

# SafeNet Authentication Service

## INTEGRATION GUIDE: USING RADIUS PROTOCOL FOR ARRAY AG SSL VPN



## Document Information

<b>Product Version</b>	1.0
<b>Document Part Number</b>	007-014054-001
<b>Release Date</b>	October 2018

## Revision History

<b>Revision</b>	<b>Date</b>	<b>Reason</b>
A	October 2018	Initial release

## Trademarks, Copyrights, and Third-Party Software

© 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

## Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- > The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages

resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.



# CONTENTS

<b>PREFACE</b> .....	<b>6</b>
Third-Party Software Acknowledgement .....	6
Description .....	6
Applicability .....	7
Environment.....	7
RADIUS Prerequisites .....	7
Audience.....	7
Support Contacts.....	7
Customer Support Portal .....	8
Telephone Support.....	8
Email Support .....	8
<b>CHAPTER 1: Authentication Flow</b> .....	<b>9</b>
<b>CHAPTER 2: SafeNet Authentication Service Setup</b> .....	<b>10</b>
Creating Users Stores .....	10
Assigning an Authenticator .....	11
Adding Array AG SSL VPN as an Authentication Node .....	11
<b>CHAPTER 3: Array AG SSL VPN Setup</b> .....	<b>13</b>
<b>CHAPTER 4: Running the Solution</b> .....	<b>20</b>
Using MobilePASS+ (or MobilePASS) .....	20
Simple Mode.....	20
Hybrid Mode.....	21
Using Gridsure.....	23
<b>APPENDIX A: Customizing the Login Page</b> .....	<b>25</b>
Push OTP-Hybrid Mode.....	25
GridSure-Hybrid Mode.....	31

# PREFACE

## Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Array AG SSL VPN.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

This document contains the following chapters:

- > "Overview" on page 9
- > "SafeNet Authentication Service Setup" on page 10
- > "Array AG SSL VPN Setup" on page 13
- > "Running the Solution" on page 20

## Description

SafeNet Authentication Service (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Array AG SSL VPN appliances allow enterprises to consolidate remote access for employees, partners, guests and other communities of interest on a single platform to minimize potential attack vectors, improve operational efficiency and provide a superior end-user experience. Drive productivity enterprise-wide, while keeping cost and complexity at a minimum.

Array Networks AG SSL VPN provides control over access to applications, desktops, files, networks, and Web sites from a broad range of remote and mobile devices – providing secure connectivity, end-point and server-side security and application-level AAA policies on a per-user basis.

This document describes how to:

- > Deploy multi-factor authentication (MFA) options in Array AG SSL VPN using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- > Configure Array AG SSL VPN to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Array AG SSL VPN environment is already configured and working with static passwords prior to implementing the multi-factor authentication using SafeNet Authentication Service.

Array AG SSL VPN can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

---

## Applicability

---

The information in this document applies to:

- > **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- > **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by service providers to deploy instances of SafeNet Authentication Service
- > **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization

---

## Environment

---

The integration environment that is used in this document is based on the following software versions:

- > **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—only when using this version. For Cloud not necessary to fill in version number.
- > **Array AG SSL VPN**—Version 9.4.0

---

## RADIUS Prerequisites

---

To enable SafeNet Authentication Service (SAS) to receive RADIUS requests from Array AG SSL VPN, ensure the following:

- > End users can authenticate from the Array AG SSL VPN with a static password before configuring the Array AG SSL VPN to use RADIUS authentication.
- > Ports 1812/1813 are open to and from the Array AG SSL VPN.

A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

---

## Audience

---

This document is targeted to system administrators who are familiar with Array AG SSL VPN, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

---

## Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or [Gemalto Customer Support](#).

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

## Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

**NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

## Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

## Email Support

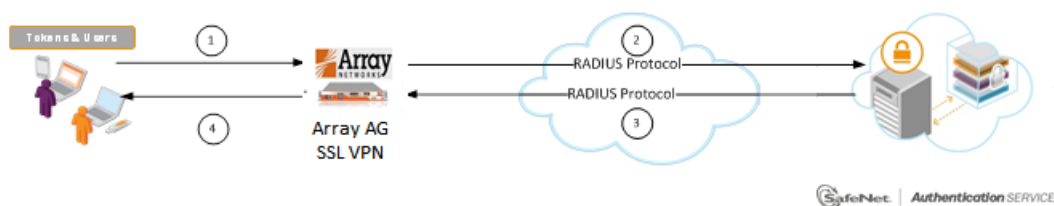
You can also contact technical support by email at [technical.support@gemalto.com](mailto:technical.support@gemalto.com).



# CHAPTER 1: Authentication Flow

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the data flow of a multi-factor authentication transaction for Array AG SSL VPN.



1. A user attempts to log on to Array AG SSL VPN using an OTP authenticator.
2. Array AG SSL VPN sends a RADIUS request with the user's credentials to SafeNet Authentication Service (SAS) for validation.
3. The SAS authentication reply is sent back to the Array AG SSL VPN.
4. The user is granted or denied access to the Array AG SSL VPN based on the OTP value calculation results from SAS.

For SafeNet Authentication Service (Cloud), a RADIUS agent is already configured and can be used without any additional agent installation or configuration requirements.

For SafeNet Authentication Service (SPE and PCE), a RADIUS agent (SAS Agent for Microsoft IAS or NPS, and FreeRADIUS) needs to be configured in the customer's environment.

For more information on how to install and configure the SAS Agent for Microsoft IAS, Microsoft NPS, and FreeRADIUS, refer to the [Agent Documentation](#).

## CHAPTER 2: SafeNet Authentication Service Setup

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Array AG SSL VPN using RADIUS protocol requires the following:

- > Creating Users Stores, page 10
- > Assigning an Authenticator, page 11
- > Adding Array AG SSL VPN as an Authentication Node, page 11

### Creating Users Stores

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- > Manually, one user at a time, using the **Create User** shortcut
- > Manually, by importing one or more user records via a flat file
- > Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the “*SafeNet Authentication Service Subscriber Account Operator Guide*” available [here](#).

All SafeNet Authentication Service documentation can be found on the [SafeNet Knowledge Base](#) site.

## Assigning an Authenticator

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Array AG SSL VPN.

The following authenticators are supported:

- > MobilePASS+
- > GrIDsure

Authenticators can be assigned to users in two ways:

- > **Manual provisioning**—Assign an authenticator to users one at a time.
- > **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the “*SafeNet Authentication Service Subscriber Account Operator Guide*” (available [here](#)) to learn how to provision the different authentication methods to the users in the SAS user store.

## Adding Array AG SSL VPN as an Authentication Node

Add a RADIUS entry in the SafeNet Authentication Service (SAS) **Auth Nodes** module to prepare it to receive RADIUS authentication requests from Array AG SSL VPN. You will need the IP address of Array AG SSL VPN and the shared secret to be used by both SAS and Array AG SSL VPN.

1. Log in to the SAS console with an Operator account, click the **COMMS** tab and then select **Auth Nodes**.
2. In the **Auth Nodes** module, click the **Auth Nodes** link.



**NOTE:** Before adding SafeNet Authentication Service (SAS) as a RADIUS server in Array AG SSL VPN, check its IP address (Primary RADIUS Server IP). The IP address will then be added to Array AG SSL VPN as a RADIUS server at a later stage.

3. Under **Auth Nodes**, click **Add**.

4. Under **Add Auth Nodes**, complete the following fields, and then click **Save**:

<b>Auth Node Name</b>	Enter a name for the Auth node.
<b>Host Name</b>	Enter the name of the host that will authenticate with SAS.
<b>Low IP Address In Range</b>	Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS (in this case, a range of IP addresses is being used).
<b>High IP Address In Range</b>	Enter the highest IP address in a range of IP addresses that will authenticate with SAS (in this case, a range of IP addresses is being used).
<b>Configure FreeRADIUS Synchronization</b>	Select this option.
<b>Shared Secret</b>	Enter the shared secret key.
<b>Confirm Shared Secret</b>	Re-enter the shared secret key.

