Previous | Contents | Index | Next

Chapter 2: Getting started with PuTTY

This chapter gives a quick guide to the simplest types of interactive login session using PuTTY.

2.1 Starting a session

When you start PuTTY, you will see a dialog box. This dialog box allows you to control everything PuTTY can do. See chapter 4 for details of all the things you can control.

You don't usually need to change most of the configuration options. To start the simplest kind of session, all you need to do is to enter a few basic parameters.

In the ‘Host Name’ box, enter the Internet host name of the server you want to connect to. You should have been told this by the provider of your login account.

Now select a login protocol to use, from the ‘Connection type’ buttons. For a login session, you should select Telnet, Rlogin or SSH. See section 1.2 for a description of the differences between the three protocols, and advice on which one to use. The fourth protocol, *Raw*, is not used for interactive login sessions; you would usually use this for debugging other Internet services (see section 3.6). The fifth option, *Serial*, is used for connecting to a local serial line, and works somewhat differently: see section 3.7 for more information on this.

When you change the selected protocol, the number in the ‘Port’ box will change. This is normal: it happens because the various login services are usually provided on different network ports by the server machine. Most servers will use the standard port numbers, so you will not need to change the port setting. If your server provides login services on a non-standard port, your system administrator should have told you which one. (For example, many MUDs run Telnet service on a port other than 23.)

Once you have filled in the ‘Host Name’, ‘Protocol’, and possibly ‘Port’ settings, you are ready to connect. Press the ‘Open’ button at the bottom of the dialog box, and PuTTY will begin trying to connect you to the server.

2.2 Verifying the host key (SSH only)

If you are not using the SSH protocol, you can skip this section.

If you are using SSH to connect to a server for the first time, you will probably see a message looking something like this:

```
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 7b:e5:6f:a7:f4:f9:81:62:5c:e3:1f:bf:8b:57:6c:5a
If you trust this host, hit Yes to add the key to
```

```
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the
connection.
```

This is a feature of the SSH protocol. It is designed to protect you against a network attack known as *spoofing*: secretly redirecting your connection to a different computer, so that you send your password to the wrong machine. Using this technique, an attacker would be able to learn the password that guards your login account, and could then log in as if they were you and use the account for their own purposes.

To prevent this attack, each server has a unique identifying code, called a *host key*. These keys are created in a way that prevents one server from forging another server's key. So if you connect to a server and it sends you a different host key from the one you were expecting, PuTTY can warn you that the server may have been switched and that a spoofing attack might be in progress.

PuTTY records the host key for each server you connect to, in the Windows Registry. Every time you connect to a server, it checks that the host key presented by the server is the same host key as it was the last time you connected. If it is not, you will see a warning, and you will have the chance to abandon your connection before you type any private information (such as a password) into it.

However, when you connect to a server you have not connected to before, PuTTY has no way of telling whether the host key is the right one or not. So it gives the warning shown above, and asks you whether you want to trust this host key or not.

Whether or not to trust the host key is your choice. If you are connecting within a company network, you might feel that all the network users are on the same side and spoofing attacks are unlikely, so you might choose to trust the key without checking it. If you are connecting across a hostile network (such as the Internet), you should check with your system administrator, perhaps by telephone or in person. (Some modern servers have more than one host key. If the system administrator sends you more than one fingerprint, you should make sure the one PuTTY shows you is on the list, but it doesn't matter which one it is.)

2.3 Logging in

After you have connected, and perhaps verified the server's host key, you will be asked to log in, probably using a username and a password. Your system administrator should have provided you with these. Enter the username and the password, and the server should grant you access and begin your session. If you have mistyped your password, most servers will give you several chances to get it right.

If you are using SSH, be careful not to type your username wrongly, because you will not have a chance to correct it after you press Return; many SSH servers do not permit you to make two login attempts using different usernames. If you type your username wrongly, you must close PuTTY and start again.

If your password is refused but you are sure you have typed it correctly, check that Caps Lock is not enabled. Many login servers, particularly Unix computers, treat upper case and lower case as different when checking your password; so if Caps Lock is on, your password will probably be refused.

2.4 After logging in

After you log in to the server, what happens next is up to the server! Most servers will print some sort of login message and then present a prompt, at which you can type commands which the server will carry out. Some servers will offer you on-line help; others might not. If you are in doubt about what to do next, consult your system administrator.

2.5 Logging out

When you have finished your session, you should log out by typing the server's own logout command. This might vary between servers; if in doubt, try `logout` or `exit`, or consult a manual or your system administrator. When the server processes your logout command, the PuTTY window should close itself automatically.

You *can* close a PuTTY session using the Close button in the window border, but this might confuse the server - a bit like hanging up a telephone unexpectedly in the middle of a conversation. We recommend you do not do this unless the server has stopped responding to you and you cannot close the window any other way.

If you want to provide feedback on this manual or on the PuTTY tools themselves, see the Feedback page.

[PuTTY release 0.60]