

## How to Integrate RSA SecurID with the Barracuda Web Application Firewall

<https://campus.barracuda.com/doc/4259933/>

The Barracuda Web Application Firewall can be configured as a RADIUS client to the RSA SecurID server system, comprised of the RSA Authentication Manager and the Radius server. Integrating the Barracuda Web Application Firewall with RSA SecurID requires three steps:

1. [Configure the RSA Authentication Manager.](#)
2. [Configure the Barracuda Web Application Firewall.](#)
3. [Verify the Setup and Authentication Process.](#)

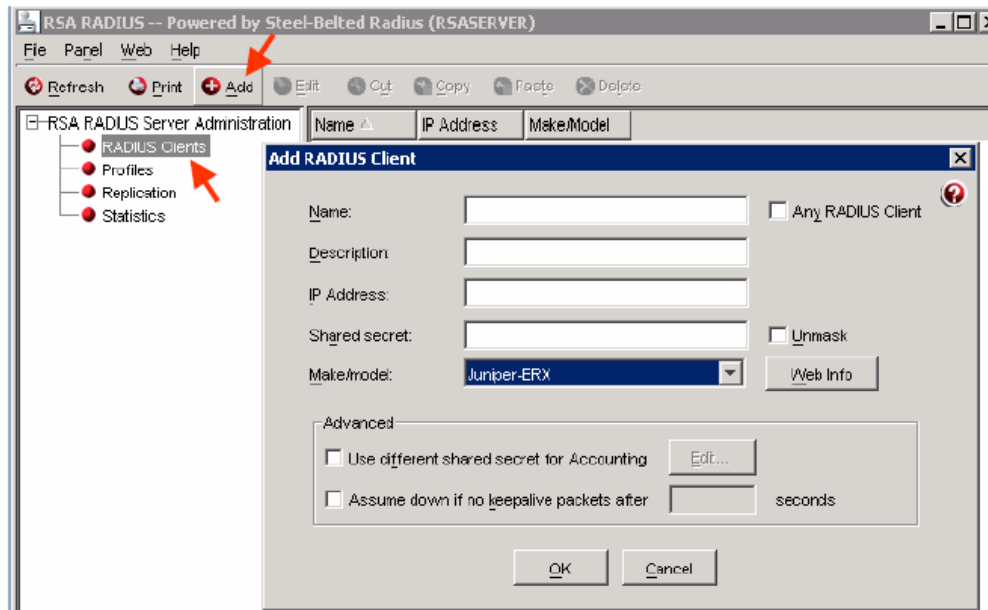
### Configure the RSA Authentication Manager

Perform the following settings on the RSA Authentication Manager Server:

1. [Configure the RADIUS protocol settings to be used by the Barracuda Web Application Firewall](#)
2. [Add the Barracuda Web Application Firewall as an Agent Host within the RSA Authentication Manager's Database](#)
3. [Import SecurID Tokens](#)
4. [Add Users to the RSA Authentication Manager and Assign Tokens](#)

