Deployment Guide
Oct-2016 rev. a

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

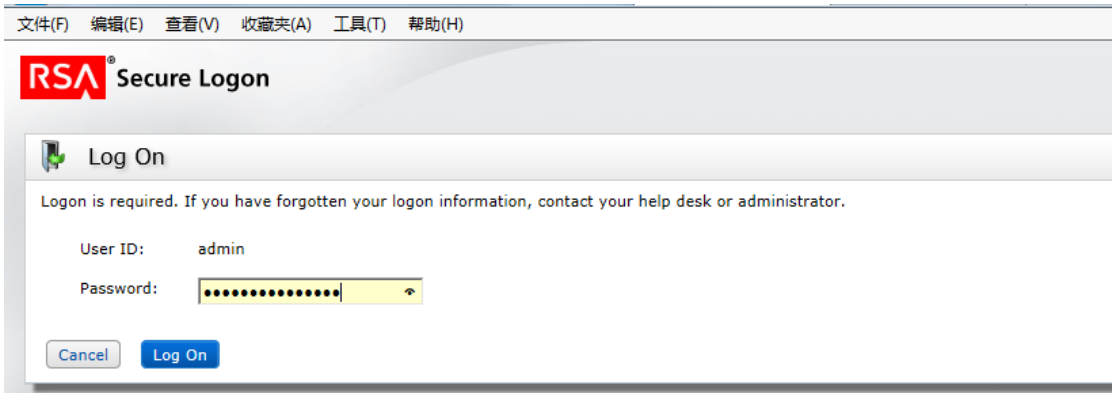
User management

Configure the vxAG or AG Series

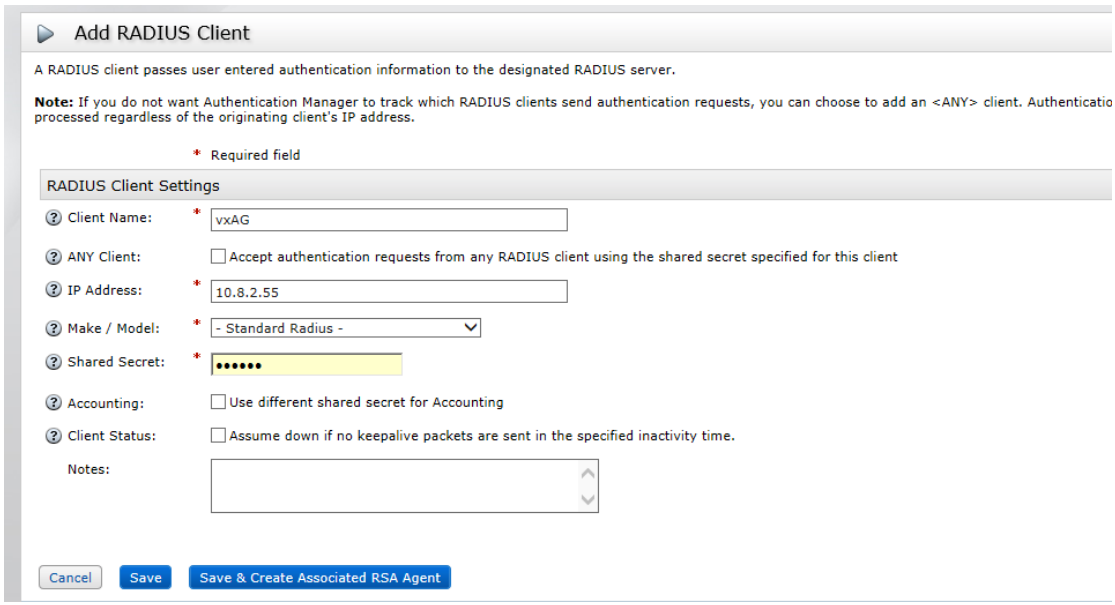
The following sections will describe these steps in detail.

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#”.