**Add Auth Node**

**Auth Nodes** | Sharing & Realms

Auth Node Name:   Exclude from PIN change requests

Resource Name:   Configure FreeRADIUS Synchronization

Host Name:  Shared Secret:

Low IP Address In Range:  Confirm Shared Secret:

High IP Address In Range:  FreeRADIUS synchronization may take up to 5 minutes to propagate in the system.

The authentication node is added to the system.

**Auth Nodes**

Auth Nodes:  
Task: Create and configure SafeNet Authentication Service Authentication Nodes.

Auth Nodes:  
Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.

Primary RADIUS Server IP:  Primary SafeNet Authentication Service Agent:  Max Auth Nodes: 20

Fallover RADIUS Server IP:  Fallover SafeNet Authentication Service Agent:

Index	Auth Node Name	Host Name	IP Address	FreeRADIUS Synchronization			
1	Array AG SSL	<input type="text"/>	<input type="text"/>	False	False	Edit	Remove

## CHAPTER 3: Array AG SSL VPN Setup

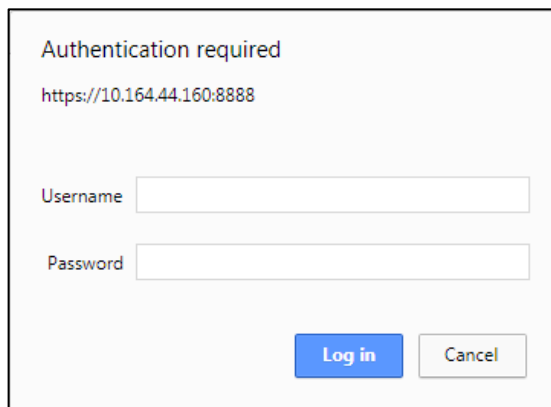
Perform the following steps to configure Array AG SSL VPN to use the RADIUS protocol as the authentication method:

1. In a web browser, open the following URL:

**https://<Array AG SSL VPN IP address>:<Port Number>**

Where,

- **<AG SSL VPN IP address>** is the IP address of Array AG SSL VPN.
  - **<Port Number>** is the Web UI port number that you configured for Array AG SSL VPN.
2. On the Array AG SSL VPN login window, enter your administrator **Username** and **Password**, and click **Log in**.



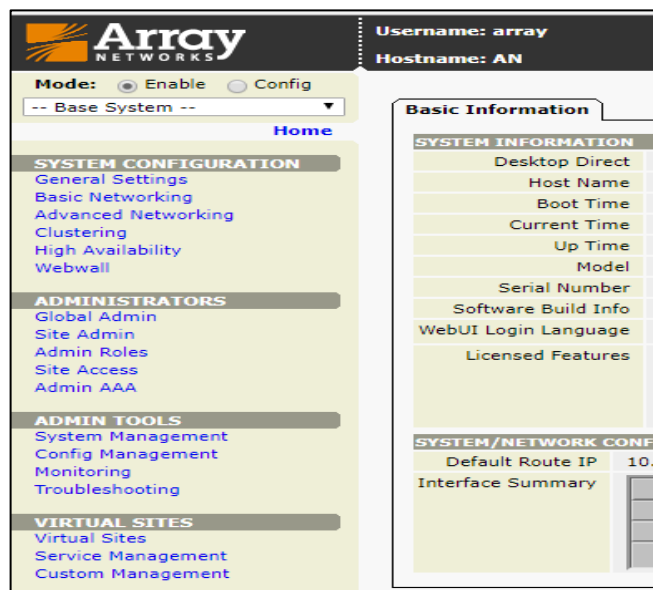
Authentication required  
https://10.164.44.160:8888

Username

Password

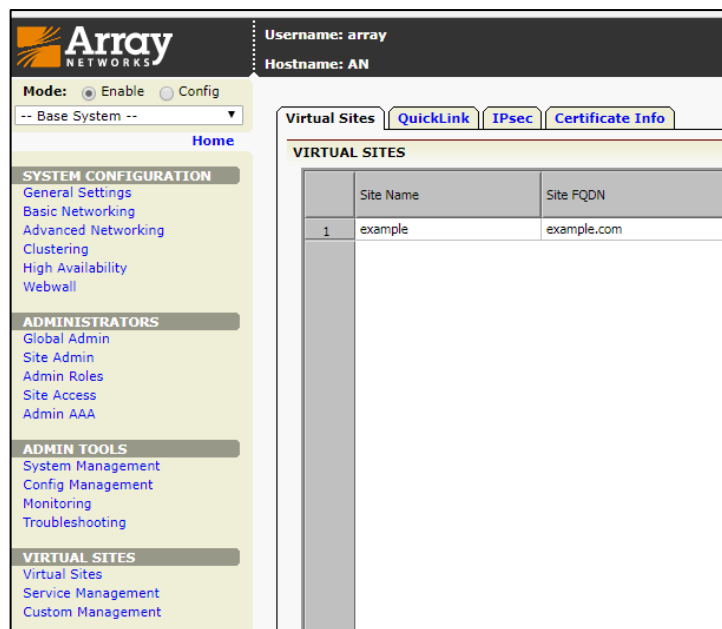
*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

- On the Array AG SSL VPN administrator dashboard, in the left pane, under **VIRTUAL SITES**, click **Virtual Sites**.



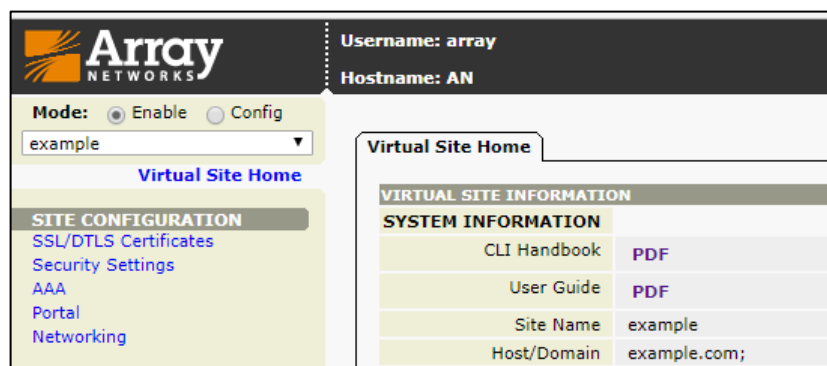
(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

- In the right pane, on the **Virtual Sites** tab, in the **Site Name** column, double-click on the virtual site name (for example, **example**) for which you would like to implement MFA.



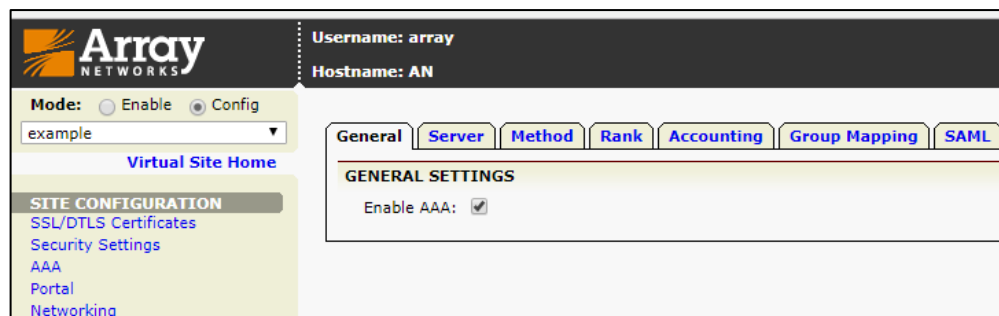
(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

5. In the left pane, perform the following steps:
  - a. Under **Mode**, select the **Config** option.
  - b. Under **SITE CONFIGURATION**, click **AAA**.