### 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.



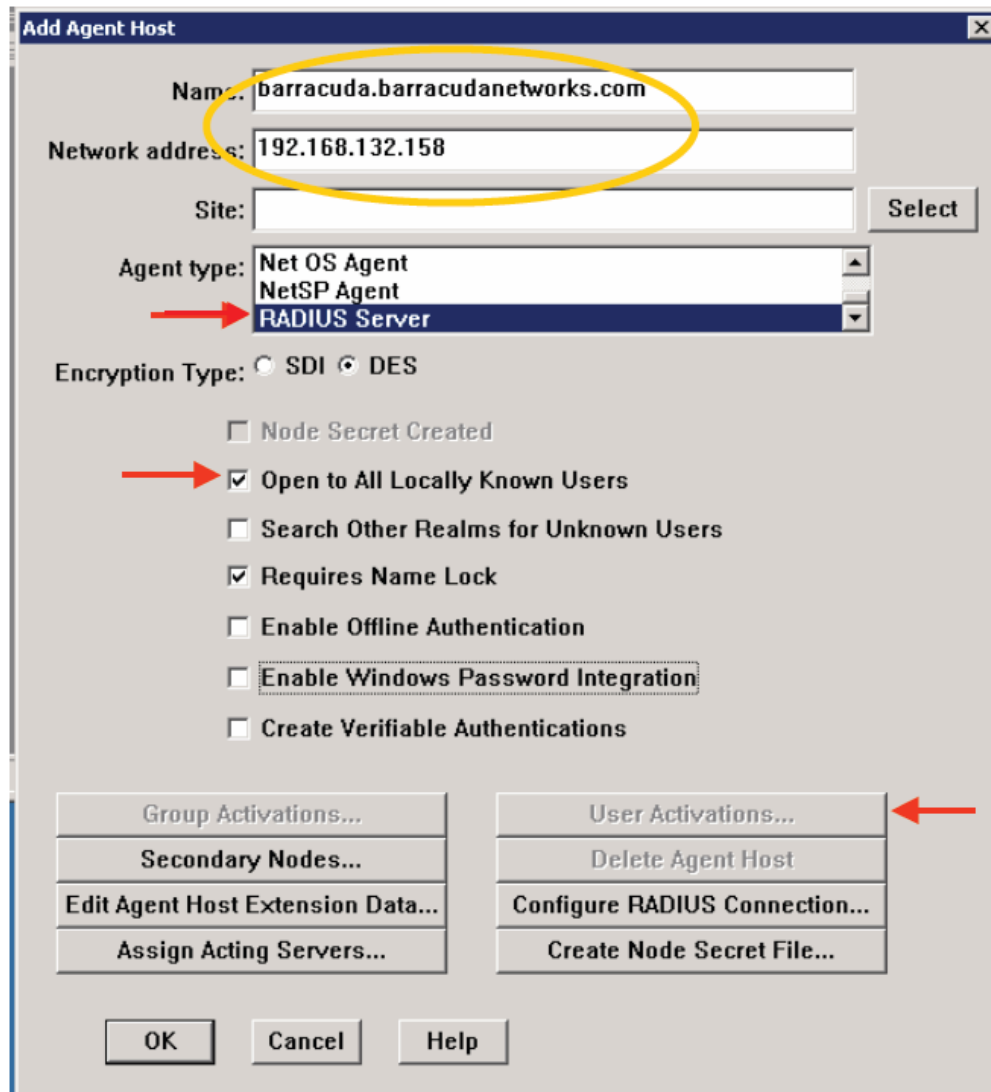
5. Specify values for the following fields:

- **Name** – Enter the hostname of the Barracuda Web Application Firewall.
- **Description** – Optional.
- **IP Address**– Enter the IP address of the Barracuda Web Application Firewall.
- **Shared Secret** – Type the secret key. You will need to configure the same Shared Secret on the Barracuda Web Application Firewall in **ACCESS CONTROL > Authentication Services > RSA SECURID**.  
As a best practice, use a unique account for this integration point and grant it the least level of privileges required, coordinating with the RSA SecurID administrator. This account requires READ privileges. For additional information, see [Security for Integrating with Other Systems - Best Practices](#).
- **Make/Model**– Select **Juniper-ERX**.

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

## Add the Barracuda Web Application Firewall as an Agent Host

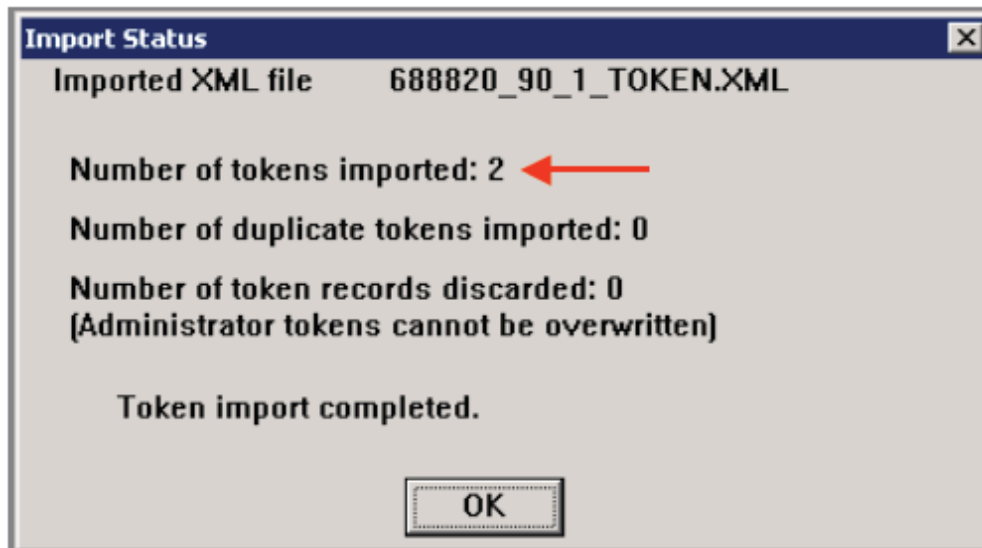
1. On the **RSA Authentication Manager Server System**, go to **Start > Programs > RSA Security** and select **RSA Authentication Manager Host Mode**.
2. Select the **Agent Host** menu, and select **Add Agent Host**. The **Add Agent Host** window appears.
3. Specify values for the following fields:
  - **Name**: Enter the hostname of the Barracuda Web Application Firewall.
  - **Network Address**: Enter the IP address of the Barracuda Web Application Firewall.
  - **Agent Type**: Select **RADIUS Server**.
  - **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**. Now, the Barracuda Web Application Firewall is added as an agent host on the RSA Authentication Manager.