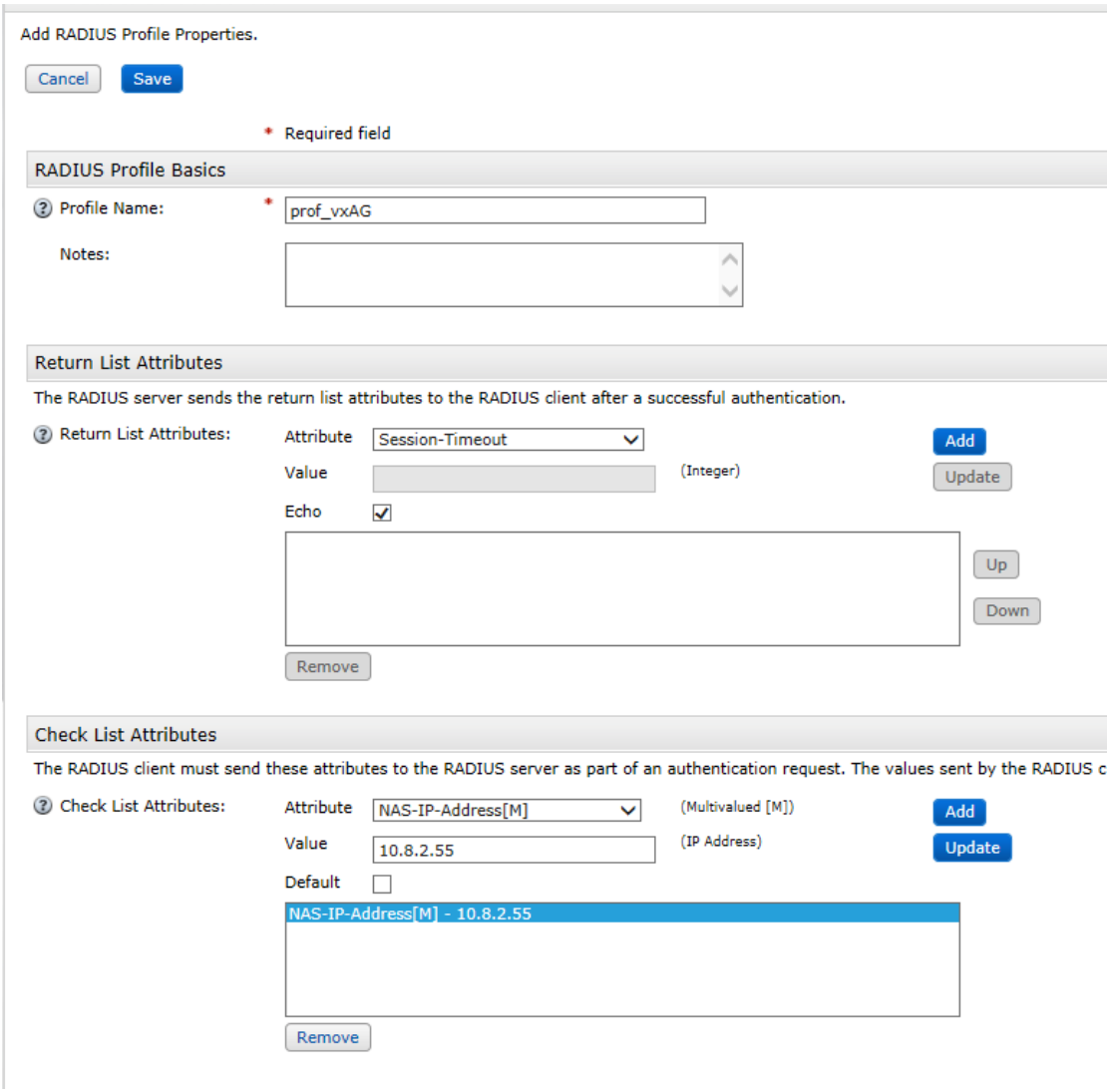


1) Navigate to RADIUS->RADIUS clients->Add new:



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.

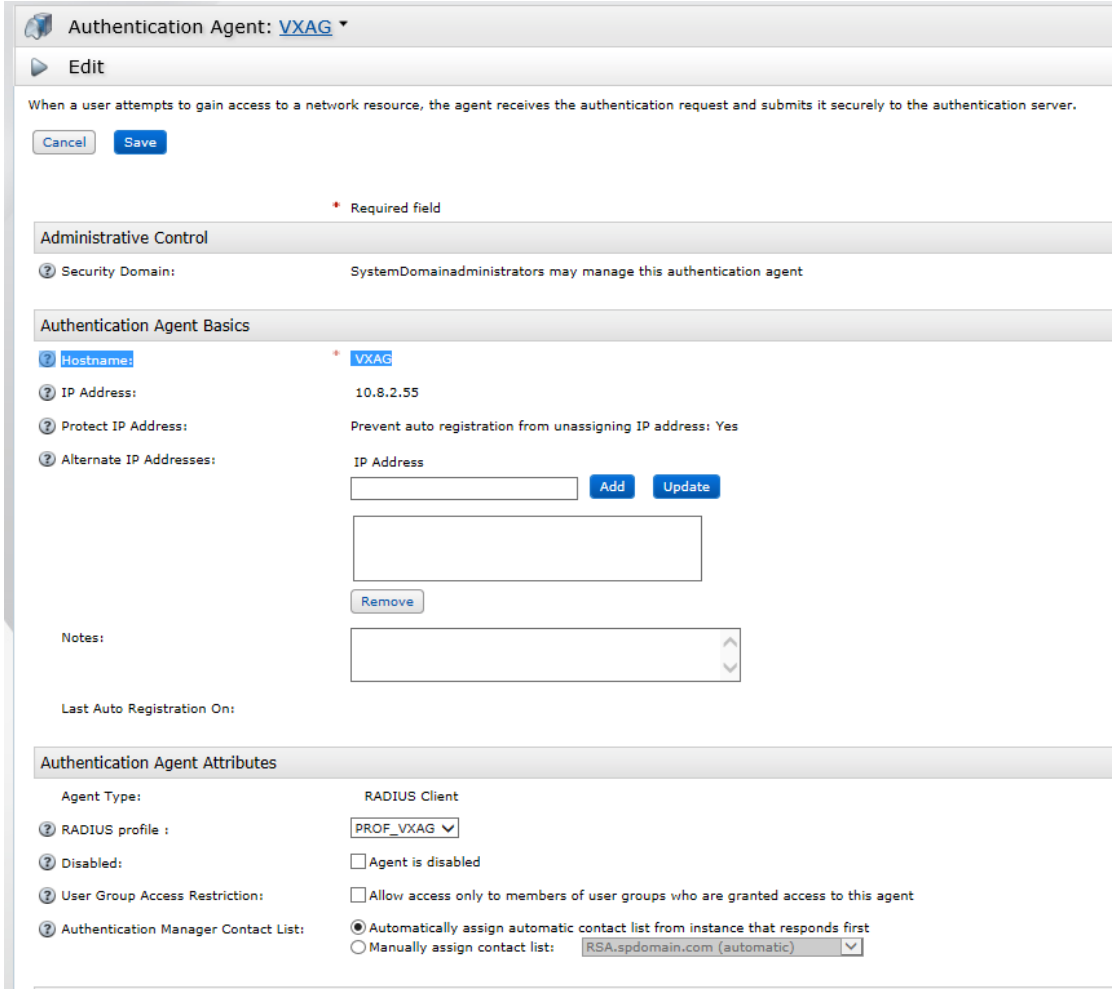
3) Navigate to RADIUS->RADIUS profiles->Add New:



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**".



