

Deploying Array Networks vxAG/AG Series SSL VPN with RSA Server



Table of Contents

1 Introduction	2
2 Configure the RADIUS Server	3
2.1 Alternative to using RADIUS Agent.....	5
2.1.1 Create the SecurID authentication agent.....	5
3 User Management	7
3.1 Configure RADIUS User Attributes	8
3.2 Import Token	8
3.3 Policies	11
3.4 Token Policy.....	12
3.5 Monitoring.....	13
4 Configure the AG.....	13

1 Introduction

Array's AG Series secure access gateways and vxAG virtual secure access gateways offer multiple methods of network access, and can be used with third-party two-factor/multifactor authentication products such as RSA's SecurID. This document describes how to integrate the AG Series or vxAG with the RSA token automation.

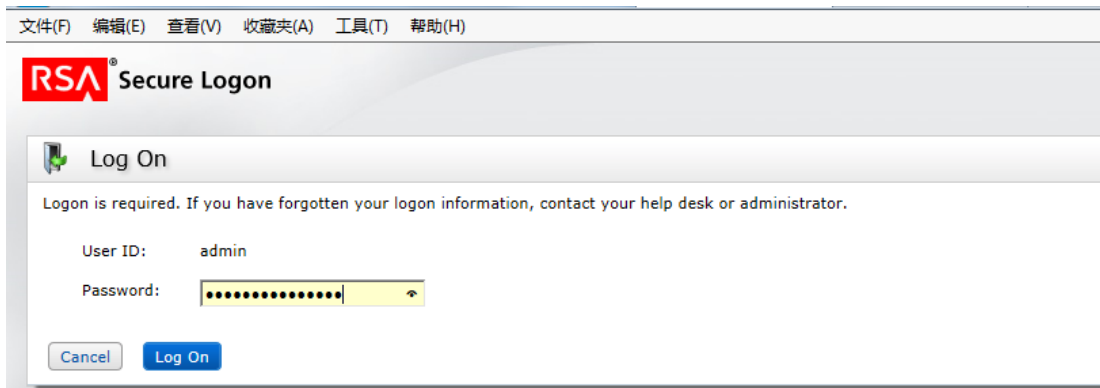
The process of integrating the Array vxAG/AG Series SSL VPN with the RSA SecurID software token consists of the following steps:

- Configure the RADIUS server
- User management
- Configure the vxAG or AG Series

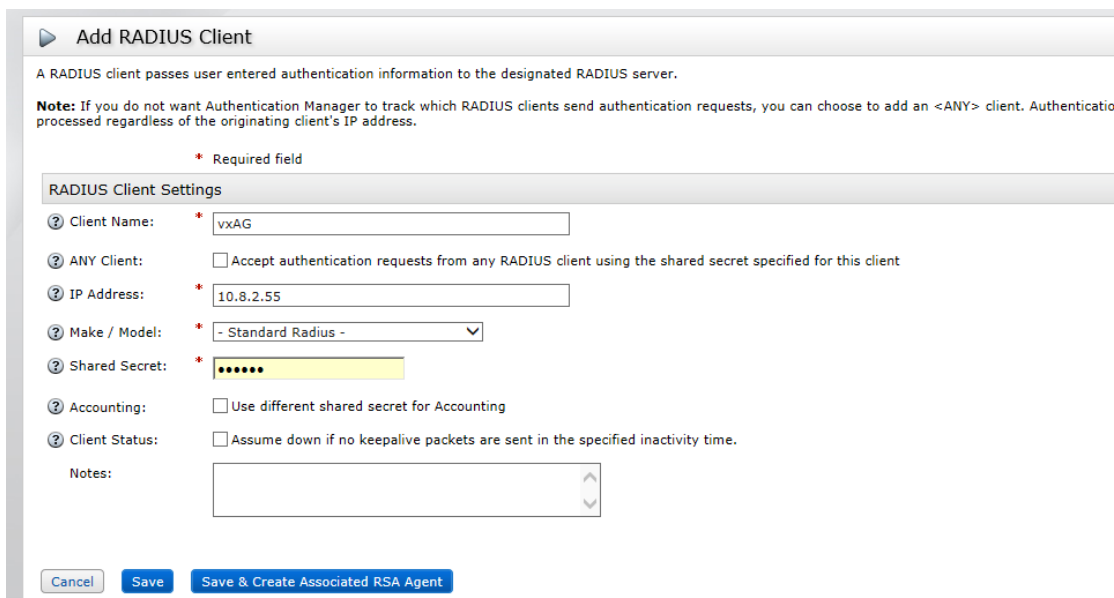
The following sections will describe these steps in detail.

2 Configure the RADIUS Server

Log in with the username and password that were configured during installation. In this example we are using username “admin” and password “arrayclick1#”.



1) Navigate to RADIUS->RADIUS clients->Add new:



2) Configure the hostname, IP address, and shared secret here. Then click “**Save and Create Associated RSA agent**”. A RADIUS agent and an associated RSA agent will be created.

3) Navigate to RADIUS->RADIUS profiles->Add New:

Add RADIUS Profile Properties.

Cancel Save

* Required field

RADIUS Profile Basics

Profile Name: * prof_vxAG

Notes:

Return List Attributes

The RADIUS server sends the return list attributes to the RADIUS client after a successful authentication.

Return List Attributes: Attribute Session-Timeout Add

Value (Integer) Update

Echo

Up Down

Remove

Check List Attributes

The RADIUS client must send these attributes to the RADIUS server as part of an authentication request. The values sent by the RADIUS c

Check List Attributes: Attribute NAS-IP-Address[M] (Multivalued [M]) Add

Value 10.8.2.55 (IP Address) Update

Default

NAS-IP-Address[M] - 10.8.2.55

Remove

- 4) Configure the profile name, return list attributes (if no attribute is required, select echo) and check list attributes. We checked the NAS-IP-Address here, and it has a value of 10.8.2.55. Requests sent from devices other than 10.8.2.55 will be rejected.
- 5) Click **Save**.
- 6) Navigate to **RADIUS->RADIUS clients->manage existing**, and click the dropdown menu beside the client name "**vxAG**". Select "**RSA agent**".

Authentication Agent: **VXAG** ▾

Edit

When a user attempts to gain access to a network resource, the agent receives the authentication request and submits it securely to the authentication server.

* Required field

Administrative Control

Security Domain: SystemDomainadministrators may manage this authentication agent

Authentication Agent Basics

Hostname: * VXAG

IP Address: 10.8.2.55

Protect IP Address: Prevent auto registration from unassigning IP address: Yes

Alternate IP Addresses: IP Address

Notes:

Last Auto Registration On:

Authentication Agent Attributes

Agent Type: RADIUS Client

RADIUS profile : PROF_VXAG ▾

Disabled: Agent is disabled

User Group Access Restriction: Allow access only to members of user groups who are granted access to this agent

Authentication Manager Contact List: Automatically assign automatic contact list from instance that responds first
 Manually assign contact list: RSA.spdomain.com (automatic) ▾

7) Change the RADIUS profile to “PROF_VXAG”. Click **Update**.

2.1 Alternative to using RADIUS Agent

In some cases you may prefer not to use a RADIUS agent. If this is the case, you will just need to create SecurID authentication agents.

2.1.1 Create the SecurID authentication agent

1) Navigate to Access->Authentication Agents->Add new:

Add New Authentication Agent

When a user attempts to gain access to a network resource, the agent receives the authentication request and submits it securely to the authentication server.

* Required field

Administrative Control

Security Domain: administrators may manage this authentication agent

Authentication Agent Basics

Hostname: *

Existing node:

IP Address:

Protect IP Address: Prevent auto registration from unassigning IP address

Alternate IP Addresses:

IP Address

Notes:


Authentication Agent Attributes

Agent Type:

Disabled: Agent is disabled

User Group Access Restriction: Allow access only to members of user groups who are granted access to this agent

- 2) For basic configurations, only the hostname and IP address are required. Fill in this information and click “**Save**”.

 **Confirmation Required**

Confirmation Required

The hostname or IP address you have entered cannot be resolved.

IP Address: **10.8.2.55**

Hostname: **VXAG**

Are you sure you want to save the agent?

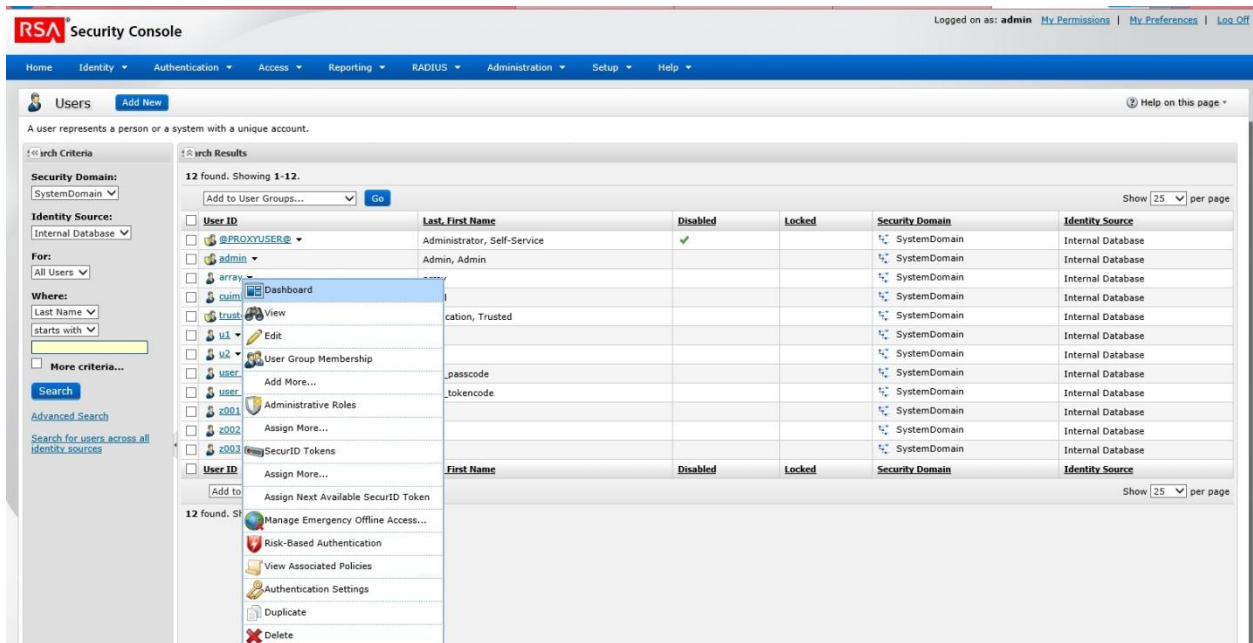
3 User Management

Navigate to **Identity->Users->Add new**:

The screenshot shows the 'Add New User' form with the following sections and fields:

- Header:** 'Add New User' with a user icon, and a description: 'A user represents a person or a system with a unique account.' Buttons for 'Cancel', 'Save', and 'Save & Add Another' are present.
- Administrative Control:**
 - Identity Source: * Internal Database
 - Security Domain: SystemDomain (dropdown) administrators manage this user
- User Basics:**
 - First Name: [text input]
 - Middle Name: [text input]
 - Last Name: * array [text input]
 - User ID: * array [text input] [What's a valid User ID?](#)
 - Email: [text input]
 - Certificate DN: [text input]
 - Notes: [text area]
- Password:**
 - Password: * [password input] [What's a valid password?](#)
 - Confirm Password: * [password input]
 - Force Password Change: Require user to change password at next logon

- 1) Enter the last name, user ID and password. Click **“Save”**.
- 2) From the User List, click the dropdown menu beside the user name (in the example, we are using “array”).



3) Select “Authentication settings”:

RADIUS

② User RADIUS Profile: PROF_VXAG

② RADIUS User Attributes:

Attribute	Value
25 - Class	A1,A

Buttons: Add, Update

25 - Class# A1,A

Buttons: Remove

3.1 Configure RADIUS User Attributes

Attribute 25 - class maps to the “external group” parameter on the AG Series. Because the user “array” belongs to external group “A1” and its parent group “A”, you will set the value of 25-class attribute to “A1,A”, then click “Add”. Then click “Save”.

3.2 Import Token

Navigate to Authentication->SecurID tokens->Import tokens job->Add new.

Add New Import SecurID Tokens Job

Select an XML token file to import, specify options, and click Submit Job.

Cancel Submit Job

* Required field

Import Job Basics

? Import Job Name: * ImportTokens_20160311_0251AM

Administrative Control

? Security Domain: SystemDomain

Import Options

? Import File: * 浏览...

? File Password: (Required only if file is password-protected.)

? Import options: Ignore all duplicate tokens
 Overwrite all duplicate tokens

Cancel Submit Job

- 1) After you click **Submit Job**, the token will be imported.
- 2) Navigate to **Authentication->SecurID tokens->Manage existing**, and select “Unassigned” to view unassigned users:

SecurID Tokens Import SecurID Tokens Help on this page

Assigned Unassigned

Hardware or software-based security tokens that can be assigned to users.

Search Criteria

Security Domain: SystemDomain

For: All Unassigned Tokens

Where: Serial Number contains

More criteria... Search

Search Results

2 found. Showing 1-2.

Serial Number	Token Type	Disabled	Requires Passcode	Replaced By Token	Expires On	Security Domain
<input type="checkbox"/> 000147233973	SecurID Software Token	✓	✓		4/30/16 8:00:00 AM CST	SystemDomain
<input type="checkbox"/> 000147233977	SecurID Software Token	✓	✓		4/30/16 8:00:00 AM CST	SystemDomain

Assign to Users... Go Show 25 per page

2 found. Showing 1-2.

Assign to Users... Go Show 25 per page

- 3) Click the dropdown menu beside a serial number, and select “Assign to user”. Then use the Search menu to list users.
- 4) Click the radio button in front of a user ID, and then click “Assign” to associate the user with the token.

SecurID Token: 000147233977 Help on this page

Assign to Users

Select user(s) to assign the selected token(s).

Search Criteria

Security Domain:
SystemDomain

Identity Source:
Internal Database

For:
All Users

Where:
Last Name
contains

More criteria...

Search

Search Results

12 found. Showing 1-12.

Show 25 per page

<input type="radio"/>	User ID	Last, First Name	Unregistered	Disabled	Locked	Security Domain	Identity Source
<input type="radio"/>	@PROXYUSER@	Administrator, Self-Service		✓		SystemDomain	Internal Database
<input type="radio"/>	admin	Admin, Admin				SystemDomain	Internal Database
<input checked="" type="radio"/>	array	array				SystemDomain	Internal Database
<input type="radio"/>	cuiml	cuiml				SystemDomain	Internal Database
<input type="radio"/>	trustedapp	Application, Trusted				SystemDomain	Internal Database
<input type="radio"/>	u1	u1				SystemDomain	Internal Database
<input type="radio"/>	u2	u2				SystemDomain	Internal Database
<input type="radio"/>	user_passcode	user_passcode				SystemDomain	Internal Database
<input type="radio"/>	user_tokencode	user_tokencode				SystemDomain	Internal Database
<input type="radio"/>	z001	z001				SystemDomain	Internal Database
<input type="radio"/>	z002	z002				SystemDomain	Internal Database
<input type="radio"/>	z003	z003				SystemDomain	Internal Database

Show 25 per page

Then token will be assigned to the user ID successfully.

Assigned **Unassigned**

Hardware or software-based security tokens that have been assigned to users.

✓ Assigned 1 token(s) to 1 user(s). For software tokens, click the token and select Distribute from the context menu.

Search Criteria

Security Domain:
SystemDomain

For:
All Assigned Tokens

Where:
Serial Number
contains

More criteria...

Search

Search Results

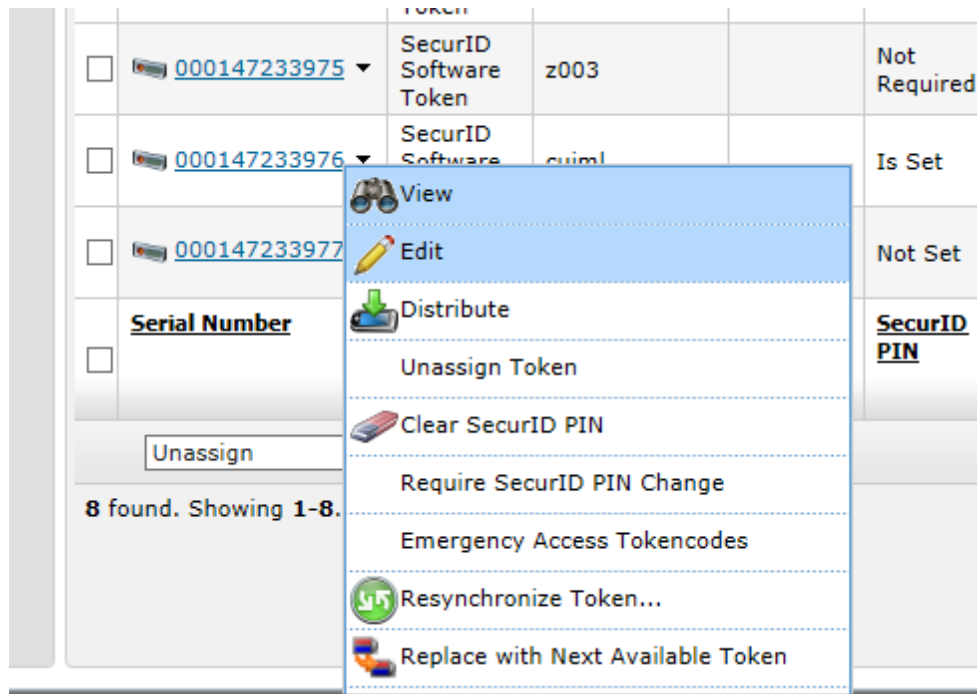
8 found. Showing 1-8.

Unassign **Go**

<input type="checkbox"/>	Serial Number	Token Type	Assigned To	Disabled	SecurID PIN	Token Status	Enabled For Emergency Online Access	Requires Passcode	Pending Replacement By Token	V B I
<input type="checkbox"/>	000147233968	SecurID Software Token	u1		Is Set	Active		✓		
<input type="checkbox"/>	000147233969	SecurID Software Token	u2		Not Set	Active		✓		
<input type="checkbox"/>	000147233971	SecurID Software Token	user_tokencode		Not Set	Active		✓		
<input type="checkbox"/>	000147233972	SecurID Software Token	user_passcode		Not Set	Active		✓		
<input type="checkbox"/>	000147233974	SecurID Software Token	z002		Not Set	Active		✓		
<input type="checkbox"/>	000147233975	SecurID Software Token	z003		Not Required	Active				
<input type="checkbox"/>	000147233976	SecurID Software Token	cuiml		Is Set	Active		✓		
<input type="checkbox"/>	000147233977	SecurID Software Token	array		Not Set	Active		✓		

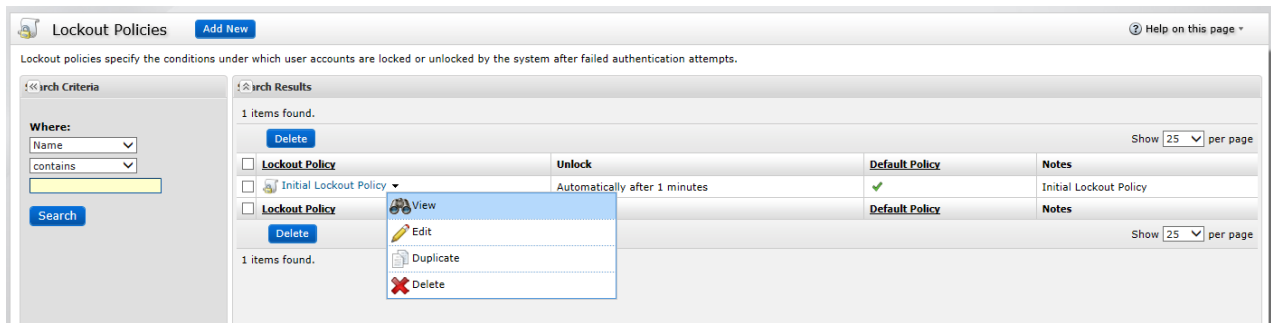
Unassign **Go**

- Click the dropdown menu beside the serial number of the assigned token, and several options will be shown. You can unassign a token, or clear the PIN for this token, via this dropdown menu.



3.3 Policies

Navigate to **Authentication->Policies->Lockout Policies->Manage existing**, and click the dropdown menu beside a policy:



- 1) Edit it as needed to apply your organization's policies:

Lockout Policy: [Initial Lockout Policy](#) ▾

Edit

Lockout policies specify the conditions under which user accounts are locked or unlocked by the system after failed authentication attempts.

[Cancel](#) [Reset](#) [Save](#)

* Required field

Lockout Policy Basics

Lockout Policy Name: *

Default Policy: Set as the default lockout policy

Notes:

Last Modified: Mar 11, 2016 1:21:12 AM CSTbyadmin

Parameters

Lock User Accounts: Allow unlimited failed authentications
 Lock accounts after consecutive failed authentications within days

Unlock: Administrators unlock user accounts
 System automatically unlocks accounts after minutes

[Cancel](#) [Reset](#) [Save](#)

You may configure the threshold of consecutive failed login trials before an account is locked, the lockout duration time and unlock method (auto or manual).

3.4 Token Policy

Navigate to **Authentication->Policies->Token policies->Manage existing**:

SecurID Token Policies [Add New](#) [Help on this page](#)

Token policies specify how SecurID PINs and fixed passcodes are created and maintained, and how incorrect passcodes are handled. The policy applies to all users managed within a security domain.

Search Criteria

Where: Name contains

[Search](#)

1 items found.

SecurID Token Policy	Minimum PIN Length	Maximum PIN Length	Maximum PIN Lifetime	Minimum Passcode Length	Maximum Passcode Length	Maximum Passcode Lifetime	Default Policy	Notes
<input type="checkbox"/> Initial Token Policy ▾	4	8	90 days	4	8	90 days	<input checked="" type="checkbox"/>	Initial Token Policy

1 items found.

[Delete](#)

[View](#)
[Edit](#)
[Duplicate](#)
[Delete](#)

1) Click the dropdown menu beside a policy name, and select **“Edit”**.

* Required field

SecurID Token Policy Basics

SecurID Token Policy Name: *

Incorrect Passcodes: Allow unlimited incorrect passcodes
 Require next tokencode after incorrect passcodes

Default Policy: Set as default SecurID token policy

Notes:

Last Modified: Mar 11, 2016 1:48:01 AM CSTbyadmin

Here you can configure the number of incorrect passcodes before the next tokencode mode activates.

3.5 Monitoring

Navigate to **Reporting->Real-time Activity Monitors->Authentication Activity Monitor**. You can monitor real-time authentication activities here.

4 Configure the AG

Under the virtual site scope, select **Site Configuration > AAA > Server > RADIUS**. Specify the Server Name and Description parameters and click the **Add** button in the Server List area.

Server Name	Description	
radius	radius	Add

In the **Server List** area, double-click the server entry to add more advanced configurations for the RADIUS server. In the **RADIUS Server Configuration** area of the displayed window, click the **Add RADIUS Server** action link to add a host for the RADIUS server. Note: if the AG virtual site has multiple IP addresses assigned, the RADIUS NASIP must be configured as below.

ADVANCED RADIUS SERVER CONFIGURATION

Server Name: RSA
RADIUS NASIP: 172.27.56.239 *This must be the LAN network IP address.*
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.*

RADIUS SERVER CONFIGURATION

Redundancy Order	Server IP	Server Port	Secret Password	Timeout	Retries	Accounting Port
1	172.27.56.96	1812	XXXXXXXXXXXXXXXXXXXX	120	5	1813

In the **Add RADIUS Server** area, specify the parameters **Server IP, Server Port, Secret Password, Timeout, Redundancy Order, Retries** and **Accounting Port**, and click the **Save** action link .

EDIT RADIUS SERVER

Server IP: 10.4.122.26
Server Port: 1812
Secret Password: *****
Timeout: 5 (Server response timeout in seconds. Optional, defaults to 5)
Redundancy Order: 1 (Host redundancy order, number 1-3 only)
Retries: 5 (Optional, the Retries value must be an integer from 1 to 65535, defaults to 5)
Accounting Port: 1813

The configuration is now complete.

About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 250 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.



Corporate Headquarters

info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA

rschmit@arraynetworks.com
+32 2 6336382

China

support@arraynetworks.com.cn
+010-84446688

France and North Africa

nsedrati@arraynetworks.com
+33 6 61174433

India

isales@arraynetworks.com
+91-080-41329296

Japan

sales-japan@
arraynetworks.com
+81-44-589-8315

To purchase
Array Networks
Solutions, please
contact your
Array Networks
representative at
1-866-MY-ARRAY
(692-7729) or
authorized reseller

Oct-2016 rev. a