Secure Shell (SSH) in HP SIM 5.x

How this paper is organized

This paper is organized into four broad areas:

- An Introduction to SSH and how it works
- SSH and HP (HP SIM) which includes information about how HP SIM uses SSH
- Common questions and tasks including a HChecklist to debug SSH on Windows
- Troubleshooting
- Appendices including: Appendix A: Changes in HP SIM 5.x, Appendix B: Tool examples, and Appendix C: Glossary

Those who are new to the topic of SSH should start with the Introduction, while SSH experts should start at SSH and HP SIM. The Troubleshooting section is important to those who need to support OpenSSH and HP SIM.

This paper is focused on the 5.x version of HP SIM, which has a number of changes in SSH handling from previous versions. A separate white paper is available for earlier versions of HP SIM, with the same background information in each paper.

Introduction

This is an era of the security conscious IT administrator. User names and passwords are no longer passed in the clear over the intranet or Internet. We are providing more secure access into managed systems so that only authorized users have access to our most sensitive information, which is on the system itself.

Telnet was one of the methods of the past for logging into a remote system and performing commands that would add, delete, and modify files. However, Telnet is not a secure method to use and does not protect network traffic.

There is a small, unassuming, yet robust solution, which is reasonably easy to use, inexpensive, and available for most of today’s operating systems. This solution is Secure Shell (SSH), which is not a shell at all but a secure remote access protocol. The SSH protocol provides security on the network, authentication, and data exchange with spoof protections and encryption.

HP SIM is a robust system management tool. Through use of the Distributed Task Facility (DTF) and SSH, HP SIM is able to securely log into remote systems on behalf of the HP SIM user of the central management server (CMS) and make modifications, additions, and run commands. The HP SIM terminology for these processes is called tasks.

This white paper provides the following:

- An overview of SSH and OpenSSH, which is an implementation of SSH
- Demonstrates how SSH is used in HP SIM 5.x
- Discusses some of the problems that can be encountered during its usage
- Presents a recommended troubleshooting method when the SSH connection does not appear to be working

Some of the programs installed into HP SIM, called plug-ins, also use the capabilities of SSH, and mention is made of plug-ins where appropriate.

The custom commands and some command line tools (MSA) of HP SIM might require that SSH be installed and configured on the CMS. Other tools (SSA) require SSH on the managed system where they are to run. Refer to Appendix B: Tool examples for examples of the MSA and SSA tools.

Why SSH?

SSH was selected to be used with HP SIM for the following reasons:

- To provide a way to securely execute commands and copy files to remote systems
- To provide secure authentication mechanisms
- To encrypt all data sent over the wire, unlike the traditional UNIX® r services
- To provide a popular, non-proprietary protocol

Origins of SSH

SSH and the SSH-1 protocol were developed in 1995 and in the same year it was documented as an Internet Engineering Task Force (IETF) Internet Draft standard. The protocol was popular and by 1997 the protocol was standardized and published as a new standardized protocol version, SSH 2.0, or SSH-2. This version was missing some of the SSH-1 features, which continue to be more widely used even though SSH-2 is a more secure protocol.

SSH was originally created to replace the UNIX r services **remsh**, **rlogin**, and **rcp**. These services provide remote shell, execution, and file copy. Unfortunately, all data passed between the communicating systems using r services is unencrypted clear text. Additionally, the authentication mechanisms are weak and vulnerable to attack. The **rhost** authentication is vulnerable to the man-in-the-middle attack, and passwords are passed over the network in clear text. SSH provides a mechanism to verify the identity of the remote system using key-based host authentication, prevents password snooping by using over-the-wire encryption of all communications between the client and server, and provides stronger user authentication methods by using public key authentication.

Origins of OpenSSH

OpenSSH (http://www.openssh.com) is gaining prominence as an SSH implementation, developed under the auspices of the OpenBSD project (http://www.openbsd.org/) and freely available under the OpenBSD license. OpenSSH is based on the last free release of the original SSH, 1.2.12, and has developed rapidly as contributions have continued. It supports both SSH-1 and SSH-2 in a single set of programs, whereas SSH-1 and SSH-2 have separate executables. While OpenSSH was developed under OpenBSD, it has been ported successfully to Linux, Solaris, AIX, HP-UX, and other operating systems. Active development has continued on OpenSSH and SSH-2, but has ceased for SSH-1.

What is SSH

SSH is not a product but rather a protocol for secure remote access based on public key encryption. It provides a specification of how to conduct secure communication over the network. Communications to and from the remote system uses the SSH protocol. This is conceptually similar to Secure Sockets Layer (SSL) which is another security protocol used in many internet communications such as Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

The SSH suite includes:

- ssh program which replaces **rlogin** and **telnet**
- scp which replaces **rcp**
- sftp which replaces **ftp**
- sshd which is the server side of the package
- Other basic utilities such as ssh-add, ssh-agent, ssh-keysign, ssh-keyscan, ssh-keygen and sftp-server

Other SSH implementations

There are a number of other implementations of SSH, most notably commercial versions of SSH1 and SSH2 maintained and sold by F-Secure Corporation.

Reference

For power users we recommend the O'Reilly reference, SSH The Secure Shell by Daniel Barrett and Richard Silverman, 2001, as an excellent reference.

How does SSH work?

SSH is a network protocol between two software modules: the SSH client, which initiates the connection and the SSH server, which responds to the client. For example, an SSH client can be run by a user to connect to a remote system which is running the SSH server.

The basic steps in setting up an SSH connection are:

1. The SSH client sends a request to the remote SSH server.
2. The SSH server responds with a public key.
3. The SSH client decides if it accepts the public key. For example, it authenticates the SSH server by comparing the key with previously obtained value.
4. The SSH client then sends user information to the remote SSH server. These credentials can be a user name and password or public key authentication.
5. The SSH server decides if it accepts the user credentials. For example, it authenticates the SSH client using the supplied password or from a previously stored public key.
6. Once authenticated, the client and server can exchange data, such as executing commands and returning results.

This is similar to a telnet connection. However, it is a secure connection with all communications using an encrypted channel.

The SSH connection process

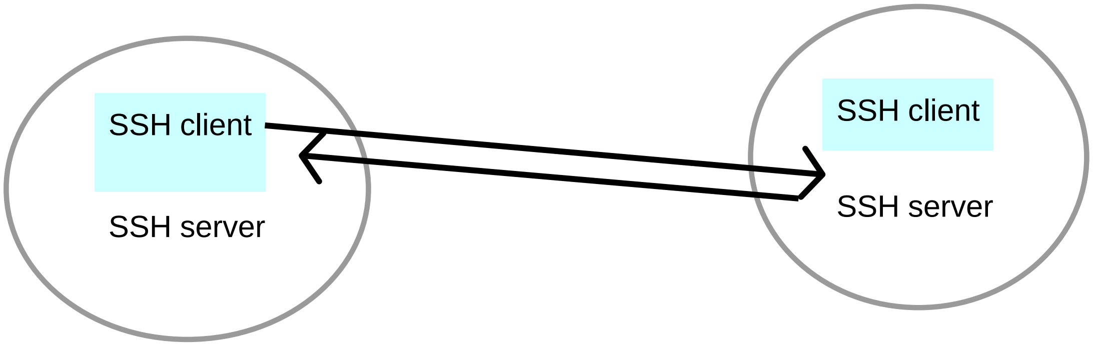
The SSH protocol is utilized to establish a connection and then to log into the remote managed system. After a successful login, any packets which follow are encrypted using the SSH protocol. Each system where SSH or OpenSSH is installed natively includes an SSH client and an SSH server.

Note: This white paper refers to SSH and OpenSSH as SSH.

The following command is a common use of SSH for connecting to another system using the command window. The command line to connect to another system:

```
$ ssh –l smith host.example.com (-v turns on verbose mode)
```

In this case, your SSH client is initiating a connection to the remote SSH server host called host.example.com using the login name of smith. You can use the –v option to turn on the verbose mode so the transaction can be followed.



SSH authentication mechanisms

Every SSH connection involves two authentications in the following order:

1. **Server Authentication**. The SSH client verifies the identity of the SSH server. This ensures the SSH server is genuine and not an imposter. It also guards against an attacker redirecting the network connection to a different machine. This prevents a man-in-the-middle attack where an attacker positions itself between the client and server and is able to view and modify the communication.
2. **User Authentication**. The SSH server verifies the identity of the user name account requesting access.

Server authentication — verification of the SSH server system

To establish a connection, the SSH client first contacts the remote system. Session keys are exchanged, and are used to encrypt all further communication between the client and server. The remote SSH server then sends its identity, known as the host key, to the SSH client for verification.

The SSH client must decide if it accepts the server's host key. Usually, this is done by comparing the returned key with a known value for that host by looking for the key in the known hosts file. If the key matches, the server is authenticated, while if the key is different, an error is reported and the client terminates the connection. If the client has never communicated with the server before, there is probably no key for this remote host. A typical interactive SSH client prompts the user to accept or reject the new key, saving the key in the known hosts file if accepted. This, accept on first use model, means that the connection is vulnerable to a man-in-the-middle attack on first use, but subsequent connections will use the stored key.

User Authentication - verification of the client user's credentials

Once the identity of the remote SSH server has been verified, the SSH client sends the user name of the user who is requesting a login, along with any credentials (based on type of authentication) of the user to the target SSH server.

The user is authenticated in one of three ways:

- Public key authentication — using key files
- Using host-based authentication — using key files
- Password authentication

Each method is attempted by the SSH client in sequence until there is a successful user authentication or after the last method is tried with no response and results in a failure.

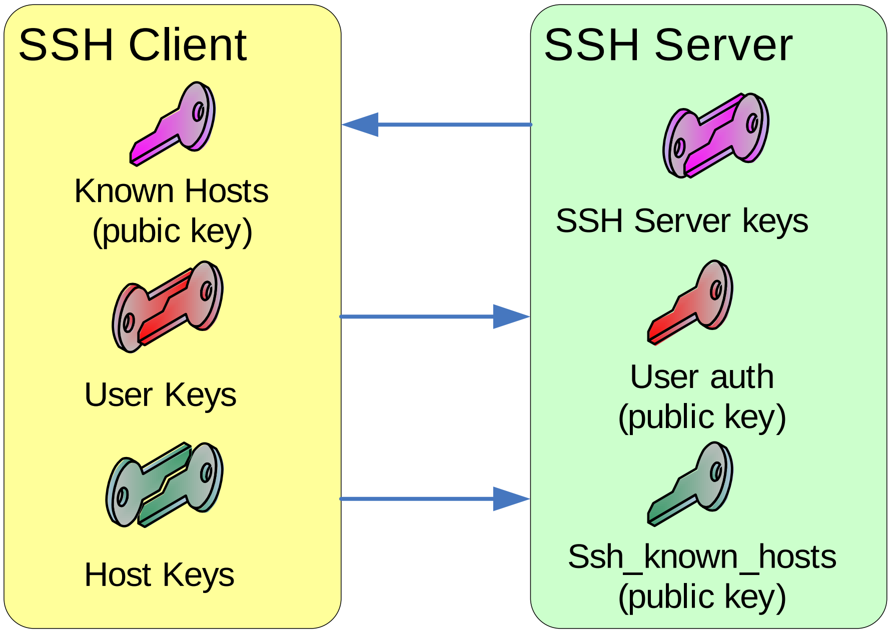
Public key authentication is the most secure way to authenticate a user and is utilized by HP SIM 4.x and 5.x. Each user has a private key to identify that user, which is kept secret at the client. A corresponding public key is used by anyone wishing to authenticate this user, and the SSH server has a copy of this public key. The SSH client uses the user's private key to encrypt a message sent to the

SSH server. The SSH server uses the user's public key to decrypt this message. If this is successful, the user is authenticated because the message must have been sent by a client with access to the private key.

Host Based authentication is very similar to the user public key authentication, and is also based on public and private keys. In this case, separate keys are not used for each user. Instead, a single key pair is used to authenticate the SSH client system and the SSH server trusts the client as to the identity of the individual users. The SSH client uses the client system's private key to encrypt a message to the server, and the SSH server uses the public key for that client system (host) to decrypt the message. If this is successful, the user supplied by the client is authenticated. HP SIM 5.x utilizes this authentication method in addition to public key authentication.

Password authentication uses the familiar mechanism to authenticate a user. The user name and password are sent over the encrypted channel to the SSH server, which authenticates the user using the supplied password. HP SIM 5.x also supports this method.

The diagram below shows how the key files are used by the SSH server and client.



SSH Server on Windows – differences

While HP-UX and most Linux distributions usually ship with SSH or OpenSSH already installed, the same is not true of Windows-based operating systems. HP SIM provides a version of OpenSSH to be used on Windows systems. This is installed along with the rest of the HP SIM software when being installed on a Windows platform (thereafter called the CMS). For managed systems, it can be installed from the Management CD, downloaded from the HP SIM website (http://www.hp.com/go/hpsim) or deployed from HP SIM to other Windows systems. Functionality has been added to HP SIM for improved deployment to all Windows systems.

SSH was originally implemented for UNIX-like operating systems and is part of OpenBSD. OpenSSH is an outgrowth of that effort. To easily port it to be used on Windows systems, an emulation layer called Cygwin is used. Cygwin provides a UNIX emulation layer so that UNIX software can be easily ported to Windows. It also includes well-known security problems. For example, it creates world-readable data structures to emulate UNIX processes. The potential exists for a non-administrator user on the managed system to interfere with tasks run on that system. To make OpenSSH more secure, the version distributed with HP SIM contains a modified Cygwin compatibility layer that restricts access to these data structures to members of the Administrator's group. The OpenSSH version shipped with HP SIM only allows Windows Administrators to log into the Windows system by way of SSH. Further, domain users must be a direct member of the Administrators group; membership of domain groups is not checked.

Cygwin mounts

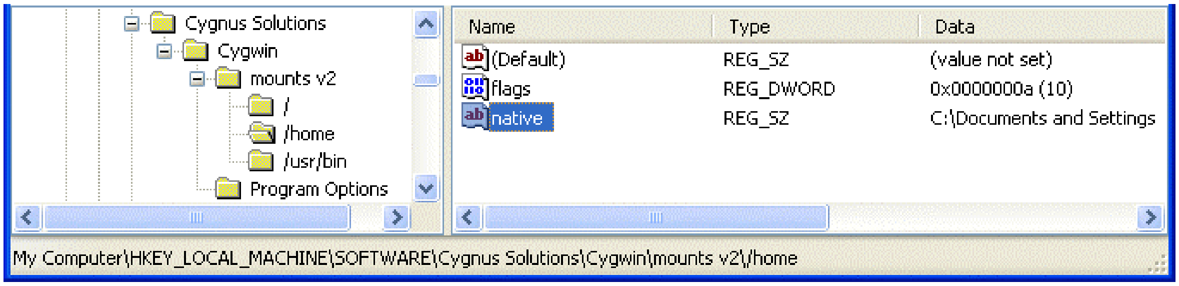
To find certain OpenSSH files, you must first determine where they are stored. The UNIX files of concern are `/etc/passwd`, `/etc/group`, and `/home/<username>`. To see the complete listing for Linux and HP-UX and where they are located for Windows, refer to Directory location of various SSH files

Cygwin emulates a UNIX environment. To locate files such as `/etc/passwd` and `/etc/group`, and the user's home directory (for example, `/home/<username>`), Cygwin sets up mount points.

In the registry, navigate to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2
```

Under this registry key the following three mount points are defined: `/`, `/home`, and `/usr/bin`.



Name	Type	Data
(Default)	REG_SZ	(value not set)
flags	REG_DWORD	0x0000000a (10)
native	REG_SZ	C:\Documents and Settings

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2\/home

The native key under each of these is set to the corresponding Windows directory. Therefore, to determine where `/home` maps to, look up the following and read the native key value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2\/home
```

This mount point defaults to C:\Documents and Settings.

Similarly, the root directory (/) defaults to `C:\Program Files\OpenSSH`. So, `/etc/passwd` is found in `C:\Program Files\OpenSSH\etc\passwd` and the `/usr/bin directory` defaults to `C:\Program Files\OpenSSH\bin`.

Passwd and group for Windows Implementations

The passwd file contains an entry for each user who is allowed to use SSH. If a user who is not listed in the password file tries to login through SSH, the connection fails with an illegal user error.

Note: The `passwd` file on Windows does not actually contain any passwords but it does contain the path of the user's home directory.

HP SIM provides a special utility **sshuser** to manage the `passwd` file. This is described later.

SSH and HP SIM

HP SIM acts as an SSH client, communicating with an SSH server that runs on a managed system (or on the CMS itself). HP SIM uses the SSH server provided with the HP-UX and Linux media. SSH is installed with recent versions of HP-UX and can be added to older versions. Various versions of Linux include SSH which is then installed automatically when the OS is installed. Testing of HP SIM has been with SSH-2 implementations.

HP SIM uses and installs OpenSSH when it is installed on Windows systems. The SSH client used by HP SIM should be compatible with other implementations of SSH or OpenSSH installed on managed systems. Testing of HP SIM has been with SSH-1.5 and 2.0 implementations. OpenSSH uses Cygwin, only one Cygwin service can exist at a time on a Windows platform, and the version provided with HP SIM has been modified to make it more secure than the open version.

The version of OpenSSH provided by HP SIM on Windows is not compatible with the F-Secure versions.

Which HP SIM features use SSH?

HP SIM uses SSH to run commands on managed systems. These commands include the Command Line Tools plus many HP-UX and Linux management tools. The Virtual Machine Management Pack (VMM) plug-in to HP SIM requires SSH on the virtual machine host system in order to deploy the VMM agent. In addition you can add your own tools that use SSH.

Custom commands are executed on the CMS platform from HP SIM. When you select a custom command to be executed against a set of managed systems, the HP SIM custom command process logs into the platform using SSH and the current HP SIM sign in, then the process is executed on the CMS platform. The list of systems is passed to the DTF through an environmental variable. The custom command then does what it was written to do against each target system. It is not necessary for the target systems to be running SSH to function properly. The custom command could operate though another protocol that, for example, network switches understand. Unlike most command line tools, only the CMS platform has to be running an SSH server to enable custom commands. This is true with some of the HP SIM plug-ins such as HP ProLiant Essentials Vulnerability and Patch Management Pack (VPM), HP ProLiant Essentials Rapid Deployment Pack (RDP) 2.0, HP ProLiant Essentials Performance Management Pack (PMP), and Open Service Event Manager (OSEM).

Command line tool execution is a powerful capability. There are two types of tools:

- Single-system aware (SSA)
- Multi-system aware (MSA)

MSA tools function similar to custom commands in that the tool is run on an execution system, which is usually the CMS platform, and the target systems are passed by using an environmental variable. The tool is responsible for communicating with the managed systems using whatever protocol it uses. Software Distributor for HP-UX is an example of an MSA tool. The execution system is the system running the Software Distributor service. SSH must be running on that system so that the CMS can contact it with information about the software to install and the managed systems on which to install it.

Unlike custom commands and command line tools, SSA tools are run directly on the managed system. The DTF opens an SSH client connection with each of the target systems, executes the command over the SSH protocol, and stores any output, including valid command output as well as error messages, in the HP SIM database. This process occurs on each target system that you selected which requires each target system to be running an SSH server. Examples of both MSA and SSA command line tools that ship with HP SIM can be found in Appendix B: Tool examples.

A special SSH bypass feature on the CMS enables MSA tools to run without SSH if they are to run on the CMS as the Administrator or root account; other MSA tools and all SSA tools and custom commands require SSH.

To summarize, the CMS must have an SSH server installed and configured to run any custom commands and most MSA command line tools, *unless* the tool is to run as Administrator or root. In addition, each managed system that you want to select as a target for an SSA command line tool must be running a properly configured SSH server.

SSH Bypass

The special SSH Bypass feature enables MSA commands to be run on the CMS without using SSH. Due to security concerns, only commands that are intended to run as root or administrator should be run with this bypass feature. The actual list of user names that use the bypass feature is listed in the HP SIM global setting property `mx_dtf_ssh_bypass_user`; the HP SIM installation includes the user Administrator or root. The current value of this property can be viewed with the following command:

```
>   mxglobalsettings -ld mx_dtf_ssh_bypass_user
    mx_dtf_ssh_bypass_user = Administrator
```

Additional users can be added by separating the user names with commas and no spaces. Domain accounts require two backslashes between the domain name and the user name, such as `domain\\user`:

```
 >   mxglobalsettings -s
     mx_dtf_ssh_bypass_user=Administrator,Domain\\SIM
```

HP SIM must be restarted after making changes to the bypass user.

How does HP SIM use SSH?

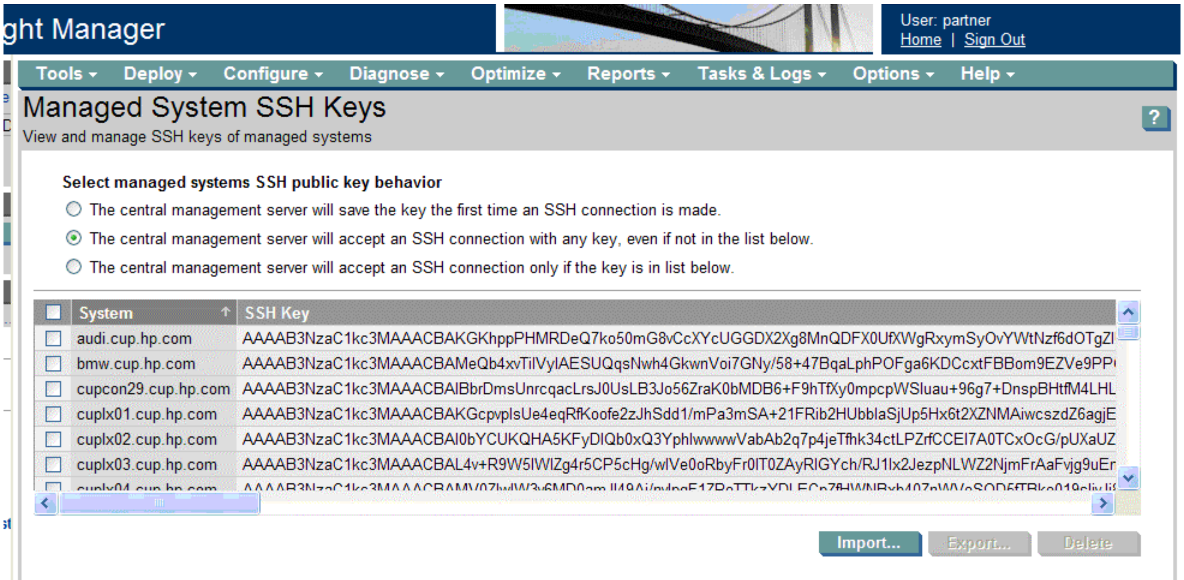
HP SIM acts like the SSH client described earlier. The main difference to an interactive SSH client is that HP SIM must be preconfigured with appropriate keys, passwords, and rules on how to handle security warnings. The following sections discuss how HP SIM is configured and the file locations used by HP SIM.

Managed system authentication

When HP SIM connects through SSH to a managed system, the SSH server on that system returns an SSH host key that identifies that system. HP SIM must decide if this key is acceptable and hence authenticate the managed system. By default, HP SIM 5.x accepts any key, which does leave HP SIM open to certain types of network attack such as a man in the middle attack where an imposter pretends to be the managed system. You can configure HP SIM to protect against such attacks by turning on SSH host key checking, causing HP SIM to compare the key with a list of known hosts. Three options are supported:

- The key is saved the first time a connection is made. On subsequent connections the key must match the saved value or the connection is refused. This option is open to a man-in-the-middle attack the very first time a connection is made, but subsequently is very secure. This option requires manual intervention if keys are ever changed. For example, if the SSH server on the managed system is reinstalled. HP SIM 4.x used this method.
- The CMS accepts an SSH connection with any key, even if it is not in `known_hosts`. The key is still saved in `known_hosts` the first time a connection is made, but no key checking is performed. This provides the easiest to manage solution, but is vulnerable to some attacks. This is similar to the default SSL option of not requiring trusted certificates, which is now the default setting for HP SIM 5.x.
- The key must already exist in the known hosts file. The connection is refused if it is not in the file. This option is the most secure but the hardest to maintain, as keys must be manually added to the list of known hosts as new systems are added or whenever keys are changed.

A tool in HP SIM 5.x (**Options→Security→SSH Keys**) enables you to change this setting, to have keys loaded on first use, and to require they be preloaded. This tool enables keys to be imported or removed from the known hosts file.



Managed System SSH Keys

View and manage SSH keys of managed systems

Select managed systems SSH public key behavior

○ The central management server will save the key the first time an SSH connection is made.

● The central management server will accept an SSH connection with any key, even if not in the list below.

○ The central management server will accept an SSH connection only if the key is in list below.

□	System	SSH Key
□	audi.cup.hp.com	AAAAB3NzaC1kc3MAAACBAKGKhppPHMRDeQ7ko50mG8vCcXYcUGGDX2Xg8MnQDFX0UfXWgRxymSyOvYWtNzf6dOTgZI
□	bmw.cup.hp.com	AAAAB3NzaC1kc3MAAACBAMeQb4xvTilVylAESUQqsNwh4GkwnVoi7GNy/58+47BqaLphPOFga6KDCcxtFBBom9EZVe9PP
□	cupcon29.cup.hp.com	AAAAB3NzaC1kc3MAAACBAIBbrDmsUnrcqacLrsJ0UsLB3Jo56ZraK0bMDB6+F9hTfXy0mpcpWSluau+96g7+DnspBHtfM4LHL
□	cuplx01.cup.hp.com	AAAAB3NzaC1kc3MAAACBAKGcpvplsUe4eqRfKoofe2zJhSdd1/mPa3mSA+21FRib2HUbblaSjUp5Hx6t2XZNMAiwcszdZ6agjE
□	cuplx02.cup.hp.com	AAAAB3NzaC1kc3MAAACBAI0bYCUKQHA5KFyDIQb0xQ3YphlwwwwVabAb2q7p4jeTfhk34ctLPZrfCCEI7A0TCxOcG/pUXaUZ
□	cuplx03.cup.hp.com	AAAAB3NzaC1kc3MAAACBAL4v+R9W5IWIZg4r5CP5cHg/wIVe0oRbyFr0IT0ZAyRIGYch/RJ1Ix2JezpNLWZ2NjmFrAaFvjg9uEr
□	cuplx04.cup.hp.com	AAAAB3NzaC1kc3MAAACBAMV0ZlwlW3v6MD0am lI49Ai/nvlngF17RaTTkzYDLECn7fHWNBxh40ZnWVoSOD5fTBko019cliv li

The setting used to manage control key checking is in the file `<HP SIM>/config/mx.properties` in Windows and `/etc/opt/mx/config/mx.properties` in Linux and HP-UX:

`MX_SSH_ADD_UNKNOWN_HOSTS=firstuse` (or 'always' or 'never')

Note: Before modifying this property, you must first stop the HP SIM service. Once you have modified the property, restart the HP SIM service.

The list of known hosts used by HP SIM is stored in this file `<HP SIM>/config/sshtools/known_hosts` in Windows and `/etc/opt/mx/config/sshtools/known_hosts` in Linux and HP-UX. Note that this is not the same file used by other SSH clients, which is typically in a user directory named .ssh.

User authentication

The managed system must authenticate the user that HP SIM has chosen to make the SSH request. The user is specified by the tool being run:

- The tool can specify an explicit account to be used for this tool through the </execute-as-user> statement in the tool definition (described later). Typically, tools run as the user root for UNIX systems or Administrator for Windows systems.
- If no explicit user is specified in the tool then it runs as the same user name as the person attempting to run the tool. For example, if user 'joe' is signed in to HP SIM and attempts to run a tool, then HP SIM attempts to connect to the managed system as user 'joe'. The managed system must have a user with this name, and it must be correctly configured to enable SSH access for that user.

All the tools shipped with HP SIM run as root or Administrator. Additional tools can be added, such as custom tools, which run as other users.

As discussed earlier, SSH supports three methods of user authentication: user public key, host key, and password. HP SIM supports all three of these methods. In most cases user public key authentication is recommended, as is the most secure. You can choose to use host key or password authentication if you want, as discussed later in Configuration Options.

The same key pair is used for both key-based mechanisms and is used for all users and all managed systems. The private key is located in the `<HP SIM>/config/sshtools/.dtfSshKey` file in Windows and `/etc/opt/mx/config/sshtools/.dtfSshKey` in Linux and H-UX, with the corresponding public key available for copying to other systems at <HP

SIM>/config/sshtools/.dtfSshKey.pub in Windows and /etc/opt/mx/config/sshtools/.dtfSshKey.pub in Linux and HP-UX.

- User public key authentication is attempted first. The SSH server on the managed system attempts to find a matching public key for the specified user. These keys are normally stored in a file authorized_keys2, which is located in the .ssh subdirectory of the specified user's home directory.
- If the user key authentication fails, host authentication is attempted. The SSH server attempts to find the public key in the list of acceptable hosts, typically stored in the etc/ssh_known_hosts file. In addition, the name of the client system (for example, the CMS) must be listed in the etc/shosts.equiv file. Refer to Directory location of various SSH files to find these files.

  Note: HP recommends that users root and Administrator not be authenticated using host-based authentication; user public key authentication is recommended instead, although password authentication can also be used.

- If neither of these methods succeed, HP SIM verifies if an SSH password has been configured for this user and managed system. This can be configured in the HP SIM user interface or command line. If present, this is passed to the SSH server which uses its own system authentication to validate the password.

HP SIM provides command line tools and Web-based interfaces to manage and configure the SSH user credentials:

- **sshuser** is a new tool for HP SIM 5.x used on a Windows managed system to manage user entries in the passwd file.
- **mxagentconfig** tool is used to copy the public key from the CMS to the managed system for user or host-based authentication. This tool can also be used to validate the SSH configuration and to remove entries from the CMS known_hosts file.
- **mxnodesecurity** is used to save passwords on the CMS for use with SSH and other protocols.
- **Install OpenSSH** installs and configures OpenSSH on Windows managed systems.
- **Configure or Repair Agents** configures users for SSH access on managed systems.
- **SSH Keys** is used to manage the authentication mode and known_hosts entries on the CMS.

Full details of these are described in the section HP SIM commands and tools.

Renamed or disabled 'Administrator' account

Often the Windows Administrator account has been renamed for security reasons, and HP SIM tools should be run with this renamed account. HP SIM automatically detects the renamed account during installation and sets the global property *WindowsAdminUserName* to this name. Any tools that are to run as Administrator automatically run with this changed name.

```
>    mxglobalsettings -ld WindowsAdminUserName
     WindowsAdminUserName = MyAdmin
```

In some circumstances the Administrator account might be disabled. In this case, you must specify a different administrative account for tools to use by changing this global property:

```
>    mxglobalsettings -s WindowsAdminUserName=MyDomain\AlternateAdmin
```

Note: HP SIM must be restarted after making changes to the Windows Administrator user name.

Add this user account to HP SIM with full-configuration-rights and authorizations on all systems, including the CMS, using the **Options→ Security→Users and Authorizations** menu or the following command:

```
>   mxuser –a MyDomain\AlternateAdmin -p full –C Administrator
```

Note: If you run the mxuser command, you must assign the appropriate authorizations to the user by running the mxauth command.

This user account will also need to be authorized for SSH access on the managed system: it must be added to the passwd file and be set up for user, host or password authentication. Running the Configure or Repair Agents tool with this user name will set up the system appropriately. Decide which method to use by referring to the Configuration steps section.

Configuration steps

When HP SIM is initially installed on the CMS system, SSH is configured in the following way:

- If installing on Windows:
  - OpenSSH is installed, with the special version of Cygwin
  - The name of the administrator account (which might have been renamed from Administrator) is saved
  - The installing user and administrator are added to the passwd file (in `C:\Program Files\OpenSSH\etc`)
  - The installing user and administrator are configured for user public key authentication
  - The administrator is configured for the SSH bypass feature
- If installing on Linux or HP-UX
  - SSH should be preinstalled from the operating system
  - The root user is configured for user public key authentication
  - The root and Administrator users are configured for the SSH bypass feature

OpenSSH can be installed on managed systems that are to run SSA tools. There are a number of ways to install OpenSSH to a Windows system:

1. Using the Install OpenSSH tool

   This is perhaps the easiest way to deploy OpenSSH to a Windows managed system. The tool runs the OpenSSH installation, adds both the user specified and the administrator user to the passwd file, and then configures these users for public key authentication from the CMS. This tool is only available on a CMS that runs on Windows and the OpenSSH can be deployed only to Windows management systems.

2. Separate OpenSSH Install

   The OpenSSH install package can run from the HP SIM download or management CD, or can downloaded separately from the HP SIM website.

   Once the installer has been run, the system must be configured for access by HP SIM. Either run the Configure or Repair Agents tool on the systems, specifying the administrator or other account to be used by SSH; or take the following steps:

   a. The user used by HP SIM must be added to the passwd file using the sshuser utility on the managed system. (The example here shows user MyDomain\MyAdmin.)

      ```
      sshuser –u MyAdmin –d MyDomain –f
      "C:\Program Files\OpenSSH\etc\passwd"
      ```

   b. The user must be an explicit member of the local administrators group, as domain groups are not checked by OpenSSH. If a domain user is used, add the user to Administrators if it is not already a member of this group.

      ```
      net localgroup administrators MyDomain\MyUser /add
      ```

c. The command completed successfully. mxagentconfig should be run on the CMS to configure public key authentication for the administrator user

```
mxagentconfig -a -n <managed system> -u administrator
```

3. Using the ProLiant Support Pack

   OpenSSH can be installed as part of software and firmware updating using a ProLiant support pack. This installs the SSH server but does not configure SSH for access from the CMS. Step 2 above (Separate OpenSSH Install) must be followed to configure the HP SIM user and keys.

Linux or HP-UX managed systems normally have SSH installed and running. See the operating system documentation for details to enable SSH if needed. SSH must still be configured for access by the CMS user. Either use the Configure or Repair Agents tool or run **mxagentconfig** to enable public key access for the root user:

```
mxagentconfig -a -n <managed system> -u root
```

After completing these steps SSH is installed and configured for use by the standard HP SIM tools, which run as root or Administrator.

Other users might also need to be configured for SSH access, including any user who is to run a custom command or a tool that does not include an execute-as-user statement and any user name that is specified in an execute-as-user statement. If additional users are to be configured you must add these users to the passwd file on the managed system using sshuser (for Windows only), and run mxagentconfig to enable access by the CMS.

Configuration Options

The above steps configure the CMS and managed system to run SSH tasks as the Windows Administrator (which might be renamed from Administrator) or as root, using public key user authentication. There are additional options, which might be useful in your environment:

- When managing Linux or HP-UX systems and using tools that run as a user (rather than as root), it might be convenient to use host-based authentication. (This is not as useful on Windows because each user must still be added to the passwd file.) Note that the root user needs specific user public key authentication as host-based authentication is not supported for root or Administrator.

  ```
  mxagentconfig -a -n <managed system> -u root –o host
  ```

- Password authentication can be used as an alternative to key-based authentication, for example, if there are problems installing the keys on the managed system. The CMS must be configured with the password to use for the managed system.

  ```
  mxnodesecurity –a –p ssh –c root:mypwd –n <managed system>
  ```

SSH files

There are a number of important files involved in correct configuration and operation of SSH.

On each managed system configured for SSH there are the following files:

- The SSH server program files
- The SSH server private key `ssh_host_dsa_key` and the corresponding public key `ssh_host_dsa_key.pub`. These keys are generated when SSH is installed and are used to identify the managed system.
- The SSH server configuration file, `sshd_config`. Among other settings, this file enables host authentication and user key authentication.
- For Windows only, the passwd file located in the `\OpenSSH\etc` directory. This file specifies which users are permitted to access to the system through SSH, along with their home directory.

- Each user configured for user public key authentication will have the user's public key in the **authorized_keys2** file. This file is in the .ssh directory of the user's home directory, as specified in the passwd file. Note that on Windows, HP SIM often uses the directory hpsimssh instead of the real home directory for a user; see the command 'sshuser' below for details.
- If host-based authentication is used, the name of the CMS system must be in the shosts.equiv file and the public key of the CMS in the `ssh_known_hosts` file. These files are in the SSH server configuration directory.

In addition, the following files are used on the CMS when making SSH requests:

- The CMS private key `.dtfSshKey` and the corresponding public key `.dtfSshKey.pub`. These are generated when HP SIM is installed and are used to authenticate users or the CMS itself.
- **known_hosts** contains the public keys from managed systems running SSH. This file might be automatically populated by HP SIM.

Directory location of various SSH files

File type	HP-UX	Linux	Windows
OpenSSH install	`/etc/opt/ssh/`	`/etc/ssh/`	`C:\Program Files\OpenSSH\`
OpenSSH keys ssh_host_dsa_key	`/etc/opt/ssh/`	`/etc/ssh/`	`C:\Program Files\OpenSSH\etc`
OpenSSH configuration sshd_config	`/etc/opt/ssh/`	`/etc/ssh/`	`C:\Program Files\OpenSSH\etc`
passwd and group files	`/etc/`	`/etc/`	`C:\Program Files\OpenSSH\etc` (uses SID for Windows user; specifies home directory)

Public key authentication authorized_keys2	`$HOME/<usr>/.ssh`	`$HOME/<usr>/.ssh`	`C:\Documents and Settings\<usr>\.ssh or`
			`C:\Documents and Settings\hpsimssh\.ssh`

Host authentication ssh_known_hosts and shosts.equiv	`/etc/opt/ssh/`	`/etc/ssh/`	`C:\Program Files\OpenSSH\etc`

CMS client ssh keys
.dtfSshKey and .dtfSshKey.pub
	`/etc/opt/mx/config/sshtools/`
	`(hidden files)`
		`etc/opt/mx/config/sshtools/`
		`(hidden files)`
			`C:\Program Files\HP\Systems Insight Manager\config\sshtools\`

known_hosts (for HP Systems Insight Manager)	`/etc/opt/mx/config/ sshtools/`	`/etc/opt/mx/config/sshtools/`	`C:\Program Files\HP\Systems Insight Manager\config\sshtools\`

Known_hosts

The list of known host keys can be found in the file `known_hosts`. It contains the public host keys of the SSH servers that are trusted by the SSH client and HP SIM. Note that, by default, HP SIM does not require host keys to match the entries in the known_hosts file.

Here is an example of a `known_hosts` file displaying two entries:

```
192.103.1.21 ssh-dss
AAAAB3NzaC1kc3MAAACBAM8yDS/qQI8pqwavOcXat4ygJFSsX1SNqXvW7sKzYrYF0k1
```

```
wk9LyUyHdnTVI8MRRQYZpOsR+UFqhHz2/emADlNSvlL2mHtd5yUbz/QKWT6ikAX7lxe
Pg1HtcDvFfLoPG8k0uENvQgb1Exfzbdf9+CpoyG0QFnrWns+xYzBW3FbpXAAAAFQCHO
IKdwA0A1qNNHPKbbCCnzOg3+wAAAIAeGMN7NuaR72bHGe9pgBd9vBh3MX/Jdh8aptFR
Tl0cj4U/0aMa5WU4z/dL9N/8/GmgGxHr1VAJjF4TaIyC0HsM7/t16TunDHr9OFddsWg
RCP3UBA28xwLI/enCuORTwcyW0M+SMMOPcPgDd74OOGN+gK107sSstMNn9ooOAGnw5A
AAAIBQwoqfiDV6Zmp+v0XO+TWr12Hta2u8ZeeWfoM1ZeQnSUyRuv0Cf1vcUFS6BeFlI
X+b7+zqtZfFP3xQTgMHk7Uf3t1NJHBSr9kI4Te3Mdj2WLClcMnEMPPqoa5w5+5GGGBC
+zPqT2t6ZZ8rqo3Hf8vJwUZvQfZrrWi5hGQa6/snnA==
```

```
Ovpc129.rse.hp.com,192.87.137.243 ssh-dss
AAAAB3NzaC1kc3MAAACBALuFgiIFPeNLJw7o4/wup7Qal8qZSRJWVe/oZb7BR9haLA9
oc5yhDv07a1xHgyAzkg3ghdoVk70QbMye44DTP4VHPzM1CQ4jSVRC8+l9sPvMPlCfAl
am66c15GInVytqExcD5zTu1wSp44oJne0yFJ9XcGLcNGP+x4wa7D2C3Mr/AAAAFQDDV
P1Kn8pJMvbq46/T86T1uMZ0QQAAAIEAk/qa4eyxlmWoPO2GxEPv9+LP1KNM2YzfZuJF
AgV6XWTbaEHYh8uDsgpjddTDi4Yu49u5xIdS1+bFjb72WQKZj46EH4BTddUNTUYVHUp
kGgwJDB8ie+jJCkqJg8wJexDJquK+EGAYYkitLpUoVUHKTFxXiX4DxfK7cv+IDZ7UAJ
AAAACAcK7VcmEBCqcgGNJXhsj1laM1ujDfxXgCzXjMdotMkib8Ye1vp3hc2MuN6BVz7
OeJTsopFTEj2J86SoT9zIl9qPO/rm3FrCIm/8VuDVezcpVIS7TyrSQWbdQwVmeAJX/u
TIJB48suUDrjlF/bsUfM1naU/kZFSwnMo09Pa+mJ/uI=
```

Note: There can be more than one key for a system in the known_hosts file. It can be listed by IP address, short DNS name, and fully qualified DNS name. Only the first key identified during the transaction is read. If incorrect, the connection is rejected.

Client Public Key Authentication

For public key client authentication as used by HP SIM, a key pair is created and stored in the `C:\Program Files\HP\Systems Insight Manager\config\sshtools` directory. The private key never leaves the client. It is used during authentication to decode messages that the remote SSH server encodes with the matching public key. The public key is not used by the SSH client. It is stored here so that it can be copied to remote systems. The public key is appended to the `authorized_keys2` file for a given user on the remote managed system. This is the list of keys that is checked by the SSH server when a remote login is being requested using public key authentication. If the key being presented by HP SIM is listed in the file, the SSH server uses it to encrypt a challenge to return to HP SIM; the SSH server enables the user to sign in provided the response to the challenge is correct. If the public key is not present, the public key authentication fails.

While the `authorized_keys2` file can be maintained manually, HP SIM provides the mxagentconfig utility to maintain this file.

Host-Based Authentication

Two files in the SSH server configuration directory (for example, `C:\Program Files\OpenSSH\etc`) are used to configure host-based authentication. The file, `shosts.equiv`, is a list of host names that are accepted for host-based authentication, for example, the DNS name of each CMS that can manage this system. The file, `ssh_known_hosts`, is a list of public keys for these host CMS systems.

Passwd and group files

For Windows systems the passwd file is located in the `C:\Program Files\OpenSSH\etc` directory. After the SSH session is established between the SSH client and the SSH server, the SSH client transmits the login user name to the SSH server. For each user name allowed to use SSH, there must be an entry in the `passwd` file. If a user name is not listed in the password file but tries to login, the connection fails with a permission denied authentication error.

The following example passwd file contains three lines for three different users: local administrator MyAdmin, local user SIM, and user joe from domain mydomain:

```
MyAdmin:unused_by_nt/2000/xp:500:513:U-BRIAN06\MyAdmin,S-1-5-21-
1148942700-1292286586-3675345140-
500:/home/Administrator:/bin/switch
```

```
SIM:unused_by_nt/2000/xp:1011:513:Account for HP SIM Service,U-
BRIAN06\SIM,S-1-5-21-1148942700-1292286586-3675345140-
1011:/home/SIM:/bin/switch
mydomain\joe:unused_by_nt/2000/xp:9159:513:JOE,U-mydomain\joe,S-1-
5-21-27163274-143742939-1512734326-9159:/cygdrive/C/Documents and
Settings/hpsimssh:/bin/switch
```

When the HP SIM OpenSSH package is installed on the Windows platform, a password entry for whatever user name is running the install, as well as Administrator is created at `C:\Program Files\OpenSSH\etc\passwd`. The Administrator user name is set due to all of the HP SIM preinstalled Windows command line tools which run as Administrator. (Note this user name might have been renamed, in which case HP SIM configures SSH with this renamed user name). The etc\group file is also created at install time, but this file should not need updating to add subsequent user names.

Additional user names are authorized by creating an entry for each one. The entry actually contains a SID and the password remains internal to Windows and is not included in this file. HP SIM provides a utility, **sshuser**, to manage this file (`C:\Program Files\OpenSSH\bin\sshuser.exe`). This command looks in the user's settings and extracts relevant information for the user name and the user's home directory. The output from sshuser is concatenated to the end of the passwd file. See to sshuser for more details.

HP SIM commands and tools

sshuser

This command is to be used on a Windows managed system to maintain the list of users that are allowed access through SSH. This command is installed with the version of OpenSSH supplied by HP SIM and it adds entries to the passwd file on a managed system.

Note: sshuser is a new utility included with the OpenSSH supplied by HP SIM 5.x and replaces the **mxpasswd** command previously available. This utility was not supplied with previous version of OpenSSH from HP. If not present on the managed system it can be copied from the HP SIM installation directory (`C:\Program Files\HP\Systems Insight Manager\lbin\sshuser.exe`).

For example, the following command permits SSH access for user joe in the Windows domain MyDomain:

```
sshuser –u joe –d MyDomain –f "C:\Program Files\OpenSSH\etc\passwd"
```

This command adds the following entry to the end of the passwd file:

```
mydomain\joe:unused_by_nt/2000/xp:9159:513:JOE,U-mydomain\joe,S-1-5-21-
27163274-143742939-1512734326-9159:/cygdrive/C/Documents and
Settings/hpsimssh:/bin/switch
```

The domain name is included with the user, to remove any conflicts between users from different domains with the same name. The home directory specified is hpsimssh rather than the user's real home directory; this is because this user has never logged into this system before and therefore does not have a real home directory assigned by Windows. The home directory specified here is used to locate the ssh keys for user authentication; as the same keys are used by HP SIM for all users, a common home directory sshuser can be used.

Sshuser also ensures that the passwd file only contains a single entry for a given user. It removes duplicate entries for the given user.

Sshuser must be run by an administrator of the system, and (for HP's implementation of OpenSSH on Windows) only administrators can be given SSH access. In addition, the user running sshuser must have sufficient rights to obtain the SID for the user being added. A local user has sufficient rights to add other local users, but a domain account must be used if domain users are to be added. If in doubt, run sshuser without the -f option to view the output of the command.

Mxagentconfig

mxagentconfig is used to configure the managed system to allow SSH access from the CMS. Different options are available to set up user public key, host-based authentication, or to validate an existing configuration. An option is also available to remove entries from the CMS `known_hosts` file.

```
mxagentconfig -a -n <managed system> -u <username> [-p <password>]
```

This option configures user-based public key authentication on the specified managed system. It places the public key (`.dtfSshKey.pub`) of the HP SIM CMS in the user's `authorized_keys2` file.

First, mxagentconfig opens an SSH connection to the specified managed system. This means that SSH has to be already installed on the managed system. If the specified system is a Windows system, then the user must already have been added to the passwd file. See the sshuser section. The SSH server uses password authentication to validate the specified user. A secure ftp (sftp) channel is then opened to allow file access to the managed system.

The user's home directory is examined for the `.ssh` subdirectory. If it does not exist, it is created. Then mxagentconfig checks for the existence of the `authorized_keys2` file. If it exists, mxagentconfig appends the public key of the CMS (`.dtfSshKey.pub`) to this file. If the file does not exist, it is created with the public key of the CMS as its first entry. At this point, the user is configured for public key authentication on the managed system.

```
mxagentconfig -a -n <managed system> -u <username> [-p <password>] –o
host
```

This option configures host-based authentication on the managed system. It requires that SSH be installed on the target system and, if the target is a Windows system, the user must be included in the passwd file. It connects to the managed system using password authentication and then uses sftp, as described above. Then it updates the files in the SSH configuration directory on the managed system: it adds the public key to the `ssh_known_hosts` file and adds the CMS name to the list of accepted hosts in the `shosts.equiv` file.

mxagentconfig -c -n <managed system> -u <username>

This version of the command does not configure the managed system but instead verifies that SSH access is correctly configured for the specified user. This command will return success if the `passwd` file allows SSH access for the specified user, the public key has been correctly set up for user or host based authentication, and the user is a member of the system's Administrators group. An error is reported if host key checking is enabled and the host key does not match the value in the `known_hosts` file. This command does not verify password authentication.

```
C:\> mxagentconfig -c –n brian06.cup.hp.com -u myadmin
myadmin@brian06.cup.hp.com: success
```

mxagentconfig -r -n <managed system>

This version of the command removes the specified host from the `known_hosts` file. This command uses the DNS server to find all versions of the system name and removes them from the file.

Mxnodesecurity

The **mxnodesecurity** utility is used to store user names and passwords on the CMS for use when accessing managed systems. It is used for all management protocols, and has been extended to support SSH password authentication. As previously mentioned, user or host key authentication is preferred and provides benefits over password authentication. Use this command if you are unable to configure key-based authentication using **mxagentconfig**.

```
mxnodesecurity –a –p ssh –c <username>:<password> –n <managed system>
```

This form of the command is used to save an SSH user name and password for use with a specific managed system. For example the following command cause HP SIM to use the password 'mypwd' whenever a task for user 'administrator' is run on system 'brian06':

```
mxnodesecurity -a -p ssh -c administrator:mypwd -n brian06.hp.com
```

Note that this password is only used if user key and host based authentication have failed, and only if the user name for the task matches this entry.

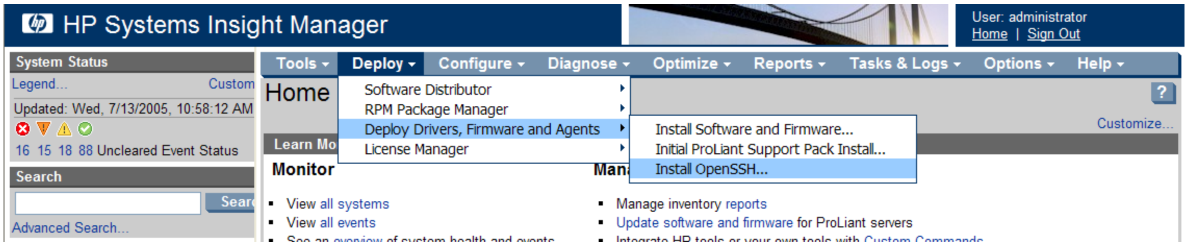
```
mxnodesecurity –l –p ssh [–n <managed system>]
```

This form of the command lists the SSH credentials for the specified system, or all systems if a system is not specified. For example the following command lists the SSH credentials for node brian06 (note that the password itself is not displayed):

```
C:\> mxnodesecurity -l -p ssh –n brian06.hp.com
TARGET NODE        PROTOCOL NAME          PASSWORD
harrison.cup.hp.com ssh      administrator ********
```

Install OpenSSH

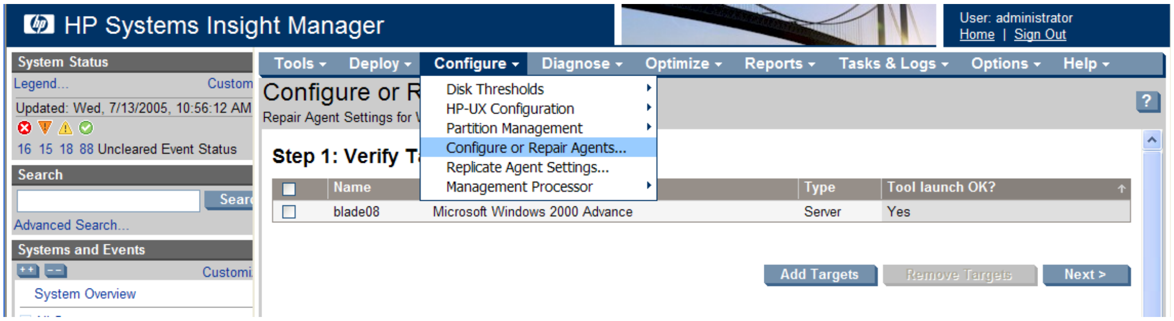
The HP SIM Deploy tools can be used to install OpenSSH on any Windows platform (**Deploy→Drivers, Firmware and Agents→Install OpenSSH**).


HP Systems Insight Manager
User: administrator
Home | Sign Out
System Status
Legend...
Custom
Updated: Wed, 7/13/2005, 10:58:12 AM
16 15 18 88 Uncleared Event Status
Search
Search
Advanced Search...
Tools
Deploy
Configure
Diagnose
Optimize
Reports
Tasks & Logs
Options
Help
Home
Learn Mo
Monitor
Mana
Software Distributor
RPM Package Manager
Deploy Drivers, Firmware and Agents
License Manager
Install Software and Firmware...
Initial ProLiant Support Pack Install...
Install OpenSSH...
Customize...
View all systems
View all events
See an overview of system health and events
Manage inventory reports
Update software and firmware for ProLiant servers
Integrate HP tools or your own tools with Custom Commands

After installing the OpenSSH software, the tool configures the installation. The user name specified when running the tool and the administrator user name (which might have been renamed from Administrator) to the passwd file. The tool then runs mxagentconfig for these users to allow this CMS access through user public key authentication: the public key of the CMS is added to the `authorized_keys2` file for each user.

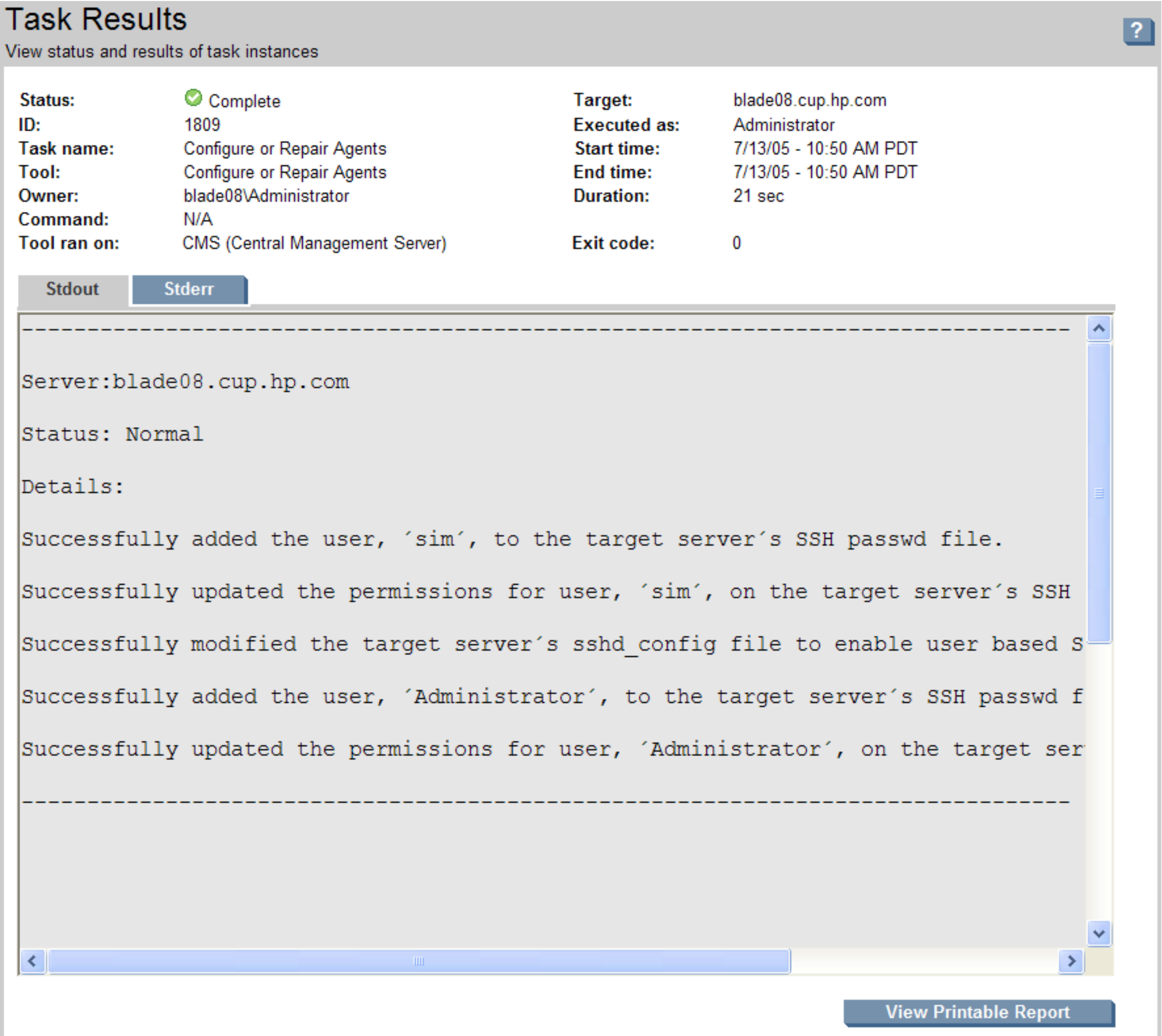
Configure or Repair Agents

The Configure or Repair Agents tool (**Configure→Configure Or Repair Agents...**) enables you to configure a number of agent settings, including SSH.



☐	Name		Type	Tool launch OK?
☐	blade08	Microsoft Windows 2000 Advance	Server	Yes

An option allows either host-based or user public key authentication to be used, and the tool adds the CMS public key to the appropriate file. For a Windows system this tool also adds the specified user to the passwd file, and ensures that the administrator user has SSH access in addition to the specified user.



Task Results

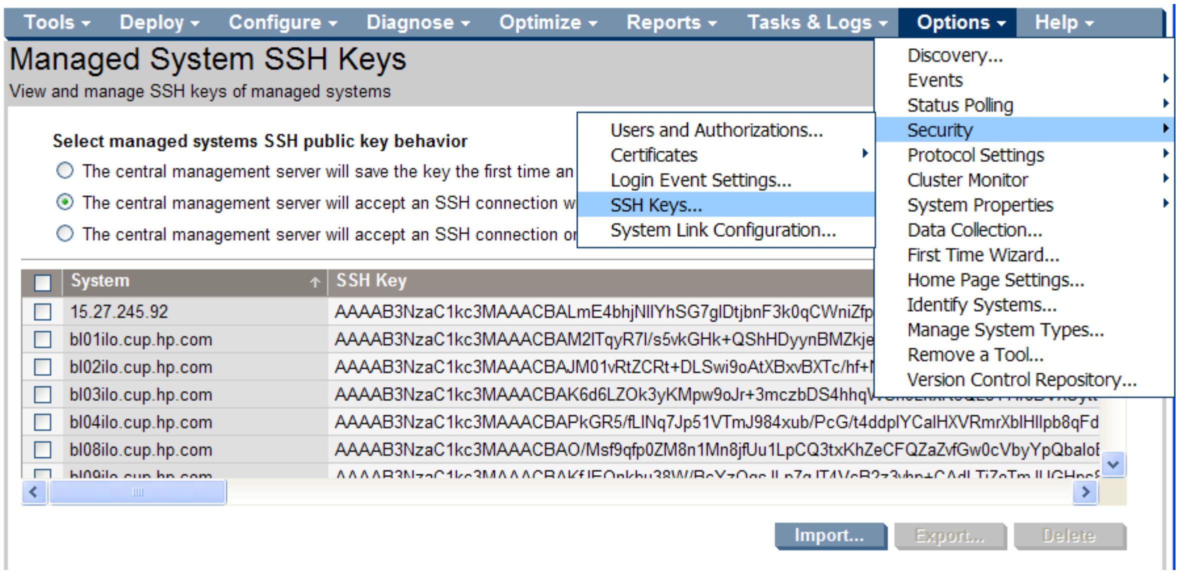
View status and results of task instances

Status:	✓ Complete	**Target:**	blade08.cup.hp.com
ID:	1809	**Executed as:**	Administrator
Task name:	Configure or Repair Agents	**Start time:**	7/13/05 - 10:50 AM PDT
Tool:	Configure or Repair Agents	**End time:**	7/13/05 - 10:50 AM PDT
Owner:	blade08\Administrator	**Duration:**	21 sec
Command:	N/A		
Tool ran on:	CMS (Central Management Server)	**Exit code:**	0

```
--------------------------------------------------------------------------------

Server:blade08.cup.hp.com

Status: Normal

Details:

Successfully added the user, ´sim´, to the target server´s SSH passwd file.

Successfully updated the permissions for user, ´sim´, on the target server´s SSH

Successfully modified the target server´s sshd_config file to enable user based S

Successfully added the user, ´Administrator´, to the target server´s SSH passwd f

Successfully updated the permissions for user, ´Administrator´, on the target ser

--------------------------------------------------------------------------------
```

SSH Keys

This tool (**Options→Security→SSH Keys...**) controls how HP SIM authenticates managed systems. The managed system's host keys can be verified against the `known_hosts` file on the CMS, and the entries in this file can be examined and changed.



Managed System SSH Keys

View and manage SSH keys of managed systems

Select managed systems SSH public key behavior

○ The central management server will save the key the first time an

● The central management server will accept an SSH connection w

○ The central management server will accept an SSH connection o

□	System	SSH Key
□	15.27.245.92	AAAAB3NzaC1kc3MAAACBALmE4bhjNlIYhSG7glDtjbnF3k0qCWniZfp
□	bl01ilo.cup.hp.com	AAAAB3NzaC1kc3MAAACBAM2lTqyR7l/s5vkGHk+QShHDyynBMZkje
□	bl02ilo.cup.hp.com	AAAAB3NzaC1kc3MAAACBAJM01vRtZCRt+DLSwi9oAtXBxvBXTc/hf+
□	bl03ilo.cup.hp.com	AAAAB3NzaC1kc3MAAACBAK6d6LZOk3yKMpw9oJr+3mczbDS4hhq
□	bl04ilo.cup.hp.com	AAAAB3NzaC1kc3MAAACBAPkGR5/fLINq7Jp51VTmJ984xub/PcG/t4ddplYCalHXVRmrXblHllpb8qFd
□	bl08ilo.cup.hp.com	AAAAB3NzaC1kc3MAAACBAO/Msf9qfp0ZM8n1Mn8jfUu1LpCQ3txKhZeCFQZaZvfGw0cVbyYpQbalol
□	bl09ilo.cup.hp.com	[illegible]

Conclusion

HP SIM uses the SSH-2 protocol to execute tasks on managed systems. This requires an SSH server to be running and accepting requests on each managed system on which tasks are to be executed.

Features of HP SIM that require SSH being installed and configured include custom commands and command line tools. HP SIM provides an OpenSSH package to be installed on Windows-based managed systems, as well as a key management tool (mxagentconfig) for setting up a user with the public key of the DTF.

The information contained here gives you an idea of remote task execution in HP SIM, and gives you an idea of where to start troubleshooting when there is a problem.

Common questions and tasks

How to change the port used by SSH

Normally, SSH servers listen on TCP port 22. If, for some reason, this must be changed, the SSH port that HP SIM uses is configurable.

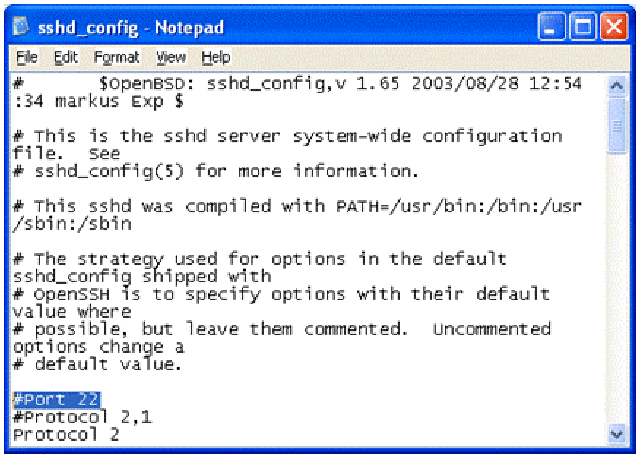
To configure the port that the SSH client for the CMS uses to initiate SSH sessions:

1. The SSH port used by HP SIM is set by changing *MX_SSH_PORT* in the `C:\Program Files\HP\Systems Insight Manager\config\mx.properties` file.
2. For example, to change the port to **6450**, add the following line to mx.properties:

   MX_SSH_PORT=6450

3. Every SSH server on each managed system and the CMS must be configured to listen on that port as well. Changing the port on the SSH servers is accomplished easily by the following method.

   a. Go to the managed system.
   b. Open the `C:\Program Files\OpenSSH\etc` directory.
   c. Edit the file `sshd_config` using Notepad or similar editor.



```
#       $OpenBSD: sshd_config,v 1.65 2003/08/28 12:54
:34 markus Exp $

# This is the sshd server system-wide configuration
file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr
/sbin:/sbin

# The strategy used for options in the default
sshd_config shipped with
# OpenSSH is to specify options with their default
value where
# possible, but leave them commented.  Uncommented
options change a
# default value.

#Port 22
#Protocol 2,1
Protocol 2
```

   d. Change the port number entry to the one used on the CMS and save the file.

Installing OpenSSH for Windows

OpenSSH is installed as a service running as an administrative user account (default is the installing user) for Windows XP and 2003. This account must have the appropriate user rights assigned in the Local Security Policy tool. OpenSSH runs as the local system account on Windows 2000 and NT4 installations.

The following rights are automatically added during OpenSSH installation:

- Log on as a service
- Create a token object
- Replace a process level token

Note: Sometimes a domain policy can prevent HP SIM from adding these rights to the installing user. HP SIM must be installed by a user who has these rights.

Installation Diagnostic File for SSH

When installation issues for the SSH portion of the HP SIM installation occur, the first location you should look in is the `initconfig.log` file. This file is located `C:\Program Files\HP\Systems Insight Manager\logs` and might provide clues.

Coexistence problems with other Cygwin installations

Multiple Cygwin-based programs can be installed but only one version of Cygwin is used. During the HP SIM installation, the OpenSSH installer checks in the registry for an existing Cygwin and if found the installation fails.

There are certain registry settings that must exist for Cygwin to function, namely the mount points previously defined. The OpenSSH installer checks for the Cygwin registry keys and refuses to install if they exist. The installation also fails if the full Cygwin distribution or any other software that uses Cygwin is installed. For example, Python distribution in WinCVS uses Cygwin. This is an unfortunate consequence of multiple Cygwin installations not being able to coexist.

There are other products in the market that use Cygwin, and HP SIM's OpenSSH distribution is not compatible with them. This includes other freely available OpenSSH distributions. If you are already using another version of OpenSSH and do not want to install the HP SIM version, you can do so. However, you must keep in mind that the HP SIM version is the only version that restricts access to the Cygwin data structures.

If you are having trouble getting the HP SIM OpenSSH package to install, search your system for the Cygwin registry keys, as well as the `cygwin1.dll` file. The location of the file might give you some idea of what software is installed that is conflicting with the OpenSSH installation.

Home Directory

When troubleshooting user authentication, one thing to check is the capitalization of the home directory, which is stored in the passwd file. OpenSSH is case-sensitive in this regard, so /home/HPsimUser is not the same as /home/hpsimuser. Check that the capitalization in the password file is the same as the directory to which it refers and that the directory is indeed the correct directory for that user.

The following is a sample passwd entry. The second-to-last field specifies the home directory, where home is the `Documents and Settings` directory:

Note: This would occur on a single line with no new lines.

```
Administrator:unused_by_nt/2000/xp:500:513:U-PCDLONG2\Administrator,S-1-
5-21-3769691966-4004114397-3833753107-
500:/home/Administrator:/bin/switch
```

Documents and Settings directory on Windows installations

When a user account is created on a Windows system, the home directory for the account is not created until the user logs into the system for the first time. If this directory is also used for SSH access the lack of the account name under `C:\Documents and Settings` can cause problems.

