HP OpenView Select Identity

Connector for Linux Systems with SSH

Connector Version: 3.9

Installation and Configuration Guide

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2006 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

- OpenSPML Toolkit from OpenSPML.org

- JGraph developed by JGraph

- Hibernate from Hibernate.org

- BouncyCastle engine for keystore management, bouncycastle.org

This product includes software developed by Teodor Danciu http://jasperreports.sourceforge.net). Portions Copyright (C) 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. (www.waveset.com). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright (c) 2001-2004, Gaudenz Alder. All rights reserved.

Trademark Notices

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

JAVA™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Documentation Map
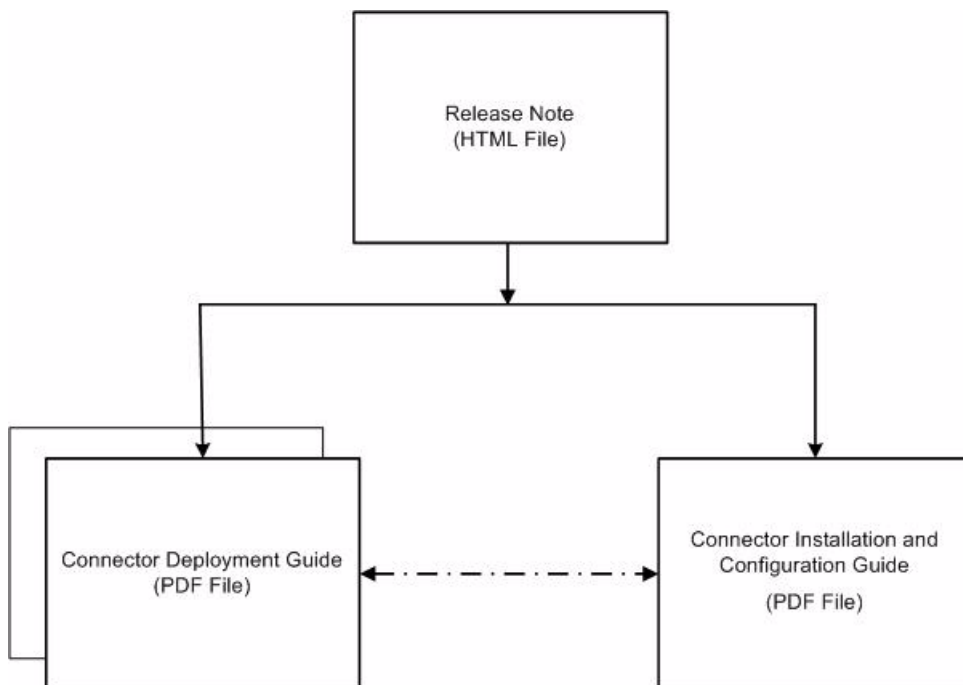
This chapter describes the organization of HP OpenView Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

Figure 1 illustrates the documentation map for HP OpenView Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1   Documentation Map

Table 1   Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Linux SSH Connector v3.9 Release Note.htm`	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	`/Docs/` subdirectory under the connector directory.

Connector Deployment Guide (for Select Identity 4.0/4.01.000)
`connector_deploy_SI4.pdf`
 	
Connector Deployment Guide (for Select Identity 3.3.1)
`connector_deploy_SI3.3.1.pdf`
	Connector deployment guides provide detailed information on:
	
	• Deploying a connector on an application server.
	• Configuring a connector with Select Identity.
	
	Refer to these guides when you need generic information on connector installation.
		`/Docs/` subdirectory under the connector directory.

Connector Installation and Configuration Guide `Linux SSH_install.pdf`	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	`/Docs/` subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP OpenView Select Identity connector for Linux. An HP OpenView Select Identity connector enables you to provision users and manage identities on Linux servers with Telnet. At the end of this chapter, you will be able to know about:

- The benefits of HP OpenView Select Identity.
- The role of a connector.
- The connector for Linux.

About HP OpenView Select Identity

HP OpenView Select Identity provides a new approach to identity management. It helps you manage the entire identity lifecycle of an enterprise application. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

About Connectors

You can establish a connection between a resource and Select Identity by using a connector. A connector is resource specific. It is installed on the system where Select Identity is installed. The combination of Select Identity and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About Linux SSH Connector

The Linux SSH connector enables HP OpenView Select Identity to perform the following tasks on Red Hat Linux 8.0 servers running SSH:

- Add, update, and remove users
- Retrieve user attributes

- Enable and disable users

- Verify a user's existence

- Change user passwords

- Reset user passwords

- Retrieve all entitlements

- Retrieve a list of supported user attributes

- Grant and revoke entitlements to and from users

    ⚠ Do not use the user's primary group as an entitlement. If the primary group is changed, it remains as an entitlement in Select Identity but not on the resource.

