SecureW2
Enterprise Client

RSA SecurID Ready Implementation Guide

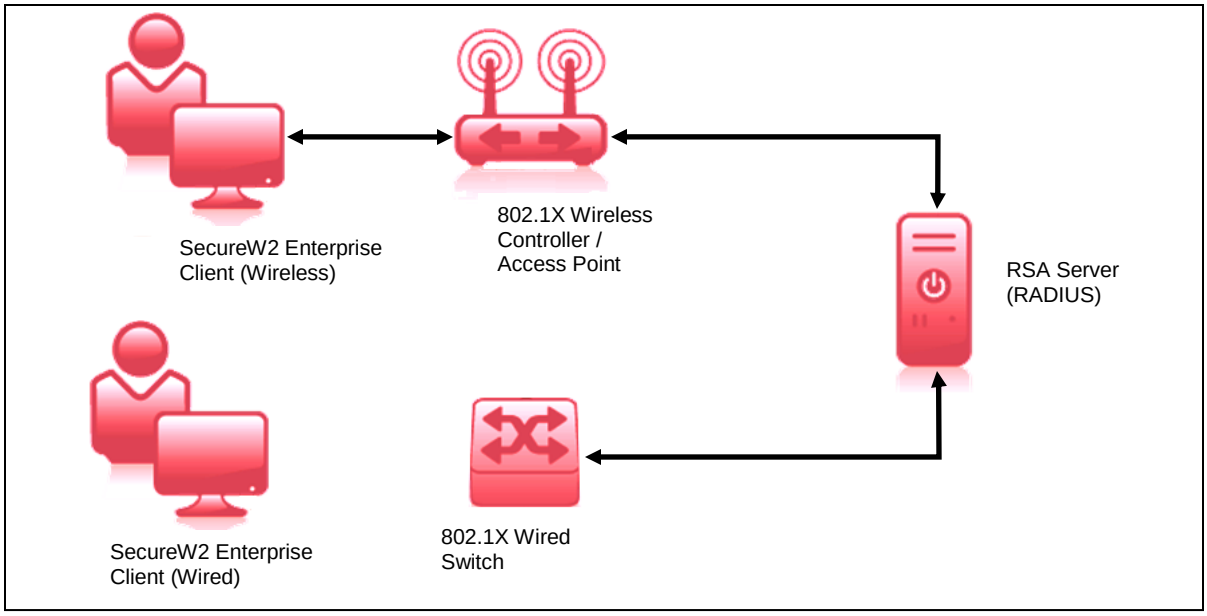
Last Modified: January 16, 2015

Partner Information

Product Information	
Partner Name	SecureW2
Web Site	www.securew2.com
Product Name	SecureW2 Enterprise Client
Version & Platform	3.5.12 for Windows XP/Vista/7/8
Product Description	SecureW2 Enterprise Client offers a comprehensive set of authentication, encryption and security features for 802.1X based access for wireless and wired networks. Enterprise client has support for a full range of Extensible Authentication Protocols (EAP) including EAP-GTC for two-factor authentication, PEAP v0 & v1, EAP-TTLS and EAP-SIM. Enterprise Client network and security settings can be pre-configured and deployed to endpoints via MSI for Microsoft GPO and other software distribution tools. Available security features include configuration lockdown and prevention of wireless bridging to wired corporate networks.

Solution Summary

SecureW2 Enterprise Client enables RSA SecurID authentication for Wireless/Wired 802.1X/EAP connections on Windows Platforms.



RSA Authentication Manager supported features SecureW2 Enterprise Client 3.5.12	
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	N/A
RSA SecurID Software Token Automation	Yes
RSA SecurID SD800 Token Automation	Yes
RSA SecurID Protection of Administrative Interface	N/A

Agent Host Configuration

To facilitate communication between the SecureW2 Enterprise Client 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 SecureW2 Enterprise Client and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduces a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Note: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

> **Note: The RSA agent name is specified in the rsa_api.properties file.**

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with SecureW2 Enterprise Clientwill occur.

If SecureW2 Enterprise Client 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
- 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 integrating the SecureW2 Enterprise Client 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 SecureW2 Enterprise Client components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring SecureW2 Enterprise Client for SecurID Authentication

Pre-requisites

SecureW2 Enterprise Client implements the client side of an 802.1X protected network. This document assumes the other aspect of the network (Network Access Points/RSA Authentication Manager/RADIUS Server) are implemented and working correctly.

Configuration via user interface

Use the SecureW2 Enterprise Client to enable RSA SecurID authentication. The configuration is for both PEAP and TTLS. This section assumes the user is familiar with the way to configure 802.1X on a Windows system, for both wireless and wired.

1. Create a new profile, use the profile DEFAULT and select **Configure**.

Figure 1. SecureW2 Enterprise Client Configuration UI

2. In the Authentication TAB select **EAP** as your Authentication method and the **SecureW2 EAP-GTC** as your EAP Type. Select **Configure** to configure EAP-GTC for RSA SecurID.

Figure 2. SecureW2 Enterprise Client Authentication TAB

3. The most commonly used settings are “Check For Software Token” and “Use Credentials User Interface”. This will give the user the optimal RSA SecurID experience. The other options are discussed in the SecureW2 General Administrators Guide.

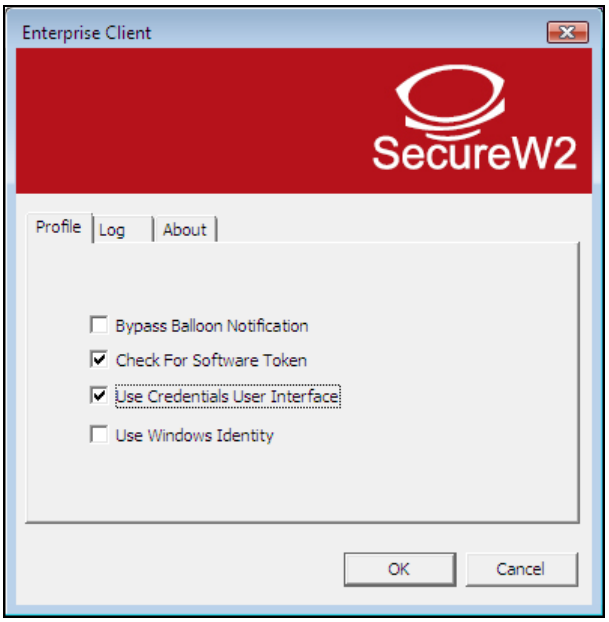


Figure 3. SecureW2 Enterprise Client EAP-GTC Configuration

Configuration via Pre-Configuration File

The following steps assume you have downloaded the SecureW2 Enterprise Client installer and have extracted it in to a temporary folder. Next create a SecureW2.inf pre-configuration file and place this file in the same temporary folder as the installer. When the installer is run it will look for this pre-configuration file and use it to pre-configure SecureW2 Enterprise Client.

For basic installation of the client please see our “SecureW2 Enterprise Client - Installation – Basic” tutorial in the “Learn” section of the SecureW2 website.

Note: It is possible to automate this process and create a single MSI package which deploys and runs the installer and pre-configuration file. This is not within the scope of this document. A tutorial can be found in the Learn section of the SecureW2 website “SecureW2 MSI Installer - Basic Setup”.

The following shows a SecureW2.inf file for basic RSA SecurID authentication. This file will setup a wireless SSID “SecureW2” configured for WPA2/AES and add a SecureW2 configuration for PEAP/GTC with RSA SecurID Authentication.

http://www.securew2.com/resources/tutorials/inf/SecureW2_eappeapeapgtc.inf

Change the settings of the SecureW2.inf file according to your network requirements.

Installation

Run the installer (or the MSI package) on the client machine. This will add the configured SSID to the list of preferred wireless networks.