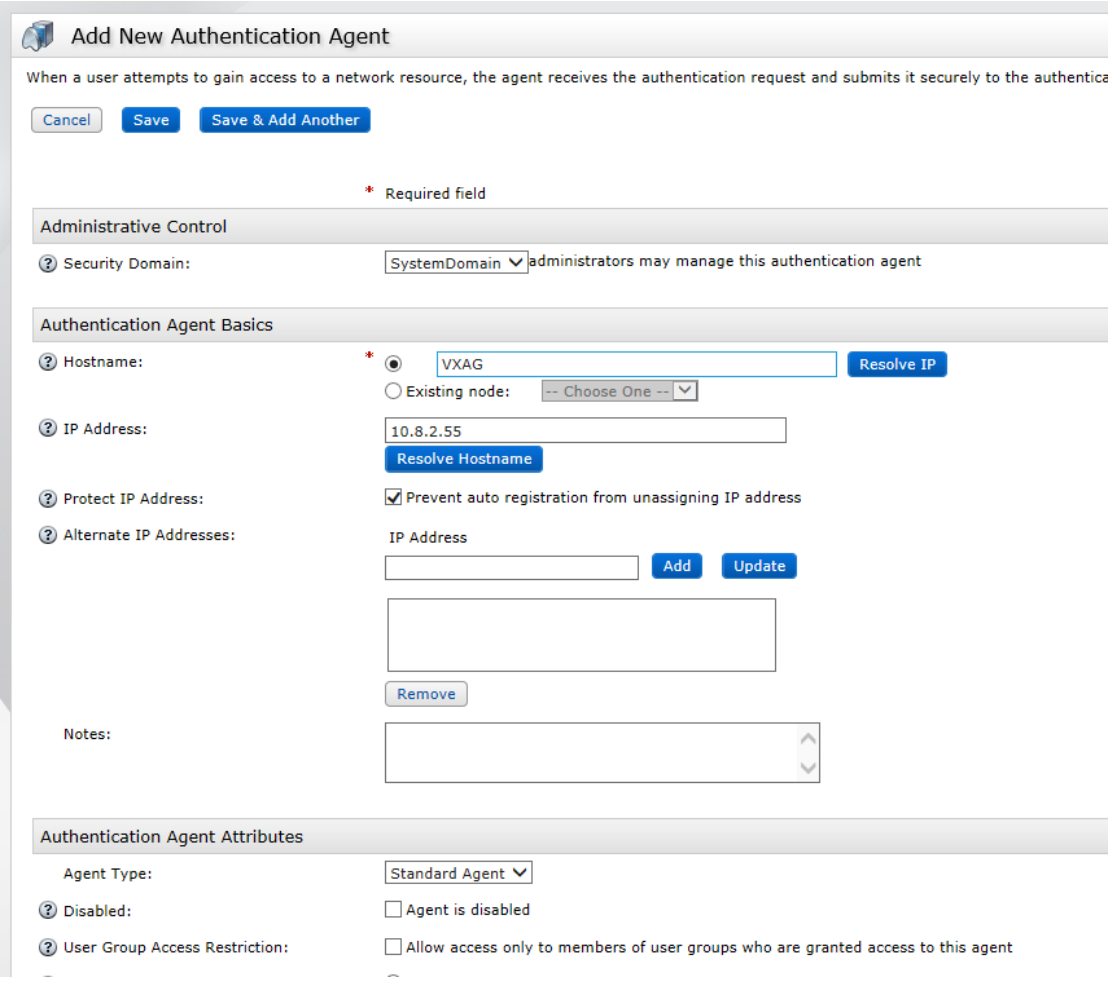
7) Change the RADIUS profile to "**PROF_VXAG**". Click **Update**.

2.1 Alternative to using RADIUS Agent

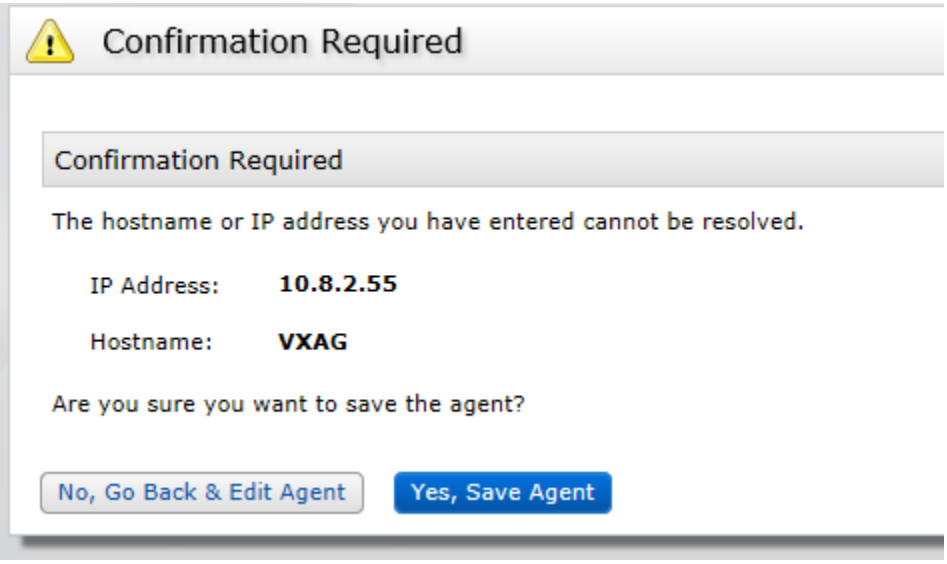
In some cases you may perfer not to use a RADIUS agent. If this is the case, you will just need to create SecurID authentication agents.

2.1.1 Create the SecurID authentication agent

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

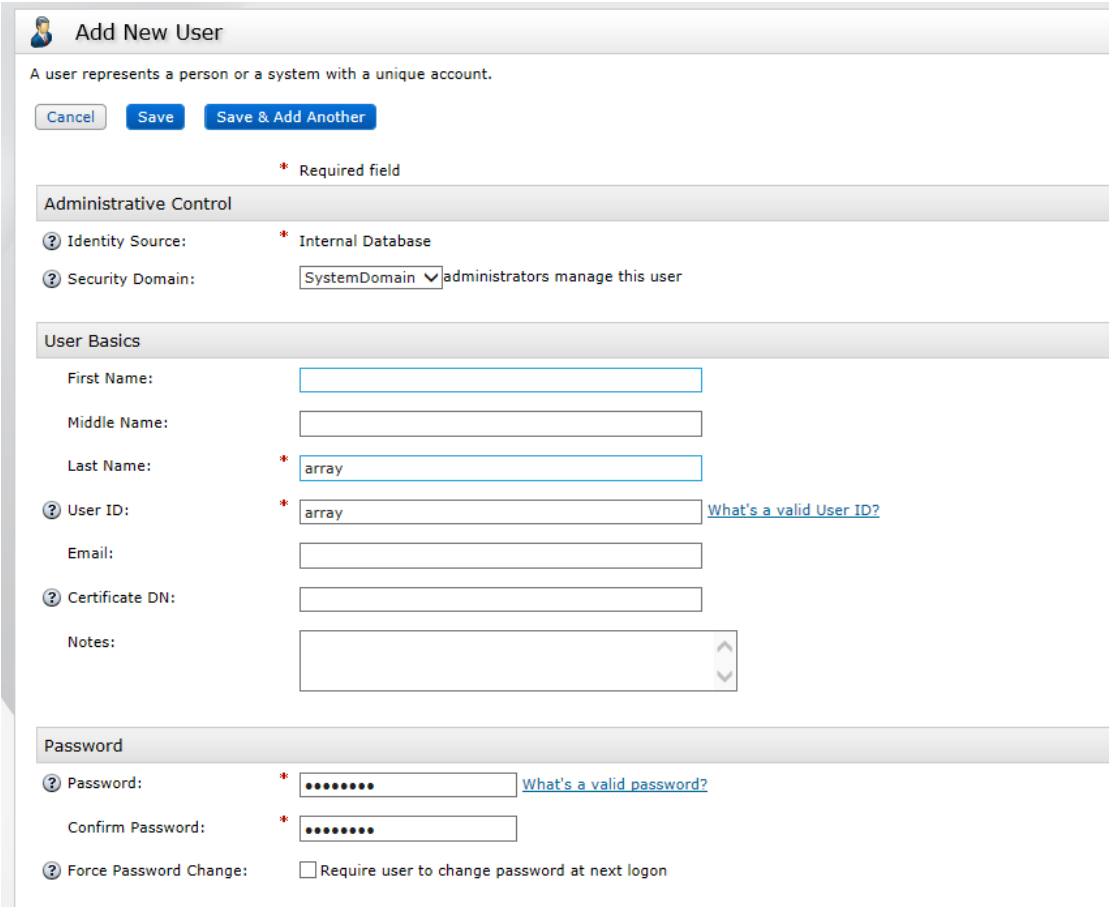


2) For basic configurations, only the hostname and IP address are required. Fill in this information and click "**Save**".

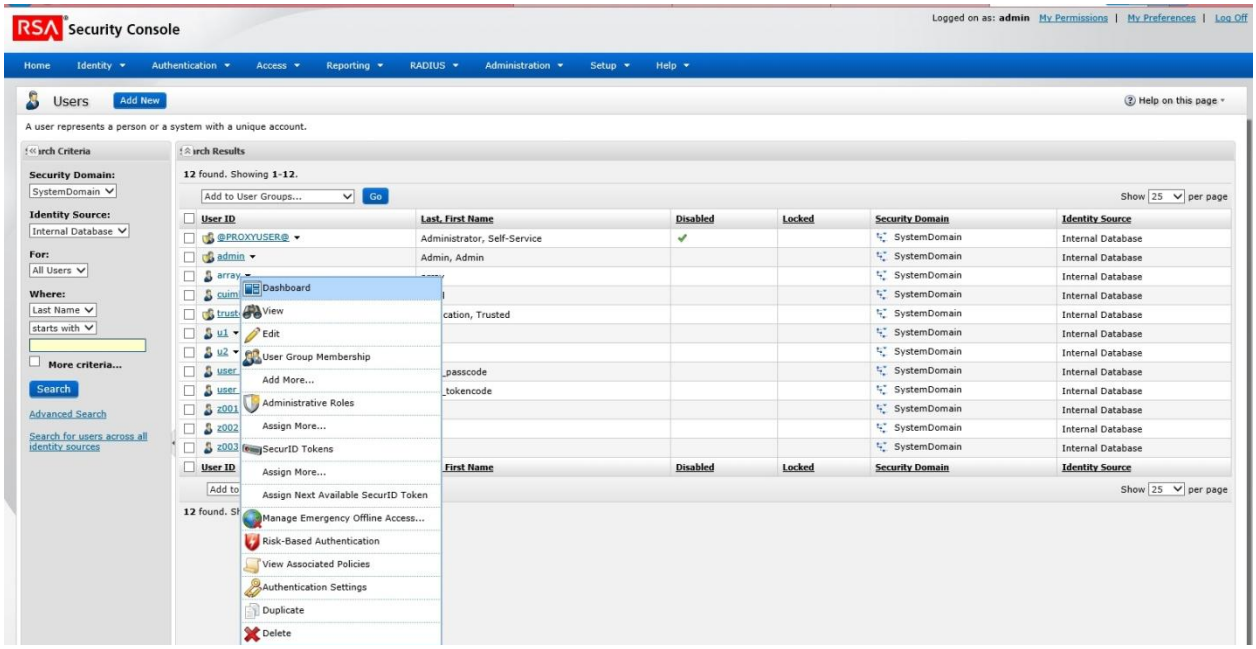


3 User Management

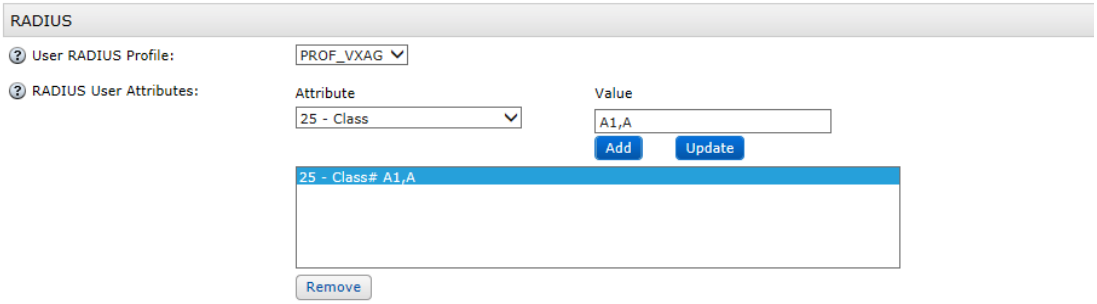
Navigate to **Identity->Users->Add new**:



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”:

