Windows Mobile How To Guide

Contents

Windows Mobile How To Guide

Overview

NOTE: this version is for Windows Mobile versions 6.x and earlier. For Windows Phone 7.x, see Windows Phone 7 How To Guide.

The Windows Mobile Swivel application, for the Windows Mobile phone allows the storage of 100 security strings or One Time Codes for PINless authentication on a .Net 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. You can use the device to get one-time codes for Swivel login and PIN change.

For the Mobile Phone Clients such as the Java based version select Swivlet How To Guide. For other phones see Mobile Phone Client.

Prerequisites

User must have Mobile Phone Client or Swivlet enabled to use this application

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

This application is not compatible with Swivel 3.8 or later

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.

Mobile App Store versions

- "Swivel Mobile Client" which is compatible with Windows 8 phones but not Windows 7 phones.
- "Swivel" which is compatible with Windows 7 phones but not Windows 8 phones.
- "Swivel Mobile" which is compatible with Windows 8 phone only and not a Windows 7 phone.

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

Windows Mobile Installation

To install it, you need either ActiveSync or Windows Mobile Device Centre installed on your computer (the latter is for Vista and Windows 7). Attach the mobile device to your computer, and copy the attached .cab file to it. Execute the cab file to install the Mobile Phone Client. You can remove the cab file once it is installed.

The first time this application is used, it must be configured with the details of the Swivel server. 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 by choosing the Configuration. Your administrator will provide you with these.

Once the Swivel server details are configured, for Swivel version 3.8 or later, you must provision your phone before you can request security strings. Press **Provision** to provision this phone with the Swivel server. You will need to request a provision code from your helpdesk, which must be used immediately. The code will be sent either to your phone as an SMS, or via email, depending on how your Swivel server is configured. Provisioning is not necessary for versions of Swivel earlier than 3.8.

Set the configuration as appropriate (note that the Swivel server must be publicly visible for the Mobile Phone Client to work, or else the phone must be able to access the Swivel server via the internal network). Once the device is configured, select the Top Up option to download 100 security strings to the phone. The phone doesn't need access to the Swivel server again until it runs out of strings and you need to Top Up again.

The **Beta** version of the software can be downloaded here: http://www.swivelsecure.com/userfiles/File/software/beta/SwivletDeploy.zip

Testing

You can top up the Mobile Phone Client and you should see a log message saying strings requested for user XXXX.

Send a user a provision code, the following should be displayed in the Swivel logs:

User "username" can now reprovision their mobile device

The user has been sent a provision code to provision their mobile client

User "username" provisioned successfully

The user has successfully provisioned their Mobile Phone Client, this message is displayed in the Swivel Administration console log.

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 virtual or hardware 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 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.

Known Issues

If you have a self-signed certificate - even if you check the box to use a self signed certificate it will ignore this setting due to a problem with the .NET framework.

Error Messages

Mobile request from unprovisioned device; the user username needs to complete the reprovision process

Security strings are being requested by an unprovisioned device. The user needs to provision the Mobile Phone Client.

User "username" provision failed, A valid session could not be loaded or created for the user

The provisioning of the Mobile Phone Client has failed, either an incorrect provision code was used or the provision code has timed out.

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

AGENT_ERROR_SESSION

Provisioning of Mobile Phone Client attempted without Provision code. Ensure user attempts with a valid provision code.

NOT FOUND

Provisioning error, this is displayed in the Swivel Windows Mobile Phone Client version 1.0 and is resolved by upgrading to version 1.2 or higher.

Tested Mobile Phones

As more information is fed back additional phones will be added here.

Mobile Phone Compatibility

Manufacturer	Model	Version	Windows Mobile Version	Operator	Compatible Y/N	.Net Applet Version
Samsung	Omnia	Not Known	6.5	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.