RSA SECURID® ACCESS

Standard Agent Implementation Guide

WatchGuard Fireware XTMv 11.12 Clients

Daniel R. Pintal, RSA Partner Engineering
Last Modified: December 14, 2016

RSA READY

Solution Summary

The extensible threat management (XTMv) solution provides complete security for small to large-sized regional offices. An all-in-one XTMv network security solution integrates complete protection while slashing the time and cost associated with managing multiple single-point security products. The XTMv supports RSA SecurID RADIUS authentication via Mobile VPN IPSec or SSL for secure, two-factor authentication to corporate assets.

RSA SecurID Access Supported Features	
WatchGuard Fireware XTMv 11.12	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes

RSA Software Token Supported Features	
Windows Automation	No
SID800 Automation	No
OS X Automation	No
iOS Automation	No
Android Automation	No
File-based Provisioning	No
CT-KIP Provisioning	No
CTF Provisioning	No

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the WatchGuard Fireware XTMv to provision RSA Authentication Manager resources. 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 WatchGuard Fireware XTMv components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

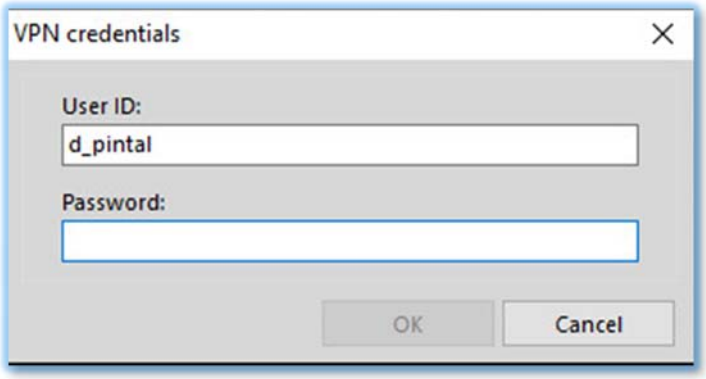
WatchGuard Fireware XTMv Configuration

Refer to the RSA Ready WatchGuard_XTM_11.12_AuthMan8_2 Implementation Guide for instructions.

Client configuration for Mobile VPN with IPSec

1. On the end user's PC install the NCP Secure Entry Client.
2. Click **Configuration** and import the end-user profile (.ini file) generated from the Fireware XTM.

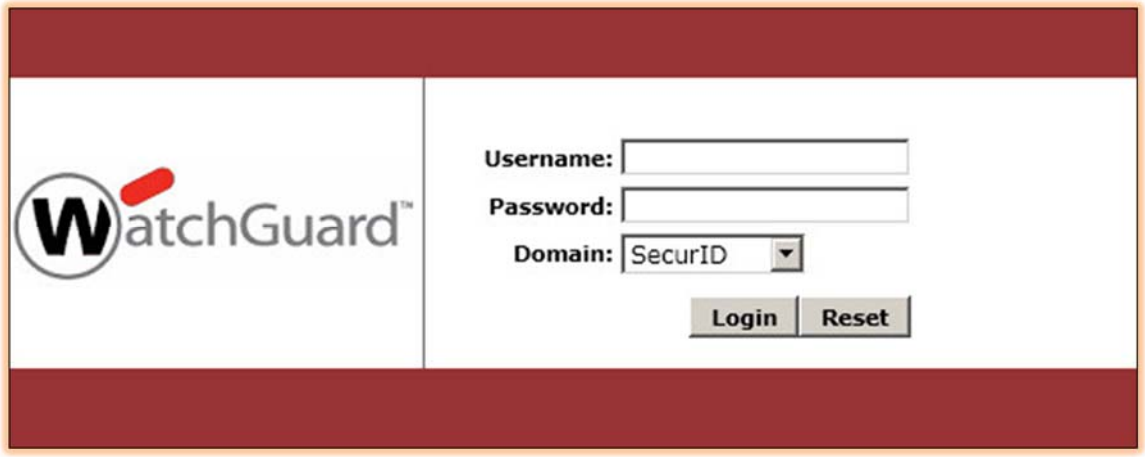
3. Click **Connection** and enter the user name and Passcode.



Screens

RSA SecurID Login Screens (Web)

Login screen:



User-defined New PIN:

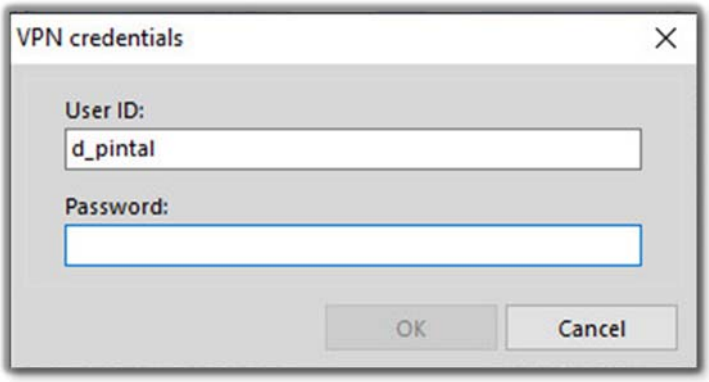
Firewall Screens (continues)

System-generated New PIN:

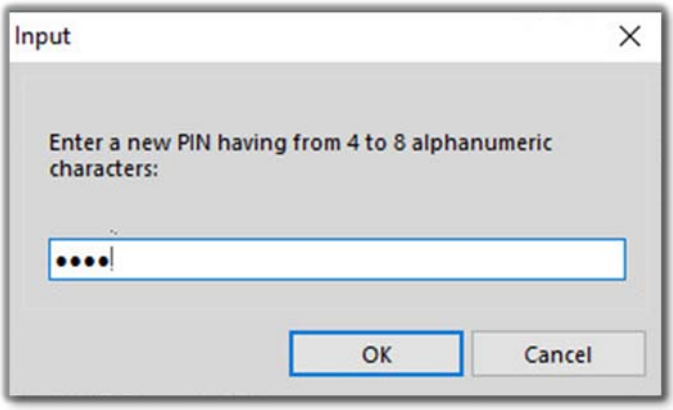
Next Tokencode:

WatchGuard Mobile VPN Desktop client

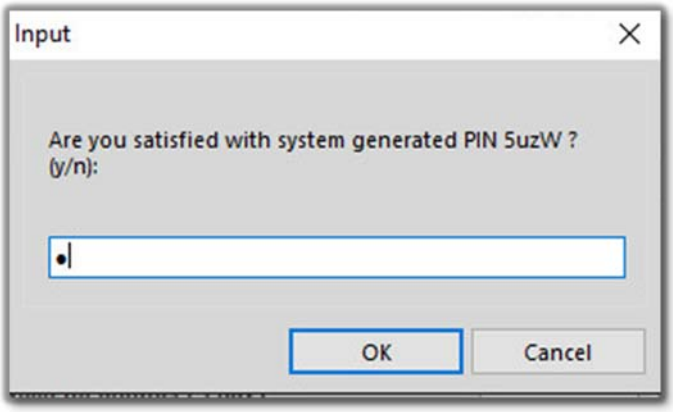
Login screen:



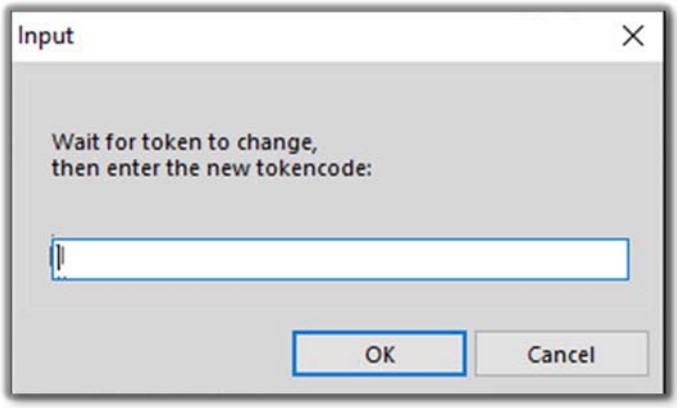
User-defined New PIN:



System-generated New PIN:



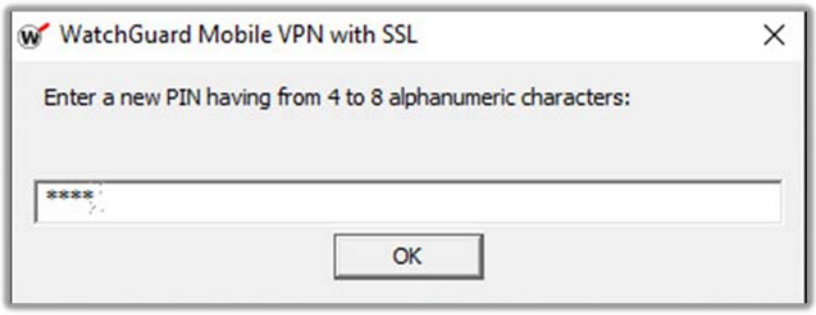
Next Tokencode:



