Novell NetWare® 6.5

www.novell.com

OPENSSH ADMINISTRATION GUIDE

March 31, 2005

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2003-2005 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

OpenSSH Administration Guide for NetWare 6.5
March 31, 2005

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

eDirectory is a trademark of Novell, Inc.
NetWare is a registered trademark of Novell, Inc. in the United States and other countries.
NetWare Loadable Module and NLM are trademarks of Novell, Inc.
Novell is a registered trademark of Novell, Inc. in the United States and other countries.
Nterprise is a trademark of Novell, Inc.
Nterprise Branch Office is a trademark of Novell, Inc.

Third-Party Materials

All third-party products are the property of their respective owners.

Contents

About This Guide 7

1 **Overview of OpenSSH on NetWare** 9

Benefits of OpenSSH . . . 9
Functions Unique to the NetWare Platform . . . 10
What's Next . . . 10

2 **Setting Up OpenSSH in Your Network** 11

Setting Up SSH on a Server . . . 11
Completing Post-Installation Configuration . . . 11
Setting Up SSH at Workstations . . . 18
What's Next . . . 18

3 **Using SSH Commands** 19

Running Commands from a Workstation or Server . . . 19
Using SSH Command Options . . . 20
Running Keyboard Commands at the SSH Server Console Screen . . . 21

A **Document Updates** 23

June 1, 2005 . . . 23

About This Guide

This guide describes how to set up and use the OpenSSH open source data encryption program that has been integrated with NetWare® software. This product provides a secure shell with encryption for use when accessing NetWare servers remotely. The majority of this guide is intended for network administrators. A few sections include information for end users. This guide is divided into the following sections:

- Chapter 1, “Overview of OpenSSH on NetWare,” on page 9
- Chapter 2, “Setting Up OpenSSH in Your Network,” on page 11
- Chapter 3, “Using SSH Commands,” on page 19

Documentation Updates

The latest version of this documentation is available at the OES documentation Web site (http://www.novell.com/documentation/oes/index.html).

Additional Documentation

Additional OpenSSH documentation is located on the Web at www.openssh.com (http://www.openssh.com).

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single path name can be written with a backslash for some platforms or a forward slash for other platforms, the path name is presented with a backslash. Users of platforms that require a forward slash, such as UNIX* and Linux*, should use forward slashes as required by your software.

Understanding the following terminology will be helpful as you use this guide:

- OpenSSH: The open source product
- SSH: The SSH protocols within the OpenSource product
- ssh: The client utility

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with NetWare 6.5. To contact us, use the User Comments feature at the bottom of any page in the online documentation.

1 Overview of OpenSSH on NetWare

OpenSSH is an open source technology that has been integrated with NetWare®. It provides a secure shell that uses encryption provided by Novell® International Cryptographic Infrastructure (NICI) technology rather than SSL to implement 128-bit (and stronger) encryption and contains fewer software import liabilities.

In NetWare 6.5, Novell has integrated OpenSSH version 3.7p1 (http://www.openssh.com) to work on NetWare so that administrators and users can access NetWare servers in their networks using methods that provide secure access and transmission of data.

Through this secure shell, users who are Admin equivalent can gain remote access to any server in your network and copy files and directories to and from other servers in your network using SSH utilities. You can also put these commands in script files to automate routine tasks.

Through this shell, end users can securely access and copy files in their home directories or other directories that they have rights to on NetWare servers from remote locations without the use of a browser or proprietary client.

Many users of telnet, rlogin, ftp, and other such programs might not realize that their passwords and data are transmitted across the Internet unencrypted. OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. Additionally, OpenSSH provides a myriad of secure tunneling capabilities.

The OpenSSH suite integrated with NetWare 6.5 includes:

- The ssh program that replaces rlogin and Telnet
- scp (replaces rcp)
- sftp (an alternative to ftp)
- sshd (server side of the package)
- Other basic utilities like ssh-keygen or sftp-server

OpenSSH supports SSH protocol versions 1.3, 1.5, and 2.0.

Benefits of OpenSSH

The following is a brief list of some of the benefits of integrating OpenSSH with NetWare.

- End users can securely access and copy files in their home directories on NetWare servers from remote locations without the use of a browser or propriety client.
- Network administrators can gain remote access to any server in their networks and copy files and directories to and from other servers in their networks using ssh utilities. They can also put these commands in script files to automate many routine tasks.