The Linux SSH connector is a one-way connector. It pushes the changes made to user data in the Select Identity database to a target server. The mapping file maps Select Identity fields to Red Hat Linux 8.0 fields.

➤ The Linux SSH connector can be used with Select Identity 4.01.000, 4.0, and 3.3.1.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the Table 2 for an overview of installation tasks.

Table 2   Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13.
	— Meet the system requirements.	See Figure on page 14.
	— Perform the pre-installation tasks.	See Pre-Installation Tasks on page 14.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 15.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 15.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 17.

3 Installing the Connector

This chapter elaborates the procedure to install the Linux SSH connector on the Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the Linux SSH connector.
- Pre-installation tasks.
- Procedure to install the Linux SSH connector.

Linux SSH Connector Files

The Linux SSH connector is packaged with the following files located in the `Linux Red Hat 8 - SSH` directory on the Select Identity Connector CD.:

Table 3   Linux SSH Connector Files

Serial Number	File Name	Description
1	`UnixTelnetConnector.rar`	It contains the connector binary files.
2	`unixtelschema.jar`	It contains the schema for the connector that contains the resource attribute related information.
3	`expect.solaris.linux.ssh.scripts.zip`	It contains the scripts used to communicate with the Red Hat Linux 8.0 server.

System Requirements

The Linux SSH connector is supported in the following environment:

Table 4   Platform Matrix for Linux SSH Connector

Select Identity Version	Application Server	Database
3.0.2	WebLogic 8.1.2 on Windows 2003	Microsoft SQL Server 2000
	WebLogic 8.1.2 on Solaris 9	Oracle 9i
	WebLogic 8.1.2 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on Solaris 9	DB2 8.2 (or DB2 8.1 Service Pack 7)
3.3	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebLogic 8.1.4 on Solaris 9	Oracle 9i
3.3.1	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i
	WebLogic 8.1.4 on Red Hat Enterprise Linux AS Release 3.0	Oracle 10g
4.0/4.01.000	The Linux SSH connector is supported on all the platform configurations of Select Identity 4.0 and 4.01.000.	

This connector is supported on Red Hat Linux 8.0.

Pre-Installation Tasks

Before you start installing the Linux SSH connector, you must perform the following tasks on the Select Identity server:

Task 1:   Install Expect

On the Select Identity server installed, obtain the Expect tool from the operating system's installation media, or download from **http://expect.nist.gov/**, and then install on the Select Identity server.

Install an SSH client on the Select Identity server to establish communication between the Linux SSH and HP-UX 11i.

SSH client can be downloaded from **http://www.openssh.com**.

Extract the contents of `expect.solaris.linux.ssh.scripts.zip` file to a local subdirectory on the Select Identity server.

Extracting Contents of the Schema File

The Schema file of the connector contains necessary mapping information to map resource attributes to Select Identity. Extract contents of the `unixtelschema.jar` file to a directory that is in the application server `CLASSPATH`. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Installing the Connector RAR

To install the RAR file of the connector (`UnixTelnetConnector.rar`) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.

While deploying the RAR on WebSphere, enter the JNDI Pool Name as **eis/UnixTelnetCon**.

After deploying the connector RAR on application server, you must configure Linux SSH connector with Select Identity. Refer to Configuring the Connector with Select Identity on page 17 for configuration steps.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Linux SSH connector with Select Identity. At the end of this chapter, you will know the procedure to configure the Linux SSH connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the Linux SSH connector with Select Identity.

1   Add a New Connector

2   Add a New Resource

3   Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

- In the Connector Name text box, specify a name for the connector.

- In the Pool Name text box, enter **eis/UnixTelnetCon**.

- Select **No** for the Mapper Available section.

Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

Refer to the following table white entering the parameters in the Basic Information and the Access Information pages:

Table 5   Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Resource Name	Linux_Server	Name given to the resource.	
Connector Name	Linux	The connector that was deployed in Add a New Connector on page 17.	Known as Resource Type on Select Identity 3.3.1.
Authoritative Source	No	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify **No** because the connector cannot synchronize account data with the Select Identity server.	
Associate to Group	Selected	Whether the system uses the concept of groups. For this connector, select this option.	Applicable only for Select Identity 3.3.1.
Host Name	server.company.com	IP Address or host name of the Red Hat Linux 8.0 machine.	
User Name	accountadmin	Login account on the Red Hat Linux 8.0 machine.	
User Password	Password123	Password for the User Name account.	
Admin Password	rootPassword	The password to gain administrator privileges.	

