How to: Two-Factor Authentication with ClearPass and RSA SecureID

<css>.page-How to: Two-Factor Authentication with ClearPass and RSA SecureID #commentform { display: none; }</css>

Introduction

This Guide will show you how to configure two-factor authentication using ClearPass, RSA SecurID Authentication Manager^[1] and the Windows 802.1X supplicant with the Aruba EAP-GTC plug-in.

Configuring ClearPass Policy Manager

This section provides instructions for configuring ClearPass Policy Manager with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

Create an RSA Authentication Source

Go to **Configuration > Authentication > Sources** and click **Add**. Select **Token Server** as the **Type**. This will expose the remainder of the configuration options for this authentication source. Provide a **Name** for the source, and optionally a **Description**. It's suggested that you uncheck the **Use for Authorization** option, as it's unlikely that the RSA authentication source is providing any additional authorization information. If you have replica (redundant) RSA Authentication Manager servers, click the **Add Backup** button for each backup server you want to add. This will expose additional tabs for configuring the backup servers.

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary	Attributes Backup 1 Backup 2 Summary
Name:	RSA Authentication Manager
Description:	
Туре:	Token Server ÷
Use for Authorization:	Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	Remove View Details
Server Timeout:	10 seconds
Backup Servers Priority:	Backup 1 Backup 2 Move Up Move Down
	Add Backup Remove

Go to the **Primary** tab, and enter the FQDN or IP Address of the primary RSA Authentication Manager as the **Server Name**. The default **Port** of 1812 should be appropriate for most applications. Then enter the RADIUS shared secret as the **Secret**. If you have added backup servers, complete the same configuration under the **Backup** tabs.

1

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary	Attributes Backup 1 Backup 2 Summary
Connection Details	
Server Name:	pe081.pe-lab.com
Port:	1812
Secret:	•••••

Authentication Course has not been sound

On the Summary tab, verify that the configuration is what you want and then click Save.

Configuration » Authentication » Sources » Add Authentication Sources

				Authent	incation source has not been saved
General	Primary	Attributes	Backup 1	Backup 2	Summary
General:					
Name:		RSA Authen	tication Manage	er	
Description	:				
Type:		TokenServer	r		
Use for Aut	horization:	Disabled			
Authorizatio	on Sources:	-			
Primary:					
Server Nam	ie:	pe081.pe-la	b.com		
Port:		1812			
Secret:		******			
Backup 1:					
Server Nam	ie:	pe082.pe-la	b.com		
Port:		1812			
Secret:		******			
Backup 2:					
Server Nam	ie:	pe083.pe-la	b.com		
Port:		1812			
Secret:		******			
Attributes:					
Туре			Name	2	Enabled as Role

< Back to Authentication Sources



Create a Service for RSA Authentications

NOTE: The following instructions assume the use of Aruba Wireless infrastructure. If your network infrastructure is different, these instructions may need to be altered.

Go to **Configuration > Services** and click **Add**. Select **Aruba 802.1X Wireless** as the service **Type**. Provide a **Name** for the service.

Configuration » Services »	Add				
Services					
Service Authentic	ation Roles Enforcement Summary				
Туре:	Aruba 802.1X Wireless				
Name:	RSA Authentication Service				
Description:	Description: Aruba 802.1X Wireless Access Service				
Monitor Mode:	Enable to monitor network access without e	nforcement			
More Options:	Authorization Posture Compliance A	udit End-hosts 🗌 Profile Endpoint	s		
Service Rule					
Matches 🔵 ANY or 💽 AL	L of the following conditions:				
Туре	Name	Operator	Value	Ť	
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	Ba ti	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	te t	
3. Radius:Aruba	Aruba-Essid-Name	EXISTS		te t	
4. Click to add					

Click **Next** to move to the **Authentication** tab. Under **Authentication Sources**, select the RSA authentication source you created in the previous section.

Configuration » Services » Add

Services					
Service	Authentication	Roles	Enforcement	Summary	
Authenticati	ion Methods:	[EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS] Select to Add		•	Move Up Move Down Remove View Details Modify
Authenticati	ion Sources:	RSA Authenticat	ion Manager [Token So	erver]	Move Up Move Down Remove View Details Modify
Strip Userna	ame Rules:	Enable to sp	ecify a comma-se	parated list of	f rules to strip username prefixes or suffixes

On the **Roles** and **Enforcement** tabs, make changes to suit your environment. On the **Summary** tab, verify that the configuration is what you want, then click **Save**.

Serv	ice Authenticatio	n Roles	Enforcement	Summary		
ervic	<u>e:</u>					
Туре:		Aruba 802.1X	Wireless			
Name	:	RSA Authentio	cation Service			
Descr	iption:	Aruba 802.1X	Wireless Access S	ervice		
Monite	or Mode:	Disabled				
More	Options:	-				
Servi	ce Rule					
Match	ALL of the following of	onditions:				
	Туре		Name		Operator	Value
1. 1	Radius:IETF		NAS-Port-Type		EQUALS	Wireless-802.11 (19)
2.	Radius:IETF		Service-Type		BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. 1	Radius:Aruba		Aruba-Essid-Na	ime	EXISTS	
uthe	ntication:					
Authe	ntication Methods:	1. [EAP PEAP] 2. [EAP FAST] 3. [EAP TLS] 4. [EAP TTLS]				
Authe	ntication Sources:	RSA Authentio	cation Manager [To	oken Server]		
Strip	Username Rules:	-				
oles:						
	1apping Policy:	-				
Role N	omonti					
Role N	ementi					
Role N Inford Use C	ached Results:	Disabled				

Configuring the Network Supplicant

After you have configured ClearPass Policy Manager to use RSA SecurID authentication, a compatible 802.1X supplicant is required to fully implement the solution. Any supplicant used for RSA SecurID authentication must support either EAP-GTC (Generic Token Code) or native SecurID authentication. The additional functionality in these supplicants enables the endpoint to respond to challenges from the RSA Authetication Manager. These challenges manifest themselves in the form of prompts to the end user for events such as NEW PIN or NEXT TOKENCODE. The native supplicants supplied with operating systems such as Windows and Mac OS X do not contain support for 2-factor authencation systems such as RSA SecurID, but may be modified to include such support. Third-party supplicants such as the Juniper Odyssey Access Client may also be used in place of the native supplicants. You can explore additional supplicant options on the RSA Ready ^[2] community.

Installing the EAP-GTC Plug-In

In the following example, the EAP-GTC plug-in (supplied by Aruba Networks) for Windows is used. This plug-in is available for download from the Aruba Networks support site ^[3], and supports 32- and 64-bit versions of Windows XP, Vista, and 7. Follow the instructions included in the EAP-GTC Plug-In User's Guide to install the plug-in on Windows.

NOTE: Windows 7 is used for the client examples.

Launch the downloaded Windows installer package. The package is unsigned so you will have click **Run** to accept the Security Warning to proceed.



Click Next, then Accept the License Agreement and click Next. Select the Complete Setup Type and click Next.



Click Install to begin the installation and then click Finish once the installation is complete.



Finally, restart your system to complete the installation.



Configuring the EAP-GTC Plug-In

After installation of the EAP-GTC plug-in, you need to manually create a Network Profile for the SSID that will use RSA SecurID. Open the Network and Sharing Center and click **Manage wireless networks**.

Control Panel 🕨	Network and Internet Network and Sharing Center	Q
Control Panel Home Manage wireless networks Change avapuer settings Change advanced sharing setting	View your basic network information and set up connections View your basic network information and set up connections See full map WIN7-X64 (This computer)	Ø
	View your active networks Connect to a network You are currently not connected to any networks.	
	Change your networking settings Set up a new connection or network Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point. Connect to a network Connect or reconnect to a wireless, wired, dial-up, or VPN network connection. Choose homegroup and sharing options Access files and printers located on other network computers, or change sharing settings. Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information.	
See also		
Internet Options		
Windows Firewall		

Click Add to create a new wireless network configuration.