## Import SecurID Tokens

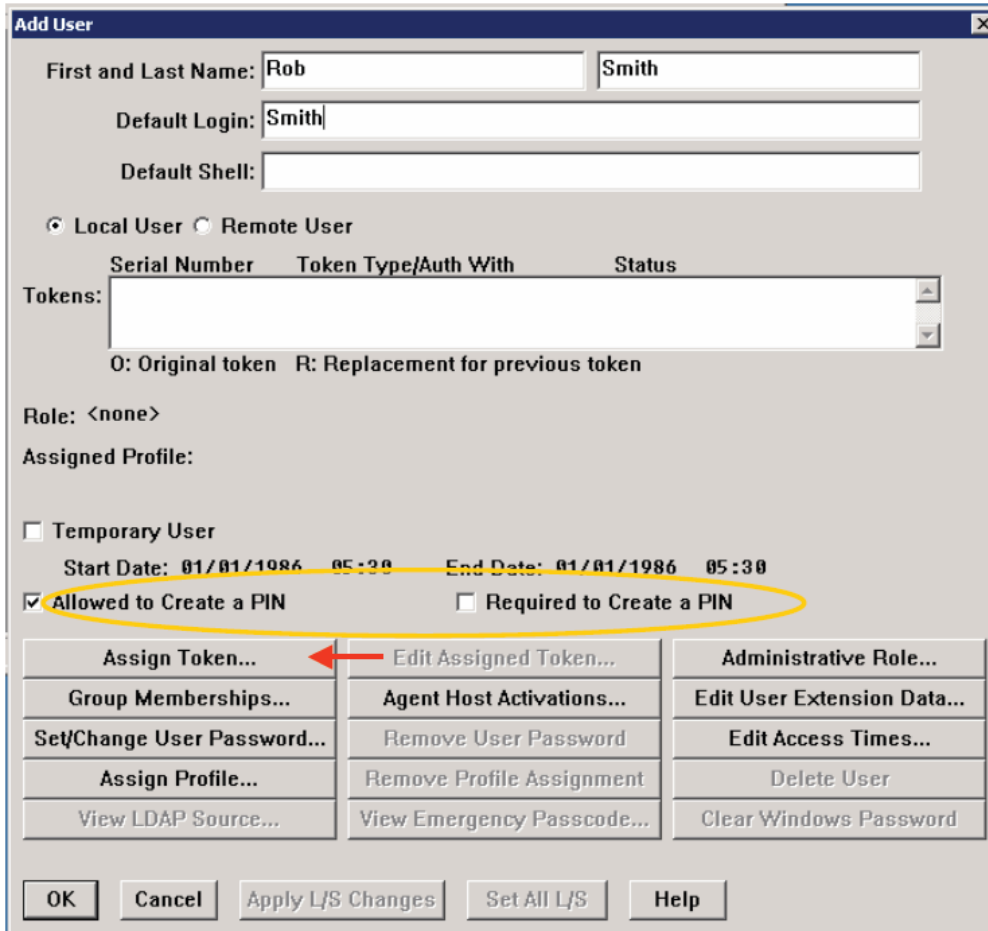
1. On the **RSA Authentication Manager Server System**, go to **Start > Programs > RSA Security** and select **RSA Authentication Manager Host Mode**.
2. From the **Token** menu, select **Import Tokens**.
3. Navigate to the token XML file provided by RSA and click **Open** to import the tokens.
4. The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



## 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 the default user name that will be used by the user to log in.
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).

