

How to Configure the RSA Authentication Manager

<https://campus.barracuda.com/doc/75694143/>

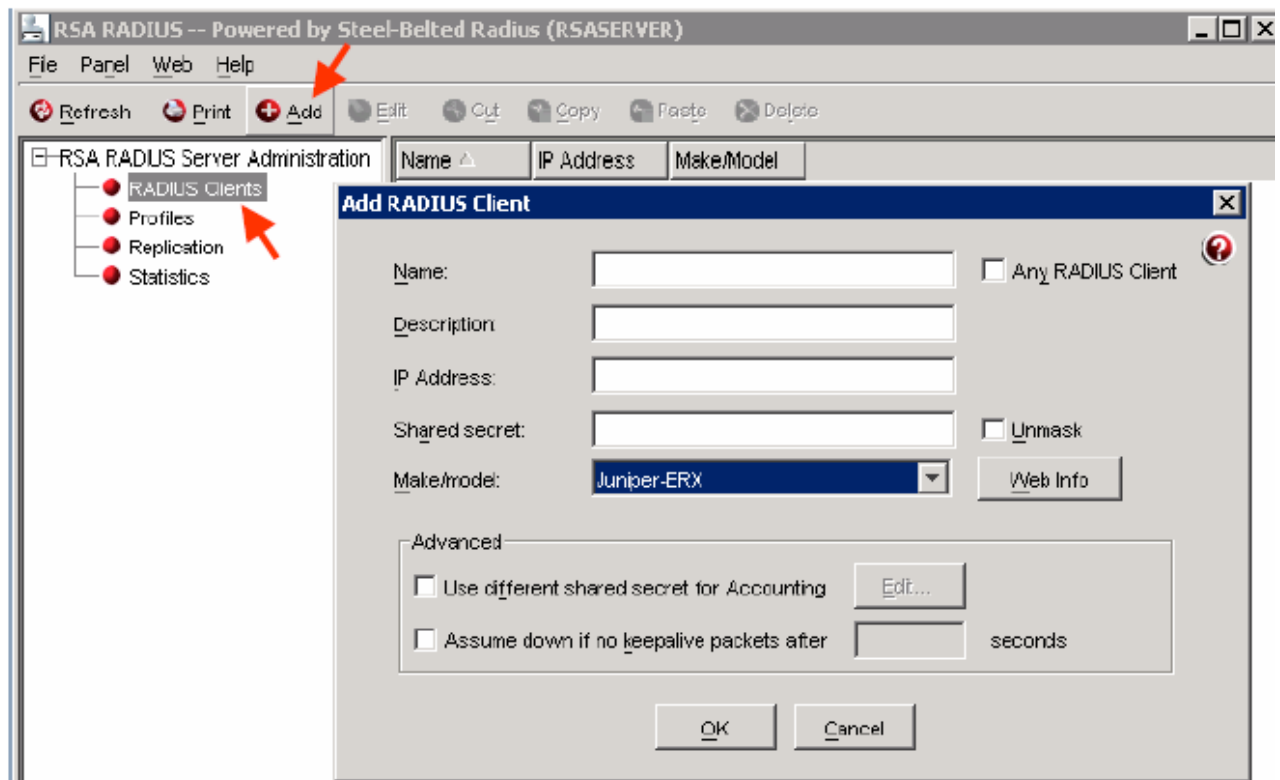
The Barracuda Load Balancer ADC can be configured as a RADIUS client to the RSA SecurID Server System, comprised of the RSA Authentication Manager and the Radius Server.

To configure the RSA Authentication Manager Server, complete the following steps:

1. [Configure the RADIUS protocol settings](#)
2. [Add the Barracuda Load Balancer ADC as an Agent Host](#)
3. [Import SecurID Tokens](#)
4. [Add Users to the RSA Authentication Manager and Assign Tokens](#)

Step 1: Configure the RADIUS Protocol Settings

1. Before configuring the RADIUS protocol, ensure the RADIUS server is up and running on the RSA Authentication Manager Server System. To check:
 1. Go to **Start > Programs > RSA Security** and select **RSA Authentication Manager Control Panel**.
 2. Select **Start & Stop RSA Auth Mgr Services** in the tree on the left pane. The **Status** of **RSA RADIUS Server** must be **Running**. If not, click **Start RADIUS** to bring it up.
2. On the **RSA Authentication Manager Server System**, go to **Start > Programs > RSA Security** and select **RSA Authentication Manager Host Mode**. Select the **RADIUS** menu, and select **Manage RADIUS Server**.
3. When the **RSA RADIUS** window appears, select **RADIUS Clients** in the tree on the left pane.
4. Click **Add**. The **Add RADIUS Client** window appears.