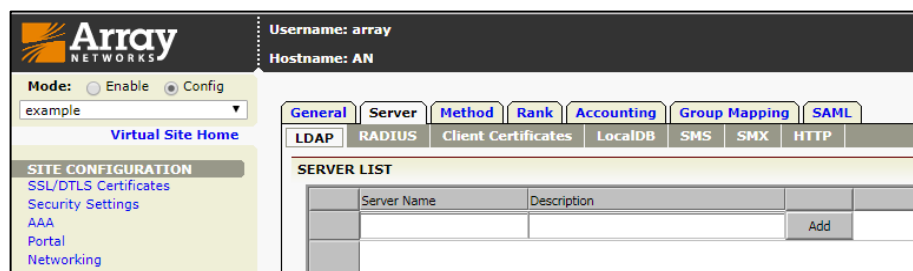
(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

6. In the right pane, on the **General** tab, ensure that **Enable AAA** check box is selected.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

7. On the **Server** tab, click the **RADIUS** tab.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

8. On the **RADIUS** tab, under **SERVER LIST**, in the **Server Name** column, enter any name for the server (for example, **SAS**), and click **Add**.

Server Name	Description	
		Add

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

9. Under **SERVER LIST**, ensure that the server (for example, **SAS**) that you just added is listed. Double-click on the server name (**SAS**).

Server Name	Description	
<input type="checkbox"/> SAS	SAS	Add

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

10. Under **RADIUS SERVER CONFIGURATION**, click **Add RADIUS Server**.

Server Name: SAS

RADIUS NA-SIP: \_\_\_\_\_

RADIUS Attribute Group: \_\_\_\_\_ (Integer from 0 to 254)

RADIUS Attribute Default Group: \_\_\_\_\_

RADIUS Attribute ClientIP: \_\_\_\_\_ (Integer value between 1 and 240)

RADIUS Attribute ClientIP Mask: \_\_\_\_\_ (Integer value between 1 and 240)

RADIUS Username Prefix: \_\_\_\_\_

RADIUS Username Suffix: \_\_\_\_\_

RADIUS Attribute Phone Number: \_\_\_\_\_

\* Note: The attribute string is used to get phone number for SMS server, if the RADIUS server is configured where to get the phone number.

Redundancy Order	Server IP	Server Port	Secret Password	Timeout	Retries	Accounting Port

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)



11. Under **ADD RADIUS SERVER**, complete the following fields, and click **Save**.

<b>Server IP</b>	Enter the <b>Primary RADIUS Server IP</b> address that is available in the <b>Auth Nodes</b> module of the SAS server. Refer to <b>step 4</b> of “ <b>Adding Array AG SSL VPN as an Authentication Node</b> ” on page 11.
<b>Server Port</b>	Enter <b>1812</b> .
<b>Secret Password</b>	Enter the <b>Shared Secret</b> that you entered earlier in <b>step 4</b> of <b>Adding Array AG SSL VPN as an Authentication Node</b> on page 11.
<b>Timeout</b>	Enter <b>60</b> .
<b>Redundancy Order</b>	Enter <b>1</b> .
<b>Retries</b>	Enter <b>5</b> .

*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

**NOTE:** RADIUS timeout must be minimum 60 seconds for the MobilePASS+ token.

**NOTE:** It is recommended to configure a secondary (failover) IP address for your Radius equipment to cover for authentication disruptions if the service provider supports it.

12. Under **RADIUS SERVER CONFIGURATION**, ensure that the new RADIUS server configured in the previous step is listed.

The screenshot shows the 'RADIUS SERVER CONFIGURATION' page. The 'ADVANCED RADIUS SERVER CONFIGURATION' section includes the following fields:

- Server Name: SAS
- RADIUS NASIP: [Empty]
- RADIUS Attribute Group: [Empty] (Integer from 0 to 254)
- RADIUS Attribute Default Group: [Empty]
- RADIUS Attribute ClientIP: [Empty] (Integer value between 1 and 240)
- RADIUS Attribute ClientIP Mask: [Empty] (Integer value between 1 and 240)
- RADIUS Username Prefix: [Empty]
- RADIUS Username Suffix: [Empty]
- RADIUS Attribute Phone Number: [Empty]

A note below the fields states: *\* Note: The attribute string is used to get phone number for SMS server, if the RADIUS server is configured where to get the phone number.*

The 'RADIUS SERVER CONFIGURATION' table is as follows:

	Redundancy Order	Server IP	Server Port	Secret Password	Timeout	Retries	Accounting Port
1	1	109.73.120.148	1812	XXXXXXXXXX	60	5	1813

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

13. Click the **Method** tab.
14. On the **Method** tab, click **Add Method**.

The screenshot shows the 'METHOD' configuration page. The table below is empty:

Method Name	Method Description	Authenticate	Authorize	OTP Authenticati	Server for Phone
-------------	--------------------	--------------	-----------	------------------	------------------

Below the table, there is a dropdown menu for 'AAA Method for Mobile VPN Clients:' and a note: *\* Note: This option only takes effect when AAA rank is off, specifying an AAA method for Mobile VPN clients.*

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

15. Under **ADD METHOD CONFIGURATION**, complete the following fields, and click **Save**.

<b>Method Name</b>	Enter a name for the method (for example, <b>SAS Method</b> ).
<b>Authentication</b>	Select the RADIUS server (for example, <b>SAS</b> ) that you created in <b>step 8</b> of this section.

The screenshot shows the 'ADD METHOD CONFIGURATION' window with the following fields and options:

- Method Name:** Text input field.
- Method Description:** Text input field (Optional).
- General Authentication Configuration:**
  - Authentication:** Dropdown menu.
  - (AND):** Dropdown menu.
  - Authorization:** Dropdown menu.
- OTP(One-time Password) Authenticate Configuration:**
  - OTP Authentication Servers:** Dropdown menu.
  - Server for Phone Number Retrieval:** Dropdown menu.

Notes:

- \* Note: for one-factor authentication method, if the authorization server is not specified, the authorization server will be set the same as the authentication server. For multi-factor authentication method, the authorization server must be specified; otherwise error message will be prompted.
- \*\* Note: The relationship among the multiple authentication servers is "AND", i.e. only users who pass authentication of each server can log in.
- \*Note: The Server for Phone Number Retrieval must be one of the AAA server (Authentication/Authorization) specified for this AAA method.
- \*\* Note: If the Server for Phone Number Retrieval is specified as an AAA server of the Client Certificate type, the Certificate SHS Configuration is necessary.

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

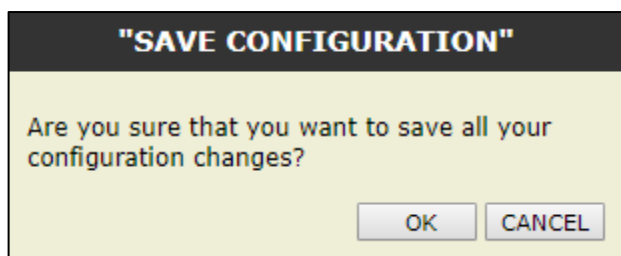
16. Ensure that the method you created in the previous step is listed under **Method**. Click **Save Configuration**.