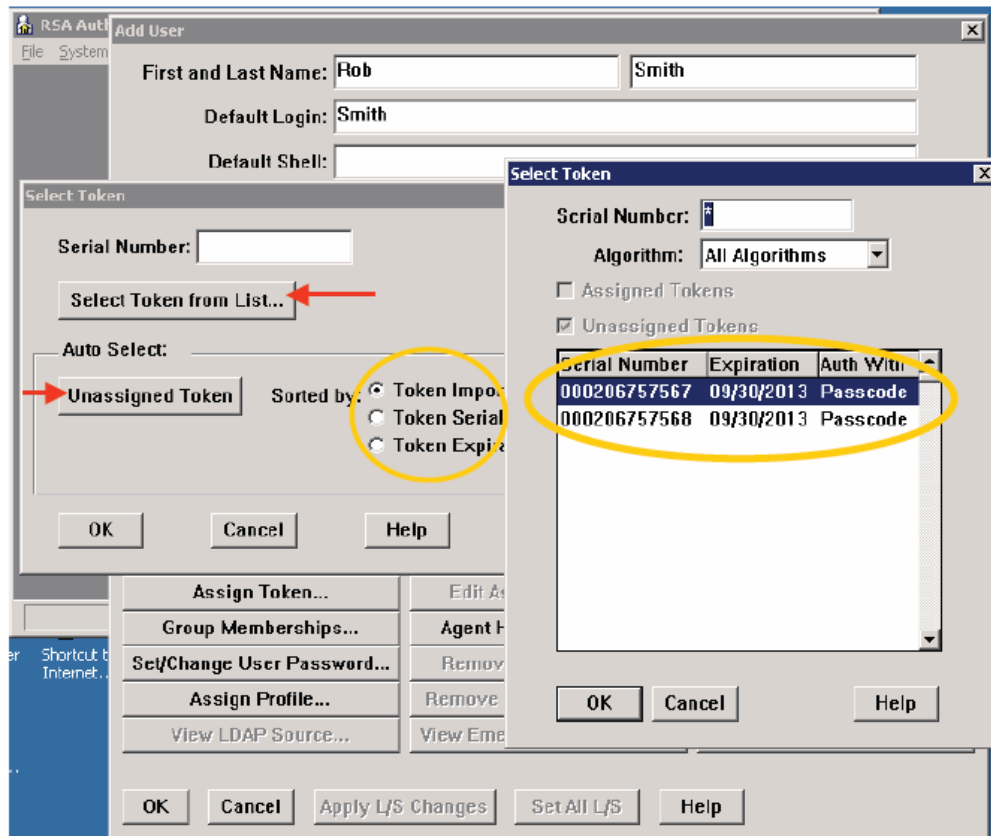
The random unpredictable code generated by the RSA SecurID authenticator at an interval of every 60 seconds is known as the **Tokencode**.

The combination of user's PIN (Personal Identification Number) and the Tokencode currently generated by the user's RSA SecurID authenticator is the user's **Passcode**.

A PIN can be generated:

1. 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.
2. If **Allowed to Create a PIN** is selected, the user may 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.
3. 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** as you prefer.

5. Select **Assign Token**. Click **Yes** to confirm. The **Select Token** window appears.
  1. 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**.
  2. 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.

## Configure the Barracuda Web Application Firewall

1. [Add the RSA SecurID server as an Authentication Service on the Barracuda Web Application Firewall](#)
2. [Associate the RSA SecurID Authentication Service with a Service](#)
3. [Configure the authorization policy for the service](#)

## Add the RSA SecurID Server as an Authentication Service

On the Barracuda Web Application Firewall web interface, go to **ACCESS CONTROL > Authentication Services**:

1. Select the **RSA SECURID** tab, and specify values for the following fields:
  - **Realm Name** – Enter the realm name.
  - **Server IP**– Enter the IP address of the RSA Authentication Server.
  - **Server Port**– Default is 1812. If you are not sure of the port, you can check on the RSA Authentication Manager server system.
    - Go to **Start > Programs > RSA Security**.
    - Select **RSA Authentication Manager Host Mode**.
    - On the **Agent Host** menu, choose **Edit Agent Host** to verify the values.
  - **Shared Secret**– Provide the same shared secret you configured on the RSA Authentication Manager in the [Configure the RADIUS Protocol Settings](#) steps. As a best practice, use a unique account for this integration point and grant it the least level of privileges required, coordinating with the RSA SecurID administrator. This account requires READ privileges. For additional information, see [Security for Integrating with Other Systems - Best Practices](#).
  - **Timeout**– Enter the time the Barracuda Web Application Firewall waits for a response from the RSA RADIUS Server before retransmitting the packet.
  - **Retries**– Enter the maximum number of times the Barracuda Web Application Firewall transmits a request packet to the RSA RADIUS server.
2. Click **Add** to save your settings.