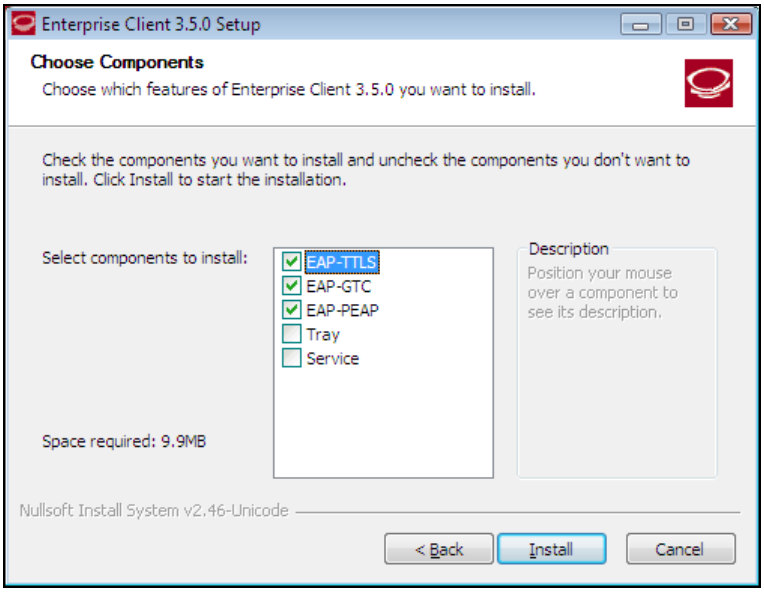


Figure 4. SecureW2 Enterprise Client Installer EAP Method Selection

Important: Make sure you select the EAP-TTLS/EAP-PEAP and the EAP-GTC options.

RSA SecurID Login Screens

End User Experience

Authentication

In a wireless environment the authentication will commence when the SSID is within range. You will be presented with the following screen:

Figure 5. SecureW2 Enterprise Client RSA SecurID Credentials

Enter the appropriate username and passcode and if correct the 802.1X authentication will proceed and a valid Ethernet connection will be available.

The following shows a selection of screenshots that an end user can expect to see within SecureW2 Enterprise Client when RSA SecurID authentication occurs.

Figure 6. System generated New PIN

Figure 7. Next Passcode

Software token support

If configured correctly and a Software token is available, SecureW2 Enterprise Client will show an extra interface allowing the user to interact with the user's Software token. The following is an example screen of when a RSA software token is detected.

Figure 8. RSA SecurID Software Token

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
RSA Software Token	4.1.2	Windows XP/Vista/7/8
SecureW2 Enterprise Client	3.5.12	Windows XP/Vista/7/8

RSA SecurID Authentication

Date Tested: January 15, 2015

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	N/A
No RSA Authentication Manager	N/A	N/A	N/A

GLS / PAR

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

Certification Test Checklist for RSA Authentication Manager

Software Token Automation

Date Tested: January 15, 2015

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
PINless Token			
Next Tokencode Mode	N/A	N/A	✓
PINpad-style Token			
Deny Alphabetic PIN	N/A	N/A	✓
Next Tokencode Mode	N/A	N/A	✓
Fob-style Token			
16 Digit Passcode	N/A	N/A	✓
Alphanumeric PIN	N/A	N/A	✓
Next Tokencode Mode	N/A	N/A	✓
Other			
System Generated PIN	N/A	N/A	✓
Password Protected PIN	N/A	N/A	✓

SID800 Token Automation

Date Tested: January 15, 2015

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
PINless Mode			
PINless Token	N/A	N/A	✓
New PIN Mode			
User Defined PIN	N/A	N/A	✓
System Generated PIN	N/A	N/A	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	N/A	✓

GLS / PAR

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

Known Issues

SecureW2 Enterprise Client v3.5.12 does not support alphanumeric software PIN.