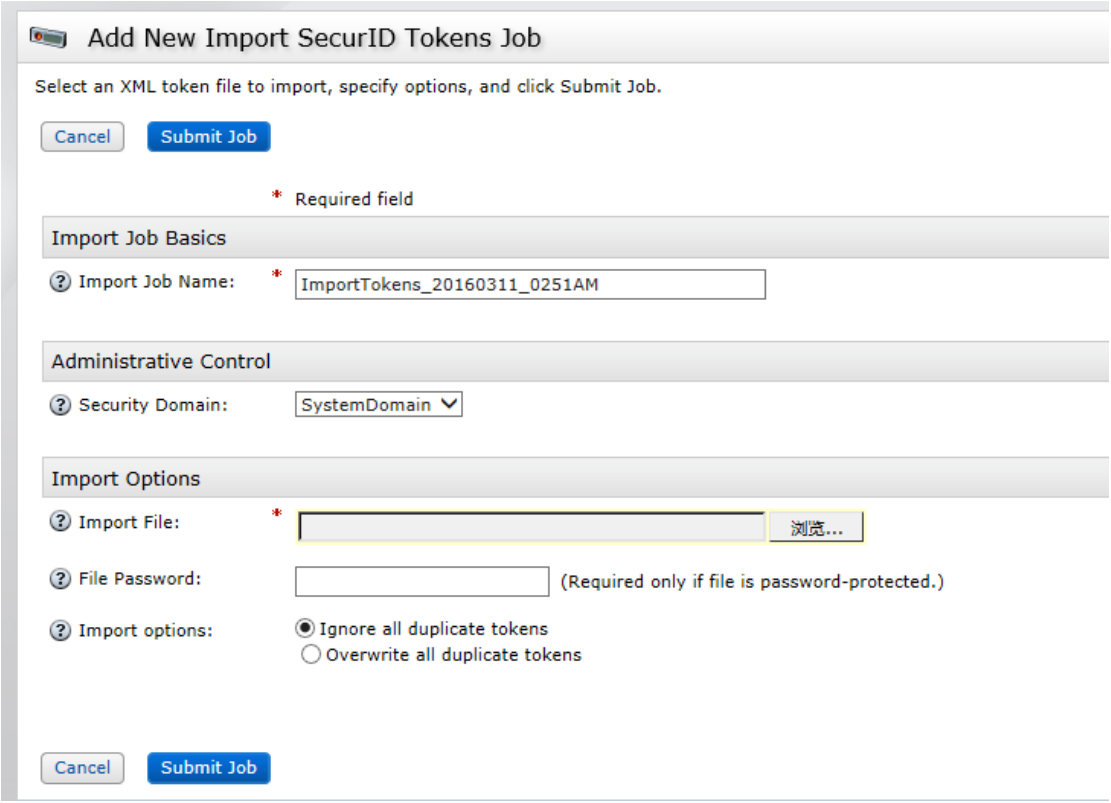


3.1 Configure RADIUS User Attributes

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**”.

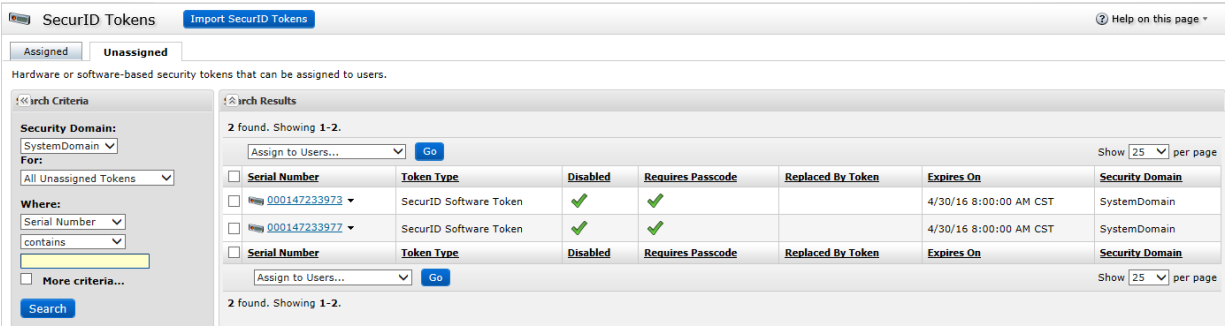
3.2 Import Token

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



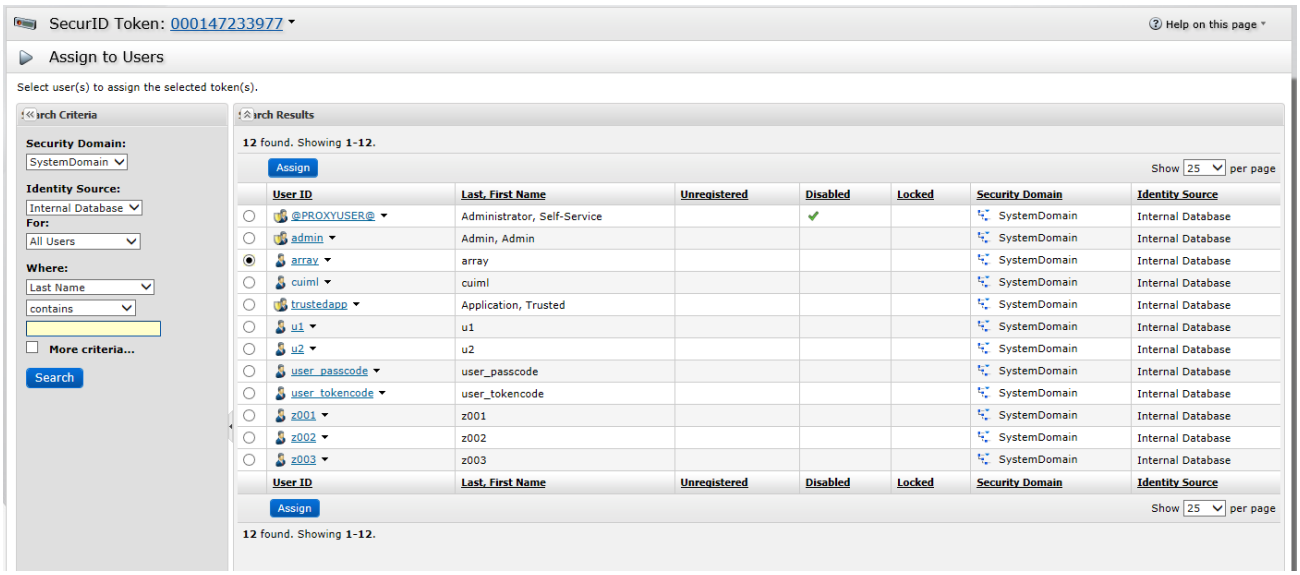
1) After you click **Submit Job**, the token will be imported.

2) Navigate to **Authentication->SecurID tokens->Manage existing**, and select "Unassigned" to view unassigned users:

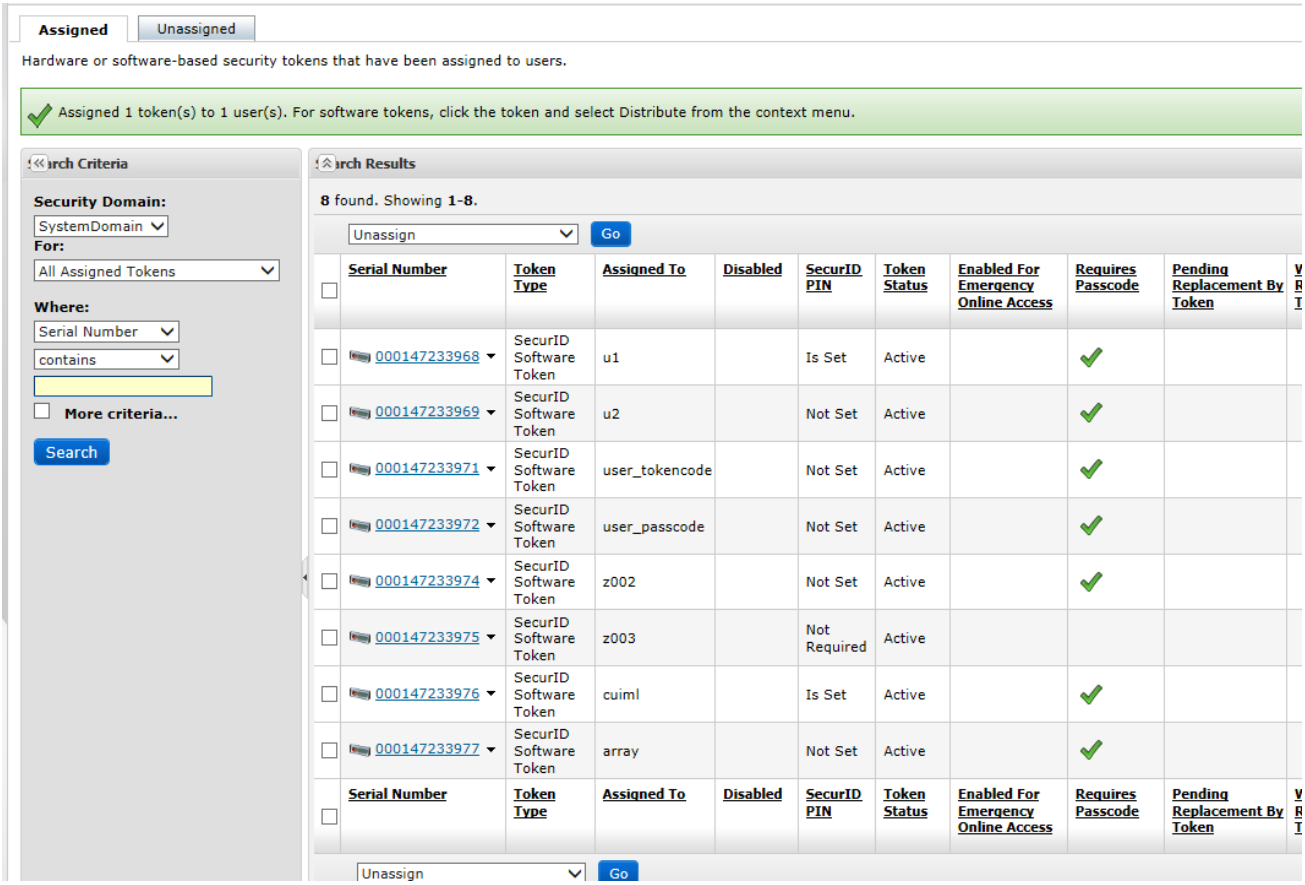


3) Click the dropdown menu beside a serial number, and select "**Assign to user**". Then use the Search menu to list users.

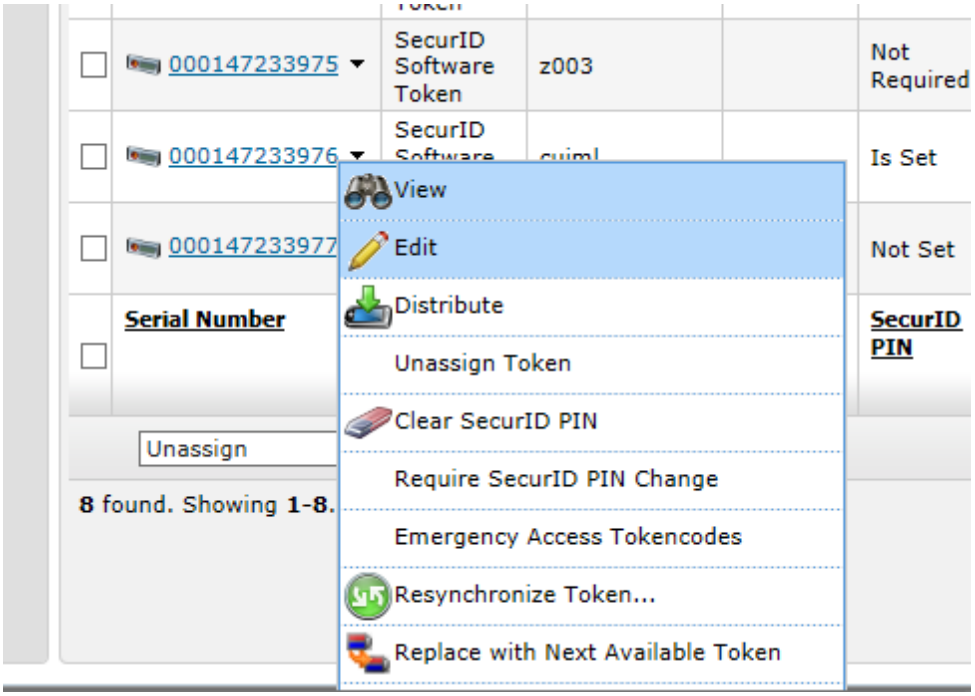
4) Click the radio button in front of a user ID, and then click "**Assign**" to associate the user with the token.