## Associate the RSA SecurID Authentication Service with a Service

On the Barracuda Web Application Firewall web interface, go to the **ACCESS CONTROL > Authentication Policies** page:

1. Click **Edit Authentication** next to the service that you want to associate with the RSA SecurID Authentication Service.
2. On the **Edit Authentication Policy** window:
  1. Set **Status** to *On*.
  2. From the **Authentication Service** list, select the RSA SecurID authentication service you created in Add the RSA SecurID Server as an Authentication Service.
  3. Specify values for other parameters, and click **Save**. For more information on how to configure an authentication policy, click **Help**.

## Configure the Authorization Policy for the Service

On the Barracuda Web Application Firewall web interface, go to the **ACCESS CONTROL >**

## Authentication Policies page:

1. Click **Add Authorization** next to the service for which you want to configure the authorization policy.
2. On the **Add Authorization Policy** window:
  1. **Policy Name:** Enter a name for the authorization policy.
  2. **Status:** Set to *On*.
  3. Specify values for other parameters as required, and click **Save**. For more information on how to configure an authorization policy, click **Help**.
4. Click **Edit** next to the policy in the **Authentication Policies** section to configure advanced authorization settings.

Authentication Services | **Authentication Policies** | Local Users/Groups | Client Certificates

To implement access control for a web application, first create an authentication service on the **Authentication Services** page. Next, on this page, click **Edit Authentication** and associate the authentication service with the web application. Finally, add an authorization policy to enable access control and enforce authentication.

AUTHENTICATION POLICIES										Help
Name	IP Address	Port	Status	Auth Services	Access Rule	Host Match	URL Match	Metadata	Options	Actions
default										
app1	10.26.77.10	80	On	RSA_SecurID_...					Edit Authentication	Add Authorization
p1			On			*	/forms/*			Edit Delete

**EDIT AUTHORIZATION POLICY** Help

Access Control URL Name: p1

Service: app1

URL Match: /forms/\*

Host Match: \*

Extended Match: \*

Extended Match Sequence: 1000

Status: ☒ On ☐ Off  
Enable or disable the authorization policy for this service.

Login Method: ☒ HTML Form ☐ HTTP Basic Authentication  
Select the login method to be used to authenticate the user.

Allow any Authenticated User: ☒ Yes ☐ No  
Specifies whether to allow any authenticated user or not.

Allowed Users:   
Specifies the list of users allowed to access this URL space. Enter one or more user names separated by newlines.

Allowed Groups:   
Specifies the list of groups allowed to access this URL space. Enter one or more groups separated by newlines.

Auth Not Done URL: /forms/login.html  
Specifies the URL to which a user is redirected, if the user tries to access a protected URL before being authenticated.

Access Denied URL:   
Specifies the URL to which a user is redirected, if an authenticated user does not have access to a requested URL.

Send Basic Authentication: ☐ Yes ☒ No  
If set to Yes, user credentials are converted to HTTP Basic Authentication header and every request

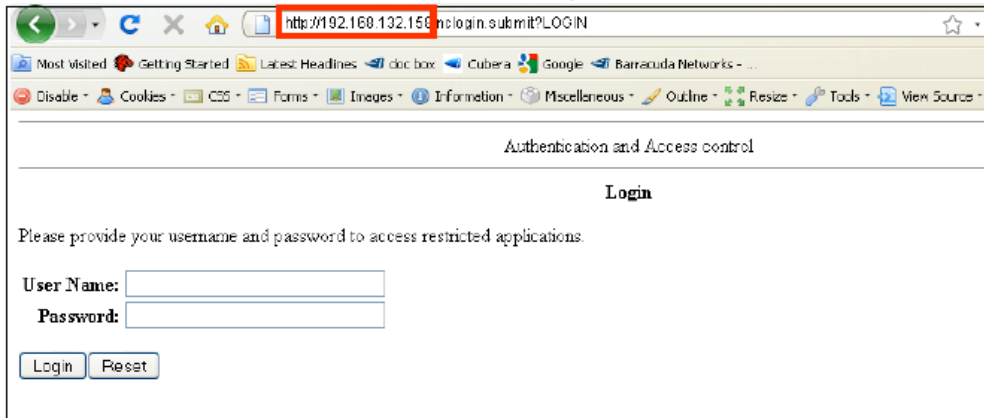
If you want users to authenticate using a custom login page when they attempt to access a resource protected by RSA SecurID, use the advanced authorization configuration and set **Auth Not Done URL** to the custom login URL.