The screenshot shows the 'METHOD' configuration window with the following table:

Method Name	Method Description	Authenticate	Authorize	OTP Authentication	Server for Phone
1 SAS Method	SAS Method	SAS	SAS		

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

17. On the **SAVE CONFIGURATION** window, click **OK**.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

18. Customize the login page to use the Push OTP token in the Hybrid mode. Refer to the **Push OTP-Hybrid Mode** section of **Appendix A** on page 25.
19. Customize the login page to use the GridSure token in the Hybrid mode. Refer to the **GridSure-Hybrid Mode** section of **Appendix A**, on page 31.

# CHAPTER 4: Running the Solution

For this integration, the following tokens are configured for authentication with the SafeNet Authentication Service (SAS):

- > MobilePASS+ (or MobilePASS)
- > GrIdSure

## Using MobilePASS+ (or MobilePASS)

The assigned applications can be accessed using the MobilePASS+ (or MobilePASS) token through the **Simple** or **Hybrid** mode.

### Simple Mode

Perform the following steps to access the assigned applications through the simple mode:

1. In a web browser, open the virtual site.

**https://<Virtual Site URL>**

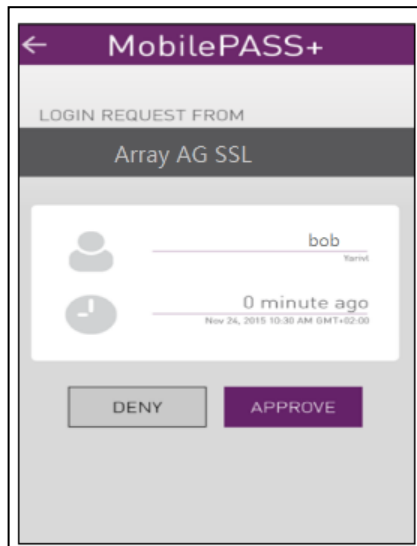
Where, **<Virtual Site URL>** is the URL or the IP address that you configured in Array AG SSL VPN.

2. On the **Login** window, perform the following steps:
  - a. In the **Username** field, enter the username.
  - b. Click **Sign In**.



*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

- On the registered mobile device, tap **APPROVE** to accept the OTP request.

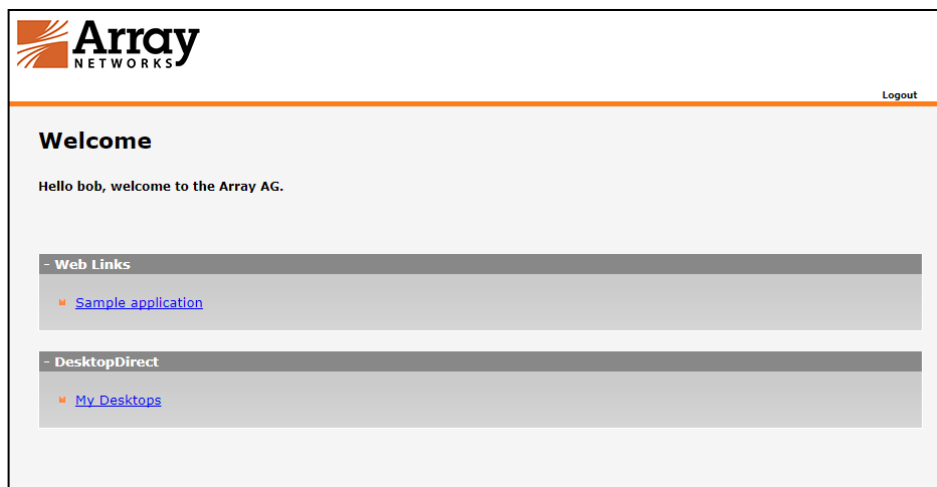


- On the **TOKEN AUTHENTICATION** screen, enter the token PIN, and tap **Continue** to send the approval with OTP to SAS.

A success message is displayed on the mobile device.



After successful authentication, you will be able to access the assigned applications.



*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

## Hybrid Mode

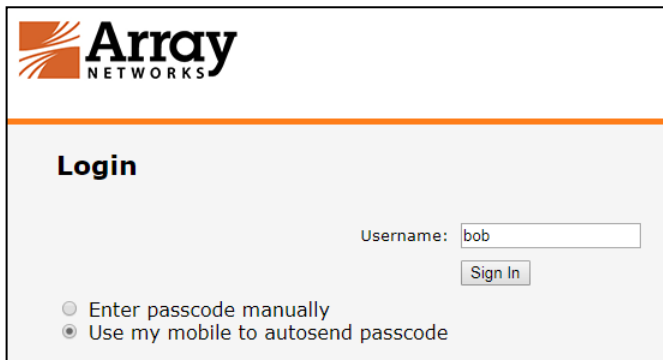
- In a web browser, open the virtual site.

**https://<Virtual Site URL>**

Where, **<Virtual Site URL>** is the URL or the IP address that you configured in Array AG SSL VPN.

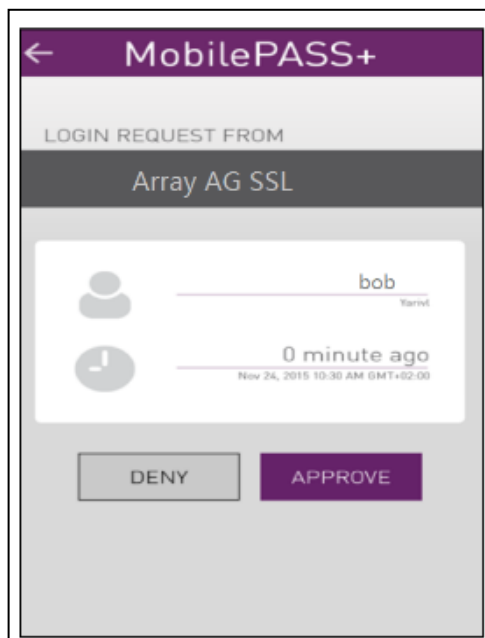
2. On the login window, perform the following steps:
  - a. In the **Username** field, enter the username.
  - b. Select any of the following options and click **Sign In**:
    - **Enter passcode manually**
    - **Use my mobile to autosend passcode**

**NOTE:** In this scenario, the **Use my mobile to autosend passcode** option is selected.



*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

3. On the registered mobile device, tap **APPROVE** to accept the OTP request.

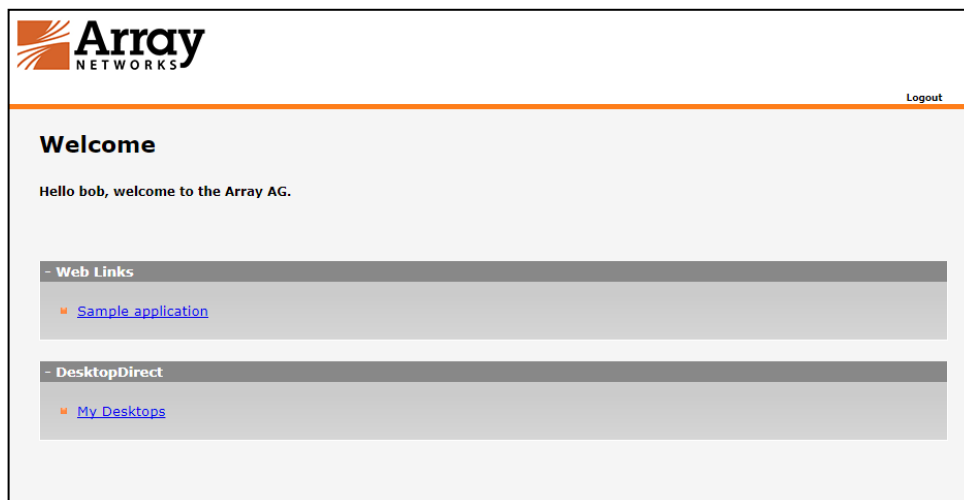


4. On the **TOKEN AUTHENTICATION** screen, enter **Token PIN**, and tap **CONTINUE** to send the approval with OTP to SAS.