Table 5   Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Executable	*On UNIX:* /tools/expect-5.21/ expect.exe *On Windows:* d:/tools/expect.exe	Path name of the Expect executable, required to run scripts.	
Script Location	*On UNIX*: /connectorScripts/ expect/Linux/ssh/ *On Windows*: \selectidentity\scripts\	Location of the scripts that are used by the connector. Note that on Windows, you should include a trailing slash in the path.	
Mapping File	UnixConnector-tel.xml	Location of the connector mapping file used to map resource attributes to Select Identity attributes.	

Map Attributes

After successfully adding a resource for the Linux SSH connector, you must map the resource attributes to Select Identity attributes. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for information on mapping and creating attributes. While mapping attributes, refer to the following table for resource specific mapping information.

Table 6   Linux SSH Mapping Information

Select Identity Attribute	Connector Attribute	Attribute on Resource	Description
User Name	username	login (login argument)	UNIX logon name
Password	password	password	Logon password
First Name	F		First Name
Last Name	L		Last Name
[First Name][Last Name]	comment	login comment (-c option)	Comment section in /etc/ passwd
Directory	directory	login home directory (-d option)	User's home directory
Shell	shell	login shell (-s option)	UNIX logon shell
defaultgroup	defaultgroup	login primary group (-g option)	Default group membership

After mapping the attributes, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP OpenView Select Identity Administrator Guide* for information on Select Identity services.

5 Uninstalling the Connector

If you want to uninstall a connector from Select Identity, perform the following steps:

- Remove all resource dependencies.
- Delete the connector from Select Identity.
- Delete the connector from application server.
- Delete the scripts and Expect tool.

See the *HP OpenView Select Identity Connector Deployment Guide* for more information on deleting the connector from application server and Select Identity.

A Overview of Scripts

The Linux SSH connector performs operations using a tool called Expect. This tool must be installed on the application server running Select Identity as described in Pre-Installation Tasks on page 14.

Each script is explained below with a description and example of its usage from the command line. Examples are tested and verified with the following arguments:

Expect executable location : `E:\cygwin\bin\expect.exe`

Scripts directory: `\cygdrive\e\telnet_scripts\HPUX_SSH`

UNIX system name: sihp1

UNIX user name : siuser

UNIX password : password

UNIX root password : password

You can run the examples on command line by replacing the arguments with those from your environment.

- `adduser.exp`

  This is the script used to add a new user to the Red Hat Linux 8.0 system. The following arguments are required:

  directory — User's home directory

  defaultgroup — User's default group

  password — User's password

  F — User's first name

  username — User's login name on the UNIX system

  shell — User's default shell

  comment — User's comment

  L — User's last name

  Example:
  ```
  E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
  adduser.exp sihp1 siuser password password directory=/tmp/june0601
  defaultgroup=bin password=password F=FirstName username=june0601 shell=/
  bin/sh comment=FirstName LastName L=LastName
  ```

- `listuser.exp`

  This script lists all users configured on the Red Hat Linux 8.0 system.

  Example:
  ```
  E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
  listusers.exp sihp1 siuser password password
  ```

- `changepassword.exp`

This script changes the password of a user on the Red Hat Linux 8.0 system. The following arguments are required:

username — User's login name on the UNIX system

password — User's new password

Example:
```
E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
changepasswd.exp sihp1 siuser password password june0601 password
```

- `changestatus.exp`

This script changes a users status on the Red Hat Linux 8.0 system. The following arguments are required:

username — User's login name on the UNIX system

status — User's enable (true) OR disable(false) status

shell — User's shell for enable and /bin/false for disable

Examples:
```
E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
changestatus.exp sihp1 siuser password password username=june0601
status=false shell=/bin/false
```

```
E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
changestatus.exp sihp1 siuser password password username=june0601
status=true shell=/bin/sh
```

- `deleteuser.exp`

This script deletes a user from the Red Hat Linux 8.0 system. The following argument is required:

username — User's login name on the UNIX system

Example:
```
E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
deleteuser.exp sihp1 siuser password password username=june0601
```

- `dotest.exp`

This script is executed whenever a new connector is created. It is responsible for validating the connection.