- Because the ssh client protocols have also been ported to NetWare, network administrators can use the ssh commands from a remote client or from a remote server on the network running NetWare 6.5 to copy files from one server to another server.
- SSH protocols allow you to connect to the server and automatically send a command, so the server will run that command and then disconnect. This means you can use automated processes.
- SSH protocols provide security of your data transmissions and communications across the Internet whether you are outside or inside a firewall. You can be confident that hackers will not be able to access your data.

Functions Unique to the NetWare Platform

Integrating OpenSSH with NetWare adds functionality to make using SSH on a NetWare server easier. Some commands work differently on NetWare than they do in other SSH implementations.

Added Functionality

- **OpenSSH Manager:** Any user that belongs to the sshadmn-Administrators group is granted access to the OpenSSH Manager to modify the configuration of OpenSSH servers. The OpenSSH Manager can be accessed via web browser ssl connection to port 2200. This tool lets you view ssh connections, change the sshd_config file more easily, set log preferences, etc.
- **SSH Log Daemon:** This agent generates the log files that contain all the logs and errors sent from all ssh-type NLM™ programs such as sshd, ssh, sftp, or scp.
- **Authentication:** OpenSSH uses password authentication through LDAP. This authentication gathers all the user's credentials from Novell eDirectory™ 8.7.3. Once a user has authenticated, the current working directory is their home directory if configured in eDirectory; otherwise, they will be at the root of the server volumes of the server they connected to. The user can navigate like they would with ftp to any directory on that server for which they have been assigned rights in eDirectory.

Differences

- **The localhost commands:** The **`ssh localhost`** command does not work on a NetWare server; however, the **`scp localhost`** and **`sftp localhost`** commands do work.

What's Next

Now that you know a little about the SSH protocols that have been ported to NetWare and what some of the benefits of using it are, you can continue with the following tasks.

To	See
Set up SSH on your server	"Setting Up SSH on a Server" on page 11
Download an SSH-compliant client on a workstation	"Setting Up SSH at Workstations" on page 18

2 Setting Up OpenSSH in Your Network

Setting up OpenSSH in your network involves the following tasks:

- Setting Up SSH on a Server (page 11)
- Setting Up SSH at Workstations (page 18)

Setting Up SSH on a Server

As a prerequisite, we recommend that you install the Apache Administration server if it wasn't installed by default. The Apache Administration server is normally installed by default unless you installed a special-purpose server that didn't require it, such as iLogin, DNS/DHCP, Pre-migration NetWare®, Virtual Office, or Novell® Branch Office™.

You can install OpenSSH either as an optional component during the NetWare custom installation or on a server after installing NetWare using the following procedure.

1. Insert the NetWare CD into the drive of the server where you want to install OpenSSH.
2. Start the NetWare GUI by entering **`startx`** at the System Console prompt.
3. Click Novell > Install > Add.
4. In the Source Path dialog box, type the path or browse to the CD.
5. Select the postinst.ni response file, then click OK.
6. On the Install Components screen, select Secure Shell from the products list.
7. Click Next.
8. When prompted, specify the administrator username, password, and context.
9. Follow the remaining screen prompts.
10. Click OK.

Completing Post-Installation Configuration

After the installation, you need to complete some additional configuration before you or your users can access files on the server.

1. Load the sshd.nlm file at the server.
2. (Optional) Edit the sys:etc\ssh\sshd_config file to change any settings from the default.

Understanding the Components

After you set up OpenSSH on your NetWare server, it should contain the following components in the indicated locations.

File	Location	Description
sshd.nlm	sys:\system	OpenSSH version 3.6p1 ported to NetWare 6.5. This is the daemon for the ssh program. It provides secure encrypted communications between two untrusted hosts over an insecure network. This daemon listens for the connections from clients.
sshd_config	sys:\etc\ssh	System-wide configuration file for the SSH daemon. The daemon reads the configuration file and executes the commands it receives based on the file's settings. You can edit this file manually or through the Web administration utility. For more information, see "Editing the Configuration File" on page 12.
ssh_host_key	sys:\etc\ssh	Private host key used to authenticate the server for the SSH protocol versions 1.3 and 1.5.
ssh_host_rsa_key	sys:\etc\ssh	Private host key used to authenticate the server for the SSH protocol version 2.0 using RSA encryption.
ssh_host_dsa_key	sys:\etc\ssh	Private host key used to authenticate the server for the SSH protocol version 2.0 using DSA encryption.
sshjni.nlm	sys:\system	Secure Shell JNI Web support
sshlogd.nlm	sys:\system	Secure Shell log daemon that generates the sshd.log file, which contains all errors sent from all ssh-type NLM™ programs such as sshd, ssh, sftp, and scp. This NLM is not a standard ssh file. This ssh module only exists on the NetWare platform.

Editing the Configuration File

The sshd_config file is located in sys\etc\ssh\. You can edit this file manually with any text editor. If your server has been set up with a DNS name, you can make changes to the file using the OpenSSH Admin utility.

We recommend making changes to the configuration using the OpenSSH Manager (OpenSSH Admin) utility because it eliminates syntax errors that you might make editing the file manually. If you manage OpenSSH on multiple servers, we recommend using this utility to import the configuration file to the eDirectory™ 8.7.3 mode and then also managing the configuration with the utility.

IMPORTANT: The Apache Admin utility must be installed and set up in order to use the OpenSSH Admin utility.

To access this utility from a browser (Netscape 6.*x* or later or IE 5.5 or later):

1. Enter **`https://ip_address or server_dns_name:2200`**, then click the SSHD Admin link under the OpenSSH Server heading.
2. Type the password information.

3 Ensure the information automatically inserted into the following fields is applicable to the user and server that you want to log in to.

- User Name
- LDAP Provider Domain Name
- Port Number 636 (or whatever it has been changed to)
- The Use SSL Connection check box (checked)

  If this check box is not checked, your password to log in to sshd will be exposed in clear text.
- The initial LDAP context

Changing the Options

The following table shows the options that you can change in the sshd_config file and the links that you can use for them in the OpenSSH Admin utility. All keyword purposes and options are specified in the sshd_config man pages (http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config&sektion=5&arch=&apropos=0&manpath) unless they are specific to a NetWare implementation.

Option	Description	Link in Admin Utility
AuthorizedKeyFile	Path to the file that contains the authorized keys. Default: .ssh\authorized _keys	Authentication
ChallengeResponseAuthentication	Challenges the user to supply authentication credentials. If the user responds with correct credentials, authentication is allowed. Default: Yes	Authentication

Option	Description	Link in Admin Utility
ClientAliveCountMax	Number of client alive messages that can be sent without sshd requiring any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd disconnects the client, terminating the session. This is very different from KeepAlive. The client alive messages are sent through the encrypted channel and, therefore, are not spoofable. Messages sent by KeepAlive are spoofable. The client alive mechanism is valuable when the client or server depends on knowing when a connection has become inactive. If ClientAliveCountMax is set to 2, unresponsive ssh clients will be disconnected after approximately 30 seconds. If ClientAliveInterval is set to 15, and ClientAliveCountMax is left at the default, unresponsive ssh clients will be disconnected after approximately 45 seconds. Default: 3	Connection
ClientAliveInterval	Timeout interval (in seconds) after which, if no data has been received from the client, sshd sends a message through the encrypted channel to request a response from the client. Default: 0 (no messages sent) This option applies to protocol version 2 only.	Connection
Compression	Enables/disables compression, which reduces traffic on a low-bandwidth connection. Default: Yes (enabled)	Connection

Option	Description	Link in Admin Utility
eDirNameContext	Search context. Use this to expand or limit access to the tree. To enable users in this context only to authenticate to sshd: o=org To allow users in this context and all subcontexts to authenticate to sshd: o=org?scope=subtree To search for a user in multiple contexts: context *context*?scope=subtree This setting is unique to a NetWare implementation.	eDirectory
HostKey	These keys are generated during the OpenSSH installation on NetWare: etc\ssh\ssh_host_key etc\ssh\ssh_host_rsa_key etc\ssh\ssh_host_dsa_key	Host Keys
IgnoreUserKnownHosts	Specifies whether sshd should ignore the user's $home/.ssh/known_hosts file during RhostsRSAAuthentication or HostbasedAuthentication. This file contains a copy of the key that the host sent the last time a connection was made. If the file is not ignored, the server prompts the user every time that user attempts to connect, asking whether the key should be accepted. Default: No	Authentication
KeepAlive	Specifies whether the system should send TCP keepalive messages to the other side. If they are sent, events such as the termination of the connection or the crash of one of the machines will be noticed. However, this means that connections will terminate if the route is down temporarily. The client will detect whether the network goes down or the remote host crashes. Default: Yes	Connection
KeyRegenerationInterval	Time (in seconds) between regeneration of keys. This prevents decrypting captured sessions by later breaking into the machine and stealing the keys. The key is never stored anywhere. If the value is 0, the key is never regenerated. Default: 3600	Authentication

Option	Description	Link in Admin Utility
ListenAddress	Address for the ssh client to listen on. Default: 0.0.0.0	Listen Address
LoginBannerFile	Path to a file that contains a greeting or specific banner text that displays when the user logs in to the server using an ssh client. Recommended path: sys:\etc\ssh Default: None	Connection
LoginGraceTime	Time interval (in seconds) before the server disconnects if the user has not successfully logged in. If the value is set to 0, there is no time limit. Default: 600	Connection
LogLevel	Verbosity level that is used when logging messages from sshd. Default: Info	Log Preferences
LogMaxFileSize	Size (in MB) for the log files. Default: 4 This setting is unique to a NetWare implementation.	Log Preferences
LogMaxRotateFiles	Maximum time (in hours) for logging to occur in one file if the default size is not reached. Default: 7 This setting is unique to a NetWare implementation.	Log Preferences
LogPath	Path to the log file The recommended location is sys:\etc\ssh\logs. This setting is unique to a NetWare implementation.	Log Preferences
LogRotationInterval	Maximum time (in hours) for logging to occur in one file if the default size is not reached. Default: 24 This setting is unique to a NetWare implementation.	Log Preferences

Option	Description	Link in Admin Utility
PasswordAuthentication	Uses a username and password to verify a user's identity. This is currently the only way to authenticate to a NetWare server with OpenSSH. Even if you do not select Yes to enable Password Authentication, Password Authentication will still be used for NetWare servers. Default: Yes	Authentication
Port	Port for SSH to listen on. Default: Port 22.	Listen Ports
Protocol	Versions of the SSH protocol that are supported.	Miscellaneous
PubKeyAuthentication	Uses cryptographic keys to verify a user's identity. A public key is stored on the server. When a user attempts to authenticate, that user's private key is verified against the public key to authenticate the user. Default: Yes	Authentication
RSAAuthentication	Allows/disables authentication using identity keys encoded with the Rivest-Shamir-Adleman (RSA) algorithm. Default: Yes This option applies to protocol version 1 only. Version 2 uses the Digital Signature Algorithm (DSA).	Authentication
ServerKeyBits	Number of bits in the ephemeral protocol version 1 server key. The larger the number of bits, the more secure the key is. If the server detects a change in this number, there could possibly be a security breech. Default: 768	Authentication
VerifyReverseMapping	Specifies whether sshd should try to verify the remote hostname and whether the authentication request is coming from the IP address it claims to be coming from. Default: No	Authentication

Setting Up SSH at Workstations

To access files using ssh commands from a workstation:

1. Download and run an SSH-compliant client.

   You can get these clients from any open source on the Internet. Some SSH-compliant clients that you could run:

   - PuTTy (tested with NetWare 6.5)
   - MindTerm
   - Absolute Telnet
   - Red Hat* Linux open ssh clients (tested with NetWare 6.5)

2. In any of the clients, change the Window Row setting from the default to a value greater than 25.

What's Next

After SSH is set up on the server and at the users workstations, you can use different ssh commands and utilities to

- Perform tasks such as copy files, run scripts, and execute server commands
- Manage your SSH connections.
- Troubleshoot problems with SSH.

For information on using the ssh commands and utilities, see Chapter 3, "Using SSH Commands," on page 19.

3 Using SSH Commands

This section includes instructions for accomplishing the following tasks

- Running Commands from a Workstation or Server (page 19)
- Using SSH Command Options (page 20)
- Running Keyboard Commands at the SSH Server Console Screen (page 21)

Running Commands from a Workstation or Server

After downloading an SSH-compliant client to your workstation, you can use the following commands to accomplish tasks on the NetWare server. The ssh, scp, and sftp client protocols have been ported to the server so you can execute these command in server to server connections as well.

Type	To
ssh	Connect and log into the specified server (hostname). You must provide your identity to the remote machine. For more information, see the ssh information at openssh.com on the Web (http://www.openbsd.org/cgi-bin/man.cgi?query=ssh).
sshd	Control how the daemon logs you in. For options and more information, see the sshd information at openssh.com on the Web (http://www.openbsd.org/cgi-bin/man.cgi?query=sshd).
ssh-agent	Not supported on NetWare. NetWare only supports password authentication.
ssh-add	Not supported on NetWare.
sftp	Perform secure file transfers with FTP-like command that works over SSH1 and SSH2 protocol. For command options and more information, see the sftp information at openssh.com on the Web (http://www.openbsd.org/cgi-bin/man.cgi?query=sftp).
scp	Copy files between hosts on a network. It uses ssh(1) for data transfer, and uses the same authentication and provides the same security as ssh(1). Scp asks for passwords or passphrases if they are needed for authentication. For command options and more information, see scp information at openssh.com on the Web (http://www.openbsd.org/cgi-bin/man.cgi?query=scp).