A success message is displayed on the mobile device.



After successful authentication, you will be able to access the assigned applications.



*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

## Using Gridsure

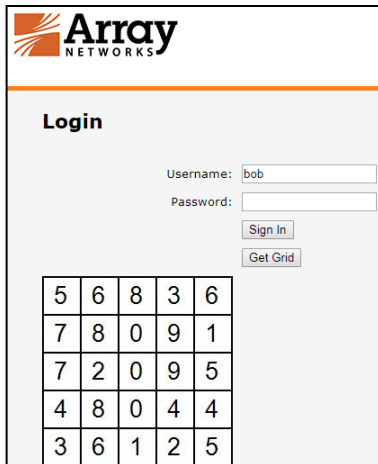
For this integration, Gridsure token is configured for authentication with the SAS solution. Perform the following steps to access the assigned applications:

1. In a web browser, open the virtual site.

**https://<Virtual Site URL>**

Where, **<Virtual Site URL>** is the URL or the IP address that you configured in Array AG SSL VPN.

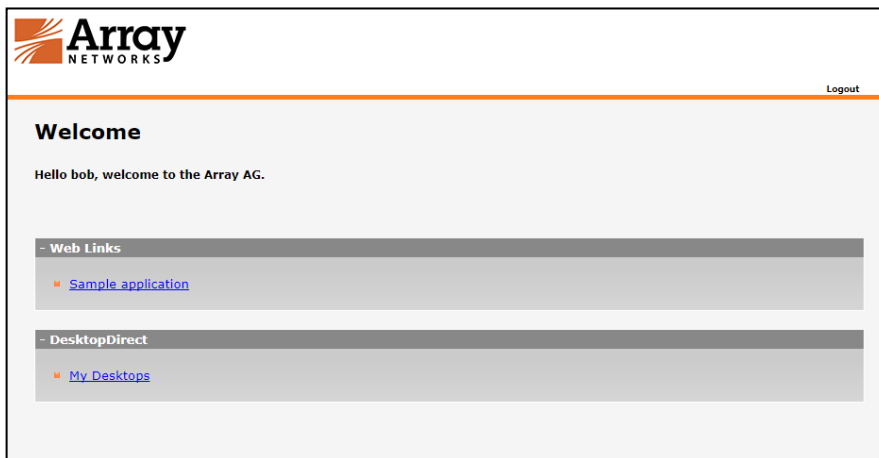
2. On the login window, perform the following steps:
  - a. In the **Username** field, enter the username.
  - b. Click **Get Grid**.
  - c. In the **Password** field, enter the grid combination.
  - d. Click **Sign In**.



5	6	8	3	6
7	8	0	9	1
7	2	0	9	5
4	8	0	4	4
3	6	1	2	5

*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

After successful authentication, you will be able to access the assigned applications.



Logout

### Welcome

Hello bob, welcome to the Array AG.

**Web Links**

- [Sample application](#)

**DesktopDirect**

- [My Desktops](#)

*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*



# APPENDIX A: Customizing the Login Page

The Login page can be customized for the Push OTP-Hybrid and GridSure-Hybrid modes.

## Push OTP-Hybrid Mode

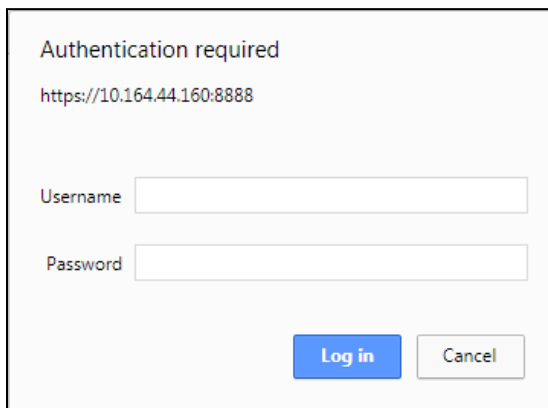
Perform the following steps to customize the login page for the Push OTP-Hybrid mode:

1. In a web browser, open the following URL:

**https://<Array AG SSL VPN IP address>:<Port Number>**

Where,

- **<AG SSL VPN IP address>** is the IP address of Array AG SSL VPN.
  - **<Port Number>** is the Web UI port number that you configured for Array AG SSL VPN.
2. On the AG SSL VPN login window, enter your administrator **Username** and **Password**, and click **Log in**.



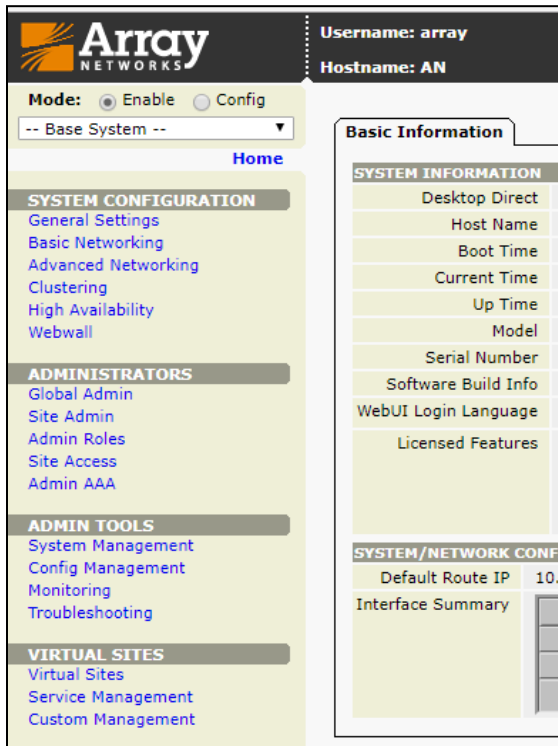
Authentication required  
https://10.164.44.160:8888

Username

Password

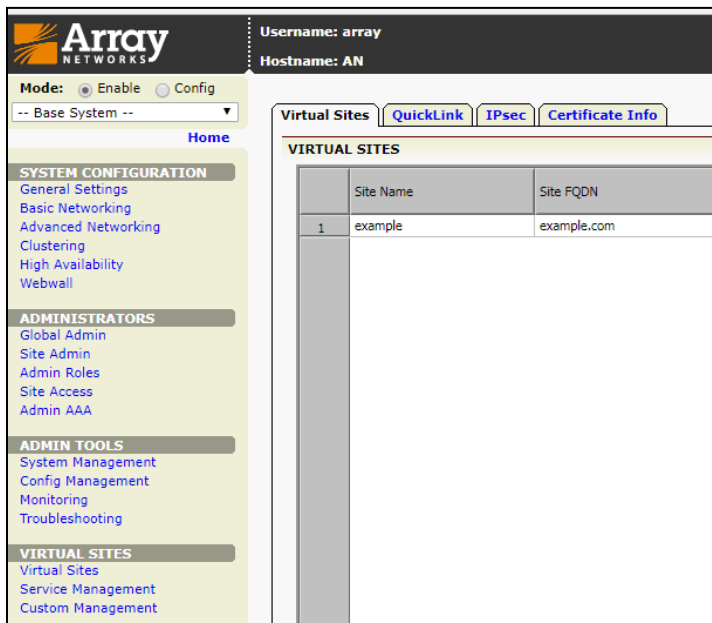
*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

- On the Array AG SSL VPN administrator dashboard, in the left pane, under **VIRTUAL SITES**, click **Virtual Sites**.



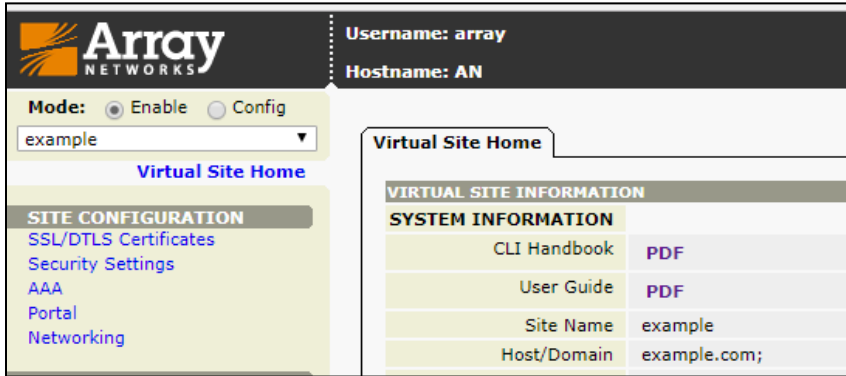
(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

- In the right pane, on the **Virtual Sites** tab, under **VIRTUAL SITES**, in the **Site Name** column, double-click on the virtual site name (for example, **example**) for which you would like to implement MFA.



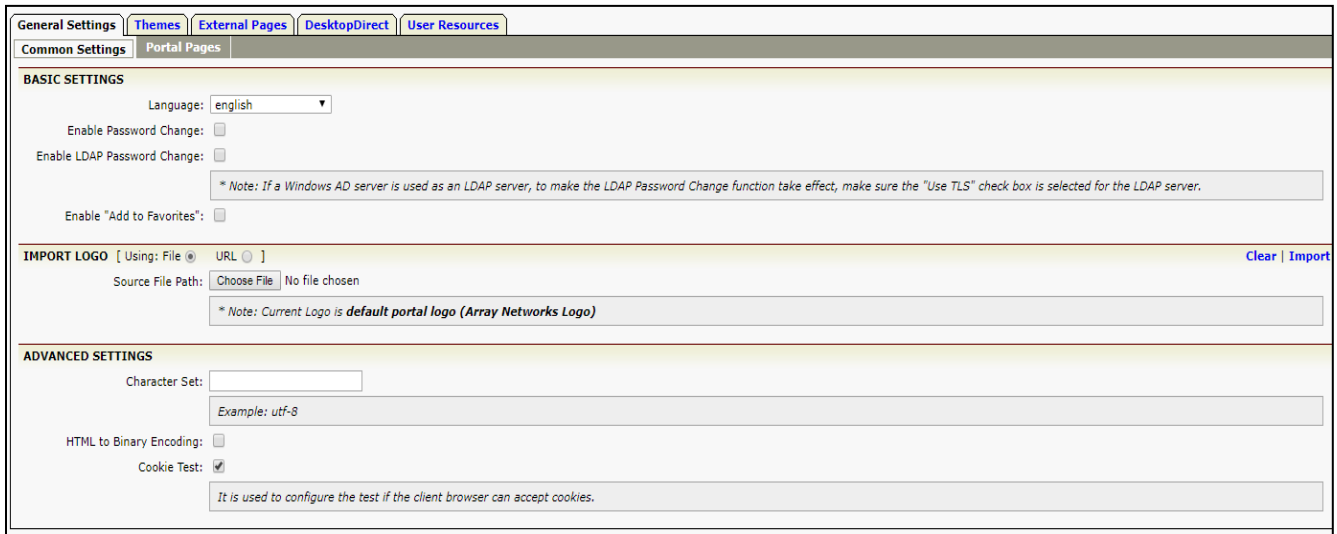
(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

5. In the left pane, perform the following steps:
  - a. Under **Mode**, select the **Config** option.
  - b. Under **SITE CONFIGURATION**, click **AAA**.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

6. In the right pane, click the **Themes** tab.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

7. On the **Themes** tab, click **Import Template**.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

8. Under **THEMES**, in the **Theme Name** column, double-click **default\_theme**.

Theme Name	Configured Pages
1 default_theme	autolaunch, challenge, client_security, ldappasschange, login, logout, ...

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

9. Under **THEME OBJECTS**, in the **Page type** column, double-click **login**.

Page type	Object Name	URL	File type
1 autolaunch	autolaunch	http://localhost/index.html	html
2 challenge	challenge	http://localhost/index.html	html
3 client_security	client_security	http://localhost/index.html	html
4 ldappasschange	ldappasschange	http://localhost/index.html	html
5 login	login	http://localhost/index.html	html
6 logout	logout	http://localhost/index.html	html
7 passchange	passchange	http://localhost/index.html	html
8 sms	sms	http://localhost/index.html	html
9 smsr	smsr	http://localhost/index.html	html
10 custom	static	http://localhost/orange_bullet.png	html
11 welcome	welcome	http://localhost/index.html	html

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

10. Under **OBJECT RESOURCES**, ensure that **Enable Rewrite** check box is not selected and in the table, for the **index.html** resource, click **Edit**.

Resource	Size (in bytes)	Edit
1 index.html	18051	Edit
2 lock_logo.gif	4692	
3 portal.css	8675	Edit

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

11. Under **EDIT OBJECT RESOURCES**, perform the following steps:

- a. Search for the following content:

```
<td align=left><input type="submit" name="submitbutton" value="Login"><input type="submit"
name="changepassbutton" value="ChangePass"></td>
</tr>
```

- b. Enter the following content below the content searched in previous step:

```

<tr>
<td>
<div>
<input type="radio" id="rdoPassword" name="rdoPassword" onClick='pushOTP(true);' checked
> Enter passcode manually</input>
<br>
<input type="radio" id="rdoPassword" name="rdoPassword" onClick='pushOTP(false);'> Use
my mobile to autosend passcode </input>
</div>
</td>
</tr>

```

- c. Search for the following content:

```

<div id="vpn_hardwareid_div"></div>
</form>

```

- d. Enter the following content below the content searched in the previous step:

```

<script language="JavaScript">
function pushOTP(value)
{
if(value != true)
{
document.getElementById("pwd_content").style.display = "none";
}
else
{
document.getElementById("pwd_content").style.display = "";
}
}
}
</script>

```

e. Click **Save**.

Select Portal Theme:  [\[Back to top\]](#)

**Themes**

**EDIT OBJECT RESOURCES** [index.html]

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<!-- Array Inc. V2 -->
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta name="robots" content="noindex,
nofollow">
<meta http-equiv="X-Frame-Options" content="DENY">
<script language="JavaScript" src="/prx/000/http/localhost/an_login.js"></script>
<script>document.title=_AN_str_title_login;</script>
<title>Login</title>
<link rel="stylesheet" type="text/css" href="portal.css">
<meta id="viewport" name="viewport" content="width=device-width,initial-scale=1.0,maximum-scale=1.0,user-
scalable=0" />
<script language="JavaScript" src="/prx/000/http/localhost/an_util.js" charset="UTF-8"></script>
<script language="JavaScript">

