

# **RSA SECURID<sup>®</sup> ACCESS**

## **Implementation Guide**

**Western Telematic, Inc.**

**WTI Devices**

Peter Waranowski, RSA Partner Engineering

Last Modified: June 28<sup>th</sup>, 2018

## Solution Summary

The Western Telematic Console Servers, Console Server + Power Control Combos and Switched PDUs (AKA WTI Devices) use RSA SecurID Authentication to allow seamless integration into enterprises already using RSA SecurID. User permission levels, individual port and plug access can be centrally managed, allowing easy deployment of many console servers to remote sites.

RSA SecurID Access Features	
WTI Console Server 6.51	
WTI Console Server + Power Control Combos 6.51	
WTI Switched PDU 2.11	
<b>On Premise Methods</b>	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
<b>Cloud Authentication Service Methods</b>	
Authenticate App	✓
FIDO Token	-
<b>SSO</b>	
SAML SSO	-
HFED SSO	-
<b>Identity Assurance</b>	

Collect Device Assurance and User Behavior	-
--	---



### Supported Authentication Methods by Integration Point

This section indicates which authentication methods are supported by integration point. The next section (Configuration Summary) contains links to the appropriate configuration sections for each integration point.

#### WTI Device integration with RSA Cloud Authentication Service

Authentication Methods	REST	IDR SAML	Cloud SAML	HFED	RADIUS
RSA SecurID	-	-	-	-	✓
LDAP Password	-	-	-	-	✓
Authenticate Approve	-	-	-	-	✓
Authenticate Eyeprint ID	-	-	-	-	✓
Authenticate Fingerprint	-	-	-	-	✓
Authenticate Tokencode	-	-	-	-	✓
SMS Tokencode	-	-	-	-	
Voice Tokencode	-	-	-	-	
FIDO Token		-	-	-	

#### WTI Device integration with RSA Authentication Manager

Authentication Methods	REST	RADIUS	UDP Agent	TCP Agent
RSA SecurID	-	✓	-	-
AM RBA		-	-	

- ✓ Supported
- Not supported
- n/t Not yet tested or documented, but may be possible



## Configuration Summary

---

All of the supported use cases of RSA SecurID Access with WTI Devices require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

**RSA Cloud Authentication Service** – WTI Devices can be integrated with RSA Cloud Authentication Service in the following way:

RADIUS Client

**[Cloud Authentication Service RADIUS Configuration](#)**  
**[WTI Device RADIUS Configuration](#)**

**RSA Authentication Manager** – WTI Devices can be integrated with RSA Authentication Manager in the following way:

RADIUS Client

**[Authentication Manager RADIUS Configuration](#)**  
**[WTI Device RADIUS Configuration](#)**

## RSA SecurID Access Server Side Configuration

---

### *RSA Cloud Authentication Service Configuration*

#### RADIUS

To configure RADIUS for Cloud Authentication Service for use with a RADIUS client, you must first configure a RADIUS client in the RSA SecurID Access Console.

Logon to the RSA SecurID Access console and browse to **Authentication Clients > RADIUS > Add RADIUS Client** and enter the **Name**, **IP Address** and **Shared Secret**. Click **Publish** to push your configuration change to the RADIUS server.

RSA Cloud Authentication RADIUS server listens on port UDP 1812.

### *RSA Authentication Manager Configuration*

#### RADIUS

To configure your RSA Authentication Manager for use with a RADIUS Agent, you must configure a RADIUS client and a corresponding agent host record in the Authentication Manager Security Console.

The relationship of agent host record to RADIUS client in the Authentication Manager can 1 to 1, 1 to many or 1 to all (global).

RSA Authentication Manager RADIUS server listens on ports UDP 1645 and UDP 1812.

#### **Configure RSA Authentication Manager for central user management**

WTI devices can receive VSA attributes supplied by the RSA Authentication Manager server via a WTI supplied dictionary file.

1. Logon to RSA Authentication Manager Operations Console and browse to **Deployment Configuration > RADIUS servers** and open the **Dictionary Files** tab.
2. Click **Add New**, browse to the WTI provided file and click **Submit**.
3. Open the **Configuration Files** tab and make the following file edits:

Open **dictionarya.dcm**, add the following text and click **Save**.

```
@wti.dct
```

Open **vendor.ini**, add the following text and click **Save**.

```
vendor-product      = western Telematic
```

```
dictionary          = wti
```

Open **radius.ini**, add the following text and click **Save & Restart RADIUS Server**.

```
AuthenticateOnly=0
```



To see the Dictionary changes in the Security Console, you need to logout and then back in.

### Configure RADIUS client for central user management.

1. Logon to RSA Authentication Manager Security Console and browse to **RADIUS > RADIUS Clients** and click **Add New** or **Manage Existing**.
2. Select **Western Telematic** from the **Make / Model** drop-down menu and open the **RSA Agent** tab.
3. Choose the **RADIUS profile** from the drop-down menu to apply the profile to all users authenticating to the client.