Type	To
ssh-keygen	Generate, manage, and convert authentication keys for ssh. For more information, see ssh-keygen information at www.openssh.com on the Web (http://www.openbsd.org/cgi-bin/man.cgi?query=ssh-keygen).
sftp-server	Use the SFTP server subsystem (started automatically by sshd). This program speaks to the server side of the SFTP protocol to stdout and expects client requests from stdin. For more information, see ssh information at www.openssh.com on the Web (http://www.openbsd.org/cgi-bin/man.cgi?query=sftp-server).
ssh-keyscan	Not supported on NetWare.

Using SSH Command Options

After downloading an SSH-compliant client to your workstation, you can send the following options with the ssh command to the NetWare server.

ssh *option* **host** *command*

Use Option	To
-a	Disable authentication agent forwarding (default).
-A	Enable authentication agent forwarding.
-b *bind_address*	Specify the local IP address to transmit from on machines with multiple address or aliased addresses
-c *cipher*	Select encryption algorithm
-C	Enable compression
-D *port*	Enable dynamic application-level port forwarding.
-e *escape_character*	Set escape character; "none" = disable (default: ~)
-f	Fork into background after authentication
-F *config_filename*	Specify the location of the config file (default: ~/etc/ssh/config). Requests **ssh** to go to the background just before command execution
-g	Allow remote hosts to connect to forwarded ports.
-i *filename*	Select an identity file for public key authentication (default: ~/.ssh/identity)
-l *username*	Log in using the specified username
-L *listen-port:host:port*	Forward local port to remote address This causes ssh to listen for connections on a port and forward them to the other side by connecting to host:port.
-m *macs*	Specify MAC algorithms for ssh protocol version 2.
-n	Redirect input from . (root)

Use Option	To
-N	Do not execute a shell or command.
-o *option*	Process the option as if it was read from a configuration file.
-p *port*	Connect to the specified port. The server must be on the same port.
-q	Do not display any warning messages
-R listen-port:host:port	Forward remote port to local address This causes ssh to listen for connections on a port and forward them to the other side by connecting to host:port.
-s	Invoke command (mandatory) as SSH2 subsystem.
-t	Allocate a tty even if command is given.
-T	Do not allocate a tty.
-v	Display verbose debugging messages. Using multiple -v increases verbosity.
-V	Display version number only.
-x	Disable X11 connection forwarding (default).
-X	Enable X11 connection forwarding.
-1	Forces ssh to try protocol version 1 only.
-2	Forces ssh to try protocol version 2 only.
-4	Forces ssh to use IPv4 addresses only.
-6	Forces ssh to use IPv6 addresses only.

Running Keyboard Commands at the SSH Server Console Screen

The following table shows the keyboard commands that can be executed at the ssh- sftp- or scp-server console screen. Each connection will generate a new console screen. For example the console screen generated from a ssh connection would appear as ssh *username ip_address*.

Console access is granted only to the Admin user and users with security equal to Admin.

Press	To
Ctrl+B	Begin (Home)
Ctrl+D	Move the cursor down (Down Arrow)
Ctrl+L	Move the cursor to the left (Left Arrow)
Ctrl+U	Move the cursor to the up on the screen (Up Arrow)
Ctrl+R	Move the cursor to the right (Right Arrow)
Ctrl+F	Switch to a different server console screen. The server GUI screen is not supported.

Press	To
Ctrl+P	Page up
Ctrl+N	Page down
Ctrl+G	Delete
Ctrl+O	Insert
Ctrl+X	Exit
Ctrl+T	Reboot server
Ctrl+E	End
Ctrl+Z	Select screen
Ctrl+H	Backspace
Ctrl+S	Setting screen
Ctrl+Q	Display SSH keyboard help screen
Ctrl+K	Access the kernel debugger screen

A Document Updates

These dates indicate when the OpenSSH documentation has been updated, and what changes have been made.

June 1, 2005

The following updates were made:

- References to eDirectory versions were changed to “eDirectory 8.7.3.”
- Links to NetWare 6.5 documentation were changed to point to the OES doc site.