function localCheckAndInit() {
    if(_AN_hardwareid_on == true && localCheckIsOk() == false) {
        var strErrMsg = _AN_str_localcheck_errmsg.replace("%s", _AN_str_localcheck_OS);
        strErrMsg = strErrMsg.replace("%s", _AN_str_localcheck_ver);
        document.getElementById("localCheckLogin").innerHTML = strErrMsg.replace("%s", "HardwareID");
        document.getElementById("localCheckLogin").style.display = "";
    }
    else {
        document.getElementById("localCheckLogin").style.display = "";
        document.getElementById("localCheckLogin").style.marginLeft = "0px";
        init();
    }
}
if (_AN_is_motionPro_site){
    document.all.user_content.style.display = "none";
}
```

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

12. Click **Back to top**.

Select Portal Theme:  [\[Back to top\]](#)

**Themes**

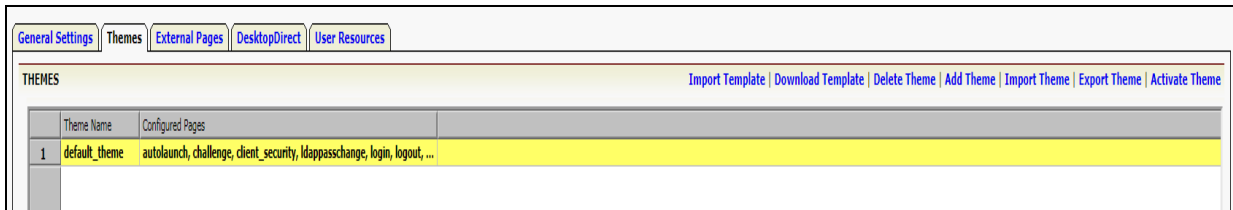
**OBJECT RESOURCES** [login]

Enable Rewrite:

	Resource	Size (in bytes)		
1	index.html	17854	<a href="#">Edit</a>	
2	lock_logo.gif	4692		
3	portal.css	8675	<a href="#">Edit</a>	

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

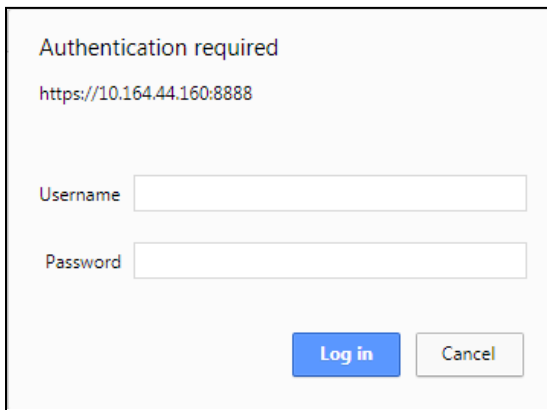
13. On the **Themes** tab, click the **default\_theme** and click **Activate Theme**.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

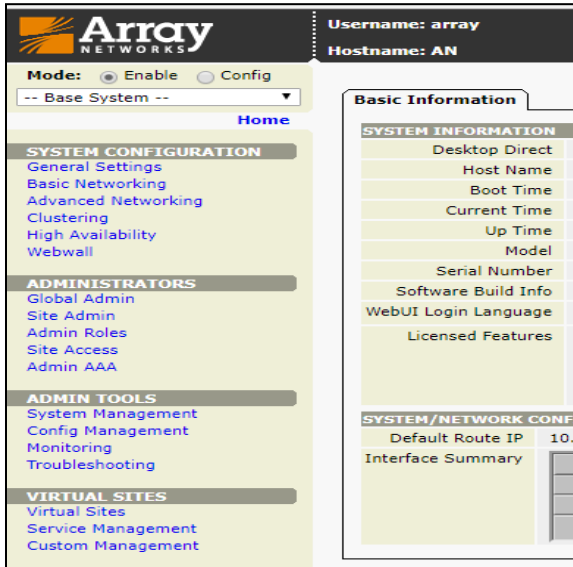
## GridSure-Hybrid Mode

- In a web browser, open the following URL:  
<https://<Array AG SSL VPN IP address>:<Port Number>>  
 Where,
  - <AG SSL VPN IP address> is the IP address of Array AG SSL VPN.
  - <Port Number> is the Web UI port number that you configured for Array AG SSL VPN.
- On the AG SSL VPN login window, enter your administrator **Username** and **Password**, and click **Log in**.



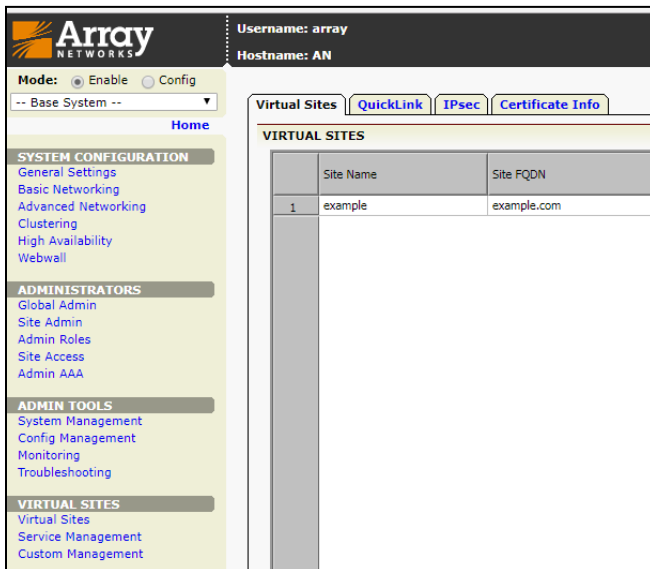
(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

- On the Array AG SSL VPN administrator dashboard, in the left pane, under **VIRTUAL SITES**, click **Virtual Sites**.



*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

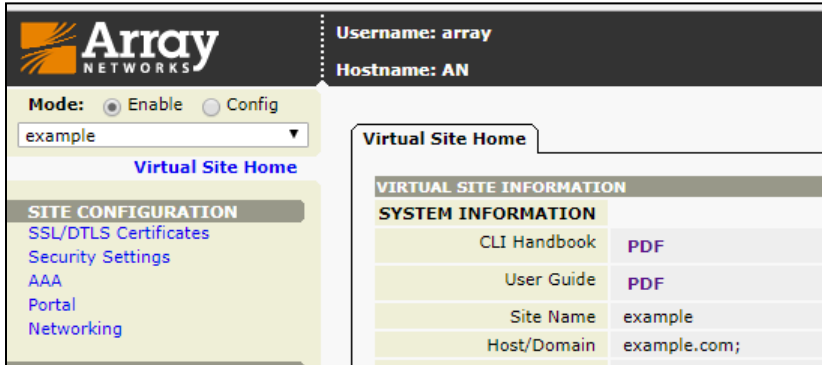
- In the right pane, on the **Virtual Sites** tab, under **VIRTUAL SITES**, in the **Site Name** column, double-click on the virtual site name (for example, **example**) for which you would like to implement MFA.



*(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)*

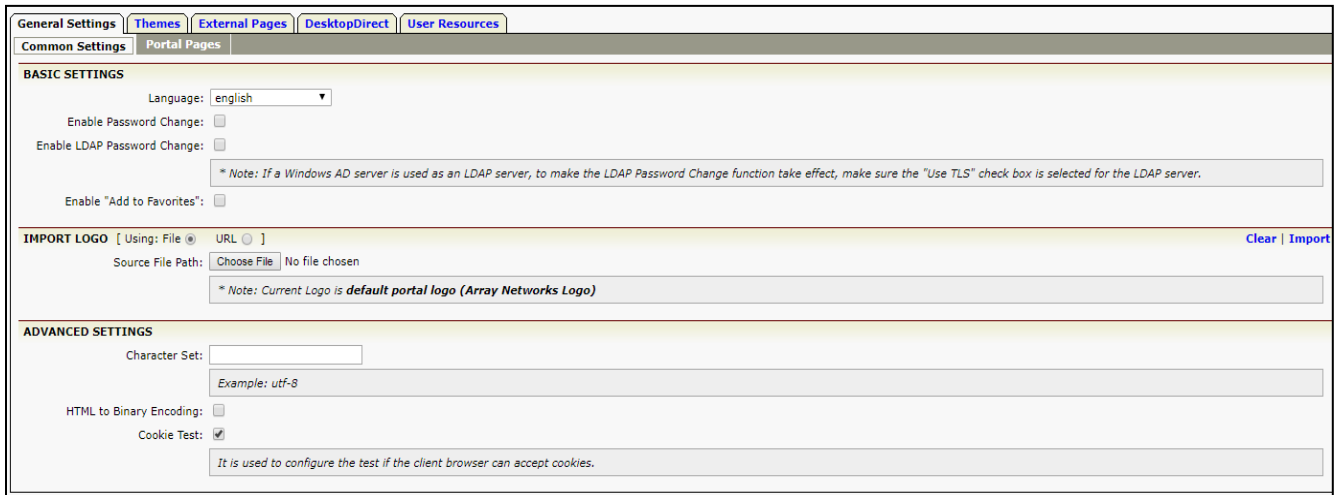


5. In the left pane, perform the following steps:
  - a. Under **Mode**, select the **Config** option.
  - b. Under **SITE CONFIGURATION**, click **AAA**.



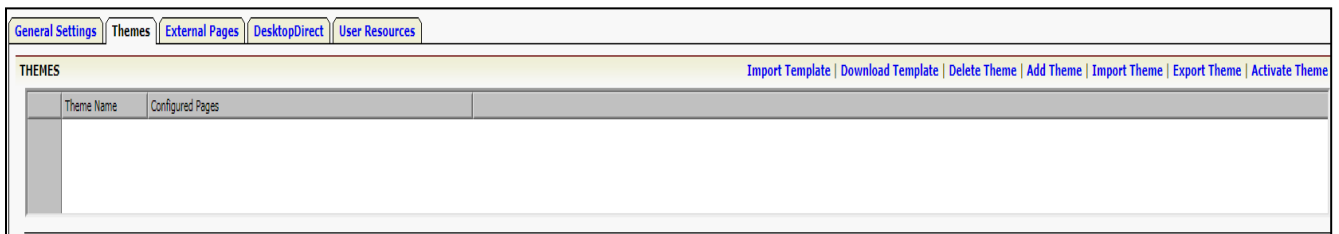
(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

6. In the right pane, click the **Themes** tab.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

7. On the **Themes** tab, click **Import Template**.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

8. Under **THEMES**, in the **Theme Name** column, double-click **default\_theme**.

Theme Name	Configured Pages
1 default_theme	autolaunch, challenge, client_security, ldapasschange, login, logout, ...

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

9. Under **THEME OBJECTS**, in the **Page type** column, double-click **login**.

Page type	Object Name	URL	File type
1 autolaunch	autolaunch	http://localhost/index.html	html
2 challenge	challenge	http://localhost/index.html	html
3 client_security	client_security	http://localhost/index.html	html
4 ldapasschange	ldapasschange	http://localhost/index.html	html
5 login	login	http://localhost/index.html	html
6 logout	logout	http://localhost/index.html	html
7 passchange	passchange	http://localhost/index.html	html
8 sms	sms	http://localhost/index.html	html
9 smx	smx	http://localhost/index.html	html
10 custom	static	http://localhost/orange_bullet.png	html
11 welcome	welcome	http://localhost/index.html	html

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

10. Under **OBJECT RESOURCES**, ensure that **Enable Rewrite** option is not selected and in the table, for the **index.html** resource, click **Edit**.

Resource	Size (in bytes)	Edit
1 index.html	18051	Edit
2 lock_logo.gif	4692	
3 portal.css	8675	Edit

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

11. Under **EDIT OBJECT RESOURCES**, perform the following steps:

- a. Search for the following content:

```
<td align=left><input type="submit" name="submitbutton" value="Login"><input type="submit"
name="changepassbutton" value="ChangePass"></td>
</tr>
```

- b. Enter the following content, below the content searched in the previous step:

```
<tr>
<td></td>
<td align=left><input type="button" name="gridButton" value='Get Grid' title="Get Grid"
onclick="grid()"></td>
</tr>
<tr>
<td>
<div id="challengeImageDiv" style="visibility:hidden; display:none;"><img id="challengeImage"
src=""/></div> </td>
</tr>
```

- c. Search for the following content:

```
<div id="vpn_hardwareid_div"></div>
</form>
```

- d. Enter the following content, below the content searched the previous step:

```
<script language="JavaScript">
function grid()
{
    var BlackShieldServerLocation = "Change to Org's Unique Self-Service URL that you will
get from SAS";
    // BlackShieldServerLocation URL might look like the following:
    // - https://cloud.safenet- inc.com/blackshieldss/O/691UML1C62/index.aspx
    var usrName = document.all.username.value;
    var challengeImg = document.getElementById("challengeImage");
    challengeImg.src = BlackShieldServerLocation +
"?getChallengeImage=true&userName=" + usrName + "&noCache=" + new Date().toString();
    var challengeDiv = document.getElementById("challengeImageDiv");
    challengeDiv.style.display="block";
    challengeDiv.style.visibility="visible";
}
</script>
```

e. Click **Save**.

Select Portal Theme:  [\[Back to top\]](#)

**Themes**

**EDIT OBJECT RESOURCES** [index.html]

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<!-- Array Inc. V2 -->
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta name="robots" content="noindex,
nofollow">
<meta http-equiv="X-Frame-Options" content="DENY">
<script language="JavaScript" src="/prx/000/http/localhost/an_login.js"></script>
<script>document.title=_AN_str_title_login;</script>
<title>Login</title>
<link rel="stylesheet" type="text/css" href="portal.css">
<meta id="viewport" name="viewport" content="width=device-width,initial-scale=1.0,maximum-scale=1.0,user-
scalable=0" />
<script language="JavaScript" src="/prx/000/http/localhost/an_util.js" charset="UTF-8"></script>
<script language="JavaScript">

function localCheckAndInit() {
    if(_AN_hardwareid_on == true && localCheckIsOk() == false) {
        var strErrMsg = _AN_str_localcheck_errmsg.replace("%s", _AN_str_localcheck_OS);
        strErrMsg = strErrMsg.replace("%s", _AN_str_localcheck_ver);
        document.getElementById("localCheckLogin").innerHTML = strErrMsg.replace("%s", "HardwareID");
        document.getElementById("localCheckLogin").style.display = "";
    }
    else {
        document.getElementById("localCheckLogin").style.display = "";
        document.getElementById("localCheckLogin").style.marginLeft = "0px";
        init();
    }
}
if (_AN_is_motionPro_site){
    document.all.user_content.style.display = "none";
}
```

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

12. Click **Back to top**.

Select Portal Theme:  [\[Back to top\]](#)

**Themes**

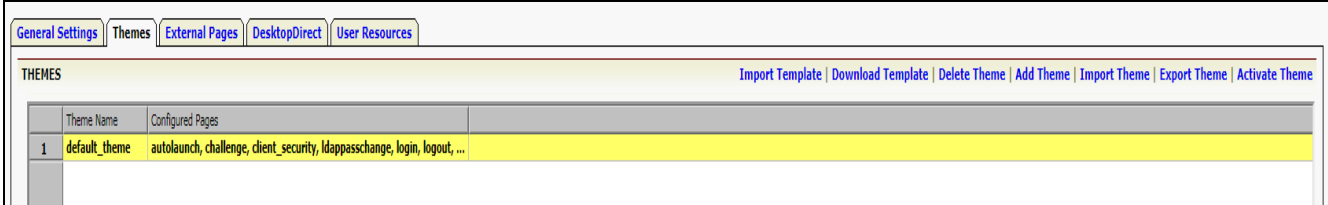
**OBJECT RESOURCES** [login]

Enable Rewrite:

	Resource	Size (in bytes)		
1	index.html	17854	<a href="#">Edit</a>	
2	lock_logo.gif	4692		
3	portal.css	8675	<a href="#">Edit</a>	

(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)

13. On the **Themes** tab, click **default\_theme** and click **Activate Theme**.



(The screen image above is from Array AG SSL VPN. Trademarks are the property of their respective owners.)