Then token will be assigned to the user ID successfully.

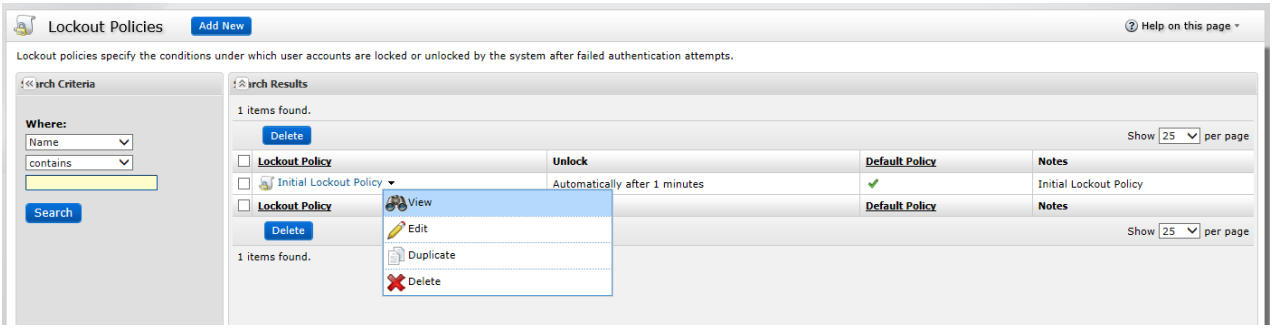


5) Click the dropdown menu beside the serial number of the assigned token,and several options will be shown. You can unassign a token, or clear the PIN for this token, via this dropdown menu.

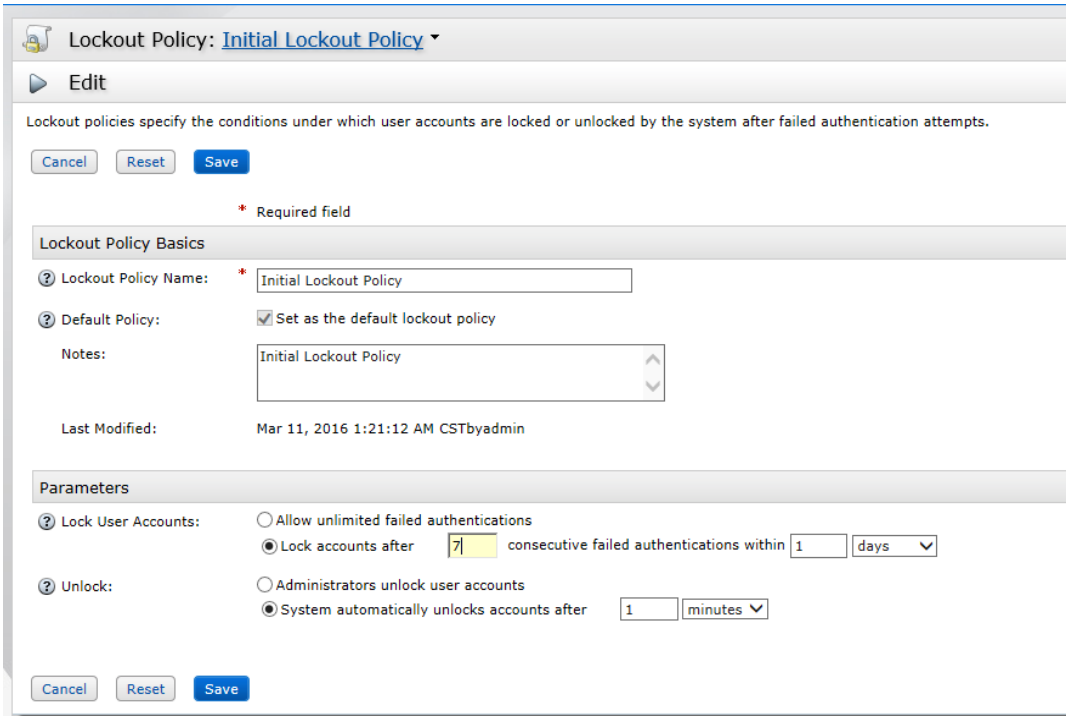


3.3 Policies

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



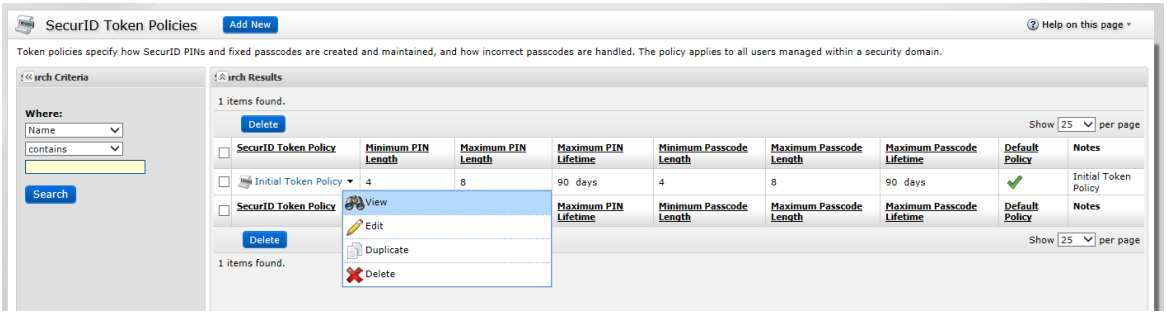
1) Edit it as needed to apply your organization's policies:



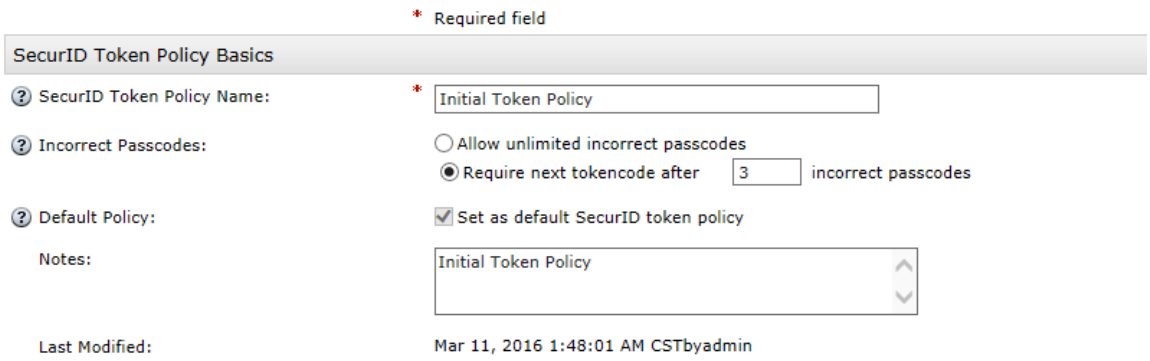
You may configure the threshold of consecutive failed login trials before an account is locked, the lockout duration time and unlock method (auto or manual).

3.4 Token Policy

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



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



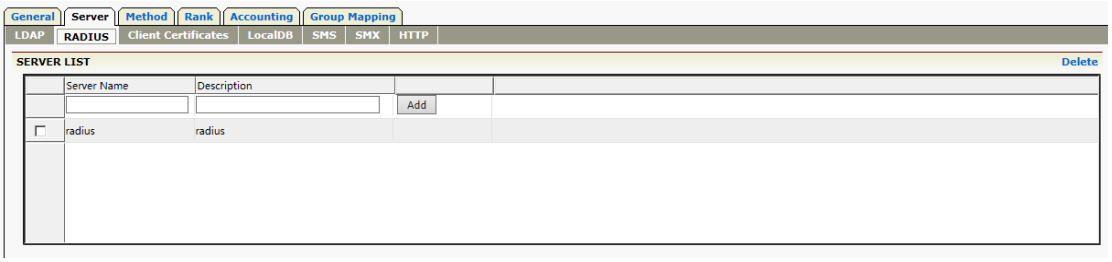
Here you can configure the number of incorrect passcodes before the next tokencode mode activates.

3.5 Monitoring

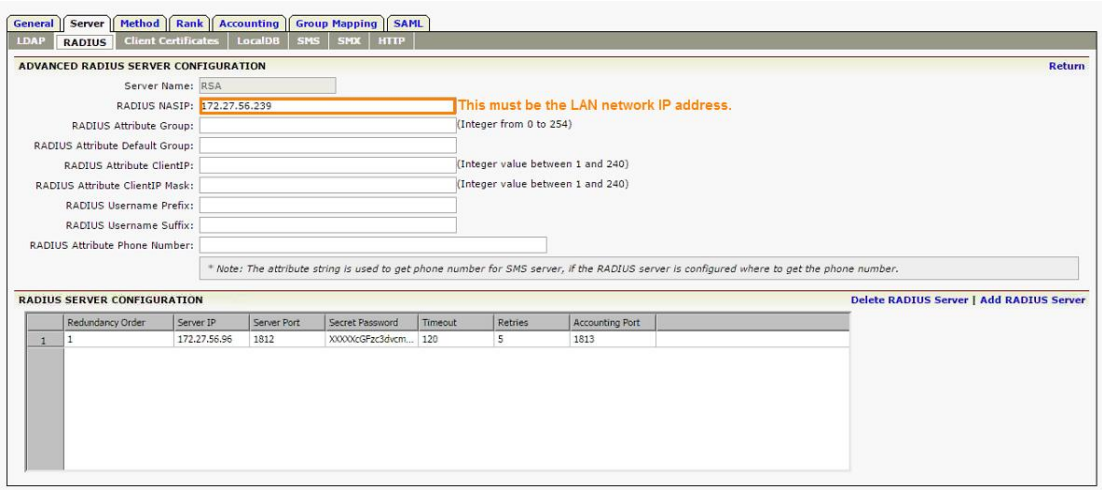
Navigate to **Reporting->Real-time Activity Monitors->Authentication Activity Monitor**. You can monitor real-time authentication activities here.

4 Configure the AG

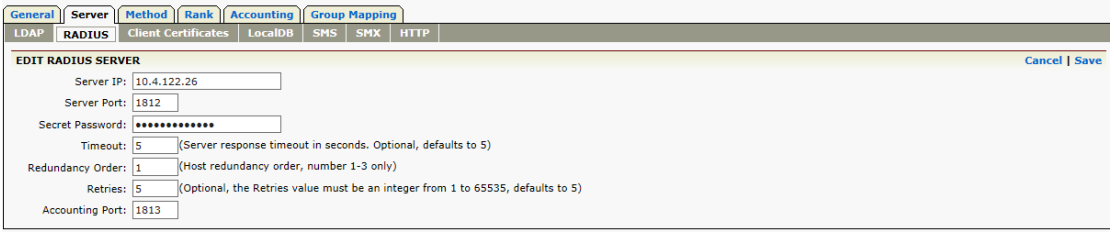
Under the virtual site scope, select **Site Configuration > AAA > Server > RADIUS**. Specify the Server Name and Description parameters and click the **Add** button in the Server List area.



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.



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 .



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

France and North Africa
nsedrati@arraynetworks.com
+33 6 61174433

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

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

© 2016 Array Networks, Inc. All rights reserved. Array Networks and the Array Networks logo are trademarks of Array Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Array Networks assumes no responsibility for any inaccuracies in this document. Array Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.