5. Specify values for the following fields:

- **Name** – Enter the hostname for the Barracuda Load Balancer ADC.
- **Description** – Optional.
- **IP Address** – Enter the IP address for the Barracuda Load Balancer ADC.
- **Shared Secret** – Type the secret key. You need to configure the same Shared Secret on the Barracuda Load Balancer ADC in **ACCESS CONTROL > Authentication Services > RADIUS**.
- **Make/Model** – Select **Juniper-ERX**.

6. Click **OK** to save your settings.

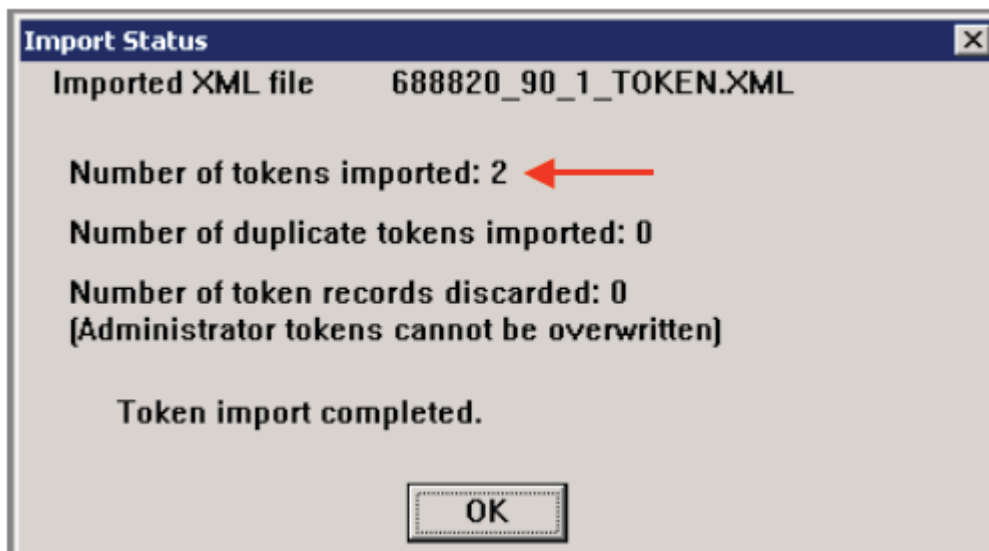
Step 2: Add the Barracuda Load Balancer ADC as an Agent Host

1. On the **RSA Authentication Manager Server System**, go to **Start > Programs > RSA Security** and select **RSA Authentication Manager Host Mode**.
2. Select the **Agent Host** menu, and select **Add Agent Host**. The **Add Agent Host** window appears.
3. Specify values for the following fields:
 - **Name** – Enter the hostname for the Barracuda Load Balancer ADC.
 - **Network Address** – Enter the IP address for the Barracuda Load Balancer ADC.
 - **Agent Type** – Select **Standard Agent**.
 - **Encryption Type** – Select **DES** or **SDI** encryption.
 - Select **Open to All Locally Known Users** and **Requires Name Lock**.
4. Click **User Activations** to assign users to the Agent host.
5. Click **OK**. You have added the Barracuda Load Balancer ADC as an Agent Host on the RSA

Authentication Manager.

