RSA SECURID® ACCESS
Standard Agent Implementation Guide

WALLIX WAB Suite 5.0

Daniel R. Pintal, RSA Partner Engineering
Last Modified: September 21, 2016

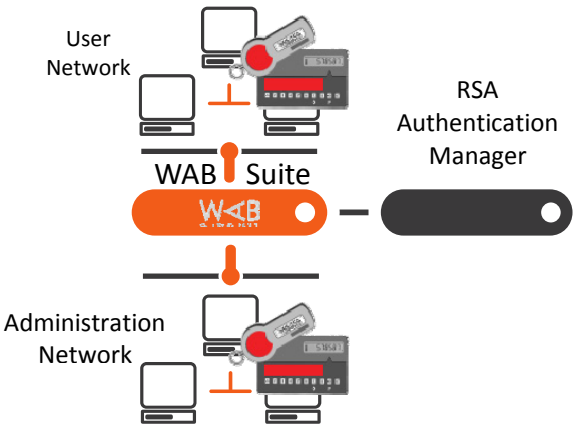
RSA READY

Solution Summary

Acting as a single gateway for privileged access to all your key systems, WALLIX DMINBASTION (WAB) Suite is an All-In-One Certified Solution comprising three key components: WAB Session Manager, WAB Password Manager and WAB Access Manager. With a short term deployment (ROI on project milestones), WAB suite platform ensures that only the right users have access to the right resources at the right time, greatly reducing the risk of security breach, while maximizing business productivity.

The WAB Suite can be configured to provide RSA SecurID two-factor authentication using the RSA Authentication Manager's RADIUS services. This allows for seamless integration with RSA SecurID authentication for WAB Suite enterprise customers who are interested in improving security by adding strong authentication to their RADIUS implementations through the RSA SecurID solution.

RSA Authentication Manager supported features	
WAB Suite 5.0	
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	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	Yes
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between the WAB Suite 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 WAB Suite and contains information about

If the WAB Suite 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

> **Important: 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 WAB Suite 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 WAB Suite components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

WALLIX WAB Suite Configuration

WAB allows you to define external authentications. These authentication methods are used to authenticate a user on WAB.

1. Select **Configuration** > **External Authentications** and click, **Add an authentication** to display the external authentication creation page.

The External Authentication creation page consists of the following fields:

- Authentication type: you must select “RADIUS”
- Authentication name: A convenient name to retrieve the authentication
- Server: IP address or hostname to connect to the RADIUS server
- Port: The default port of the RADIUS server is 1812
- Secret: This is the RADIUS Secret as set during Agent Host Configuration.

2. Create an External Authentication for every Authentication server to be used including primary and replica(s).

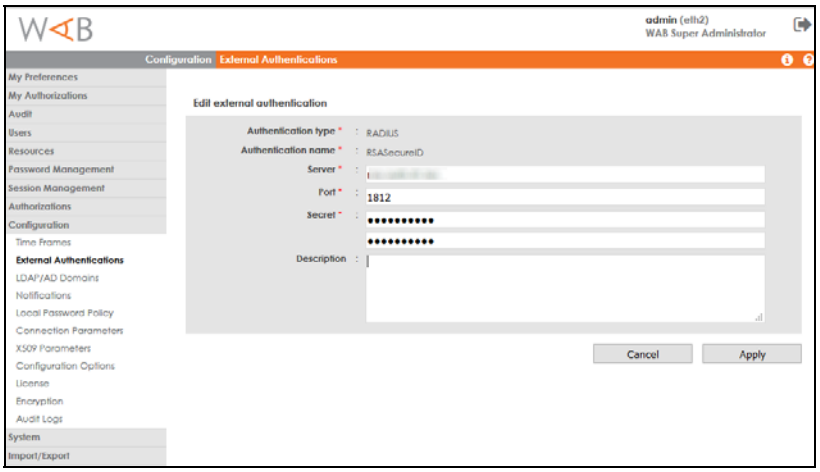


Figure 1. Edition of External Authentication

3. From the menu select **Users**> **Accounts** then select the user who is permitted use of the RSA SecurID token to identity. For each user select the related external authentication servers.

Important: Authentications will be used in the order specified until the first success.

