Blackberry

Contents

Overview

For Verion 2 of the Swivel Blackberry App see Blackberry 2.0.

The Swivel Mobile Phone Client allows 99 security strings or One Time Codes for PINless authentication to be stored on the Blackberry. These can be updated at any time from the client.

For Blackberry Devices of OS Version 4.5 and later a Blackberry Client app exists as described below. For earlier devices the Swivel app can be installed; please refer to the Swivlet How To Guide

There are two versions of the Blackberry Mobile Phone client one for Versions 3.8 and later and one for earlier versions.

This article covers the Blackberry client for Swivel, for other phones see Mobile Phone Client.

Prerequisites

- On the Swivel Administration Console the user must have Swivlet or Mobile Client enabled to use the Java Applet (or other Mobile Client App)

- The Swivel server must be reachable from the mobile phone to receive security strings

- The index is required to be entered as nn on the end eaxample: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

- Where SSL communications are used the server must have a valid certificate for the hostname. If a self signed certificate is used it would need to be installed on the handset.

- RADIUS authentications made against Swivel must use PAP RADIUS authentication since with other RADIUS protocols such as CHAP and MSCHAP the access device requests the OTC from Swivel.

- Virtual or hardware appliances using Swivel 3.8 may require an upgrade on their proxy to provision a mobile device, see Appliance Proxy Server Upgrade

- Swivel 3.8 requires the mobile phone to be provisioned before use, see Mobile Provision Code

Versions

Swivel Blackberry Mobile Client 1.7.1 (Awaiting App Store release, available for the Blackberry Enterprse Server as file download (see below)) 23/02/2015

- Supports Quick provision
- Requires Swivel 3.8 to 3.10

Swivel Blackberry Mobile Client 1.6 release 05/12/2013 (please note his is labelled as version 3.0)

- You can now "Get Server Settings" and provision the device using a URL from a text message
- It is possible for the server to allow users to navigate through the security strings backwards as well as forwards
- Several UI/UX improvements

Swivel Blackberry Mobile Client 1.6

- Added a "Get Server Settings" screen where users can use a 10-digit code they have been given to download the server settings
- Added server configurable ability to automatically extract otc prompting user for PIN

Swivel Configuration

Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from the Mobile Phone Client, the user must have the Mobile Client authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see RADIUS Configuration Note: The access device must be configured to use PAP for authentication.

- For Agent-XML authentication see XML Authentication Configuration

Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See Mobile Provision Code.

Mobile Client Policies

For the Server based policies see Mobile Client Policies

Installing the Client

There are a number of ways to install the client. Via Blackberry App World is the recommended approach.

All the files required for either method are available here Blackberry Software

Via Blackberry App World

After logging into the Blackberry App World search for Swivel. The version of the app created by Swivel Secure Ltd is the correct version. Install this. Updates should be managed through the App World application.

Over the air

To install the client over-the-air you need to use the browser on you blackberry device and navigate to the location of the client .jad file.

This will instigate the download and installation of the client.

You may be prompted to allow the application "trusted status". You should respond Yes to this. You do not need to edit the applications permissions.

You can place the files required to perform OTA provision on a web-server of your choosing or you can install the client from the demo site.

https://demo.swivelsecure.com/Rim/PinsafeClient.jad

If you wish to use the client with Swivel 3.7 or older, you can use a version that is backward compatible.

https://demo.swivelsecure.com/Rim/pre38/PinsafeClient.jad

When used in conjunction with pre 3.8 versions, there is no requirement to provision the client

Blackberry Desktop

It is also possible to install the application via the Blackberry Desktop software.

For this you need to extract the application. From the desktop software select import and then select the .alx file.

However the .alx file may need to be edited to reflect your device Java and OS version.

Blackberry Enterprise Server

The software for the Blackberry Enterprise can be downloaded here | Swivel BB Mobile Client 1.7.1.zip

Navigation

You can navigate either using the selectable buttons on the user-interface or the menus. Certain devices lend themselves to different methods.

To get back to the main screen from any other screen use the cancel option.

Configuration

Before you can provision the client you need to configure it.

If a SSD server is being used, then select **Get Server Settings** and enter the Server ID, otherwise the settings can be manually entered with information from the Swivel System administrator.

The manual configuration screen has the following entries:

Debug This is a message field that shows the last error encountered or action completed relating to the client attempting to connect to the Swivel server. It is a read-only field

Username As recognised by the Swivel Authentication Platform

Server The host name of the Swivel Authentication Platform as accessible by the client. **nb** No http:// or https:// prefix required.

Context The context or path the client should use on the host to me able to communicate with the platform. For virtual or hardware appliances this would be proxy by default.

Port The port the client should use on the host to me able to communicate with the platform. For virtual or hardware appliances this would be 8443 by default.

SSL Is SSL communication required. Default is yes for virtual or hardware appliances.

PINless Is the user a PINless user.

Once these settings are complete the client can be provisioned.

If using in pre version 3.8 client there will be no debug field but there will be a pre38 setting which must be selected to use the client with a pre 3.8 version.

If pre38 is set then there is no need to provision the client.

Provisioning

In order to provision the client you need to obtain a provision code. This will usually be sent to you by the administrator of your Swivel Platform or you maybe able to request one to be sent. A provision code is a 10 character code that you enter on the provision screen. Once you enter the code and select provision, the client will contact the platform and if the code is valid you device will be provisioned. See also Mobile Provision Code.

Downloading Strings

To download security strings select the refresh option.

Authentication

To authenticate using the client select the authenticate option. This will then display the security string you need to use to authenticate. Note the actual format you need to enter into the login-form is 1234nn or Swivel version prior to 3.10 1234,nn where 1234 represents your one-time code and nn represents the string index.

Troubleshooting

Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. The index is required to be entered as nn or ,nn example 2924,01 otherwise it will see it as a dual channel authentication.

If the login continues to fail, try subtracting 1 from the security string index, example for 7432,32 try 7432,31.

Error Messages

AGENT_ERROR_NO_SECURITY_STRINGS, **AGENT ERROR NO SECURITY STRINGS**

See AGENT ERROR NO SECURITY STRINGS

net.rim.device.cldc.io.ssl.TLSIOException (net.rim.device.api.crypto.tls.TLSAlertException

When configuring the Blackberry App with an SSL connection, the hostname for the Swivel servers public IP should be used rather than the IP address.

HTTP error 0 ()

Ensure that the option to use SSL is enabled if HTTPS is being used.

Known Issues

Blackberry only support HTTP and not HTTPS for the Provision URL.

Tested Mobile Phones

The following phones have been tested

Mobile Phone Compatibility

Manufacturer	Model	Version	Operator	Compatible Y/N	Client Version
Blackberry	Curve 8520	v4.2.0.135	O2	Y	1.0.1
Blackberry	Curve 8900	(Emulator)	N/A	Y	1.0.1
Blackberry	9300	v6.6.0.195	Not Known	Y	Not Known
Blackberry	9300	v6.6.0.207	Not Known	Y	Not Known
Blackberry	Torch 9810	v6	O2	Y	1.0.1
Blackberry	Q10	-	-	Y	2.0.x
Blackberry	Z10	-	-	Y	2.0.x