Authorization using RSA is not possible using the RADIUS protocol when communicating with the RSA SecurID Server. Native authorization can be done through the Barracuda Web Application Firewall in this case.



## Verify the Setup and Authentication Process

1. Navigate to the restricted URL by entering the IP address into the address bar of your web browser.
2. The default authentication page, or the custom login page for authentication if you configured it on **ACCESS CONTROL > Authorization** , will be presented.



3. Depending on your configuration, you will be prompted to enter your user name and password. If configured in Passcode mode, you will be offered a system generated PIN, or instructed to provide a PIN.

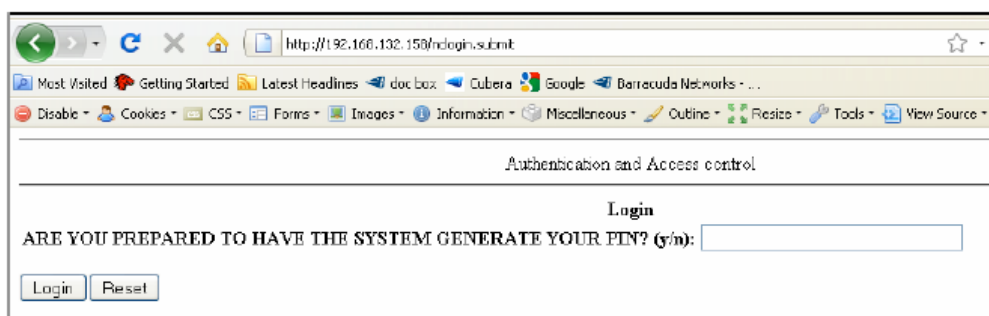


### System Generated Pin Screens

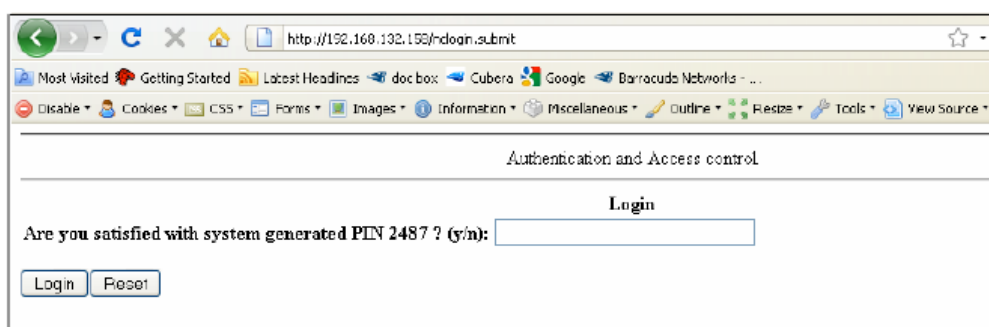




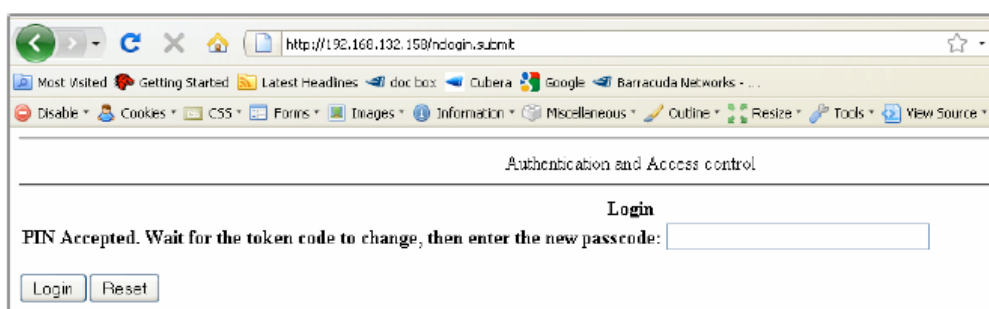




A screenshot of a web browser window showing the first step of the login process. The address bar displays 'http://192.168.132.150/ndlogin.submit'. The page title is 'Authentication and Access control'. Below this, the heading 'Login' is centered. The main text asks 'ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE YOUR PIN? (y/n):' followed by a text input field. At the bottom, there are two buttons: 'Login' and 'Reset'.



A screenshot of the second step in the login process. The browser window and address bar are identical to the first screenshot. The page title remains 'Authentication and Access control'. The heading 'Login' is still centered. The main text now asks 'Are you satisfied with system generated PIN 2487 ? (y/n):' followed by a text input field. The 'Login' and 'Reset' buttons are still at the bottom.



A screenshot of the third step in the login process. The browser window and address bar are identical to the previous screenshots. The page title remains 'Authentication and Access control'. The heading 'Login' is still centered. The main text now says 'PIN Accepted. Wait for the token code to change, then enter the new passcode:' followed by a text input field. The 'Login' and 'Reset' buttons are still at the bottom.

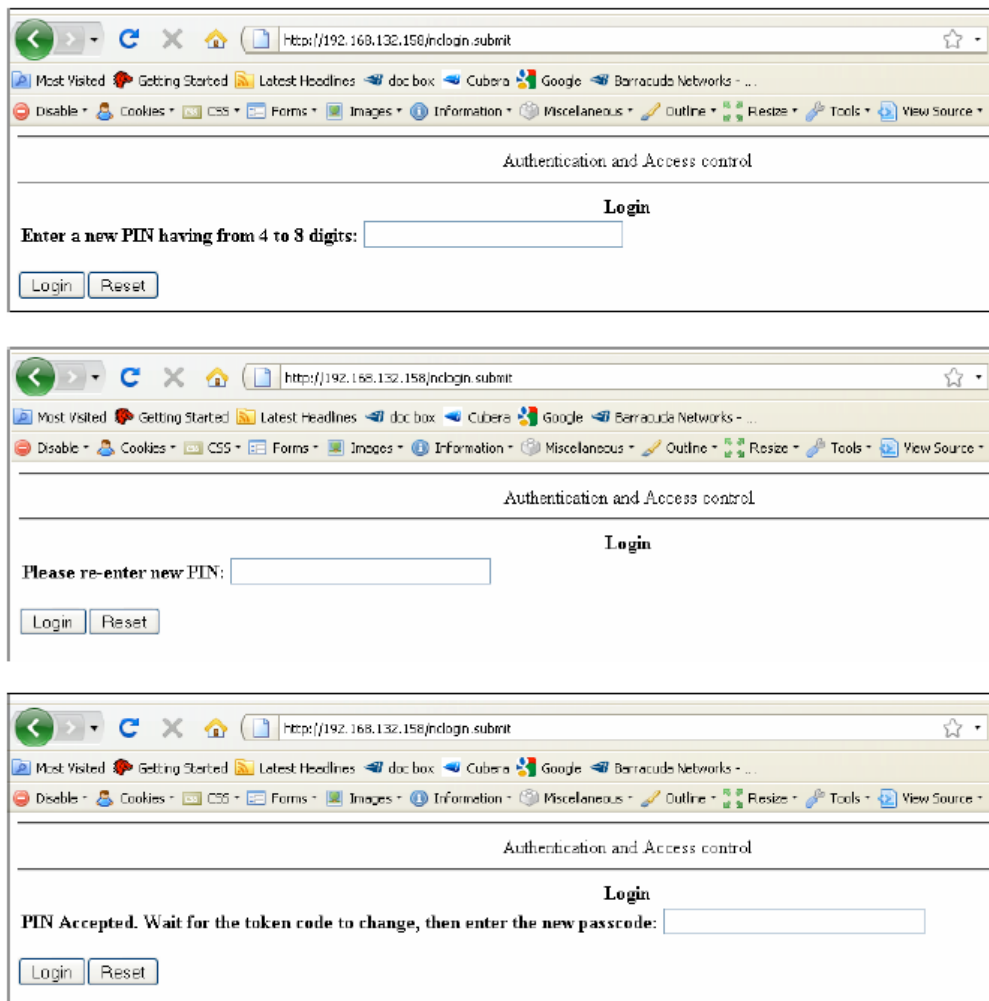
## User Generated Pin Screens









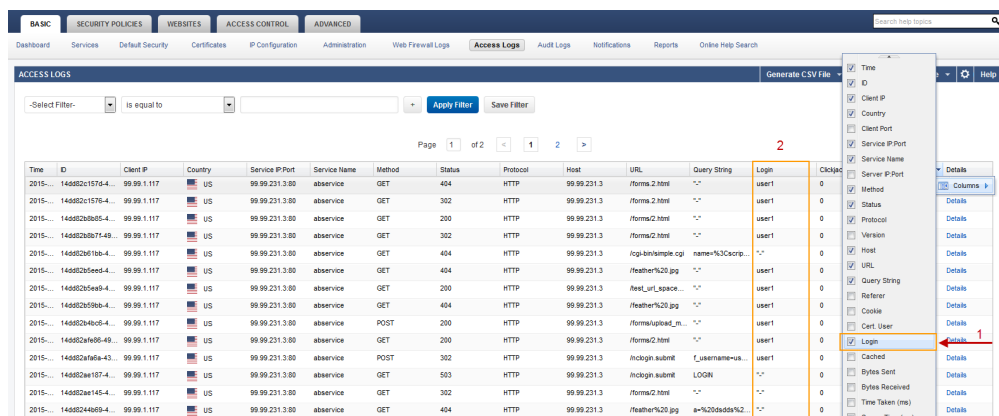


The first screenshot shows the initial login page with the URL `http://192.168.132.158/ndlogin.submit`. It features a "Login" section with a prompt "Enter a new PIN having from 4 to 8 digits:" and a text input field. Below the input field are "Login" and "Reset" buttons.

The second screenshot shows the same page after a failed login attempt, with the prompt "Please re-enter new PIN:".

The third screenshot shows the page after a successful login, with the prompt "PIN Accepted. Wait for the token code to change, then enter the new passcode:".

- To verify your login results, navigate to **BASIC > Access Logs** on your Barracuda Web Application Firewall and enable the Login column by selecting the **Login** checkbox under the Detail column.



The screenshot shows the "ACCESS LOGS" page in the Barracuda WAF interface. The "Login" checkbox under the "Details" column is checked, as indicated by a red arrow labeled "1". The table displays log entries with columns for Time, ID, Client IP, Country, Service IP/Port, Service Name, Method, Status, Protocol, Host, URL, Query String, Login, Clicks, and Details. A red arrow labeled "2" points to the "Login" column header.

