Bitzer Mobile Inc.

Bitzer Enterprise Application Mobility

RSA SecurID Ready Implementation Guide

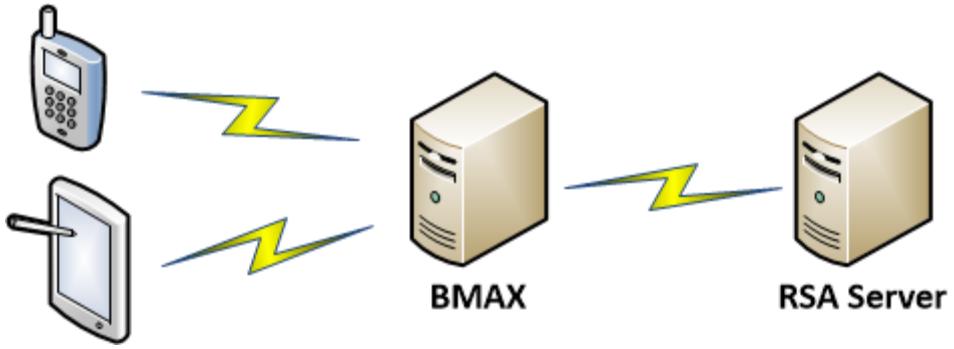
Last Modified: August 1, 2013

Partner Information

Product Information	
Partner Name	Bitzer Mobile Inc.
Web Site	www.bitzermobile.com
Product Name	Bitzer Enterprise Application Mobility (BEAM)
Version & Platform	BEAM 2.5 IOS, Android and Windows
Product Description	BEAM isolates corporate access and data from employee's personal apps on mobile devices. It extends the trust gained within an internal network out to a secure workspace on mobile devices. The user experience is similar to login at the office and allows seamless access to all authorized resources without having to set up a VPN or continuously re-authenticate.

Solution Summary

BEAM is implemented in two components, BMAX as a RADIUS client for communication to RSA server and mapping a custom protocol to Bitzer clients for the required functionality. BMAX implements the RADIUS protocol using RFC 2865 and RFC 2869. BEAM is FIPS 1402 compliant and uses its patent technology to separate Active Directory authentication and SSO without the use of constrained delegation in Active Directory.



RSA SecurID supported features	
BEAM 2.5 IOS, Android and Windows	
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

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

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 BEAM server component (BMAX) will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for BMAX to communicate with 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: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

BEAM Configuration

This section provides instructions for configuring BEAM 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.

This guide provides a summary of instructions for installing and configuring the BMAX Server with RSA RADIUS authentication.

First install and configure the BMAX server component, and then install the client using the appropriate configuration file generated by the BMAX server.

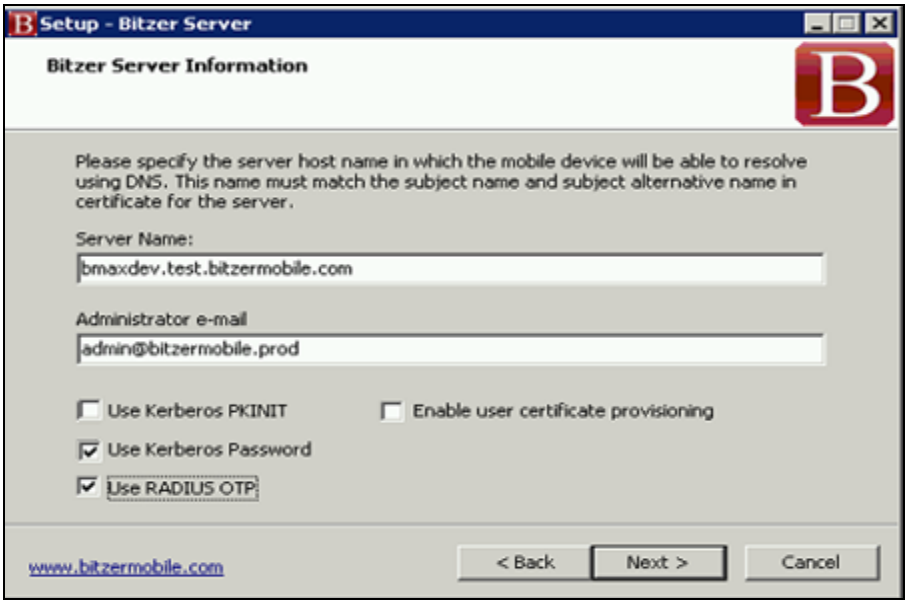
> **Note: Please reference the BMAX Gateway installation guide for the complete procedure.**

BEAM Server Component BMAX

The BMAX server component has a windows setup program provided by Bitzer Mobile. The installation setup program will allow all options to be specified in a new installation to configure the BMAX server (RADIUS client) to communicate with RSA authentication servers.

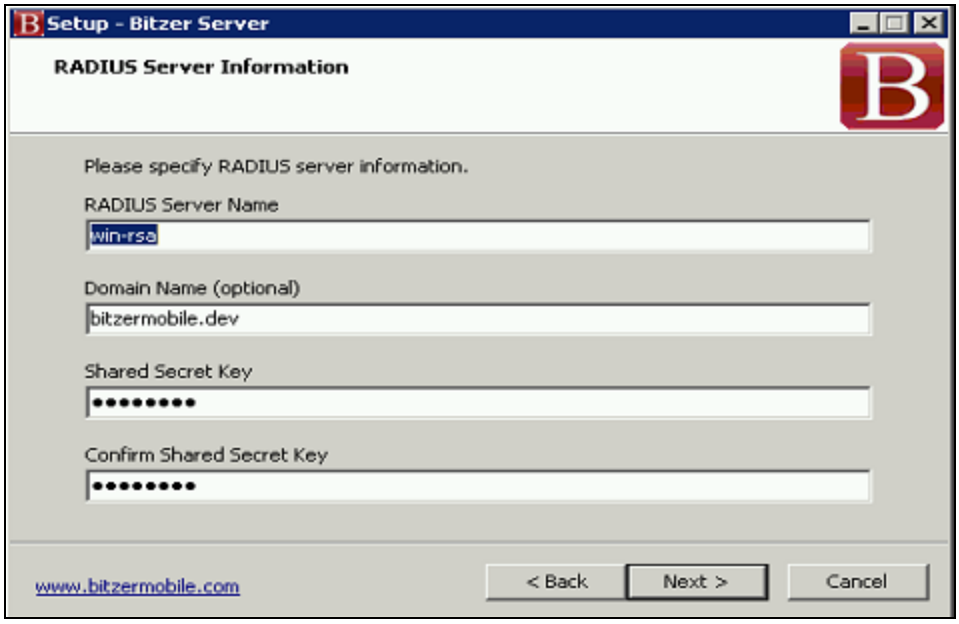
BMAX Server Information screen

During the BMAX Server installation, select **Use Kerberos Password** and **Use RADIUS OTP** to enable RSA RADIUS OTP authentication.



RADIUS Server Information screen

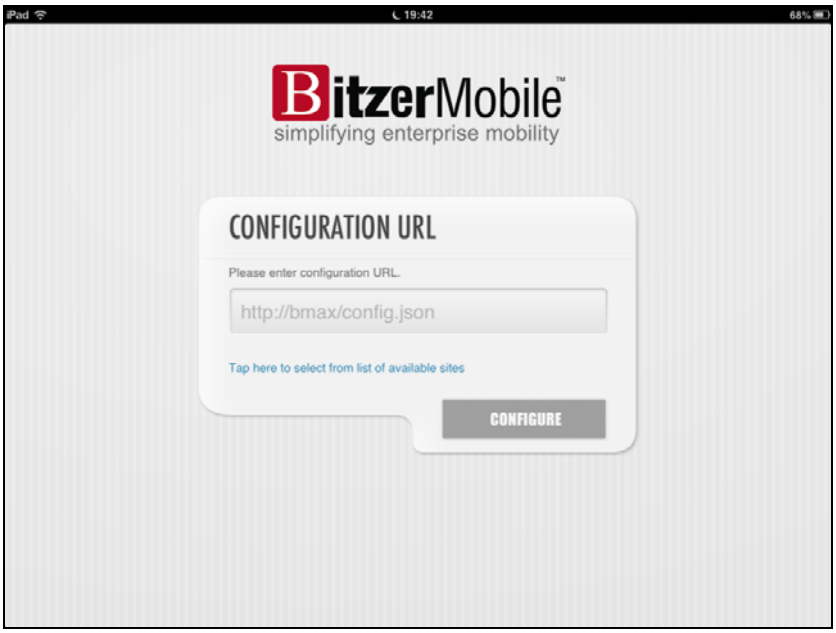
When Use RADIUS OTP authentication is selected the following screen will be shown. BMAX supports the standard RADIUS protocol as an addition to Kerberos passwords for two-factor authentication. Enter the **RADIUS Server Name**, optionally specify a default domain depending on the configuration of the RADIUS server, and select the appropriate **Shared Secret Key** for the RADIUS server.



Note: To add a secondary RADIUS Server separate names with a comma or edit the radius.conf file after installation.

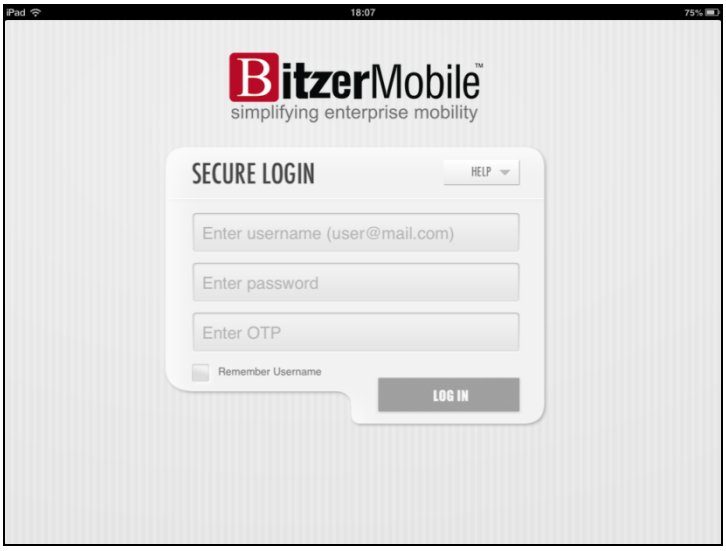
BEAM Client Component

The method for installing the BEAM client component depends on the device type. Once the Bitzer client is installed, the configuration step and behavior is the same for all devices. To configure the Bitzer mobile application on the device, enter the configuration URL that was created based upon the BMAX server installation.



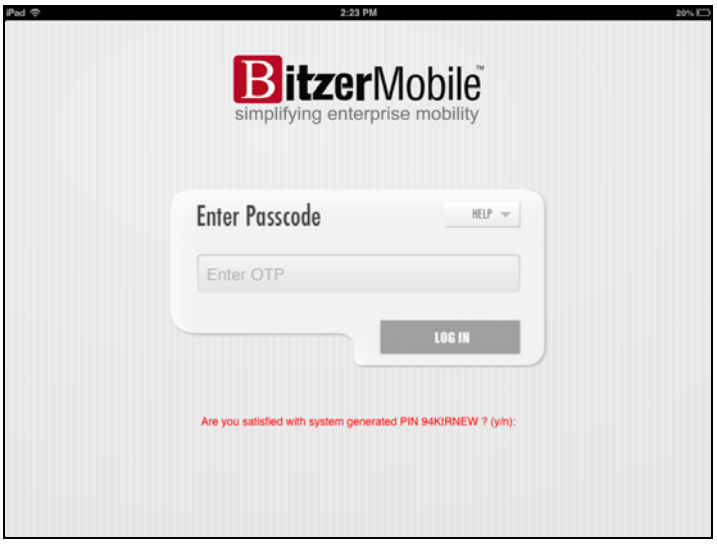
RSA SecurID Login Screens

Login screen:



User-defined New PIN:

System-generated New PIN:



Next Tokencode:

:

Certification Checklist for RSA Authentication Manager

Date Tested: August 1, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
BEAM	2.5	Windows 2008 R2
Beam Android Client	1.8.3683	Android
Beam IOS Client	2.3.2	iOS
Beam IOS Client	2.6.0	Windows

RSA SecurID Authentication – RADIUS Protocol					
	Windows	**OS X**	**Android**	**iOS**	**Other**
New PIN					
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

DRP / PAR

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