Gigamon
GigaVUE H Series

RSA SecurID Ready Implementation Guide

Last Modified: June 23rd, 2014

Partner Information

Product Information	
Partner Name	Gigamon
Web Site	www.gigamon.com
Product Name	GigaVUE H Series
Version & Platform	4.0
Product Description	Gigamon GigaVUE® offers modular-based intelligent traffic visibility fabric nodes. This extends traffic visibility to more remote portions of the network running critical applications that require monitoring.

Solution Summary

The GigaVUE H Series delivers performance and intelligence as a Traffic Visibility Fabric™ node, with port density and speeds that scale to your needs from 1Gb to 100Gb. With an intuitive web-based interface (H-VUE) and a powerful CLI, the Visibility Fabric is able to replicate, filter, and selectively forward network traffic to monitoring, management, and security tools.

Gigamon GigaVUE supports SecurID authentication through RADIUS to protect console access. This allows customers who are interested in improving security by adding strong two-factor authentication for administrative access.

! Important: SecurID authentication is not supported through the H-VUE Web Management Interface. Although a basic SecurID authentication will work, RADIUS challenge-response is not supported. This only works through console/SSH access.

RSA Authentication Manager supported features	
Gigamon GigaVUE H Series	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	No
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	No
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes*

***See Important Note Above**

Agent Host Configuration

To facilitate communication between the Gigamon GigaVUE and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the Gigamon GigaVUE and contains information about communication and encryption.

Gigamon GigaVUE communicates with the RSA Authentication Manager via RADIUS. Therefore a RADIUS client that corresponds to the agent host record must be created in the 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: The RADIUS client's hostname must resolve to the IP address specified.**

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Gigamon GigaVUE 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 Gigamon components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring Gigamon GigaVUE

Launching the GigaVUE Web Management Interface

H-VUE provides you with an intuitive, drag-and-drop interface for your H Series Visibility Fabric nodes. Although the familiar command-line interface will always be available for all configuration tasks, H-VUE simplifies many common tasks, allowing you to configure packet distribution visually instead of entering text in the CLI. All the administration tasks of this guide will be performed through the H-VUE web interface.

1. Browse to the login page of the GigaVUE H Series device. (e.g. https://192.168.1.1*)*
2. Login with the administrator's username and password that was created during the initial setup of the device.
3. Click **Login**.

4. Click **OK** to the Login message(s).

Adding a RADIUS Server

1. At the main menu, click **System > User Setup > RADIUS** tab.
2. Scroll down to the bottom of the page to **Add New RADIUS Server**.
3. Enter the **Server IP** address of the Authentication Manager server. (e.g. 10.100.50.29)
4. Enter the **Auth Port**. (e.g. 1812)
5. Enter the *Shared Secret* in the **Key** field.

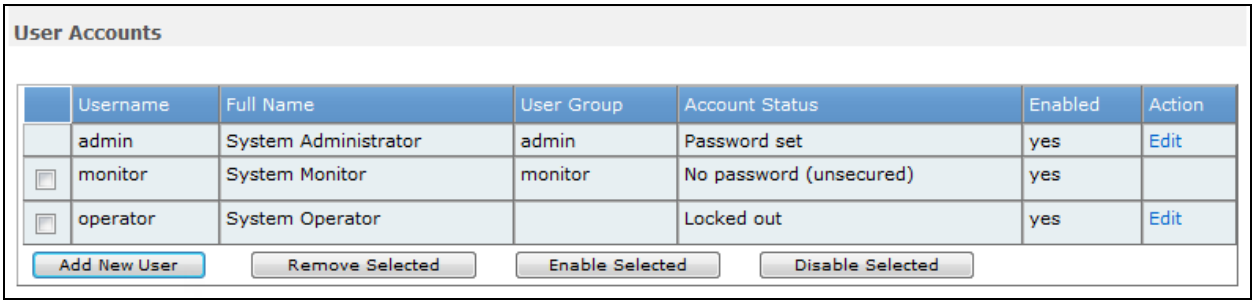
> **Note: The Shared Secret is setup on the RSA Authentication Manager Server when adding a new Agent Host record for the Gigamon device.**

6. Enter **60** in the **Timeout** field.
7. Enter **0** in the **Retransmit** field.
8. Click the **Add RADIUS Server** button.

9. Next, repeat steps **7–12** to add any Authentication Manager Replica servers.

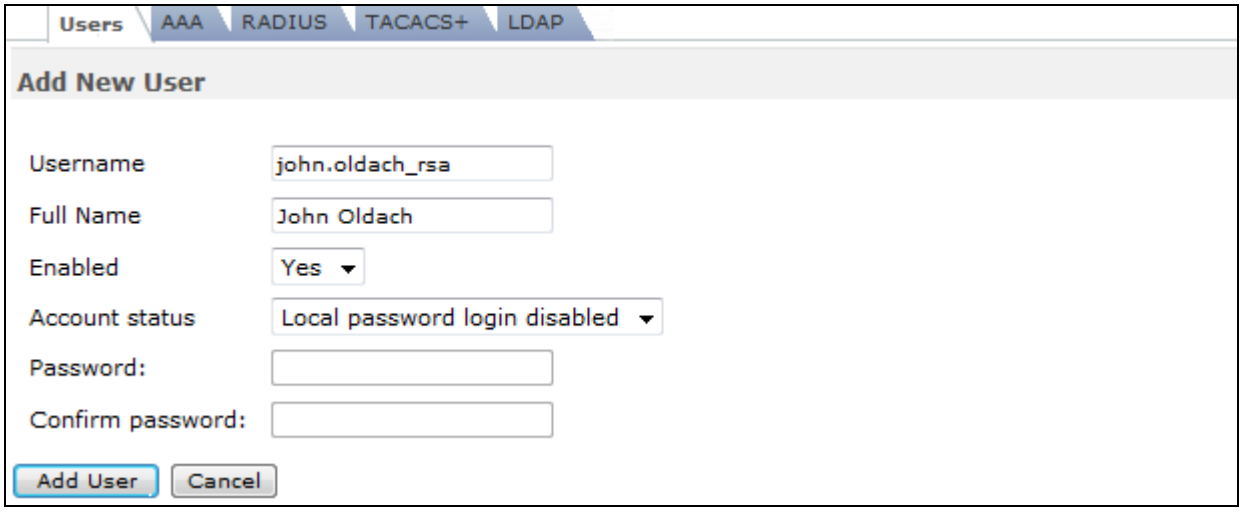
Adding a User Account

1. At the main menu, click **System > User Setup > Users** tab.
2. Click the **Add New User** button.



3. Enter the **Username** you wish to grant access to the system. This username must also exist in the RSA Authentication Manager Server database.
4. Enter the **Full Name** of the user.
5. Select **Yes** for the Enabled drop-down menu.
6. For Account status, select **Local password login disable**.

7. Click the **Add User** button.



Note: After adding the user, you can then assign that user to a User Group in the Permissions tab. This will specify what level of access a given user has on a selected port. For more information on user permissions, see the Gigamon H-VUE online help.

Configuring the Authentication Method List

After creating the RADIUS server and adding a user to the system, the next step is to enable RADIUS as an authentication method. Perform the following steps to enable RADIUS.

1. At the main menu, click **System > User Setup > AAA** tab.
2. Next, enable **RADIUS** in at least one of the four pull-down menus for the *Authentication Method List*. In this example, we'll select **RADIUS** authentication for the second method.

3. Click **Apply**.

RSA SecurID Login Screens

Login screen:

```
login as: john.oldach_rsa

Gigamon GigaVUE H Series

Using keyboard-interactive authentication.
Password:
```

User-defined New PIN:

```
login as: john.oldach_rsa

Gigamon GigaVUE H Series

Using keyboard-interactive authentication.
Password:

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

System-generated New PIN:

```
login as: john.oldach_rsa

Gigamon GigaVUE H Series

Using keyboard-interactive authentication.
Password:

ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE YOUR PIN? (y/n):y

Are you satisfied with system generated PIN 8jqUG6w ? (y/n):y
```

Next Tokencode:

```
login as: john.oldach_rsa

Gigamon GigaVUE H Series

Using keyboard-interactive authentication.
Password:

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

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.0	Virtual Appliance
Gigamon GigaVUE H Series	4.0	Appliance

RSA SecurID Authentication

Date Tested: June 23rd, 2014

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

JJO

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