Step 3: Import SecurID Tokens

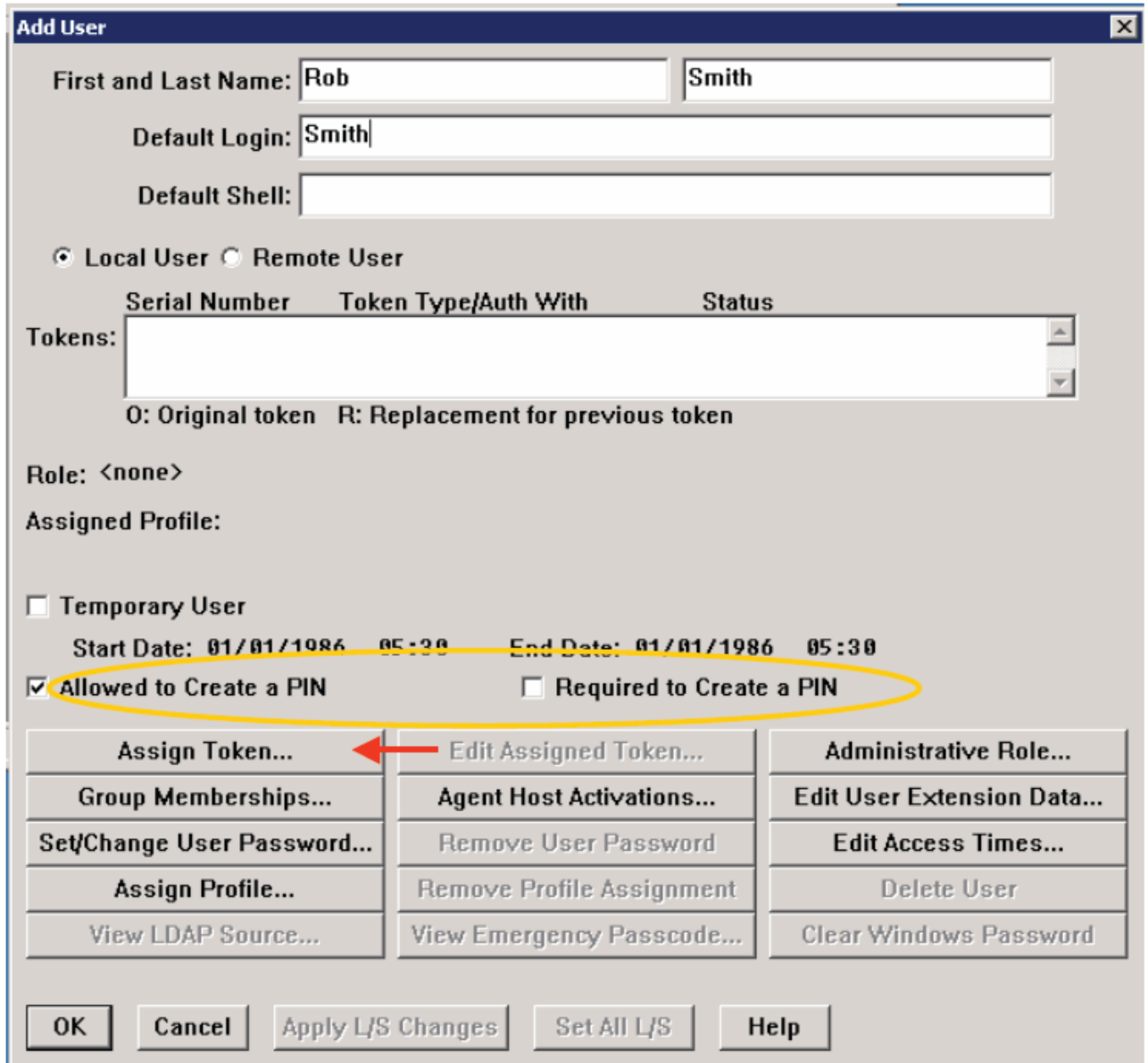
1. On the **RSA Authentication Manager Server System**, go to **Start > Programs > RSA Security** and select **RSA Authentication Manager Host Mode**.
2. From the **Token** menu, select **Import Tokens**.
3. Navigate to the token XML file provided by RSA and click **Open** to import the tokens.
4. The **Import Status** window appears displaying the number of tokens imported.



Step 4: Add Users to the RSA Authentication Manager and Assign Tokens

On the **RSA Authentication Manager Server System**, go to **Start > Programs > RSA Security** and select **RSA Authentication Manager Host Mode**.

