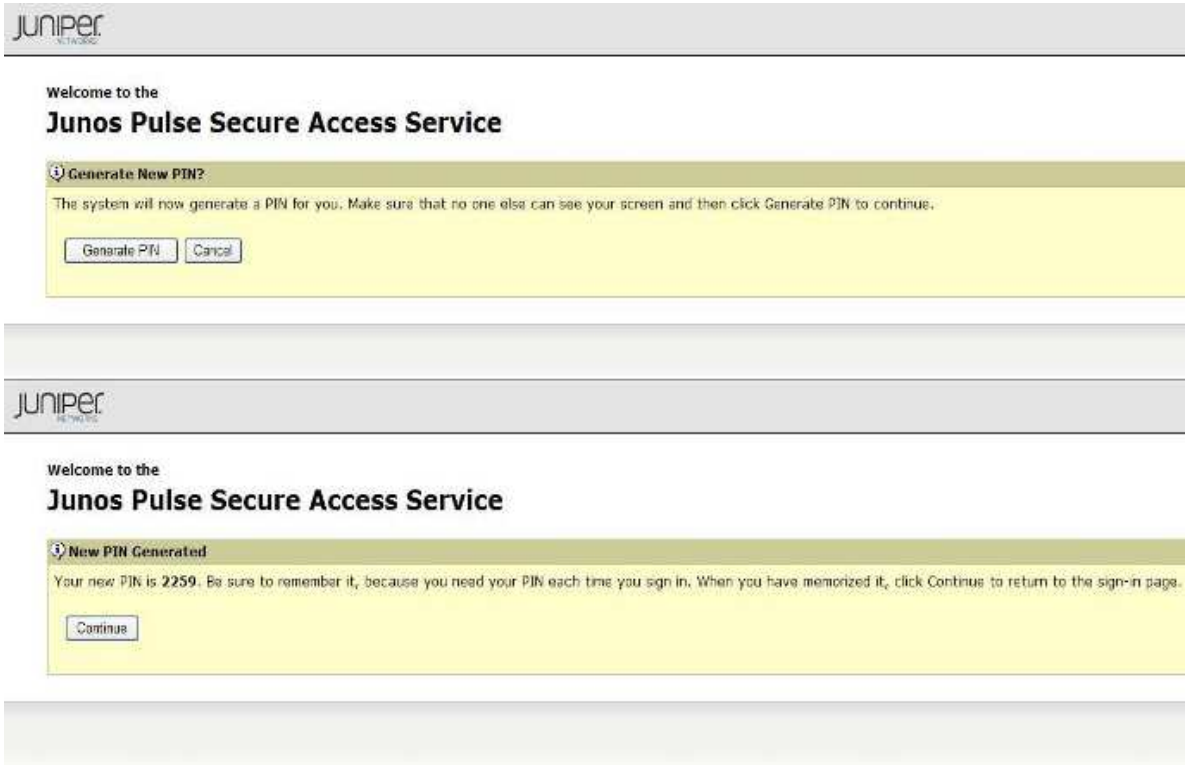
The SA supports the following ACE challenges:

- New PIN Mode
- System Generated PIN Next TOKENCODE Screen

New Pin Mode:



System Generated PIN:



Next Token Code Screen: