Array Networks

SPX SSL VPN

RSA SecurID Ready Implementation Guide

Last Modified: September 16, 2014

Partner Information

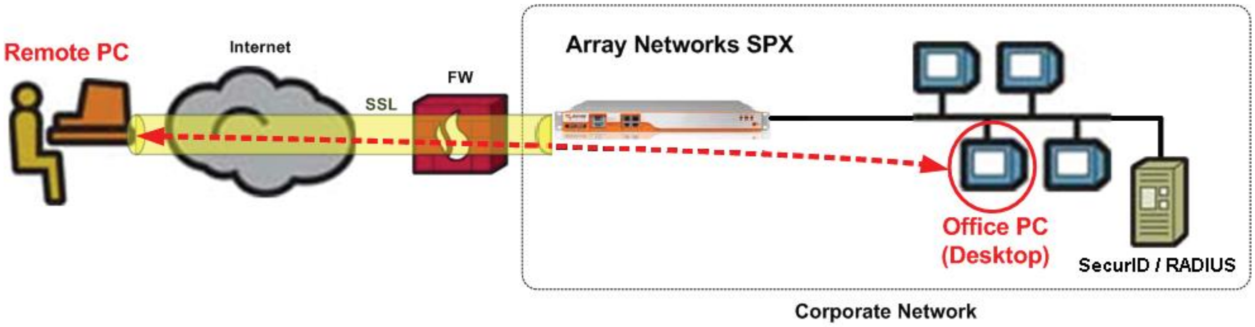
Product Information	
Partner Name	Array Networks
Web Site	www.arraynetworks.com
Product Name	SPX
Version & Platform	8.4.6.2
Product Description	Engineered from the ground up for high-performance security and access control, the Array Networks SPX SSL VPN Series delivers local and remote access that supercharges productivity and user job performance. Whether working at home or a branch office, a wireless hotspot or kiosk, using notebook PCs, PDAs or cell phones, workers can quickly and easily access email, file shares and applications just as if they were at the office.

Solution Summary

The Array Networks SPX supports authentication with external LDAP, RADIUS, Microsoft Active Directory, and RSA SecurID servers. The Array SPX also provides a local authentication database. On the Array SPX, the administrator creates virtual sites which are like authentication gateways. Users access the portal page of the virtual site to authenticate before gaining access to network resources. The scope of this guide is to show how to setup and configure Array SPX solution to authenticate users to an RSA Authentication Manager via SecurID and RADIUS methods. For a more in depth explanation of how to configure Array SPX, please refer to the documentation provided by Array Networks.

The virtual site's portal login page can also be customized to utilize Risk-Based Authentication. When configured, a user accessing the virtual site's login page will be redirected to the RSA Secure Logon page. The user logs into the system using their RSA credentials. If the logon is determined to be low-risk, the user is granted access to the portal. If the logon is determined to be high-risk, the user can be challenged with life questions or ODA to further prove the user's identity.

RSA Authentication Manager supported features	
Array Networks SPX 8.4.6.2	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	Yes
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Authentication Agent Configuration

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 following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Array SPX will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for Array SPX to communicate with RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

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 documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	/tmp/sdconf.rec
Node Secret	In Memory

Risk-Based Authentication Integration Script

To protect a web-based application with risk-based authentication (RBA), you must generate an integration script using the RSA Security Console, and deploy it to the applications default logon page. The script redirects the user from the web-based application's default logon page to a customized logon page that allows RSA Authentication Manager to authenticate the user with RBA.

The following steps should be taken prior to generating the integration script.

- Download the integration script template for the SPX Series from the following link: **https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=881813901&arg12=downloaddirect&transaction=signon&quiet=true**
- Verify that the most recent RBA integration script template is installed on your Authentication Manager system by comparing the header of the installed integration script template to the header of the downloaded integration script template.
- Install the downloaded integration script template if it is newer than the installed script template, or if the script template for your agent is not installed.

Please refer to RSA documentation for more information on RBA integration scripts.

Partner Product Configuration

Before You Begin

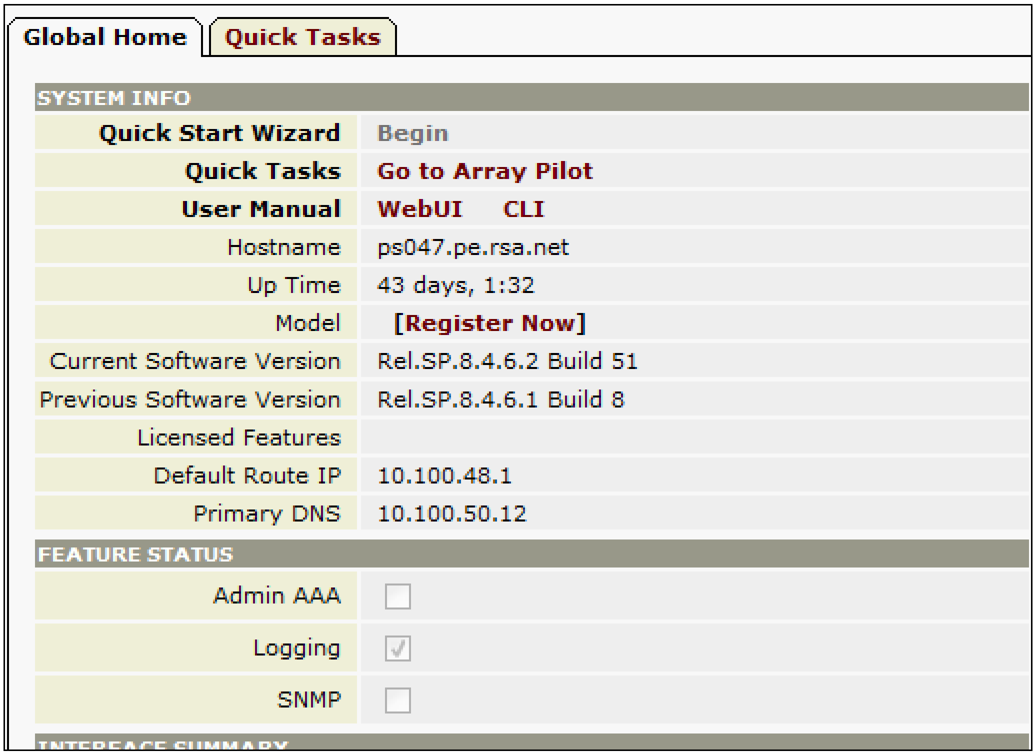
This section provides instructions for configuring the Array SPX with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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 Array SPX components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Array SPX Quick Start Wizard

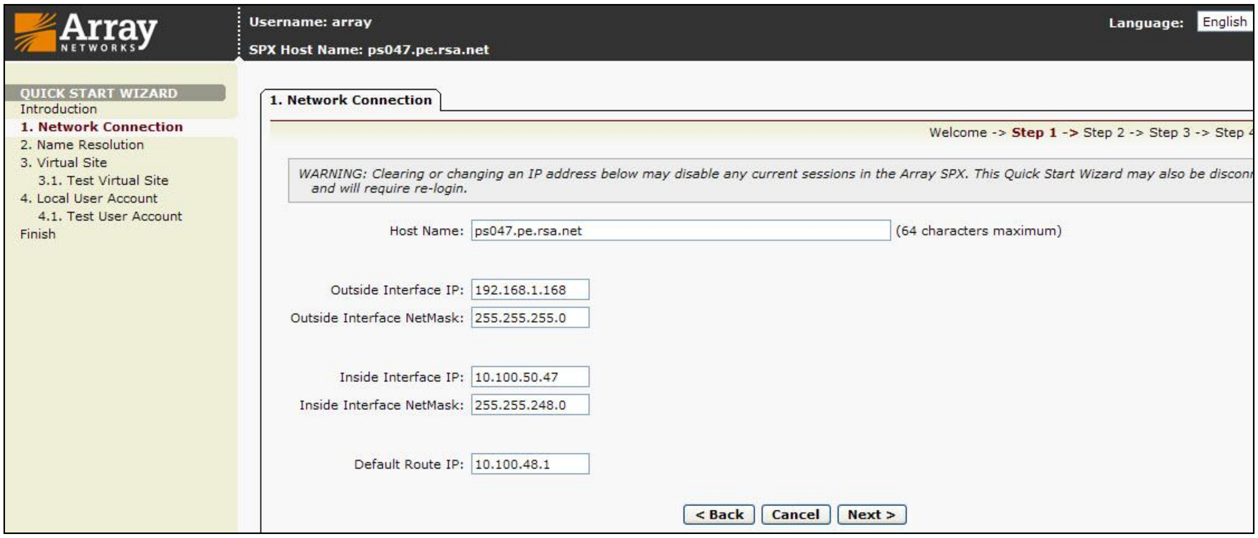
1. Log into the Array's web interface via ***https://<arrayhostname>:8888***.
2. From the top left pane, change the mode to **Config** mode.
3. On the Global Home page click *Quick Start Wizard* **Begin**.



SYSTEM INFO	
Quick Start Wizard	Begin
Quick Tasks	**Go to Array Pilot**
User Manual	**WebUI** **CLI**
Hostname	ps047.pe.rsa.net
Up Time	43 days, 1:32
Model	**[Register Now]**
Current Software Version	Rel.SP.8.4.6.2 Build 51
Previous Software Version	Rel.SP.8.4.6.1 Build 8
Licensed Features	
Default Route IP	10.100.48.1
Primary DNS	10.100.50.12
FEATURE STATUS	
Admin AAA	□
Logging	☑
SNMP	□
INTERFACE SUMMARY	

4. The Quick Start Wizard home page will open. Click **Next** to begin.

5. On the Network Connection page configure the IP Address information for your network and click **Next.**



Username: array
SPX Host Name: ps047.pe.rsa.net
Language: English

WARNING: Clearing or changing an IP address below may disable any current sessions in the Array SPX. This Quick Start Wizard may also be disconn and will require re-login.

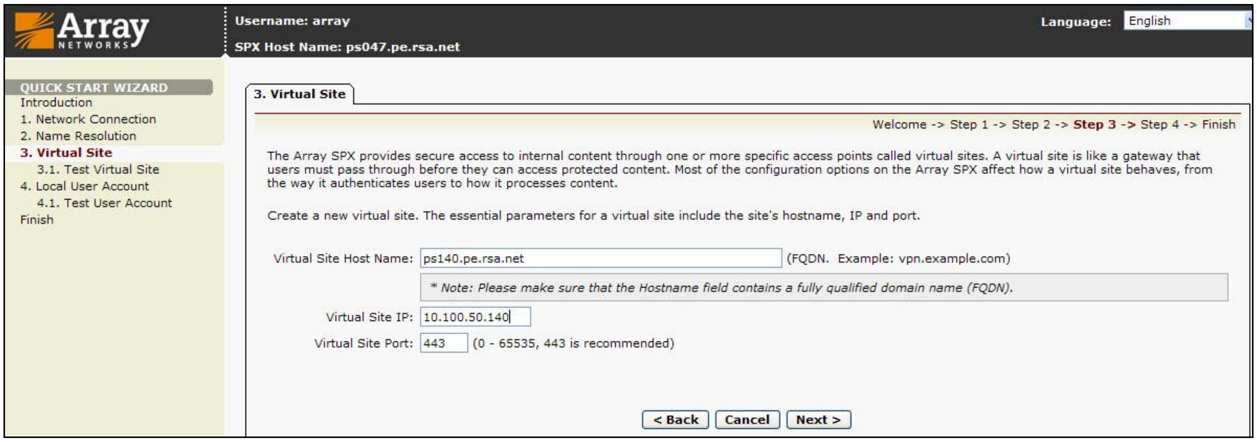
Host Name: ps047.pe.rsa.net (64 characters maximum)

Outside Interface IP: 192.168.1.168
Outside Interface NetMask: 255.255.255.0

Inside Interface IP: 10.100.50.47
Inside Interface NetMask: 255.255.248.0

Default Route IP: 10.100.48.1

6. On the Name Resolution page configure the appropriate **DNS** and **WINS** values and click **Next**.
7. On the Virtual Site page create a virtual site on the Array SPX. A virtual site is like an authentication gateway for your users to pass through before gaining access to network resources. The https page will be generated from the information entered on this screen.



Username: array
SPX Host Name: ps047.pe.rsa.net
Language: English

The Array SPX provides secure access to internal content through one or more specific access points called virtual sites. A virtual site is like a gateway that users must pass through before they can access protected content. Most of the configuration options on the Array SPX affect how a virtual site behaves, from the way it authenticates users to how it processes content.

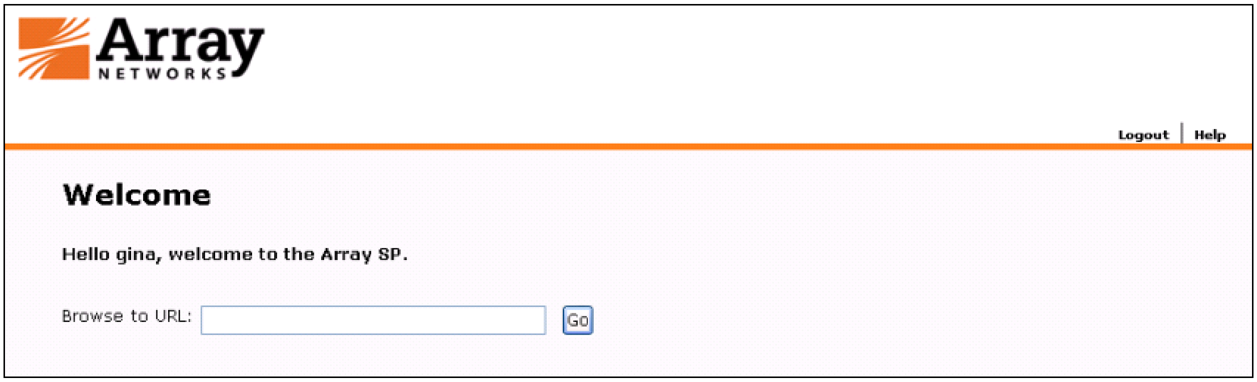
Create a new virtual site. The essential parameters for a virtual site include the site's hostname, IP and port.

Virtual Site Host Name: ps140.pe.rsa.net (FQDN. Example: vpn.example.com)

* Note: Please make sure that the Hostname field contains a fully qualified domain name (FQDN).

Virtual Site IP: 10.100.50.140
Virtual Site Port: 443 (0 - 65535, 443 is recommended)

8. Configure a local user name and password, which will be used to validate access via the virtual site https page. Next, test the virtual site by browsing to ***https://<arrayhostname>:443*** and logging in with the local user name and password. A successful login will present you with a **Welcome** screen where you can enter a URL to gain access to your network resources. Click **Logout** to go to the next step.



Welcome

Hello gina, welcome to the Array SP.

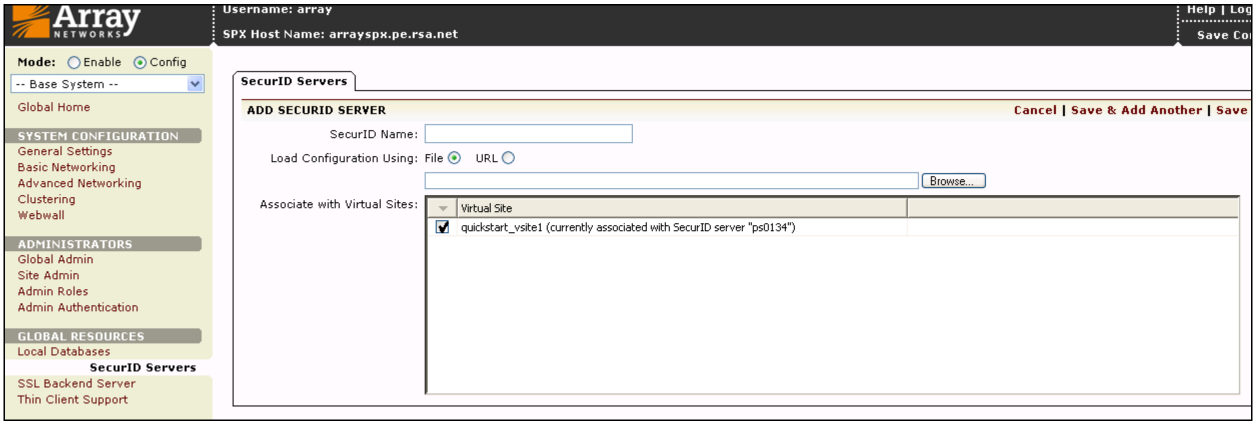
Browse to URL:

9. The L3VPN screen is optional. Select **Skip** at the bottom of the screen.
10. Click **Finish** to save the configured settings. This completes the **Quick Start Wizard**.

Configuring RSA Native SecurID

1. From the top left pane, change the mode to **Config** mode.
2. Navigate to **GLOBAL RESOURCES**, select **SecurID Servers**.
3. On the right hand pane, select **Add**.
4. Enter the **SecurID Name**.
5. Choose either **File** or **URL** depending on the location of the sdconf.rec file.
6. Enter the path of where the sdconf.rec file is located.
7. Check one or more **Virtual Sites** the sdconf.rec file will be associated with.
8. Click **Save**.

Note: These steps are not part of the Quick Start Wizard and need to be done via the left hand tool bar.



Username: array

SPX Host Name: arrayspx.pe.rsa.net

Mode: ○ Enable ● Config

ADD SECURID SERVER

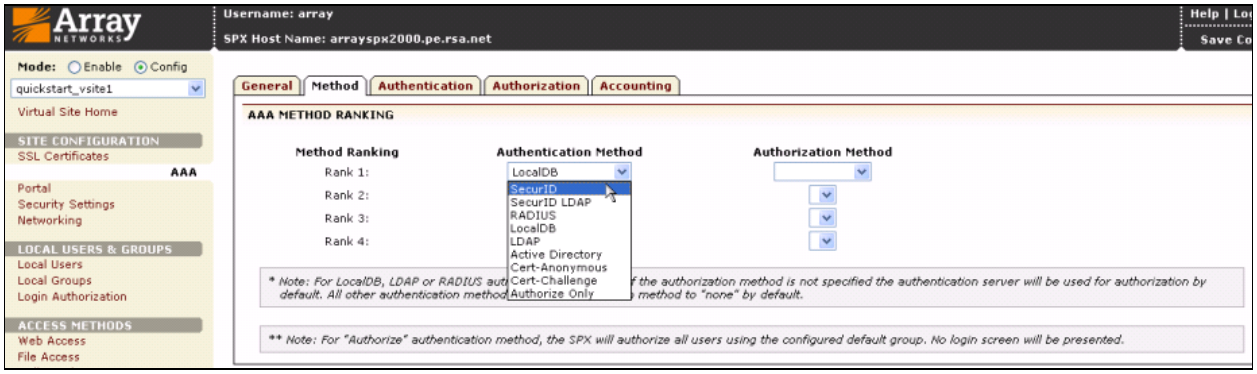
SecurID Name:

Load Configuration Using: File ● URL ○

Associate with Virtual Sites:

	Virtual Site
☑	quickstart_vsite1 (currently associated with SecurID server "ps0134")

9. On the top left pane, confirm the mode is still in **Config** mode.
10. In the pull down field at the upper left, select the appropriate **Virtual Site**.
11. Navigate to **SITE CONFIGURATION > AAA**, select the **Method** tab on the right hand pane.
12. Set **Rank 1** and select **SecurID** from the pull down tab.
13. Click **Save Changes**.



Username: array
SPX Host Name: arrayspx2000.pe.rsa.net

Mode: ○ Enable ● Config
quickstart_vsite1

AAA METHOD RANKING

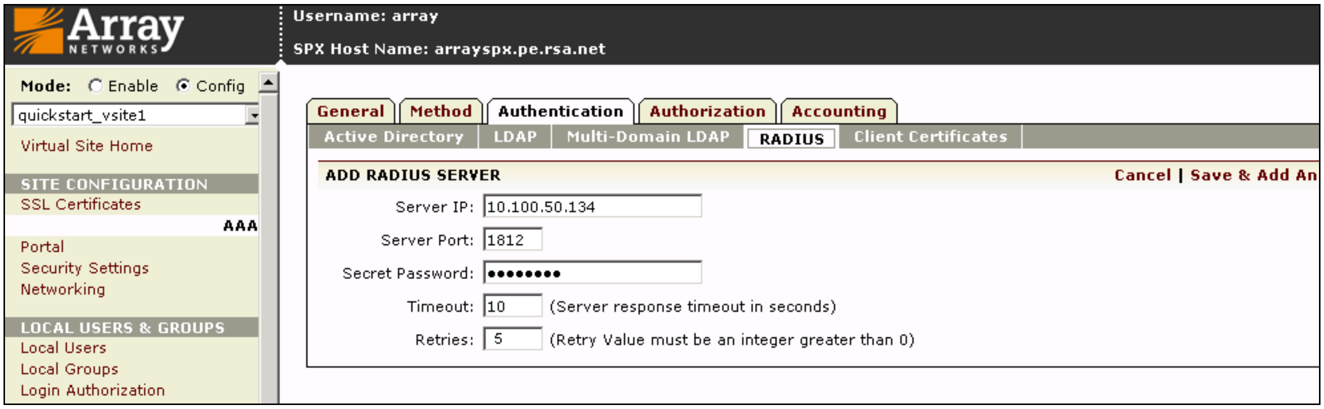
Method Ranking	Authentication Method	Authorization Method
Rank 1:	LocalDB	
Rank 2:		
Rank 3:		
Rank 4:		

* Note: For LocalDB, LDAP or RADIUS aut f the authorization method is not specified the authentication server will be used for authorization by default. All other authentication method method to "none" by default.

** Note: For "Authorize" authentication method, the SPX will authorize all users using the configured default group. No login screen will be presented.

Configuring RSA SecurID via RADIUS Protocol

1. Log into the Array SPX Administration webUI.
2. On the top left pane, change the mode to **Config** mode.
3. Select the appropriate Virtual Site from the pull down menu located below the mode selection.
4. Navigate to **SITE CONFIGURATION** and click on **AAA**.
5. On the right hand pane, click on the **Authentication** tab located in the middle of the screen.
6. Select **RADIUS** then select **Add Radius Server**.
7. Enter the **Server IP**, **Server Port**, **Secret Password** (shared secret), **Timeout** and **Retries** values of the RADIUS server and click **Save.**



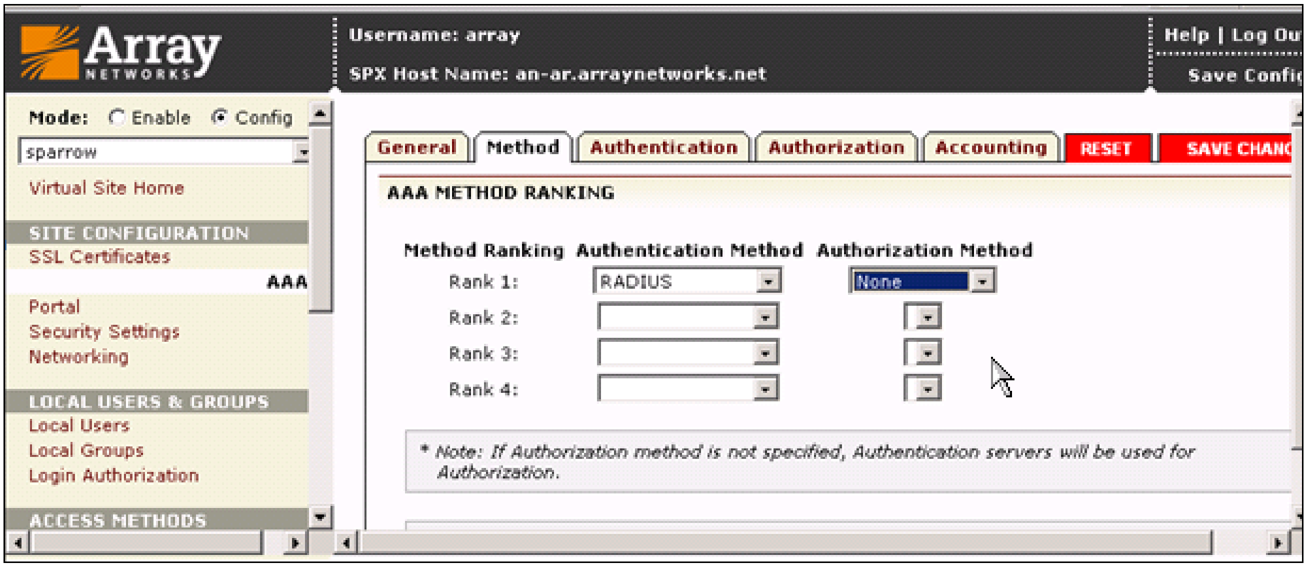
Username: array
SPX Host Name: arrayspx.pe.rsa.net

Mode: ○ Enable ● Config
quickstart_vsite1

ADD RADIUS SERVER

Server IP: 10.100.50.134
Server Port: 1812
Secret Password: ••••••••
Timeout: 10 (Server response timeout in seconds)
Retries: 5 (Retry Value must be an integer greater than 0)

8. On the left pane, navigate to **SITE CONFIGURATION > AAA,** select the **Method** tab on the right hand pane.
9. Select **Rank 1** and select **RADIUS** from the pull down.
10. Click **Save Changes**.



Username: array
SPX Host Name: an-ar.arraynetworks.net

Mode: ○ Enable ● Config
sparrow

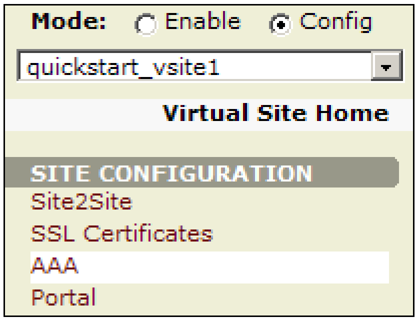
AAA METHOD RANKING

Method Ranking	Authentication Method	Authorization Method
Rank 1:	RADIUS	None
Rank 2:		
Rank 3:		
Rank 4:		

* Note: If Authorization method is not specified, Authentication servers will be used for Authorization.

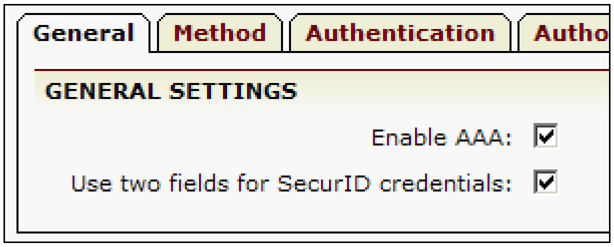
Configure Virtual Site for On-Demand Authentication (ODA)

1. Log in to the Array Networks WebUI. Ensure that the **Mode** is set to **Config**.
2. Select the appropriate Virtual Site from the pulldown menu. The chosen Virtual Site must be associated with the SecurID configuration created in the previous section. After ensuring this, select the **AAA** link in the navigation panel.



Mode: ○ Enable ● Config
quickstart_vsite1

3. On the **General** tab, make sure that the **Enable AAA** and **Use two fields for SecurID credentials** are checked.

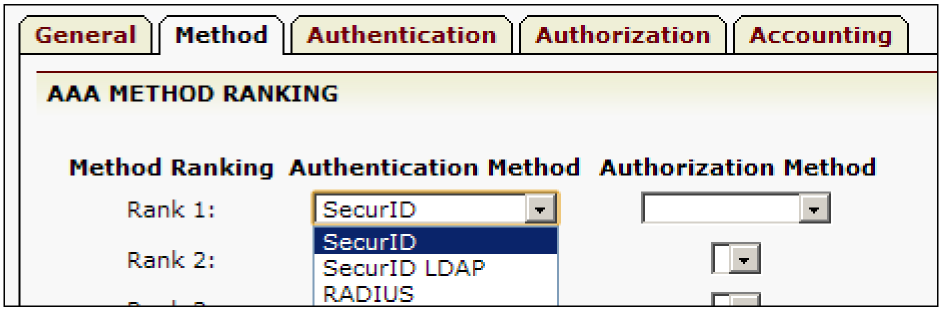


GENERAL SETTINGS

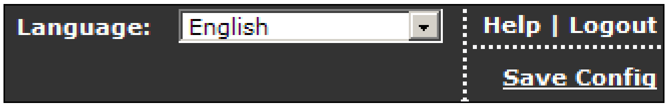
Enable AAA: ☑

Use two fields for SecurID credentials: ☑

4. On the **Method** tab, select **SecurID** as the Rank 1 Authentication Method. A red **Save Changes** button will appear. Click this button to save the changes you have made.



5. The Virtual site is now configured for SecurID authentication. Click the **Save Config** link in the upper-right corner to write the configuration changes to memory.



Customize Virtual Site for Risk-Based Authentication (RBA)

! Important: This section makes use of the SPX Series Controller's powerful portal theme customization features. Usage of these advanced features is outside the scope of this guide.

Before proceeding, be sure you are familiar with creating and importing a custom portal theme by referring to the Array Networks SPX WebUI guide.

1. If you have not done so already, download and install the RBA integration script template as explained in the "Risk Based Authentication Script Template" section of this document. The integration script template must be installed on your RSA Authentication Manager before proceeding.
2. Download the integration script for the authentication agent corresponding to your SPX device. This file should be named **am_integration.js**.

Note: In order to perform Risk-Based Authentication, you must incorporate the contents of am_integration.js into the login page of the Virtual Site you wish to customize. This example creates a theme with a copy of the default login page that the SPX device uses. In practice, your organization may already be using a custom login page. Your case will almost certainly differ—this example is only intended to serve as a guide.

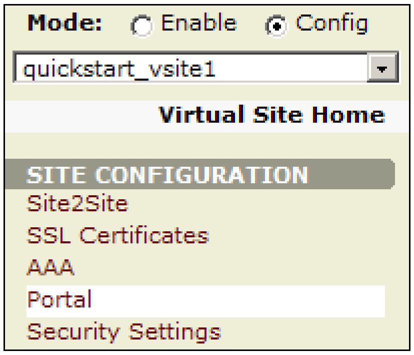
3. Using Array Networks' process for creating a custom portal theme, create a custom login page and paste the contents of **am_integration.js** as a JavaScript page element. This example uses the normal SPX login page. Paste the JavaScript in an existing script element in the page's header.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Login</title>
<link rel="stylesheet" type="text/css"
href="/prx/000/http/localhost/portal.css">
<script language="JavaScript"
src="/prx/000/http/localhost/an_util.js"></script>
<script language="JavaScript">
<!--
if (self != top) {
    top.location = self.location;
}
if (_AN_nav_get_cookie(4) == 'open') {
    _AN_show_help('login_securid');
}

//Paste contents of am_integration.js here

//-->
</script>
</head>
```

4. At the bottom of the script add a line of JavaScript that changes the **window.onload** action to call the **redirectToIdP()**. This code can be placed in any appropriate part of the page. For this example, we place it in a pre-existing block of scripting at the bottom of the login page.

```
<script language="JavaScript">
document.login_form.elements[0].focus();
window.onload = redirectToIdP();
</script>
```

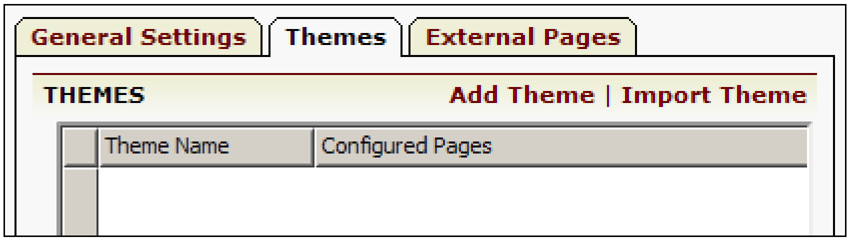
5. Bundle the customized login page into a zip file that contains your custom theme. The zip file contents must adhere to a certain format in order to properly import into the SPX device. Refer to Array Networks' documentation for details on this format.
6. Using the WebUI, select the Virtual Site for which you would like to customize the login page. Select the **Portal** link on the left navigation panel.



Mode: ○ Enable ● Config

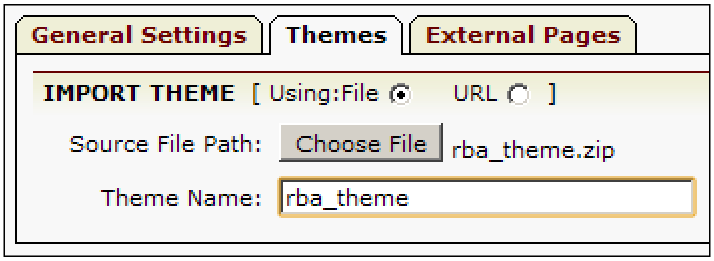
quickstart_vsite1

7. On the **Themes** tab, click **Import Theme** to import the new custom theme.



	Theme Name	Configured Pages

8. Choose the zip file that contains the custom theme and give the theme a name. Click **Import** to import the theme.

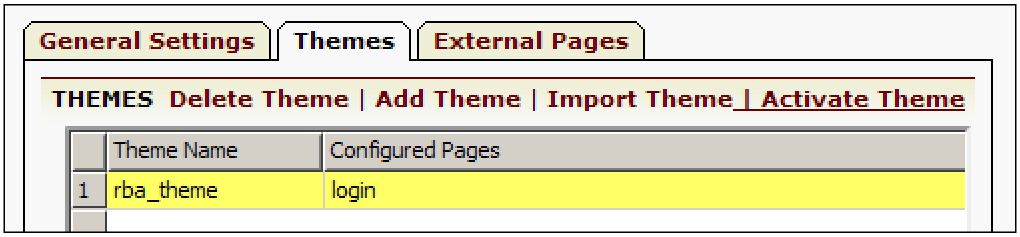


IMPORT THEME [Using:File ● URL ○]

Source File Path: rba_theme.zip

Theme Name: rba_theme

9. The new theme appears in the list. Click on the theme and click **Activate Theme**. This will make the new theme active for the portal. There is no need to reboot the device, but make sure to save the configuration to memory.

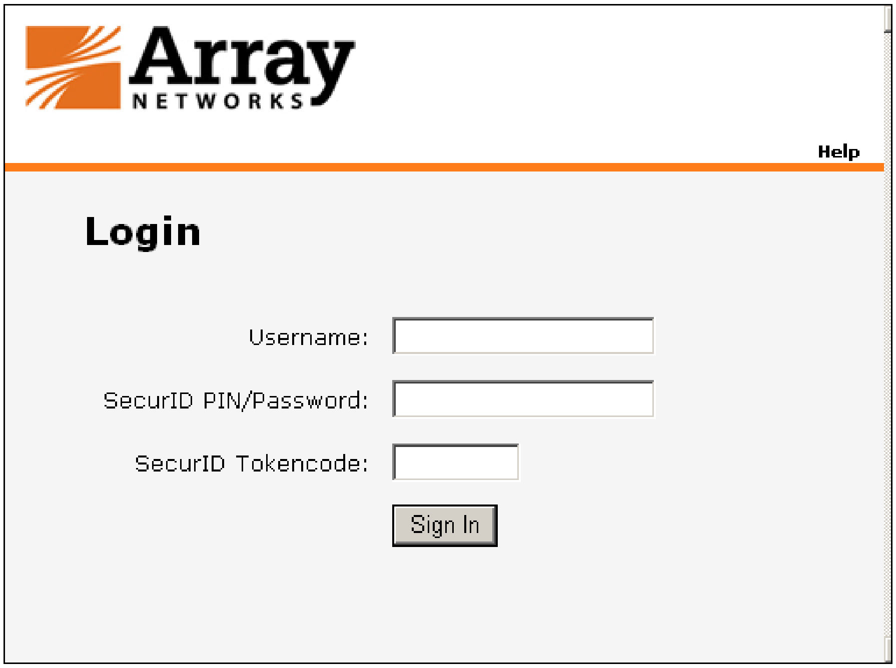


	Theme Name	Configured Pages
1	rba_theme	login

Users accessing the login page will now be redirected to the RSA Risk-Based Logon page. Risk-Based Authentication can be disabled at any time by deactivating the custom theme.

Native RSA SecurID Login Screens

Login screen:



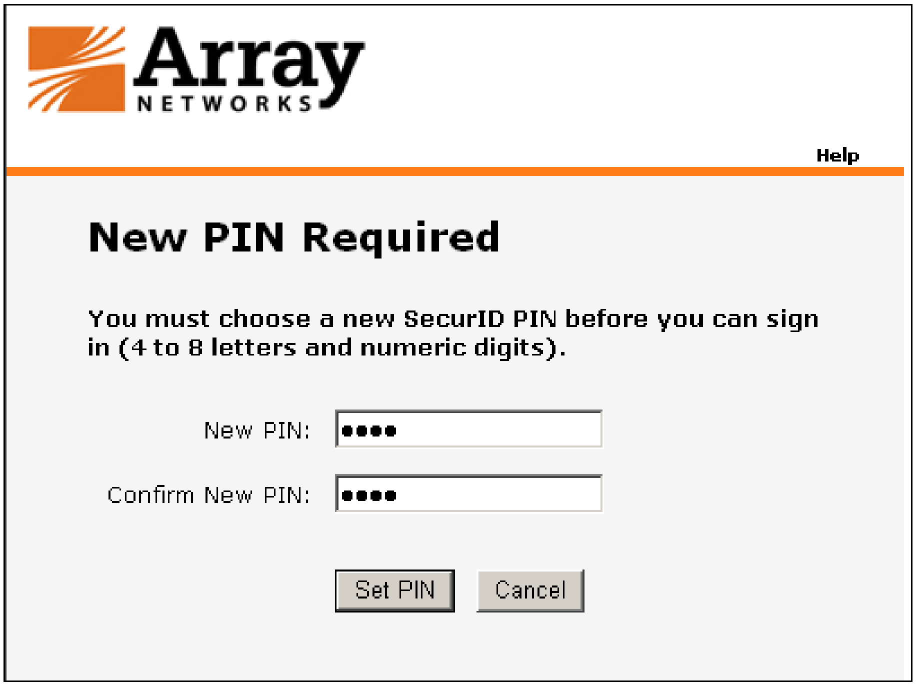
Login

Username:

SecurID PIN/Password:

SecurID Tokencode:

User-defined New PIN:



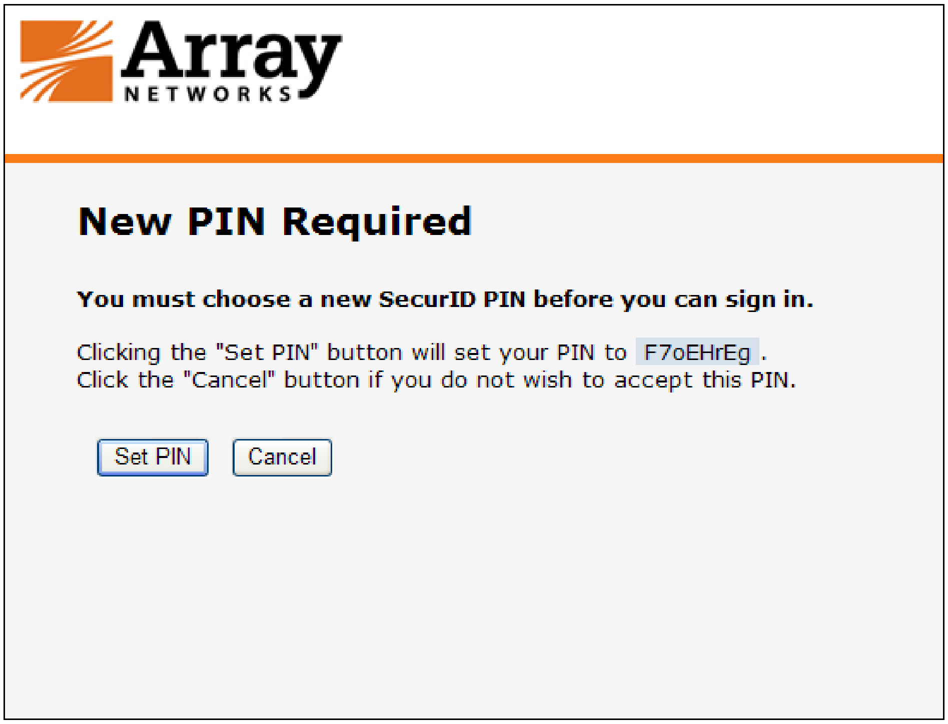
New PIN Required

You must choose a new SecurID PIN before you can sign in (4 to 8 letters and numeric digits).

New PIN: ●●●●

Confirm New PIN: ●●●●

System-generated New PIN:

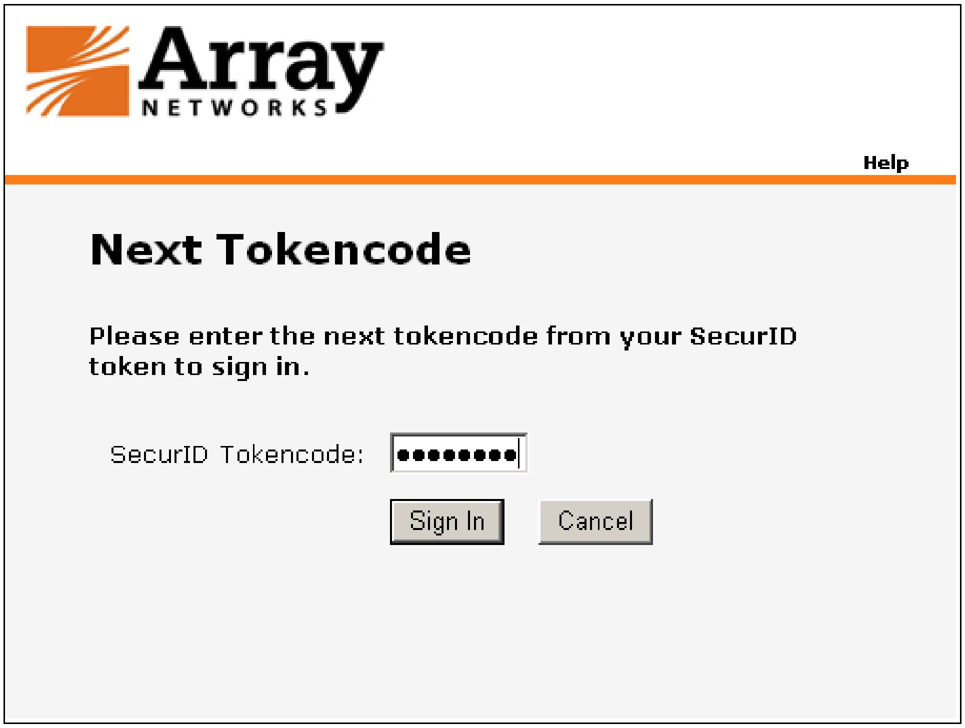


New PIN Required

You must choose a new SecurID PIN before you can sign in.

Clicking the "Set PIN" button will set your PIN to F7oEHrEg .
Click the "Cancel" button if you do not wish to accept this PIN.

Next Tokencode:



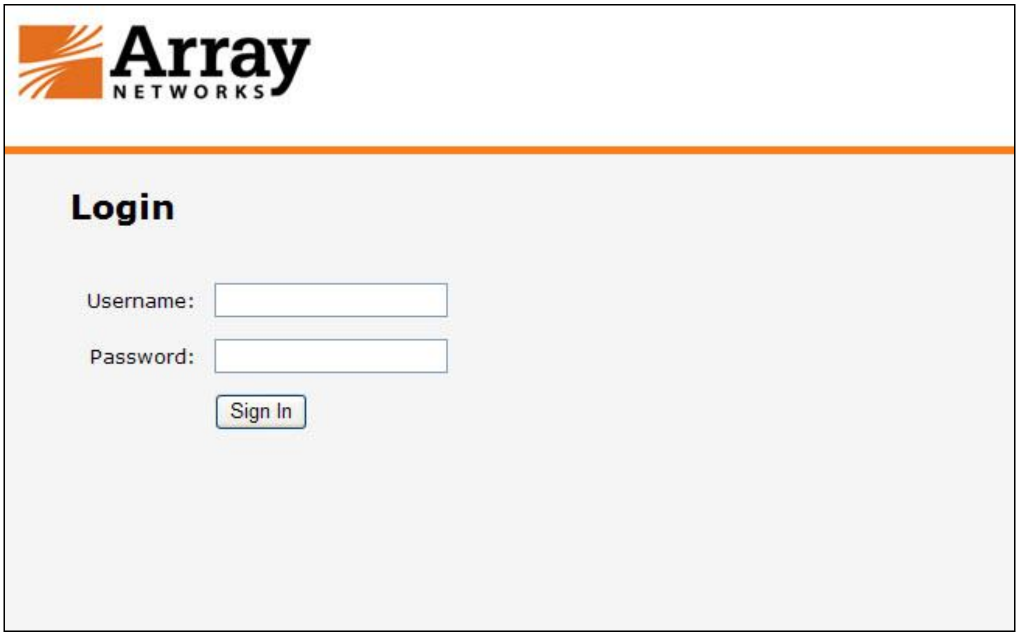
Next Tokencode

Please enter the next tokencode from your SecurID token to sign in.

SecurID Tokencode: ●●●●●●●●●

RSA SecurID Login Screens via RADIUS

Login screen:

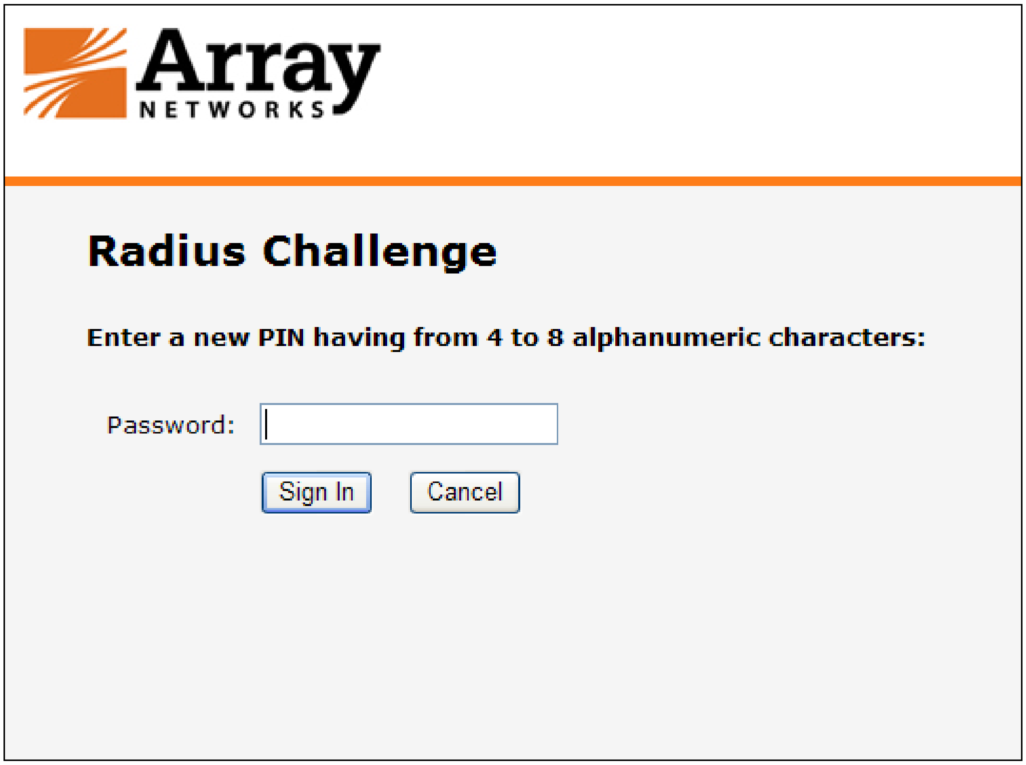


Login

Username:

Password:

User-defined New PIN:

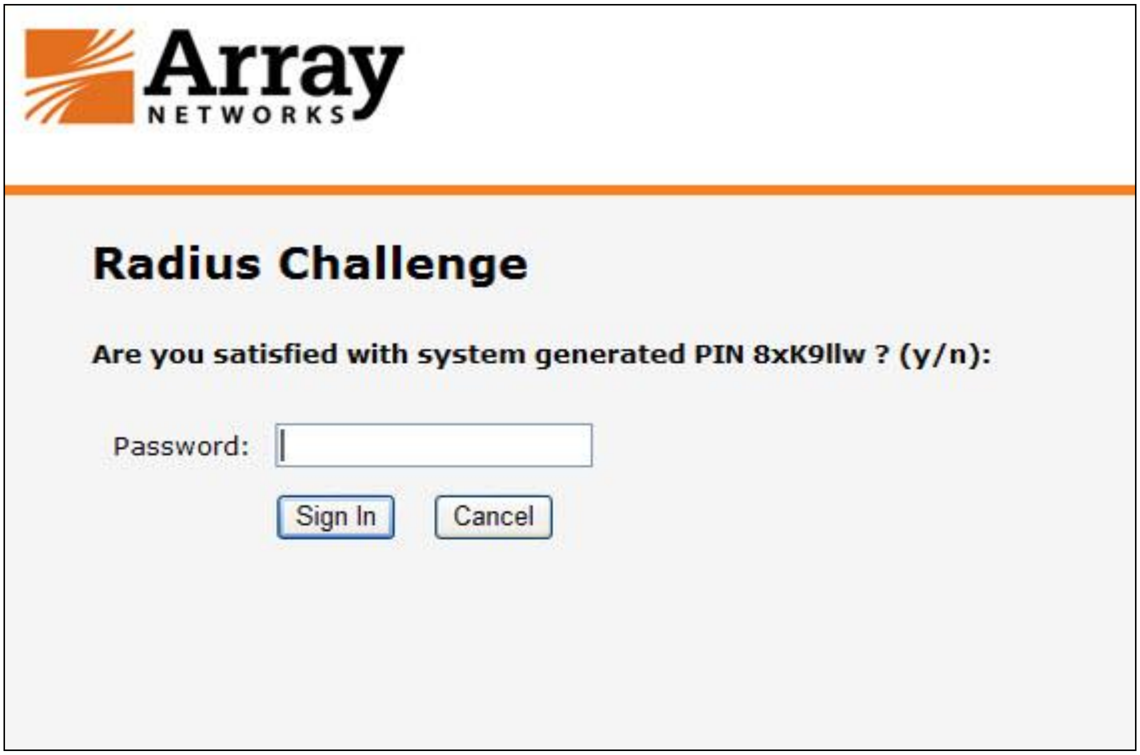


Radius Challenge

Enter a new PIN having from 4 to 8 alphanumeric characters:

Password:

System-generated New PIN:

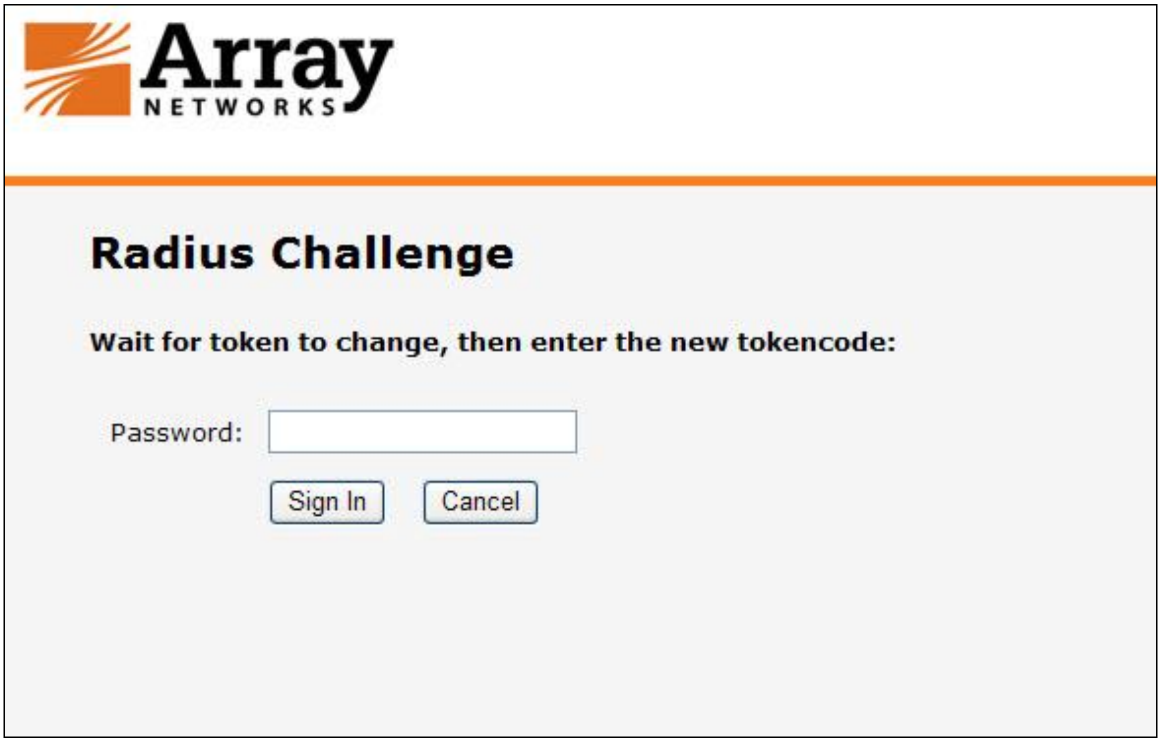


Radius Challenge

Are you satisfied with system generated PIN 8xK9llw ? (y/n):

Password:

Next Tokencode:



Radius Challenge

Wait for token to change, then enter the new tokencode:

Password:

Certification Checklist for RSA Authentication Manager

Date Tested: September 16, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
Array Networks SPX 2000	8.4.6.2	ArrayOS

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	✓
System Generated PIN	✓	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	✓
Deny PIN Reuse	✓	Deny PIN Reuse	✓
Passcode			
16-Digit Passcode	✓	16-Digit Passcode	✓
4-Digit Fixed Passcode	✓	4-Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	✓
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	✓
On-Demand New PIN	✓	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	✓
No RSA Authentication Manager	✓	No RSA Authentication Manager	✓

RSA Risk-Based Authentication Functionality			
RSA Native Protocol		**RADIUS Protocol**	
Risk-Based Authentication			
Risk-Based Authentication	✓	Risk-Based Authentication	✓
Risk-Based Authentication with SSO	N/A	Risk-Based Authentication with SSO	N/A

GLS

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration