PuTTY for Symbian OS User's Guide

Table of Contents

Legal Notice ... 3
1 Introduction ... 4
2 Installation ... 5
2.1 9200 Communicator Series ... 5
2.2 Series 60 ... 5
3 Basic Usage ... 6
3.1 Common Usage ... 6
3.2 9200 Communicator Series ... 6
3.3 Series 60 ... 7
4 Settings ... 8
4.1 Common Settings ... 8
4.2 Settings Files ... 9
5 Public-key Authentication ... 11
5.1 Creating Keys ... 11
5.2 Configuring PuTTY ... 11
5.3 Troubleshooting ... 11
6 Troubleshooting ... 13
6.1 General Problems ... 13
6.1.1 Delete \system\apps\putty\defaults ... 13
6.2 Network problems ... 13
6.2.1 Try a Different Access Point or Service Provider ... 13
6.2.2 Try Connecting from a Computer ... 13
6.2.3 Enable logging ... 13
References ... 14

Legal Notice

PuTTY for Symbian OS is free software, and comes with no warranty. Some PuTTY distribution packages are cryptographically signed. The signatures do not indicate any additional warranties or guarantees, they simply act as further proof that the packages originate from their original authors.

1 Introduction

This document is a brief user's guide for PuTTY for Symbian OS. It describes PuTTY installation, basic usage, configuration, and public key authentication support. In addition, the last chapter lists some troubleshooting hints in case PuTTY does not work.

The document assumes that you are familiar with SSH concepts and have used SSH on other platforms before. In addition, you should be familiar with the Symbian OS phone you use, including using the system applications and installing new ones.

There is plenty of documentation on SSH protocols and applications available on the Internet. You should also check with your server's system administration for any local guides you might have. You can also check Barrett's and Silverman's book [BaSi01].

2 Installation

This chapter documents the PuTTY installation procedure. It follows standard Symbian conventions, so readers familiar with Symbian OS application installation can skip to the next chapter.

Important security note: As an SSH client, PuTTY is security-critical software. To ensure that the copy you are installing has not been tampered with, always check the package signatures before proceeding. For the 9200 Communicator series, the installation .SIS packages are signed themselves, so after installing the certificates on your device, the system will check the signatures automatically. For Series 60, use PGP or GnuPG to check the PGP signatures before installing.

2.1 9200 Communicator Series

PuTTY installation packages for the 9200 Communicator Series are signed with a self-signed certificate. To be able to verify the packages, you'll need to install the certificate to the device. The steps needed are:

1. Fetch the certificate from http://www.s2.org/~pekangas/petteri_kangaslampi_2004.cer.zip and unzip it.
2. Verify the certificate. Its MD5 sum is `0493d8fc479dc444d4cdbd52ebf7162c`. A PGP signature is available at http://www.s2.org/~pekangas/petteri_kangaslampi_2004.asc, the key is http://www.s2.org/~pekangas/pekangas.public.asc. The key is also available at the MIT keyserver, http://pgp.mit.edu/ (ID 2A5111C9).
3. Copy the certificate to a file in the communicator.
4. Open Certificate manager from the communicator's Control panel.
5. Select "Add" and choose the file
6. Select the certificate from the list, select "View details", select "Trust settings" and enable "Software installation"

After installing the certificate, install the .SIS package normally. The 9200 Communicator versions are distributed in files named `putty_9200_`*`version`*`.sis`. Download the version you want, unzip the file, and transfer the .SIS package from the archive to your Communicator. You can then install the package by opening it from Messaging or using the File Manager. After installation, a PuTTY icon will be visible in the Extras menu.

2.2 Series 60

Installation packages for Series 60 are not signed by themselves, so you'll need to use the respective PGP signatures to verify their authentity. The packages are signed with the PGP key available http://www.s2.org/~pekangas/pekangas.public.asc and at the MIT key server, http://pgp.mit.edu/ (ID 2A5111C9).

Series 60 releases are distributed in files named `putty_s60_`*`version`*`.zip`. Download the version you want, verify its PGP signature, unzip the file, and transfer the .SIS package from the archive to your phone. You can then install the package by opening it from the Messages Inbox. After the file has been installed, reboot the phone by switching it off and back on again.

3 Basic Usage

This chapter documents basic PuTTY usage, including starting the application, connecting to a server, and exiting the software. Section 3.1 discusses common use on all platforms, section 3.2 covers issues specific to the Nokia 9200 Communicator series, and section 3.3 repeats this for Series 60.

Important security note: PuTTY for Symbian OS uses the SSH 1 protocol by default due to performance reasons. SSH 1 is vulnerable to man-in-the-middle attacks if new or changed host keys are accepted without verifying them. Therefore it is very important to **verify all new or changed host keys** before accepting them. Otherwise the connection security may be compromised.

3.1 Common Usage

Start PuTTY normally. When you run PuTTY for the first time, it will initialize its random number generator with noise recorded from the microphone. You can place the device close to a noise source, but even normal background noise should have more than enough randomness for this. PuTTY will continue to generate more randomness from keypresses and other events as it is used, but you can repeat the initialization process by selecting “Initialize random number generator” from the menu.

To connect, select “Connect” from the menu or a command button. Type in the name or IP address for the computer you wish to connect to, and select “OK”. On Series 60 you can change to a non-standard port at the same window. On a 9200 Communicator use the Settings window.

Next PuTTY will prompt you to select the internet connection or access point to use. Note that PuTTY requires a full internet connection or an internet access point, a **WAP-only access point will not work**. This is especially important on Series 60 and GPRS, since most operators use a separate access point for WAP and internet access, and typically advertise the settings for their WAP access point only.

After the network connection is established, PuTTY will connect to the SSH server. If you use SSH protocol version 2, this can take up to a couple of minutes. Be patient!

Some common error messages you may encounter are listed in Table 1.

Host name lookup failed	The server you tried to connect to cannot be found. Check that you typed the host name correctly, and that you are not using a WAP-only access point.
Socket connect failed: Could not connect	PuTTY could not connect to the SSH server. This error typically occurs when an SSH server is not running in the target host, or it is running in a different port. Check that the host name is correct and verify that the server is not running in a non-standard port.
Socket connect failed: Timed out	PuTTY could not connect to the SSH server. This error typically occurs when trying to use a WAP-only access point.

Table 1 Common connection errors

When connecting to a server for the first time, PuTTY will prompt you to verify and accept the server host key. **It is important to verify the key is correct**, otherwise connection security may be compromised. After verifying the key, select “Accept and Save” to save the key for future use, “Accept Once” to use it for this session only, or “Reject” if you cannot verify the key.

When the server identity has been verified, PuTTY will prompt you for your username and password. After this is done, the SSH connection will be open and you can start using the server.

3.2 9200 Communicator Series

Since the 9200 Communicator devices have a full keyboard, using PuTTY is straightforward. All keys on the keyboard send the characters printed on the labels, and the `Ctrl` key works directly. Some special characters not available on all language versions of the Communicator keyboard are

available in the `Tools` menu, and the `Chr` key opens the system character selection window. Note that the vertical bar symbol available in the character selection window is not the same as the Unix pipe character. To send the pipe, press `Shift+Ctrl+P` or select `Tools/Send Character/Pipe` from the menu.

The Communicator version supports two different fonts, small and large, and an optional full-screen mode. These can be changed from the `View` menu. In most cases, using large font and full-screen mode gives the best user experience. The default is small font and partial screen mode, as this results in a standard 80x24 character terminal window. The other combinations are listed in Table 2.

Font	***Display***	***Terminal***
Small	Partial screen	80x24
Small	Full-screen	106x25
Large	Partial screen	74x14
Large	Full-screen	91x14

Table 2 Communicator display modes and font sizes

3.3 Series 60

Since Series 60 devices do not have a full keyboard, text cannot be typed directly. The number keys simply transmit the numbers printed on the keys, while the four-way selector sends cursor keys when moved and `Enter` when pressed. Use `Send/Text` and `Send/Line` from the menu to send a line followed by a newline, or text without a newline. You can use the normal predictive text input features in your phone. Use the other selections in the `Send` to send a number of special keys not available otherwise, or `Ctrl+key` and `Alt+key` combinations.

The Series 60 version supports a number of different fonts that can be selected from the `Settings/Screen font` menu. The `Settings/Toggle full screen` menu item enables or disables full-screen mode, while `Settings/Toggle inverse screen` toggless reverse video support (white text on black background).

4 Settings

PuTTY for Symbian OS has a number of different settings that affect the behaviour of the application. While the default values should work fine for most users, using PuTTY can be more convenient and more efficient if the settings are customized for each users' needs. This chapter documents the settings available in the user interface, describes how settings can be saved and restored, and gives some hints on using settings efficiently.

4.1 Common Settings

Most of the settings are common for all PuTTY versions. Table 3 lists the settings, their locations in the user interface, and gives a brief description for each setting. The 9200 Communicator UI locations are relative to the Settings dialog in the Settings menu, while the Series 60 locations are from the

Name	9200 UI	Series 60 UI	Description
User name	`Authentication / Username`	`Authentication / Username`	The user name to use for SSH authentication. If you set the user name here, PuTTY will not prompt for it when connecting.
Private key file	`Authentication / Private Key File`	`Authentication / Private key file`	Private key for public key authentication. See chapter FIXME for more information on public key authentication.
Host name	`Connection / Host`	`Connection / Host:port`	The server to connect to.
Port	`Connection / Port`	`Connection / Host:port`	The TCP port to use. Note that PuTTY always uses the SSH protocol, regardless of the port. The default value, 22, should be valid for all common configurations.
SSH version	`Connection / SSH Version`	`Connection / Protocol version`	The SSH protocol version to use. SSH versions 1 and 2 are supported. By default PuTTY uses SSH 1 if available, and SSH 2 otherwise. SSH 2 is more secure, but makes connecting much slower.
Log type	`Logging / Log Type`	`Log parameters / Log type`	Logging type. In normal use the type should be set to “no logging”. For troubleshooting and debugging information set the type to “SSH data & debug”.
Log file	`Logging / Log File`	`Log parameters / Log file`	The log file. The logging information defined above is written to this file. Logging is mainly used for development and debugging, but it can be useful for troubleshooting any connection problems. The log file may contain sensitive information, such as passwords.
Full-screen mode	`View Menu / Full Screen`	`Toggle full screen`	Full-screen mode. In full-screen mode only the terminal window is visible.
Screen font	`View Menu / Large Font`	`Screen font`	The font in use. Using a larger font make the text bigger, but reduces the amount of text that the terminal window can hold. The 9200 version only supports two fonts, large and small terminal font, while the Series 60 version has a number of different fonts available.
Reverse video mode	*Not Available*	`Toggle inverse video`	In reverse video mode PuTTY uses white text on black background. The default is black on white.

Table 3 PuTTY Settings

4.2 Settings Files

By default PuTTY settings only apply to the current session. If you wish to create settings only once, and use the same settings in future sessions, you'll need to save the settings to a file, or save them as the PuTTY default settings.

Select `Save settings` from the `Settings` or `Settings and Tools` menu to save the current settings to a file, and `Load settings` to load settings from a file to PuTTY. All settings listed in able

Table 3 are saved and loaded. Use `Save as default` to save the current settings as the default. These settings will then be loaded automatically each time PuTTY starts. `Reset to (original) defaults` will reset the current settings back to original PuTTY defaults. This can be useful if you accidentally alter some setting that causes problems.

Tip: If you typically connect to the same SSH server all the time, set your user name and the server host name in the settings, and save those as defaults. This makes connecting much more convenient, especially on Series 60.

Second tip: PuTTY has a recognizer module for settings files. This means that you can start PuTTY with the settings you want by simply opening a settings file from a file manager or other application. On the 9200 Communicator you can also create shortcuts by selecting the appropriate settings file in the system File Manager and choosing `Add to Desk` from the `File` menu. If you routinely use a number of different SSH servers, creating separate settings for each and adding those to the Desk can make life much easier.

5 Public-key Authentication

Like all modern SSH clients, PuTTY for Symbian OS supports public-key authentication in addition to basic passwords. This chapter describes how to create suitable key pairs, and how to configure PuTTY for public-key authentication. This document does not discuss SSH server configuration, so you should make sure you can set up public-key authentication with the server you use before attempting to use it with a mobile terminal. Note that OpenSSH and SSH Tectia Server from SSH Communications Security use a different configuration syntax. See [SSH04] and [OpenSSH04] for more information on server configuration.

5.1 Creating Keys

PuTTY for Symbian OS can only use key files created with PuTTYgen on a PC. PuTTYgen ships with PuTTY for Windows, and is available for download at the PuTTY web page [PuTTY04]. If you do not have it installed, download the latest version, verify its authentity, and install it.

To create a key pair, start PuTTYgen, and configure it as follows:

Type of key to generate: **SSH1 (RSA)**
Number of bits in a generated key: **1024**

Select `Generate` to create the key and move your mouse cursor around the window to generate random numbers for the generator.

After the key has been created, PuTTYGen will prompt you to set a key comment and optionally a passphrase. The key comment should be a short description for the key, such as `Joe@6600`. Setting a passphrase for the key will make it more secure, since the key cannot be used without knowing the passphrase, but entering long passphrases can be inconvenient on a mobile phone. If you are confident you can keep your phone secure, using a public key without a passphrase can make using PuTTY much easier.

After setting the comment and passphrase, use `Save public key` and `Save private key` to save the public and private parts of the keypair to files. Transfer the private key file to your phone, using PC Suite, a memory card reader, or some other mechanism, and note the directory where it is stored. Transfer the public key to your SSH server, and configure the server to accept connections with that key.

It's a good idea to configure PuTTY for Windows to use the same private key, and verify that you can connect using the key, before attempting to use the key from a mobile phone.

5.2 Configuring PuTTY

If you created your SSH keys following the instructions in section 5.1, and have configured your SSH server correctly, configuring PuTTY to use the keys for authentication is simple. Simply select `Settings and tools / Authentication / Private key file` on Series 60 or `Settings / Settings / Authentication / Provate Key File` on a Communicator and choose the private key file you just created. When you now connect to a server, PuTTY will first attempt to authenticate using the key. If you still get prompted for a password, public key authentication failed for some reason.

When you have public key authentication working, it's a good idea to save the settings as the default values for future use. Simply select the private key file as before, and select `Save as defaults` from the settings menu. All future connection attempts will now use public key authentication.

5.3 Troubleshooting

SSH public key authentication can fail for several different reasons. The most common problems are incorrect key file formats, server configuration problems, and protocol mismatches. This section lists some useful troubleshooting tips.

File format problems: PuTTY only works reliably with private key files created with PuTTYgen. If you wish to use an existing key created with other tools, you can try to convert the key to PuTTY format using PuTTYgen on Windows.

Server configuration: Ensure that you have configured the server correctly, and check that you can connect from a PC using the same key. Note that OpenSSH and SSH Tectia Server from SSH Communications Security use a different configuration syntax.

Protocol mismatches: SSH protocol versions 1 and 2 use different keys. If you created a SSH 1 key, as instructed in section 5.1, make sure that the preferred SSH protocol version is set to `SSH 1`, and that the server supports SSH 1. Some new SSH servers only support SSH 2 by default.

In general, the first thing to do when public key authentication fails is to enable logging from PuTTY. Set a log file, set logging type to `SSH data & debug`, try to connect, and see what information gets written to the log file. The log files are plain text files, and can be viewed with Notepad or any other text editor on a PC. A couple of hints:

- If the log file doesn' t contain the line `Trying public key "key_file_name"`, PuTTY didn't even attempt to use public-key authentication, and something is most likely wrong with your key.
- If you see a message "`Server refused our public key`" on the user interface, or a packet of type 15 (`SSH1_SMSG_FAILURE`) in the log as a response to the private key, the server did not accept the key, and most likely the server configuration is wrong.

6 Troubleshooting

In general PuTTY tends to either work without problems or not work at all with a given configuration. However, there are some things that may help, and this section lists a few tricks to try. The most up-to-date version of these troubleshooting tips are available on the PuTTY for Symbian OS WWW pages [S2PuTTY04].

Unless separately noted these tips apply to all PuTTY for Symbian OS versions. Many of the tricks require a more advanced file manager application than the one shipped with the device. Remember also that directly manipulating files in the system directory can be dangerous and lead to problems, so proceed at your own risk and remember to back up your data!

6.1 General Problems

6.1.1 Delete \system\apps\putty\defaults

Sometimes PuTTY may fail to start because the default configuration file is corrupted. The easiest fix is to delete the file. It is located in `\system\apps\putty\defaults`, on the drive where PuTTY was installed (`C:` for internal memory, `D:` for memory card on the 9200 Communicator series, `E:` for memory card on Series 60).

If this helps, and you can figure out what you did when the configuration file got corrupted, please file a new bug report with instructions on how to reproduce the problem..

6.2 Network problems

6.2.1 Try a Different Access Point or Service Provider

If PuTTY starts and a network connection is set up, but the SSH connection does not open (no username or password prompt), there may be a problem in the access point or dialup server you use. Some operators, for example, disable SSH access from some of their GPRS access points. If this happens, try using a different access point (GPRS, Series 60) or dialup server (CSD or HSCSD).

Note that PuTTY needs an "internet" access point to work. Many operators have different GPRS access points for WAP use, but those can only be used to connect to the operators' WAP gateway. Those access points won't work. If unsure, ask your operator what access point to use for internet connections from a PC.

6.2.2 Try Connecting from a Computer

If the SSH connection still fails, try using the phone as a modem and connecting from a PC using the same dialup server or GPRS access point. If that fails, the problem is most likely that the access point or dialup server does not let SSH traffic through, and there is nothing PuTTY can do about it.

6.2.3 Enable logging

PuTTY for Symbian OS supports logging to a file. The log can contain useful information on the connection, and help you determine what the problem is. It is also useful to attach a log file to bug reports, but please check first that the log does not contain secrets such as passwords.

Logging can be enabled as follows:

- **Series 60:** From the menu, select `Settings and tools / Log parameters / Log type / SSH data and debug`, and from the same menu select the log file you wish to write to.
- **9200 Communicator series:** From the menu, select, `Settings / Settings`, open the `Logging` tab, set the log type to `SSH data and debug` and choose the log file name.

See chapter 4 for more details on using PuTTY settings.

The log files are regular text files, and can be viewed with Notepad or other text editor. Most file manager applications can even view them in the device itself.

References

[BaSi01] Barrett, Daniel J.; Silverman, Richard: *SSH, The Secure Shell: The Definitive Guide*. O'Reilly & Associates, 2001.

[SSH04] : *SSH Tectia Server (Unix) 4.0 Documentation*. SSH Communications Security, 2004. http://www.ssh.com/support/documentation/all/server-unix/4.0/

[OpenSSH04] The OpenSSH Project: *OpenSSH Manual Pages*. The OpenSSH Project, 2004. http://www.openssh.com/manual.html

[PuTTY04] Simon Tatham: *PuTTY WWW Pages*. Simon Tatham, 2004. http://www.chiark.greenend.org.uk/~sgtatham/putty/

[S2PuTTY04] Kangaslampi, Petteri: *PuTTY for Symbian OS WWW Pages*. Petteri Kangaslampi, 2004. http://s2putty.sourceforge.net/