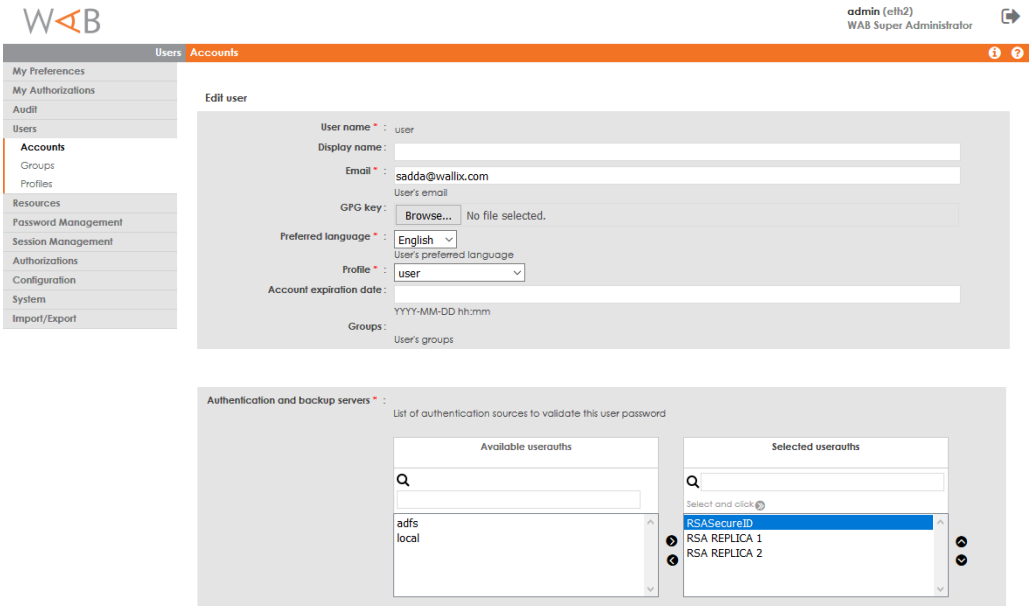
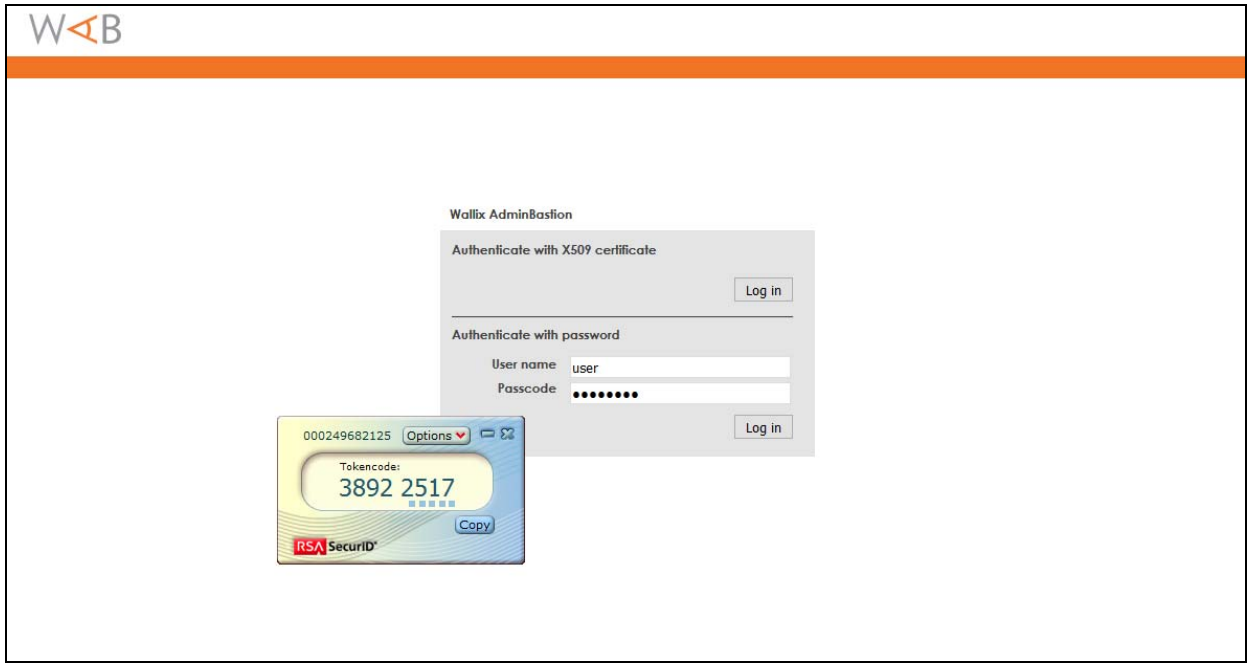


Figure 2. Selection of external authentications

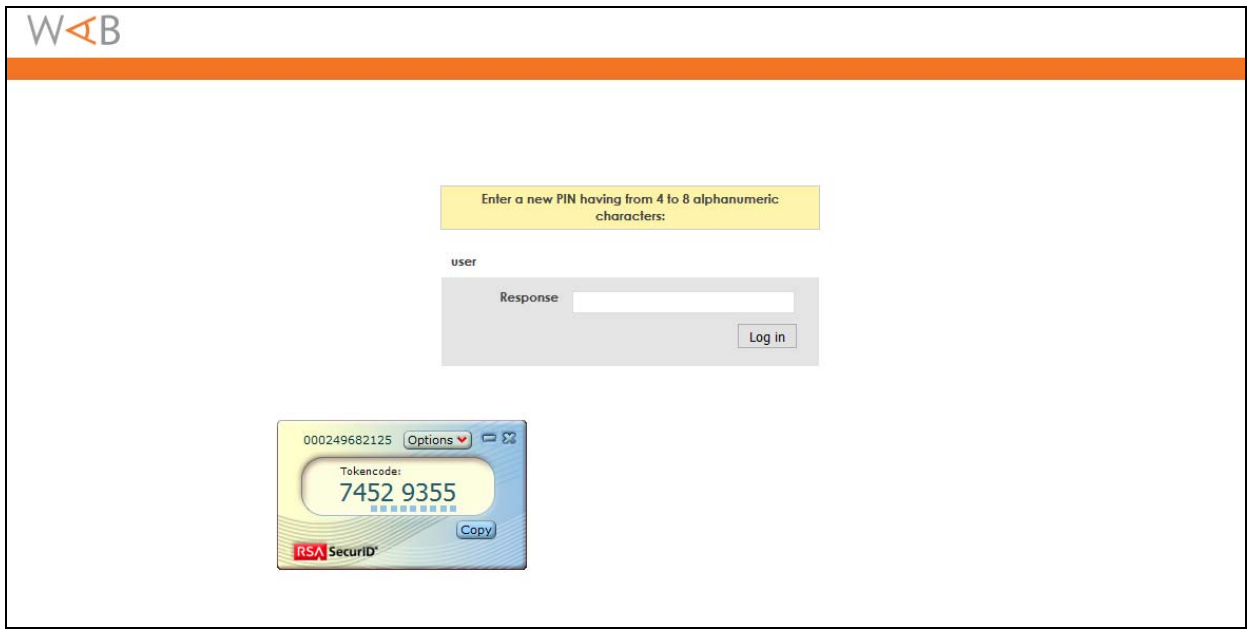
Important: If many users need to be edited, it is possible to set the authentications by importing a User CSV file from the "Import/Export / CSV" page.

RSA SecurID Login Screens

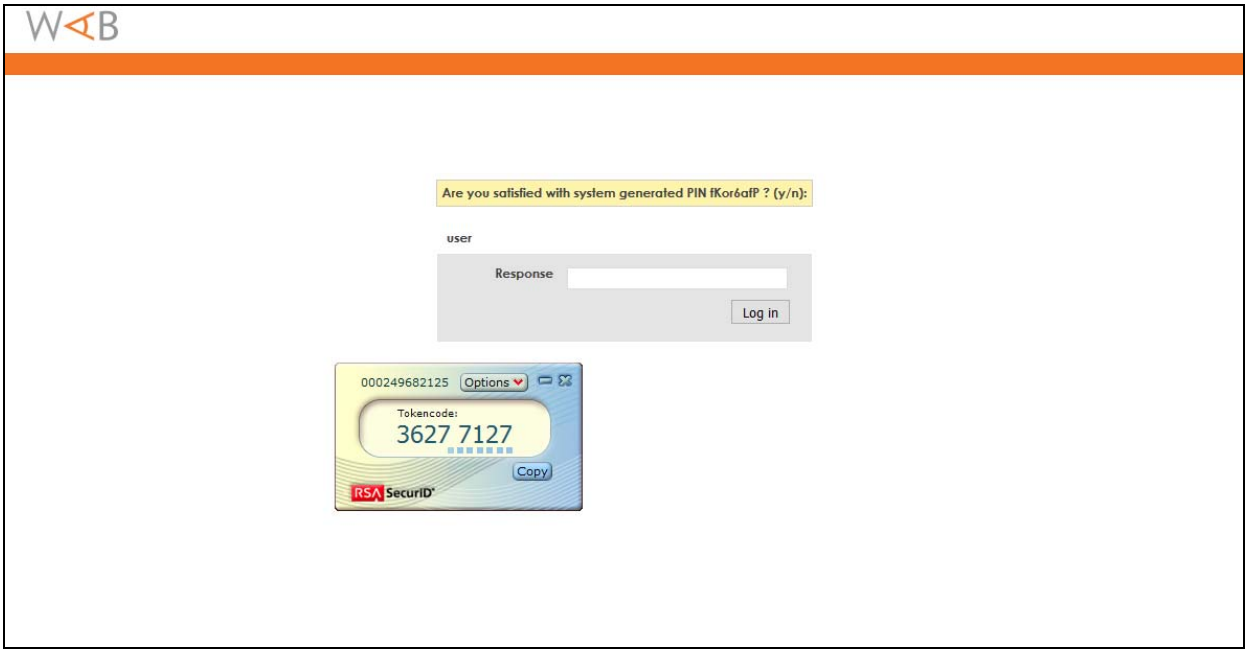
Login screen:



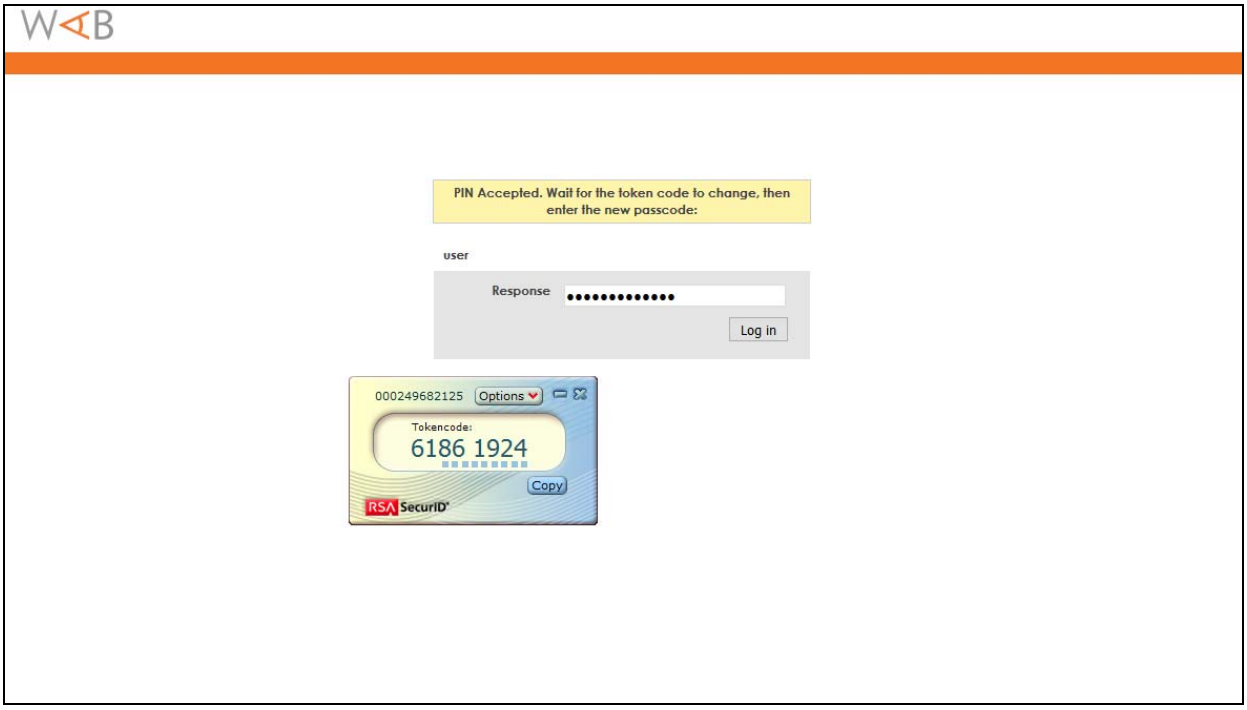
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA SecurID Access

Date Tested: September 21, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
RSA Software Token	5.0.0.292	Windows 10 x64
WAB Suite	5.0.0	

RSA SecurID Authentication

Date Tested: September 21, 2016

Mandatory Functionality	Native UDP	Native TCP	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	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

After logon failure and pin change the user is required to return to the main login screen to authenticate.