Example:
```
E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/dotest.exp
sihp1 siuser password password
```

- `finduser.exp`

This script is used to search for a user on the Red Hat Linux 8.0 system. The following argument is required:

username — User's login name on UNIX system

Example:
```
E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
finduser.exp sihp1 siuser password password june0601
```

- `genericcmd.exp`

  This script is used to enable the execution of any command required by Select Identity. The following argument is required:

  command — Command that needs to be executed; if a space exists in the command, quote the command

  Example:
  ```
  E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
  genericcmd.exp sihp1 siuser password password "/bin/cat /etc/group"
  ```

- `modifyuser.exp`

  This script is used to modify a user on the Red Hat Linux 8.0 system. The following arguments are required:

  directory — User's new home directory

  defaultgroup — User's new default group

  password — User's password

  F — User's new first name

  username — User's login name on the UNIX system

  shell — User's new default shell

  comment — User's new comment

  L — User's new last name

  gname — Group names separated by commas to which the user needs to be added

  Examples:
  ```
  E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
  modifyuser.exp sihp1 siuser password password directory=/home/june0601
  defaultgroup=bin password=password F=abc username=june0601 shell=/bin/ksh
  "comment=abc K" L=K
  ```

  ```
  E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
  modifyuser.exp sihp1 siuser password password
  gname=adm,daemon,mail,lp,root username=june0601
  ```

- `getgroups.exp`

  This script is used to get all group names for which the current user has membership on the Red Hat Linux 8.0 system. The following argument is required:

  username — User's login name on the UNIX system

  Example:
  ```
  E:/cygwin/bin/expect.exe -f /cygdrive/e/telnet_scripts/HPUX_SSH/
  getgroups.exp sihp1 siuser password password june0601
  ```

B   Troubleshooting

The following information is provided to help you diagnose connectivity and configuration problems that you may encounter when using the connector to provision users on the resource. You may need to consult your system or web application administrator for detailed help.

- On the Select Identity server, if installed on a Windows system, ensure that Cygwin's `bin` directory is included in the Windows server's PATH environment variable.

- If an error indicating that `org.apache.log4j.Logger` could not be found is displayed while deploying the connector, be sure to exclude `log4.jar` from the Java classpath.

- Verify that the paths to SSH and Telnet are configured properly on the Red Hat Linux 8.0 system. Use the **which ssh** and **which telnet** commands to find the paths to SSH and Telnet. If the paths are different than the paths specified in the Expect scripts, use the paths found on the Red Hat Linux 8.0 system. You may want to specify the full paths to SSH and Telnet in the scripts.

- Ensure that the SSH and Telnet daemons are configured and running on the target Red Hat Linux 8.0 system. Use **ps -ef | grep sshd** and
  ps -ef | grep telnetd to determine if the daemons are is running.

- The default UNIX prompt of resource system should be $, #, %, or >.

- Verify that SSH and Telnet allow enough connections to handle provisioning requests. The number of connections depends on the number of connections allowed by the application server for the connector. To view the connection configuration and connections on the application server, perform one of the following procedures:

  On WebLogic:

  To view the connection configuration:

  a   Log on to the WebLogic Server Console.

  b   Navigate to ***My_domain*** → **Services** → **JDBC** → **Connection Pools** → ***connection_pool***.

  To monitor current connections:

  a   Navigate to ***My_domain*** → **Deployments** → **Connector Modules** → ***connector***.

  b   Click the **Monitoring** tab to view connections.

  On WebSphere:

  To view the connection configuration:

  a   Log on to the WebSphere Application Server Console.

  b   Click **Resources** → **Resource Adapters**.

  c   Click the connector.

  d   Click **J2C Connection Factories** in the Additional Properties table.

  To monitor current connections, you must use the Tivoli performance viewer and click ***application_server*** → ***J2C_connection_pool***.

Consult with your system or application server administrator for further help diagnosing problems related to connections that do not close, connections that time out, connections that cannot be opened, and so on.

- Depending on the system implementation and software versions, you may experience connectivity problems when the connector communicates with the Red Hat Linux 8.0 system. If so, edit each script that includes the following:

```
set force_conservative 0 ;
```

Set the force_conservative property to **1**, as follows:

```
set force_conservative 1 ;
```

This forces Expect to pause (1/10th of second) before sending data. Some processes, such as Telnet, may ignore keystrokes if they are sent too quickly. Thus, the short delay prevents the keystroke from arriving too quickly, before Expect is prepared to receive it.