And/or

4. Choose the **RADIUS profile** from specific user accounts' **Authentication Settings** to set/override at the user level.

### Configure RADIUS profile for central user management

Set up a user permission level, individual port and plug access.

1. Logon to the RSA Authentication Manager Security Console and browse to **RADIUS > RADIUS Profiles** and click **Add New** or **Manage Existing**.



2. Under **Return List Attributes**, Choose the **Attribute** you want to add and the **Value** and then **Add**.

Return List Attributes

The RADIUS server sends the return list attributes to the RADIUS client after a successful authentication.

Return List Attributes:

Attribute

WTI-Super

Value

3

(Integer)

Echo
☐

Add
Update

3. Click **Save** when finished.

## Partner Product Configuration

---

### *Before You Begin*

This section provides instructions for configuring the WTI Device with RSA SecurID Access. 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.

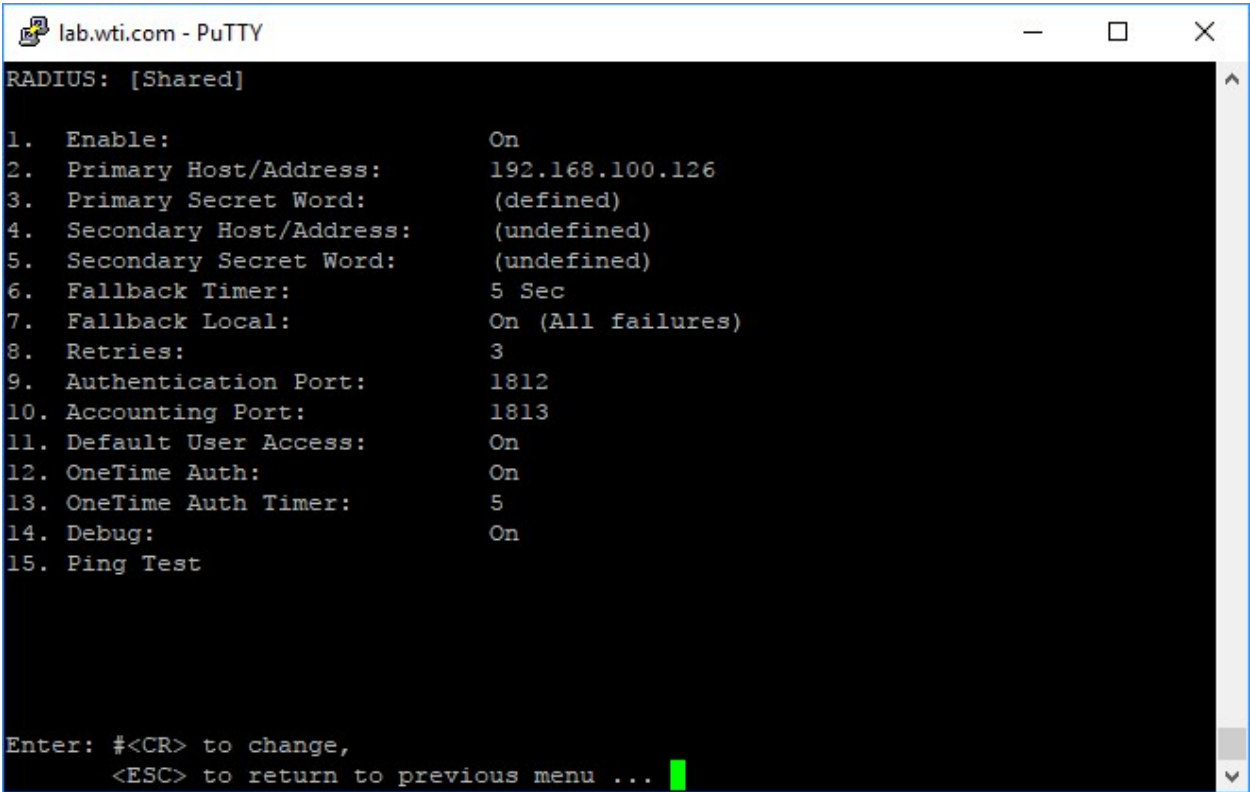
All WTI Device components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### **WTI Device RADIUS Client Configuration**

Complete the steps in this section to integrate with RSA SecurID Access using RADIUS authentication protocol.

1. To configure the RADIUS client on the WTI device, connect via SSH to a WTI Device, and then enter `\n` and then choose option 29.
2. From this RADIUS screen set "Enable" to On, enter your "Primary Host/Address" and "Primary Secret Word".

When integrating with RSA Cloud Authentication service, you should increase the "OneTime Auth Timer" value so that users will have a more time to authenticate using mobile-based methods. 60 seconds is recommended.



