Java Mobile Phone Client

Contents

- 1 Swivlet How To Guide
- 2 Overview
- 3 Prerequisites
- 4 Swivel Server Configuration
    - 4.1 Configuring Swivlet User Access
    - 4.2 Configuring the Swivel Authentication
    - 4.3 Mobile Provisioning
- 5 Swivlet Installation on Phone
- 6 Swivlet Configuration on Phone
    - 6.1 Mobile Provision Code
- 7 Testing
- 8 Options
    - 8.1 Preconfiguring the Swivlet
- 9 Troubleshooting
- 10 Error Messages
- 11 Known Issues and Limitations
- 12 Tested Mobile Phones
- 13 RADIUS Considerations

Swivlet How To Guide

Overview

The Swivlet is now deprecated. The Swivlet will only work with Swivel versions up to and including 3.7. For later versions see Mobile Phone Client.

Mobile phone apps are now named *Mobile Phone Client*, the Swivlet referring explicitly to the Java Mobile Phone Client.

The Swivel Mobile Phone Client or Java Applet or Midlet, for the mobile phone allows the storage of 99 security strings or One Time Codes for PINless authentication, on a java enabled mobile phone. The PIN is not stored on the phone. Requesting a top up from the Swivel server resets all the security strings on the mobile phone, providing 99 security strings for authentication. The value of 99 security strings is fixed and cannot be changed. You can use the device to get one-time codes for Swivel login and PIN change.

Prerequisites

Swivel 3.7 or less, for later versions see Mobile Phone Client for other supported apps.

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

Security strings must be entered including the comma and sequence number e.g. nnnn,nn

Appliances using Swivel 3.8 may require an upgrade on their proxy to provision a mobile device, see Appliance Proxy Server Upgrade

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.

Swivel Server Configuration

Configuring Swivlet User Access

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

Configuring the Swivel Authentication

Swivel can authenticate users 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

Note: The access device must be configured to use PAP for authentication.

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.

Swivlet Installation on Phone

The Swivlet can be provided on a web page and deployed by the client using a web browser to download it to their phone. The Phone should detect that it is a java application and install it.

The Swivlet can be downloaded from a mobile phone here: https://demo.swivelsecure.com/provision (This is the Swivlet version 2 which includes Mobile provision support for Swivel 3.8 onwards)

Another way of provisioning the Swivlet would be by a WAP push to the mobile Phone

Swivlet Configuration on Phone

The Swivlet needs to be configured with the following information:

Server URL: The Swivel server IP or hostname

Context: The Swivel installation path (usually pinsafe or proxy)

Username: The username used for authentication

Mobile Provision Code

Swivel versions 3.8 and higher require each Mobile device to be Provisioned with a Code sent from the Swivel server. To provision a phone see Mobile Provision Code. Swivel versions earlier than Swivel 3.8 do not need to be provisioned.

Testing

You can top up the Swivlet and you should see a log message saying strings requested for user XXXX or *security strings fetched for user: XXXX*

Options

Preconfiguring the Swivlet

You may need to edit the .jad file as this indicates to the browser where to get the .jar file

(see MIDlet-Jar-URL:https://demo.swivelsecure.com/provision/Swiveler.jar).

The .jad file is also available here: PinsafeClient.jad

You can also edit the .jad file to preconfigure the client

Pinsafe-Context: /pinsafe

Pinsafe-URL: http://demo.swivelsecure.com:8080

Pinsafe-Username: yourUsername

```
L10N-Bundle: com.swiveltechnologies.l10n.bundle.Bundle_en_US
L18N-Bundle: com.swiveltechnologies.l18n.bundle.Bundle_en_US
MIDlet-1: Swivlet 2,,com.swiveltechnologies.Swivlet2
MIDlet-Jar-Size: 58140
MIDlet-Jar-URL:https://demo.swivelsecure.com/provision/Swiveler.jar
MIDlet-Name: Swivlet2
MIDlet-Vendor: Swivel Technologies
MIDlet-Version: 2.1.0
Main-Menu: com.swiveltechnologies.ui.menu.Remote
MicroEdition-Configuration: CLDC-1.0
MicroEdition-Profile: MIDP-1.0
One-Time-Code-Render: com.swiveltechnologies.render.otc.Standard
Pin-Change-Render: com.swiveltechnologies.render.otc.StandardPinChange
Pinsafe-Context: /pinsafe
Pinsafe-URL: http://demo.swivelsecure.com:8080
Pinsafe-Username: yourUsername
Provision-Type: com.swiveltechnologies.provision.type.Remote
Security-String-Generator: com.swiveltechnologies.generate.ss.Remote
```

Troubleshooting

Is the Swivel server accessible on the internet

Check the connection settings to the Swivel server

Check the Swivel logs for any error messages

Can the phone access the internet

Does the Swivel applet application have authorisation to access the network connection

Can the phone use self signed certificates if a https connection is being used

If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP

Download new security strings to the phone and retest

If the proxy port (8443) on the appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.

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 example 2924,01 otherwise it will see it as a dual channel authentication.

Error Messages

903 Loss of service HTTP error 400: bad request

The JAD file references http and needs to be changed to https

SwivletException : SE007: java.io. IO exception:-5120

This error message has been seen with an incorrectly configured DNS entry

com.swiveltechnologies.SwivletException: SE007: javax.microedition.io.ConnectionNotFoundException: Protocol not found: net.rim.device.cldc.io.http.Protocol

This message has been seen when using a blackberry with the Java Mobile Phone Applet without Internet access enabled for the applet. To enable internet access to the Swivlet, select Options, then security, then Application Permissions, select the Swivlet application then press the blackberry button and configure the options available to the applet.

Com.swiveltechnologies.SwivletException:SE007:java.io.IOException:Timed out

This error message has been seen on a Blackberry Swivlet that cannot connect to the Swivel server. Check network settings, and if the application is allowed access to the internet.

Com.swiveltechnologies.SwivletException:SE005:java.io.IOException:Timed out

This error message has been seen on a Blackberry Swivlet where the context has been incorrectly configured.

Com.swiveltechnologies.SwivletException:SE005:java.io.IOException:Failed to transmit

This has been seen on a Blackberry Swivlet where the security strings may already be at 99. Try using one and then requesting new strings.

Requesting Please wait..., 0 to 10 displayed repeatedly then Com.swiveltechnologies.SwivletException:SE007:java.io.InterruptedIOException:Local connection timed out after # 120000

This has been seen on a Blackberry swivlet where the swivlet cannot connect to the Swivel server, check network connectivity.

com.swiveltechnologies.SwiveletException:SE007:

javax.microedition.pki.CertificateException:Certificate failed verification

The Swivel Swivlet is unable to validate the certificate installed on the Swivel server from which the security strings are to be downloaded.

AGENT_ERROR_NO_SECURITY_STRINGS, **AGENT ERROR NO SECURITY STRINGS**

The OTC is being entered without the ,nn at the end of the OTC, whereby nn is the number given with the security string

Known Issues and Limitations

The current version only supports one device per user.

Tested Mobile Phones

As more information is fed back additional phones will be added here. Note that the operator may not supply Java run time environments so we have listed the operator as well.

Mobile Phone Compatibility

Manufacturer	Model	Version	Operator	Compatible Y/N	Swivlet Version
Blackberry	8520	v4.2.0.135	Not Known	Y	Not Known
Blackberry	8820	v4.2.2.175	Orange UK	Y	Not Known
Blackberry	9300	v6.6.0.195	Not Known	Y	Not Known
Blackberry	9300	v6.6.0.207	Not Known	Y	Not Known

Nokia	E52	Not Known	Not Known	Y	Not Known
Nokia	E71	Not Known	Not Known	Y	Not Known

RADIUS Considerations

One thing to be aware of is that when using RADIUS authentication, except for the PAP protocol, you must use every string from the phone for authentication. If you generate a string and don't use it, authentication will fail until you Top Up again. This is an unavoidable consequence of the way most RADIUS protocols work.