1. From the **User** menu, select **Add User**.



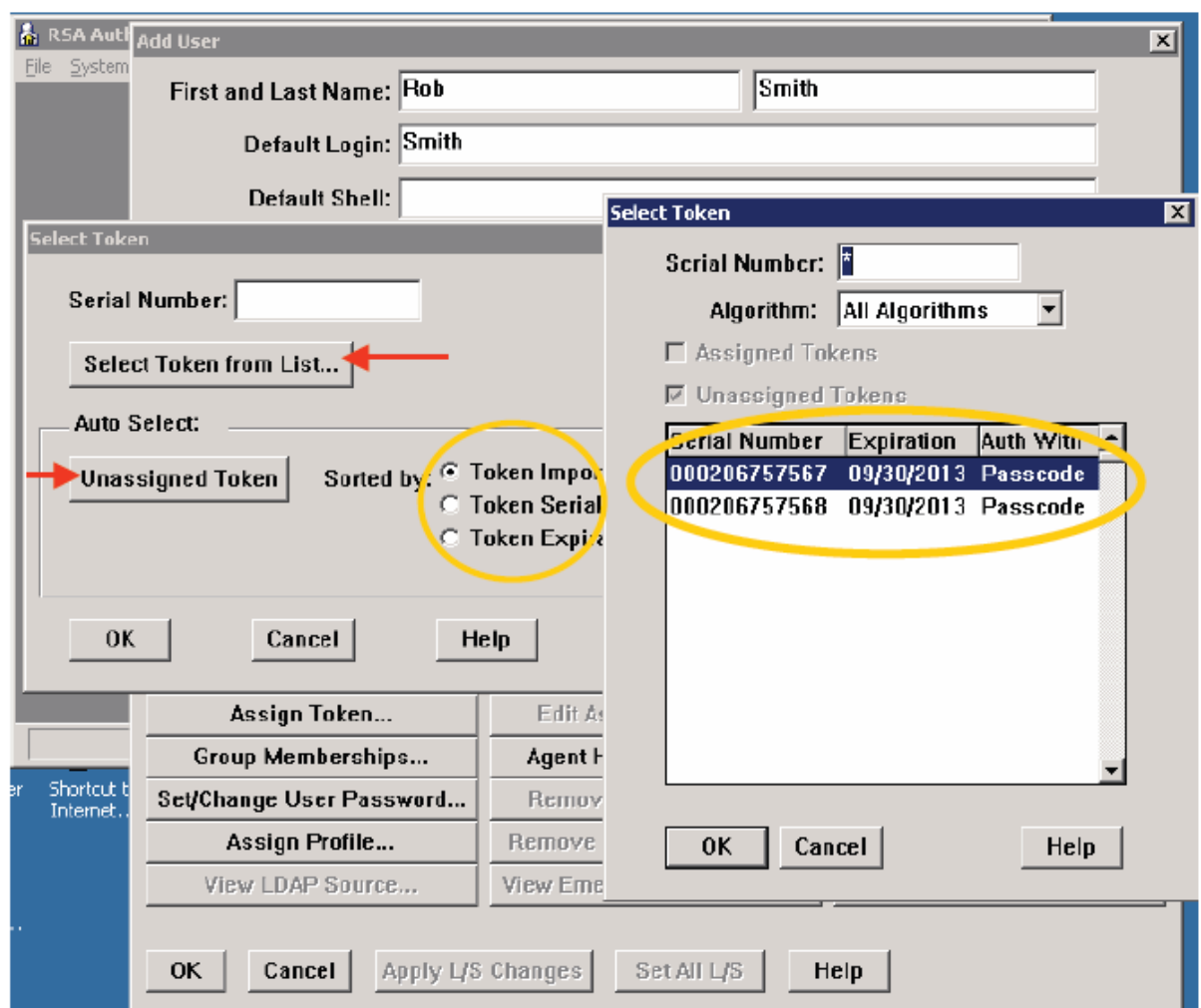
2. The **Add User** window appears. Specify values for the following fields:
 - **First and Last Name** – Enter a user's first and last name.
 - **Default Login** – Enter user's default username.
3. Users on the RSA Server can be authenticated in two ways: **Token Mode** or **Passcode Mode** (default). In **Token Mode**, users authenticate using the Tokencode currently generated by the RSA SecurID authenticator. In **Passcode Mode**, users authenticate using a Passcode (Personal Identification Number (PIN) followed by the Tokencode).

The code generated by the RSA SecurID authenticator is known as the **Tokencode**. The Tokencode changes continuously at a specified interval (typically every 60 seconds). The user's Passcode is the combination of the user's PIN and the user's current Tokencode.

A PIN can be generated:

- If **Allowed to Create a PIN** or **Required to Create a PIN** is NOT selected, the system generates the PIN and gives it to the user.

- If **Allowed to Create a PIN** is selected, the user can choose to create a PIN or have the system generate the PIN. The user is offered a system generated pin, and if declined, is prompted to enter a PIN.
 - If **Required to Create a PIN** is selected, the user must enter a PIN and is prompted to do so when logging in.
4. Select **Allowed to Create a PIN** or **Required to Create a PIN**.
 5. Select **Assign Token**. Click **Yes** to confirm. The **Select Token** window appears.
 - To automatically assign a token, select the method by which you want to sort the token using **Sorted by** in the **Auto Select** section. Click **Unassigned Token**, and then click **OK**.
 - To manually select the token, click **Select Token from List**. In the **Select Token** window, select the serial number for the token to assign, and click **OK**.



6. Give the user the serial number of the assigned token.

The RSA Authentication Manager configuration is now complete.

Next Step

Now that you have configured the RSA Authentication Manager to operate in conjunction with the Barracuda Load Balancer ADC, you now need to configure the service supported by RSA Authentication on the Barracuda Load Balancer ADC:

- [How to Configure the RSA Authentication Service on the Barracuda Load Balancer ADC](#)

Figures

1. RADIUS_Client_Window.png
2. RADIUS_Import_Status.png
3. RSA_Add_User.png
4. RSA_Select_Token.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.