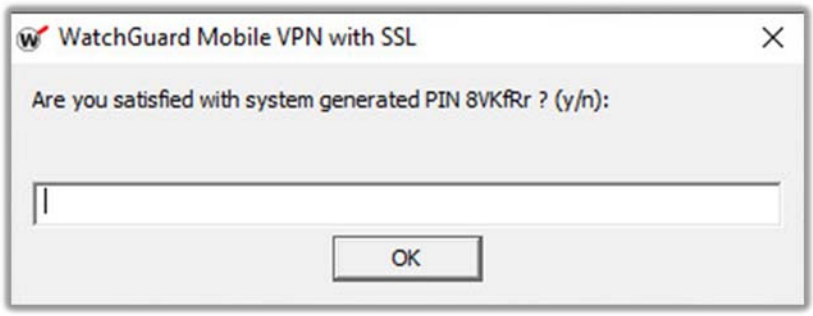
WatchGuard Mobile VPN with SSL Desktop client

Login screen:

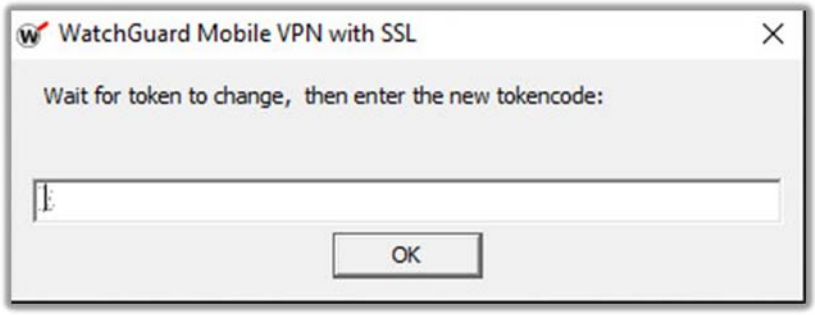
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA SecurID RADIUS Access

Date Tested: December 12, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
WatchGuard Mobile VPN with SSL	11.11.1	Windows 10
WatchGuard Mobile VPN	12.10	Windows 10

WatchGuard Mobile VPN

RSA SecurID Authentication - RADIUS

Date Tested: December 12, 2016

	Windows	OS X	Android	iOS	Other
New PIN					
Force Authentication After New PIN	✓	N/A	N/A	N/A	N/A
System-Generated PIN	✓	N/A	N/A	N/A	N/A
User Defined (4-8 Alphanumeric)	✓	N/A	N/A	N/A	N/A
User Defined (5-7 Numeric)	✓	N/A	N/A	N/A	N/A
Deny 4 and 8 Digit PIN	✓	N/A	N/A	N/A	N/A
Deny Alphanumeric PIN	✓	N/A	N/A	N/A	N/A
Deny PIN Reuse	✓	N/A	N/A	N/A	N/A
Passcode					
16-Digit Passcode	✓	N/A	N/A	N/A	N/A
4-Digit Fixed Passcode	✓	N/A	N/A	N/A	N/A
Next Tokencode Mode					
Next Tokencode Mode	✓	N/A	N/A	N/A	N/A
On-Demand Authentication					
On-Demand Authentication	✓	N/A	N/A	N/A	N/A
On-Demand New PIN	✓	N/A	N/A	N/A	N/A
Load Balancing / Reliability Testing					
Failover (3-10 Replicas)	✓	N/A	N/A	N/A	N/A
No RSA Authentication Manager	✓	N/A	N/A	N/A	N/A

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

WatchGuard Mobile VPN with SSL

RSA SecurID Authentication - RADIUS

Date Tested: December 12, 2016

	Windows	OS X	Android	iOS	Other
New PIN					
Force Authentication After New PIN	✓	N/A	N/A	N/A	N/A
System-Generated PIN	✓	N/A	N/A	N/A	N/A
User Defined (4-8 Alphanumeric)	✓	N/A	N/A	N/A	N/A
User Defined (5-7 Numeric)	✓	N/A	N/A	N/A	N/A
Deny 4 and 8 Digit PIN	✓	N/A	N/A	N/A	N/A
Deny Alphanumeric PIN	✓	N/A	N/A	N/A	N/A
Deny PIN Reuse	✓	N/A	N/A	N/A	N/A
Passcode					
16-Digit Passcode	✓	N/A	N/A	N/A	N/A
4-Digit Fixed Passcode	✓	N/A	N/A	N/A	N/A
Next Tokencode Mode					
Next Tokencode Mode	✓	N/A	N/A	N/A	N/A
On-Demand Authentication					
On-Demand Authentication	✓	N/A	N/A	N/A	N/A
On-Demand New PIN	✓	N/A	N/A	N/A	N/A
Load Balancing / Reliability Testing					
Failover (3-10 Replicas)	✓	N/A	N/A	N/A	N/A
No RSA Authentication Manager	✓	N/A	N/A	N/A	N/A

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