Time	ID	Client IP	Country	Service IP/Port	Service Name	Method	Status	Protocol	Host	URL	Query String	Login	Clicks	Details
2015-...	1468021574-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	404	HTTP	99.99.231.3	/forms/2.html	..	user1	0	Details
2015-...	1468021576-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	302	HTTP	99.99.231.3	/forms/2.html	..	user1	0	Details
2015-...	1468026365-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	200	HTTP	99.99.231.3	/forms/2.html	..	user1	0	Details
2015-...	1468026367-49...	99.99.1.117	US	99.99.231.3.00	abservice	GET	302	HTTP	99.99.231.3	/forms/2.html	..	user1	0	Details
2015-...	1468026368-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	404	HTTP	99.99.231.3	/cgi-bin/sample.cgi	name=%3Cscript>..	..	0	Details
2015-...	1468026369-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	404	HTTP	99.99.231.3	/feather%20.jpg	..	user1	0	Details
2015-...	1468026370-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	200	HTTP	99.99.231.3	/feather%20.jpg	..	user1	0	Details
2015-...	1468026371-4...	99.99.1.117	US	99.99.231.3.00	abservice	POST	200	HTTP	99.99.231.3	/forms/upload_m_...	..	user1	0	Details
2015-...	1468026372-49...	99.99.1.117	US	99.99.231.3.00	abservice	GET	200	HTTP	99.99.231.3	/forms/2.html	..	user1	0	Details
2015-...	1468026373-43...	99.99.1.117	US	99.99.231.3.00	abservice	POST	302	HTTP	99.99.231.3	/ndlogin.submit	f_username=us...	user1	0	Details
2015-...	1468026374-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	503	HTTP	99.99.231.3	/ndlogin.submit	LOGIN	..	0	Details
2015-...	1468026375-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	302	HTTP	99.99.231.3	/forms/2.html	..	..	0	Details
2015-...	1468024409-4...	99.99.1.117	US	99.99.231.3.00	abservice	GET	404	HTTP	99.99.231.3	/feather%20.jpg	a=%3Cscript>..	..	0	Details



## Figures

1. WAFRSA1.png
2. AddAgentHost.png
3. ImportToken.png
4. AddUser.png
5. SelectAssignToken.png
6. Advanced\_Settings\_Auth\_Policy.png
7. DefaultLogin.png
8. AllowedtoCreatePin.png
9. SystemGeneratedPin.png
10. UserGeneratedPin.png
11. Access\_Logs.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.