A10 Networks
Thunder Series

RSA Ready Implementation Guide for RSA SecurID

Last Modified: 2/10/15

Partner Information

Product Information	
Partner Name	A10 Networks
Web Site	www.a10networks.com
Product Name	Thunder Series
Version & Platform	2.7.2 P4, 4.0 and later
Product Description	A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure.

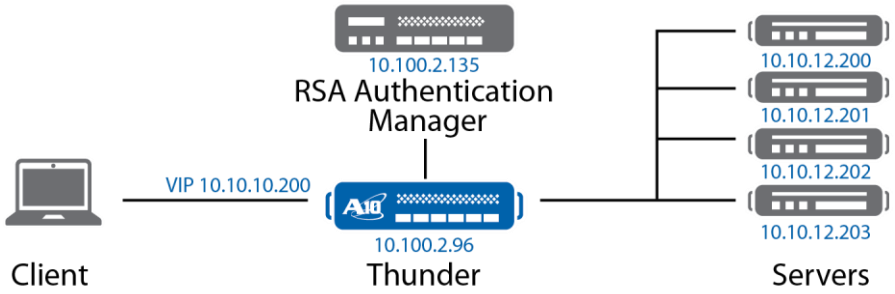
Solution Summary

A10 Application Access Management (AAM) offers a flexible choice of authentication schemes, seamless integration of authentication services and enhances security. One of the AAM features is the seamless integration with RSA Authentication Manager. The A10 authentication process communicates with RSA SecurID through the management interface or it may also defined in one of the data interfaces.

The A10 Thunder Series Application Delivery Controller (ADC) supports RSA SecurID Authentication via RADIUS. The A10 ADC provides two-factor authentication for secure access to the back-end servers. The back end servers are typically enterprise applications such as SharePoint, Exchange or websites. In order to define what is accessible via Authentication, a aaa-policy must be configured in the A10 ADC, which includes a url list of the allowed applications. Consequently, an authentication template is required with the A10 configuration which defines the authentication type, authentication logon type and authentication server information. Finally, the aaa-policy has to be bound to the VIP for the authentication to work.

RSA Authentication Manager supported features	
A10 Networks Thunder Series	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	N/A
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	N/A
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	N/A
On-Demand Authentication via Native SecurID UDP Protocol	N/A
On-Demand Authentication via Native SecurID TCP Protocol	N/A
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	N/A
RSA SecurID SD800 Token Automation	N/A
RSA SecurID Protection of Administrative Interface	Yes

Solution Overview



Agent Host Configuration

To facilitate communication between the A10 Networks 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 A10 Networks and contains information about communication and encryption.

If A10 Networks will be communicating with RSA Authentication Manager via RADIUS, then 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 or IP Addresses for network interfaces
- RADIUS Secret

(Note: this information will be configured within the RADIUS aaa authentication server configuration)

Note: The RADIUS client's hostname must resolve to the IP address specified.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the A10 Networks Thunder Series 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 A10 Networks components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Documenting the Solution

The Thunder ADC device provides the following management interfaces

Graphical User Interface (GUI)

Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

> **Note: HTTP requests are redirected to HTTPS by default on the Thunder device.**

By default, Telnet access is disabled on all interfaces, including the management interface. SSH, HTTP and HTTPS are enabled by default on the management interface only, and disabled by default on all data interfaces.

Command-Line Interface (CLI)

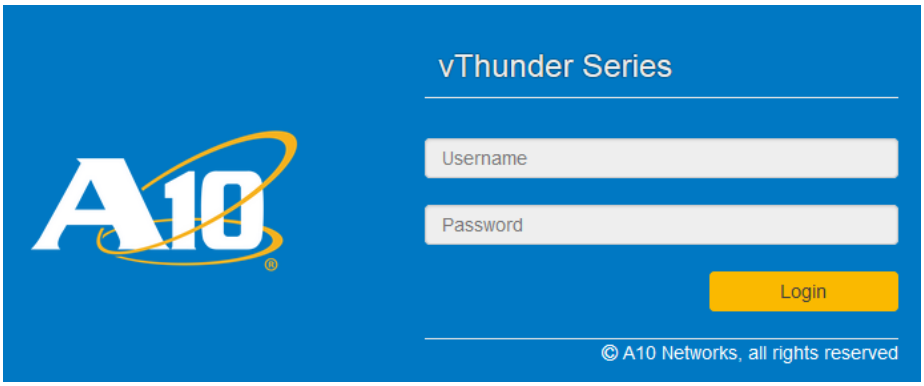
Text-based interface in which commands are entered on a command line. The CLI is directly accessible through the serial console or over the network using either of the following protocols:

- Secure protocol – Secure Shell (SSH) version 2
- Unsecure protocol – Telnet (if enabled)

Please consult the **Appendix** for an A10 sample configuration via CLI.

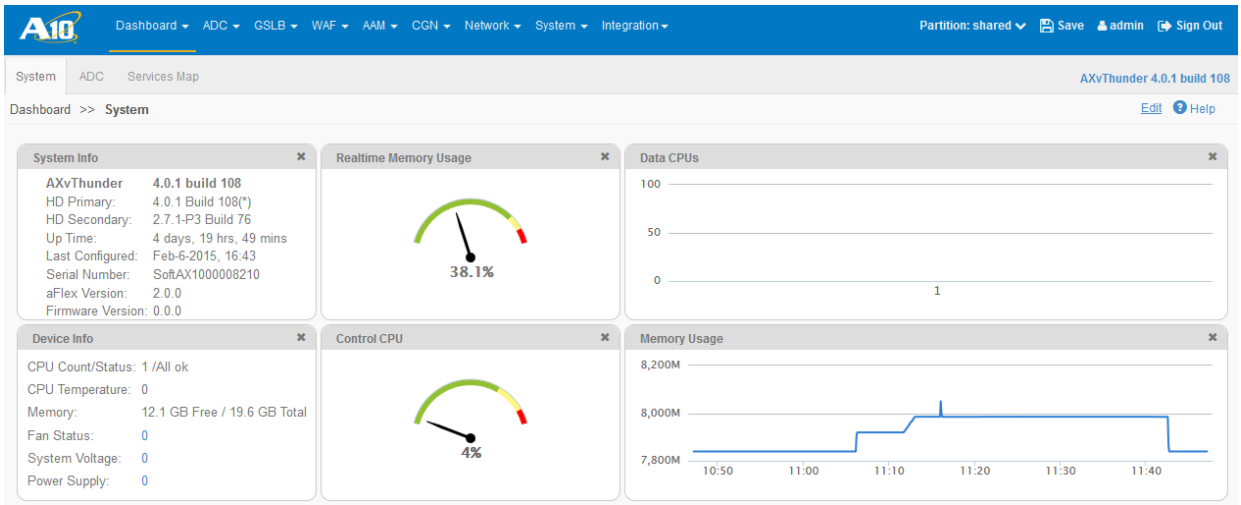
Configuring the Thunder ADC Device via the A10 GUI

To log onto the A10 GUI, open your web browser and input the management IP address of the Thunder device (**https://<management-IP-address>/**). The A10 logon dialog is displayed. The name and appearance of the dialog may differ depending on the browser you are using.



Note: The default admin credentials are username "admin", password "a10." It is strongly advised that the default password be changed after initial login.

Enter your admin username and password and click **OK**.



To integrate the A10 ADC and the RSA Authentication Server, the first task is to configure the A10 device to provision the RSA Authentication Server in the A10 GUI. To do this, navigate to **AAM>Auth Servers>** and click **Create**:

Name: Add the name of the RADIUS Server

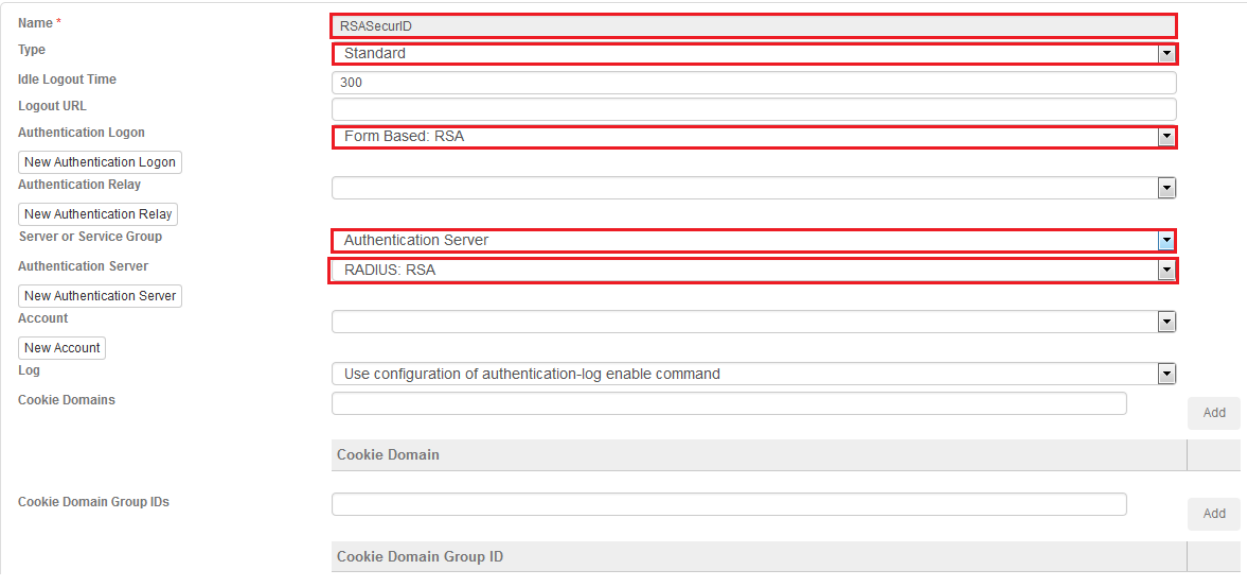
Shared Secret: Add a share secret password that will match from the RSA Authentication Server

Host: Enter the IP address or the Hostname of the RADIUS server

Configuring Additional A10 AAM Parameters

This section provides instruction on how to configure the A10 AAM parameters. These configurations are required for A10 for the solution to work with RSA SecurID. This includes the creation of Authentication Templates, AAA Policies, and Authorization Policies. To configure these features, navigate to **AAM > Policies and Templates**.

To create the Authentication template, click **Create:**



Name: RSASecurID

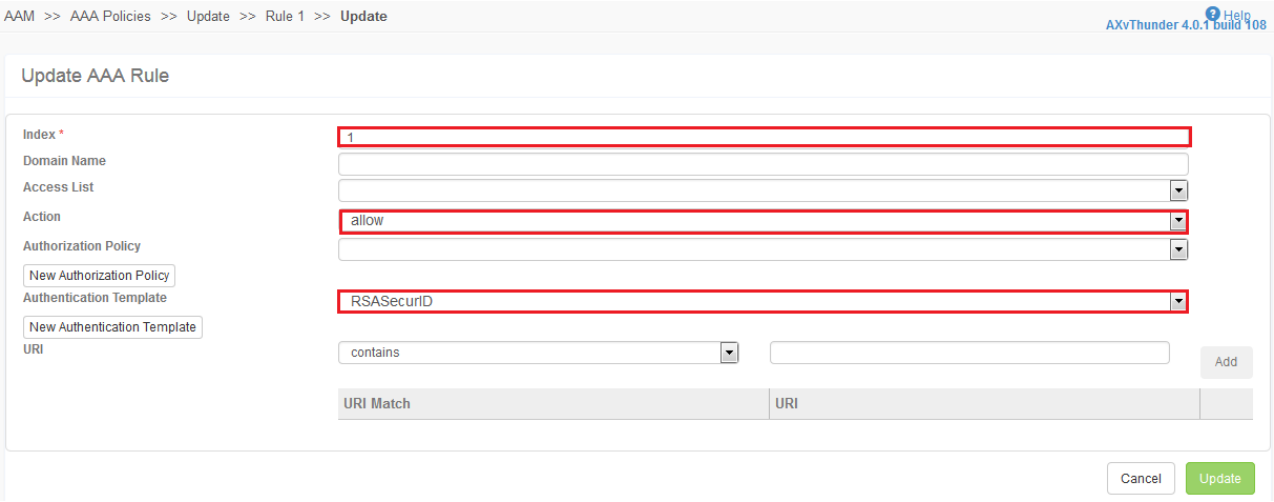
Authentication Type: Select **standard**

Authentication logon: In this example we have preselected **Form-Based** logon. You have also the option of selecting **HTTP Logon**, but it needs to be defined by selecting **New Authentication Logon**. Once the Authentication Logon is defined you can select the **Authentication logon type**.

Server or Service Group: Select Authentication Server

Authentication Server: Select the Authentication Server that was defined earlier from the drop down. In this case, the name of the RADIUS Authentication server is **RSA**.

To configure the AAA Policy, navigate to **AAM > Policies and Templates > AAA Policies** and click **Create**. To create the AAA Policy enter the name as **RSA** and click **create**. You will be displayed with a **AAA Rules** option. Under AAA Rules, click **create**.



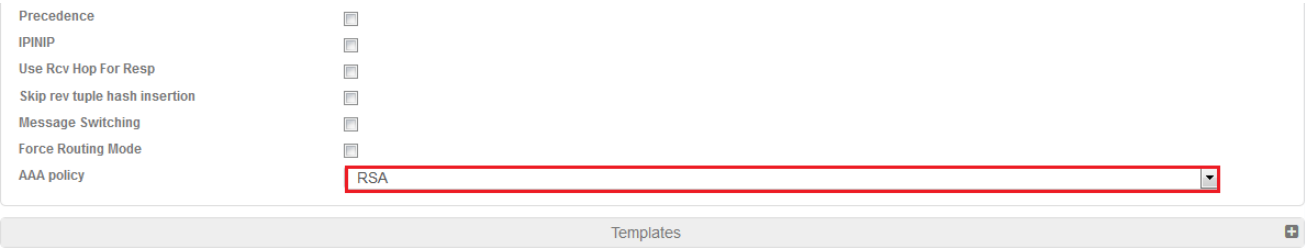
Index: 1 (Unique Identifier from the range of 1-256)

Action: Select **Allow**

Authentication Template: Select **RSASecurID** from the drop down menu.

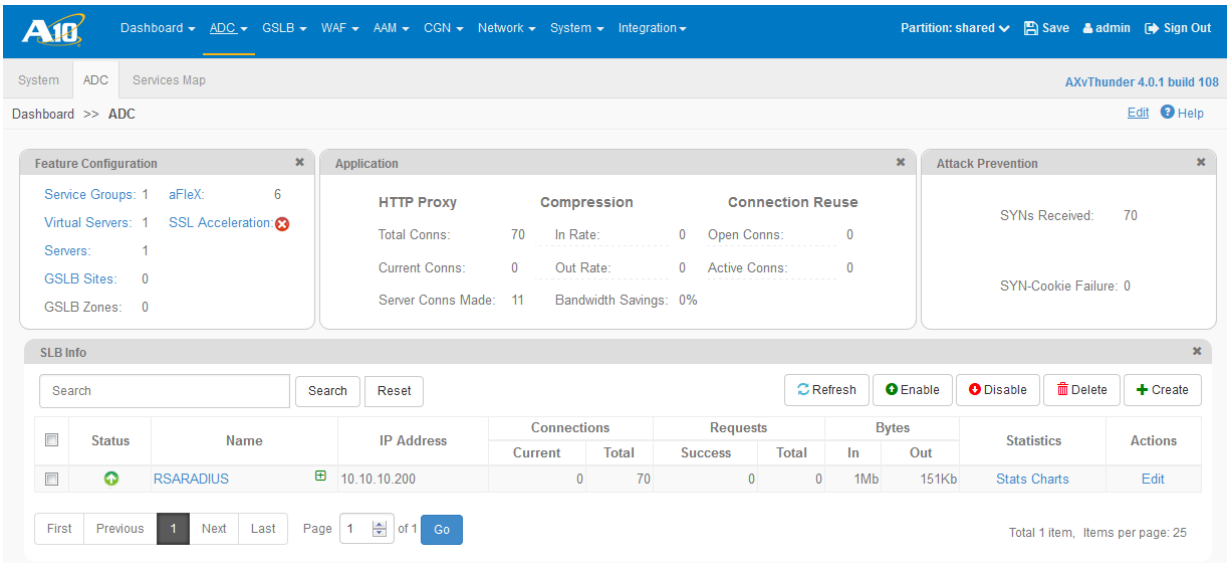
Once configured click the **Create** button.

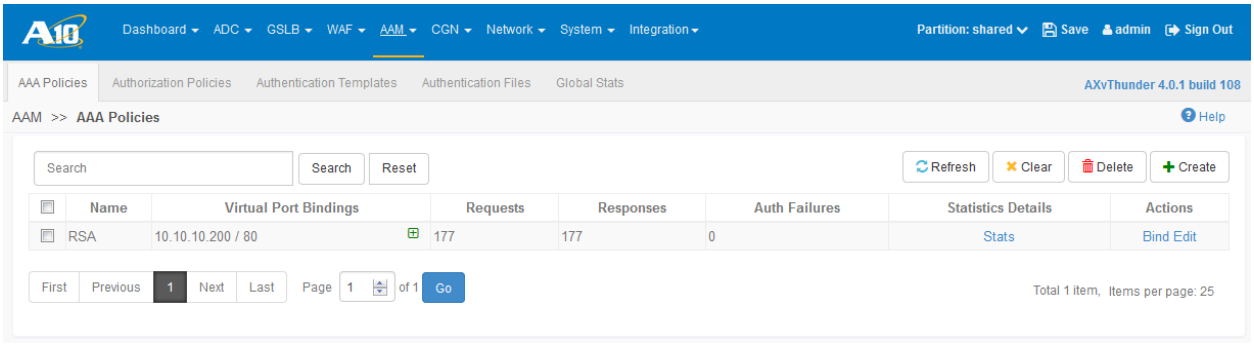
The final step of the A10 configuration is binding the AAA policy to the Virtual IP. To do this, navigate to **ADC > Virtual Services** of the VIP. Navigate through the **General Fields** section and locate the **AAA Policy** section. From the drop down, select **RSA** which is the name of the AAA policy that was created earlier.



Monitoring AAA Authentication

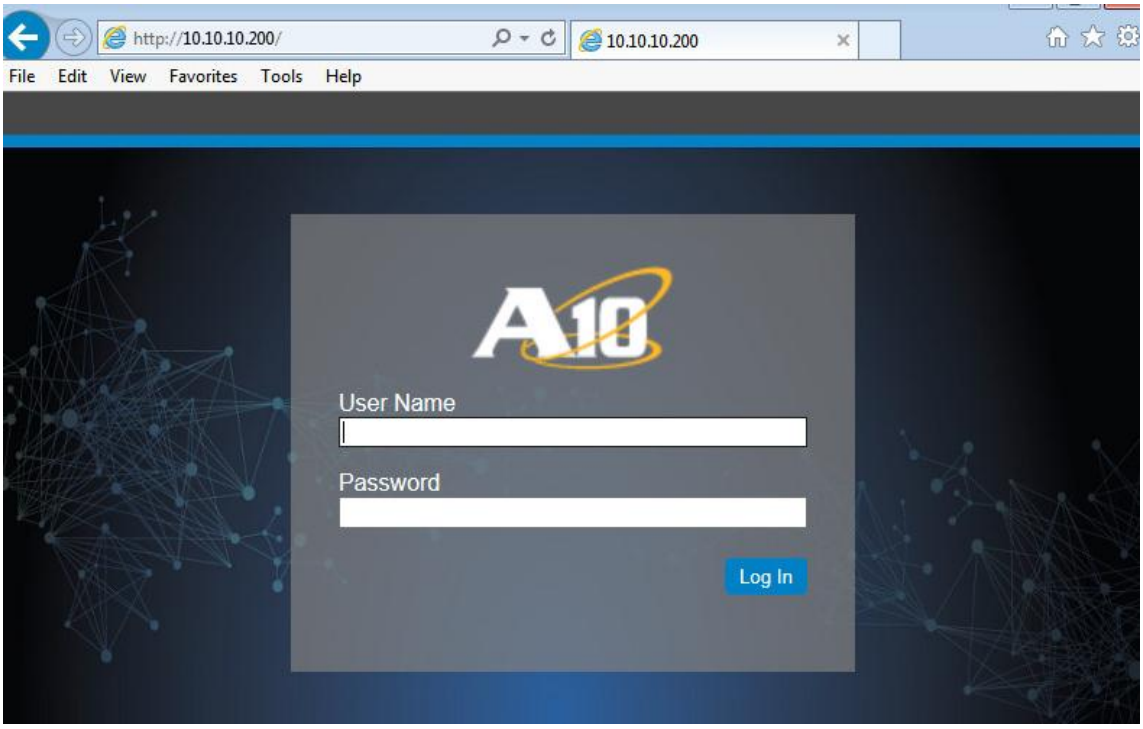
There are a few items in the A10 GUI dashboard you can use to make sure the authentication service is in working order. You can use the ADC within the A10 GUI dashboard, or you can use the **AAA Policies** monitor. Ensure that statistics are increasing after navigating to the Virtual IP address.





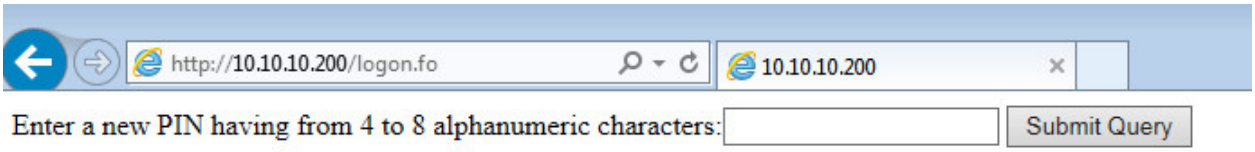
RSA SecurID Login Screens

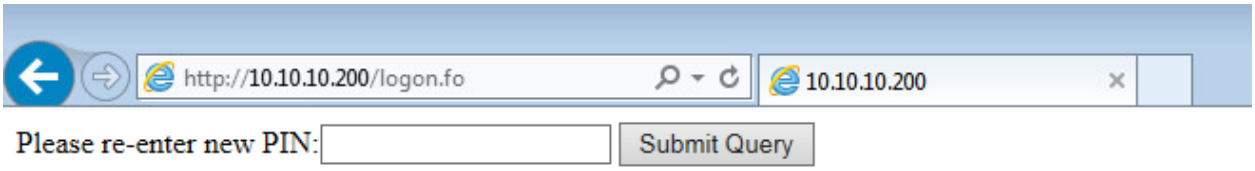
Main RSA SecurID Login Screen

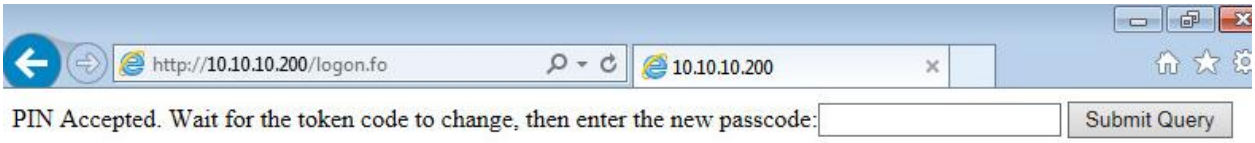


Note: The logon screen can be customized to include additional wording or your company logo.

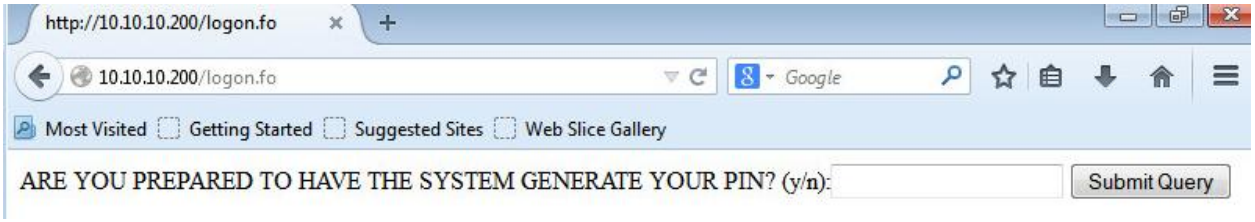
User-defined New PIN

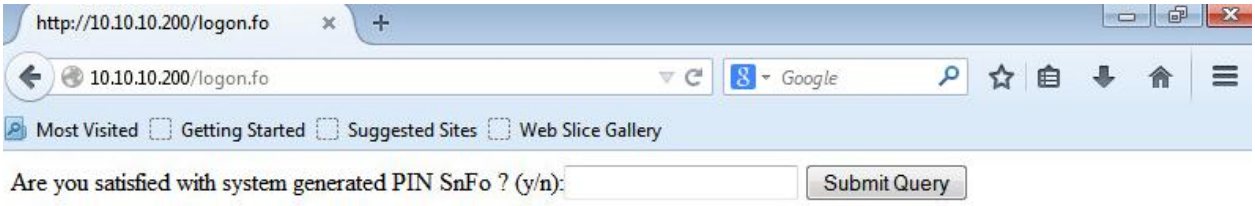


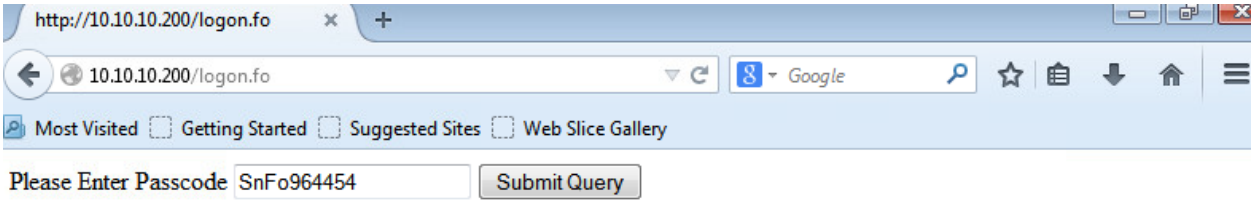




System-Generated New PIN







Next Tokencode

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
Thunder ADC	2.7.2 P4 & 4.0	vThunder, Thunder & AX Series

RSA SecurID Authentication

Date Tested: 2/10/15

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	✓

JEC / PAR

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

Appendix

A10 CLI Sample Configuration

```
hostname RSA
timezone America/Los_Angeles
interface management
  ip address 10.100.2.96 255.255.255.0
  ip default-gateway 10.100.2.1
interface ethernet 1
  enable
  ip address 10.10.10.1 255.255.255.0
interface ethernet 2
  enable
  ip address 10.10.12.1 255.255.255.0
aam authentication logon form-based RSA
  portal default-portal
aam authentication server radius RSA
  host 10.100.2.135
  secret encrypted WCoEx8HmE5oIH3fBJznxEjwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
slb server apache2 10.10.12.200
  port 80 tcp
aam authentication template RSASecurID
  type standard
  logon RSA
  server RSA
aam authorization policy RSA
  attribute-rule 1
aam aaa-policy RSA
  aaa-rule 1
    action allow
    authentication-template RSASecurID
slb service-group http-sg tcp
  member apache2 80
slb virtual-server RSARADIUS 10.10.10.200
  port 80 http
    source-nat auto
    service-group http-sg
    aaa-policy RSA
multi-config enable
end
```