Click Manually create a network profile to create a new network profile.

G and Manually connect to a wireless network	
How do you want to add a network?	
Manually create a network profile This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).	:
Create an ad hoc network This creates a temporary network for sharing files or an Internet connection	
	Cancel

Enter the following information into the Wireless Network Information window, then click Next:

- Network name: Enter the network SSID
- Security type: Select WPA2-Enterprise, WPA-Enterprise, or 802.1X from the pull-down list. This selection should match your network settings.
- Encryption type: Select AES, TKIP, or WEP as appropriate from the pull-down list.

	Long the second	
Manually connect to	a wireless network	
Enter information	or the wireless network you want to add	
Network name:	RSA	
Security type:	WPA2-Enterprise	
Encryption type:	AES	
Security Key:	Hide characters	
Start this connect	ion automatically	
Connect even if t	ne network is not broadcasting	
Warning: If you s	elect this option, your computer's privacy might be at risk.	
	Ne	ext Cancel

Click Change connection settings.

ר

The **Wireless Network properties** dialog box appears with the **Connection** tab selected. Make changes as appropriate for your environment, then click on the **Security** tab.

RSA Wireless Network F	Properties
Connection Security	
Name:	RSA
SSID:	RSA
Network type:	Access point
Network availability:	All users
Connect automati	ally when this patwork is in same
Connect automati	cally when this network is in range
Connect to a more	a petwork is not broadcacting its name (SSID)
Connect eventing	ie network is not broadcasting its name (3510)
	OK Cancel

Select **Microsoft: Protected EAP** (**PEAP**) from the **Choose a network authentication method** pull-down menu. Make other changes as appropriate, then click **Setting**.

NOTE: While EAP-Token appears in both the inner and outer authentication method lists, you should only select it as an inner method. Select PEAP as the outer method.

RSA Wireless Network P	roperties	×
Connection Security		
Security type: Encryption type:	WPA2-Enterprise AES	
Choose a network aut Microsoft: Protected	thentication method: EAP (PEAP) Settings dentials for this connection ead.)
Advanced settings		
	ОК Са	ancel

Select **EAP-Token** from the **Select Authentication Method** pull-down list. Make any other changes appropriate for your environment, then click **OK**.

NOTE: When you select EAP Token as the authentication method, no dialog box is displayed if you click on the Configure button.

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AddTrust External CA Root
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
cppm.cloud.clearpassbeta.com Onboard CA
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert High Assurance EV Root CA
Do not prompt user to authorize new servers or trusted certification authorities
cei uncauori autionues.
Select Authentication Method:
EAP-Token Configure
Enable East Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK Cancel

Click the **Advanced** button if you need to make any changes to the **Advanced Properties** such as the Authentication Mode.



Click **OK** when you've made all the necessary changes.

Configuring RSA Authentication Manager



See the for guidelines on setting up RSA Authentication Manager. Make sure you set up RSA Authentication Manager for RADIUS.

RSA SecurID Login Screens

Login Dialog

Enter Credentials	×
User name:	
Password:	•••••
Logon domain:	
C	OK Cancel

User-Defined New PIN

EAP GTC	EAP GTC
Enter a new PIN having from 4 to 8 alphanumeric characters:	Please re-enter new PIN:
••••	••••
OK Cancel	OK Cancel

System-generated New PIN

EAP GTC	EAP GTC	
ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE YOUR PIN? (y/n):	Are you satisfied with system generated PIN xUMT0L ? (y/n):	
• Cancel	•I OK Cancel	

Next Tokencode

EAP GTC	Type ingrappents	x
Wait for token to change, then enter the new tokencode:		
•••••	ОК	Cancel

Historical

FOR HISTORICAL REFERENCE: Configure CPPM to use RSA Token server as Authentication Source.PDF

References

- [1] http://en.wikipedia.org/wiki/SecurID
- [2] https://community.emc.com/community/connect/rsaxchange/rsa-ready/content
- [3] http://support.arubanetworks.com/ToolsResources/tabid/76/DMXModule/514/EntryId/114/Default.aspx

Article Sources and Contributors

How to: Two-Factor Authentication with ClearPass and RSA SecureID Source: https://arubapedia.arubanetworks.com/hp/index.php?oldid=45373 Contributors: Rfiler

Image Sources, Licenses and Contributors

File:2014-11-13_11-53-48.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-13_11-53-48.png License: unknown Contributors: Maintenance script File:2014-11-13_11-56-04.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-56-04.png License: unknown Contributors: Maintenance script File:2014-11-13 11-59-31.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13 11-59-31.png License: unknown Contributors: Maintenance script File:2014-11-13_12-07-53.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-13_12-07-53.png License: unknown Contributors: Maintenance script File:2014-11-13_12-12-26.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_12-12-26.png License: unknown Contributors: Maintenance script File:2014-11-13_12-15-04.png Source: https://arubapedia.arubanetworks.com/hp/index.php?ititle=File:2014-11-13_12-15-04.png License: unknown Contributors: Maintenance script File:2014-11-14_11-03-52.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-14_11-03-52.png License: unknown Contributors: Maintenance script File:2014-11-14_11-03-55.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-14_11-03-55.png License: unknown Contributors: Maintenance script File:2014-11-14_11-03-53.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-14_11-03-53.png License: unknown Contributors: Maintenance script File:2014-11-14_11-03-54.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-14_11-03-54.png License: unknown Contributors: Maintenance script File:2014-11-14_11-03-56.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-14_11-03-56.png License: unknown Contributors: Maintenance script File:2014-11-14 11-03-58.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-14 11-03-58.png License: unknown Contributors: Maintenance script File:2014-11-14_11-03-59.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-14_11-03-59.png License: unknown Contributors: Maintenance script File:2014-11-14_12-12-01.png Source: https://arubapedia.arubanetworks.com/hp/index.php?iitle=File:2014-11-14_12-12-01.png License: unknown Contributors: Maintenance script File:2014-11-14_12-12-19.png Source: https://arubapedia.arubanetworks.com/hp/index.php?ititle=File:2014-11-14_12-12-19.png License: unknown Contributors: Maintenance script File:2014-11-14_12-12-49.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-14_12-12-49.png License: unknown Contributors: Maintenance script File:2014-11-14_12-12-59.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-14_12-12-59.png License: unknown Contributors: Maintenance script File:2014-11-13_14-43-28.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-13_14-43-28.png License: unknown Contributors: Maintenance script File:2014-11-13 14-43-39.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13 14-43-39.png License: unknown Contributors: Maintenance script File:2014-11-13_14-44-04.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-13_14-44-04.png License: unknown Contributors: Maintenance script File:2014-11-13_14-45-13.png Source: https://arubapedia.arubanetworks.com/hp/index.php?itile=File:2014-11-13_14-45-13.png License: unknown Contributors: Maintenance script File:Secured By RSA SecurID AM 80 Ready Test Guide.doc Source:

https://arubapedia.arubanetworks.com/hp/index.php?title=File:Secured_By_RSA_SecurID_AM_8_0_Ready_Test_Guide.doc License: unknown Contributors: Maintenance script File:2014-11-13_11-41-12.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-12.png License: unknown Contributors: Maintenance script File:2014-11-13_11-41-18_01.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-18_01.png License: unknown Contributors: Maintenance script File:2014-11-13_11-41-20.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-20.png License: unknown Contributors: Maintenance script File:2014-11-13_11-41-14.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-14.png License: unknown Contributors: Maintenance script File:2014-11-13_11-41-14.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-14.png License: unknown Contributors: Maintenance script File:2014-11-13_11-41-15.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-14.png License: unknown Contributors: Maintenance script File:2014-11-13_11-41-42.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-42.png License: unknown Contributors: Maintenance script File:2014-11-13_11-41-42.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-42.png License: unknown Contributors: Maintenance script File:2014-11-13_11-41-42.png Source: https://arubapedia.arubanetworks.com/hp/index.php?title=File:2014-11-13_11-41-42.png License: unknown Contributors: Maintenance script