## Certification Checklist for RSA SecurID Access

### Certification Environment Details:

RSA Authentication Manager 8.2 SP1, Virtual Appliance

WTI Console Server 6.51

WTI Console Server + Power Control Combos 6.51

WTI Switched PDU 2.11

### ***RSA Cloud Authentication Service***

Date Tested: December 1, 2017

Authentication Method	REST Client	RADIUS Client
RSA SecurID	-	✓
LDAP Password	-	✓
Authenticate Approve	-	✓
Authenticate Eyeprint ID	-	✓
Authenticate Fingerprint	-	✓
Authenticate Tokencode	-	✓



SMS Tokencode	-
Voice Tokencode	-
FIDO Token	-

**RSA Authentication Manager**

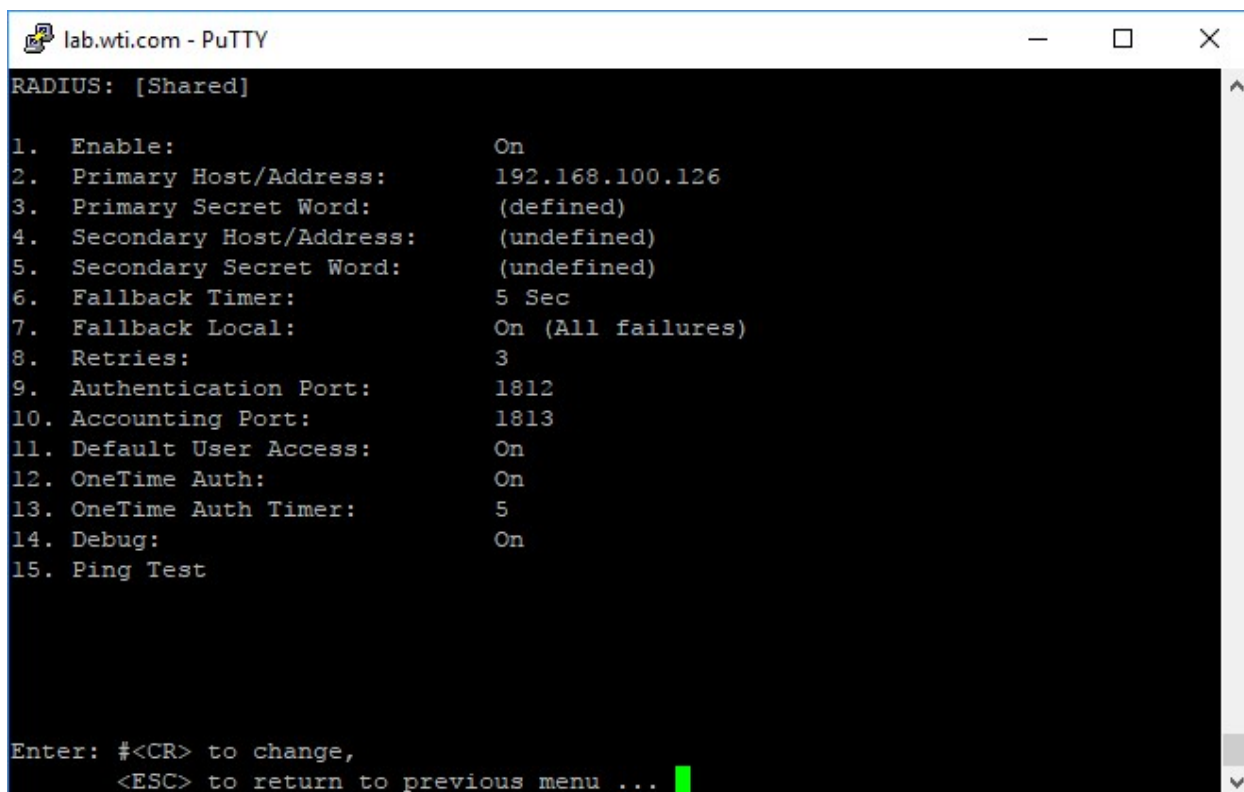
December 1, 2017

Authentication Method	REST	UDP	TCP	RADIUS
	Client	Agent	Agent	Client
RSA SecurID	-	-	-	✓
RSA SecurID Software Token Automation	-	-	-	-
On Demand Authentication	-	-	-	✓
Risk-Based Authentication		-		-

✓ = Passed, X = Failed, - = N/A

## Agent Tracing

To enable WTI Device RADIUS debugging information, connect via SSH to a WTI Device, and then enter \n and then choose option 29.



```
lab.wti.com - PuTTY
RADIUS: [Shared]

1.  Enable:                               On
2.  Primary Host/Address:                 192.168.100.126
3.  Primary Secret Word:                 (defined)
4.  Secondary Host/Address:              (undefined)
5.  Secondary Secret Word:              (undefined)
6.  Fallback Timer:                      5 Sec
7.  Fallback Local:                      On (All failures)
8.  Retries:                            3
9.  Authentication Port:                 1812
10. Accounting Port:                    1813
11. Default User Access:                On
12. OneTime Auth:                      On
13. OneTime Auth Timer:                 5
14. Debug:                             On
15. Ping Test

Enter: #<CR> to change,
      <ESC> to return to previous menu ...
```

Choose the menu option “Debug” is set to **On**.