The **sshuser** utility supplied with HP SIM works around this problem by specifying a common directory for all SSH users. This directory, `hpsimssh`, is created by HP SIM in the Documents and

Settings directory. The `authorized_keys` file in this directory provides public key authentication for any user configured to use this directory.

Modifying the HP SIM tools

You will not normally need to modify the tools included with HP SIM. Tools configured to run as Administrator can run as an alternate user using the steps described earlier in the HP SIM commands and tools.

You can follow the directions below if you do need to change the user that is used to run a specific tool.

1. Modify the Windows HP SIM tools to use the new user account:
   a. Navigate to the tools directory. For example, `C:\Program Files\HP\Systems Insight Manager\tools`.
   b. Search the tools directory for the tool to be modified. Alternatively you may create a tool definition file from an existing tool using the mxtool command. For example:
      ```
      mxtool –lf –t netstat > netstat.xml
      ```
   c. Edit `netstat.xml` for example, using Notepad.
   d. Find each execute-as-user line in the XML file:
      ```
      <execute-as-user>Administrator</execute-as-user>
      ```
   e. Make changes to reflect the following:
      ```
      <execute-as-user> MyDomain\MyUser</execute-as-user>
      ```
      (Note that you can delete the execute-as-user line altogether, in which case the tool runs with the same user name as the HP SIM user who runs the tool.)
   f. Run mxtool to update the tool definition:
      ```
      mxtool –m –f netstat.xml –x force.
      ```
2. Configure each of your managed systems that is to run tools with this user account:

   If this user account was used to install OpenSSH, then the managed system should be correctly configured. If a different account is used then either run the Configure or Repair Agents tool on the systems, specifying the administrator or other account to be used by SSH; or take the following two steps:
   a. On Windows, the administrator user should be added to the passwd file using the sshuser utility on the managed system.
      ```
      sshuser –u MyUser –d MyDomain –f "C:\Program
      Files\OpenSSH\etc\passwd"
      ```
   b. mxagentconfig should be run on the CMS to configure public key authentication for the administrator user
      ```
      mxagentconfig -a -n <managed system> -u MyDomain\MyUser
      ```

Troubleshooting

Diagnostic tool to check SSH setup

The **mxagentconfig** tool can be used to check whether SSH on the target system is configured properly to be used with HP SIM. This option verifies whether the SSH connection can be successfully authenticated for the specified user using the HP SIM user public key and host-based authentication methods. If the authentication is successful, HP SIM is able to execute tools on the target system.

The syntax to use from the CMS platform is the following:

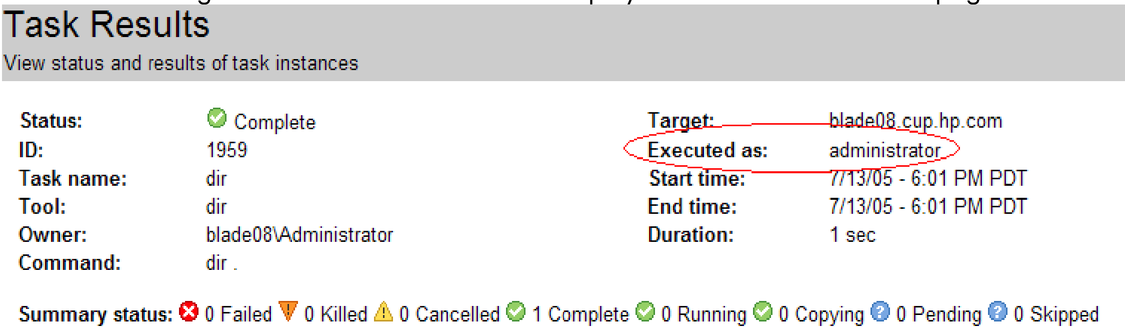
```
    mxagentconfig -c –u username –n targetsystemname
```

Checklist to debug SSH on Windows

The following checklist will help identify the cause of any problems you find with running SSH tasks on Windows. Note that it is important you are running with the latest version of HP SIM and the latest version of OpenSSH for HP SIM.

1. What user name are tasks to run as?

   This is a key question to answer, as this user must be configured for SSH access on the target managed system. The user can be specified in the tool that is to be run, although some tools run as the user signed into HP SIM. The user is displayed on the **Task Results** page.



Task Results

View status and results of task instances

Status:	✓ Complete	**Target:**	blade08.cup.hp.com
ID:	1959	**Executed as:**	administrator
Task name:	dir	**Start time:**	7/13/05 - 6:01 PM PDT
Tool:	dir	**End time:**	7/13/05 - 6:01 PM PDT
Owner:	blade08\Administrator	**Duration:**	1 sec
Command:	dir .		

Summary status: ✗ 0 Failed ▼ 0 Killed ⚠ 0 Cancelled ✓ 1 Complete ✓ 0 Running ✓ 0 Copying ? 0 Pending ? 0 Skipped

   Tools supplied by HP SIM to run on Windows systems will specify the Administrator user. These tools can run as an alternate user if the administrator has been renamed or disabled; check the WindowsAdminUserName property to determine the user name to be used:

```
       > mxglobalsettings -ld WindowsAdminUserName
       WindowsAdminUserName = MyAdmin
```

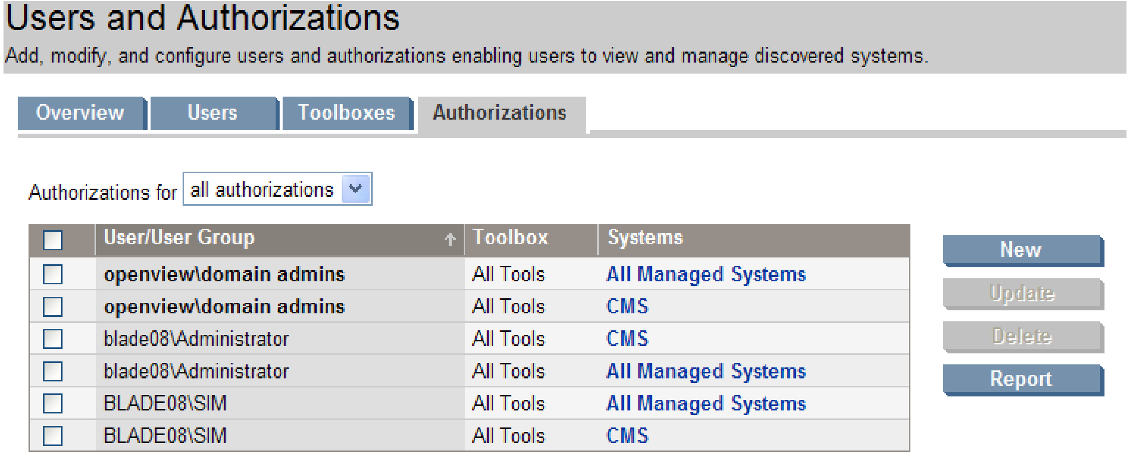
2. Is this user name valid?

   Check the operating system to ensure that the user from step 1 is a valid Windows account that can log into the target system.

   Check the Administrators group of the target system to ensure that this user is a member because only administrators can use the OpenSSH supplied by HP SIM.

   Important: Domain users must be explicit members of the local Administrators group; the OpenSSH supplied by HP SIM does not check membership of domain groups when determining access permission.

   Some tools supplied by HP SIM must run other tools as part of their operation. To do this, the user must be a valid HP SIM user with authorizations for the target systems. Check the HP SIM authorizations to ensure that this user is a valid HP SIM user and has authorizations to run tools on the CMS.



Users and Authorizations

Add, modify, and configure users and authorizations enabling users to view and manage discovered systems.

Authorizations for: all authorizations

☐	User/User Group	Toolbox	Systems
☐	**openview\domain admins**	All Tools	All Managed Systems
☐	**openview\domain admins**	All Tools	CMS
☐	blade08\Administrator	All Tools	CMS
☐	blade08\Administrator	All Tools	All Managed Systems
☐	BLADE08\SIM	All Tools	All Managed Systems
☐	BLADE08\SIM	All Tools	CMS

3. Is the OpenSSH server installed and working correctly?

   Verify that OpenSSH is installed on the target system and that the service OpenSSH Server is running. You can use the Install OpenSSH tool to install the software on a managed system. If it is installed but not running, check the system application log for any errors from the OpenSSH or SSH applications.

   The OpenSSH installer makes some security setting changes if you are running Windows 2003 or Windows XP SP2. Local security policy settings must allow these settings:

   a. Open the **Control Panel→Administrative Tools→Local Security Policy** to open the security policy window.
   b. Find the policies for **Create a token object**, **Replace a process level token** and **Log on as a service**. The account used to run OpenSSH service should have been added to each of these policies. You can manually add the policy by double-clicking each of these privileges in turn and adding service account. The account used for OpenSSH must have all three of these policies.
   c. After double-clicking, click **Add User or Group**, and enter the service account name in the **Enter the object names to select** field.
   d. Click **Check Names** to verify the entry and then click **OK**.

   You can verify operation of the SSH server using the SSH command line utility. This is shipped with OpenSSH and allows interactive login using SSH. Try to log in using the user name from step 1, including the domain name if applicable.

   ```
   CMS> ssh administrator@blade08
   administrator@blade08's password:****
   Last login: Tue Jul 12 11:31:48 2005 from mysystem.hp.com
   Microsoft Windows 2000 [Version 5.00.2195]
   (C) Copyright 1985-2000 Microsoft Corp.

   C:\Documents and Settings\Administrator>
   ```

   You can run SSH with the –v option to produce verbose output, which can help diagnose any problems.

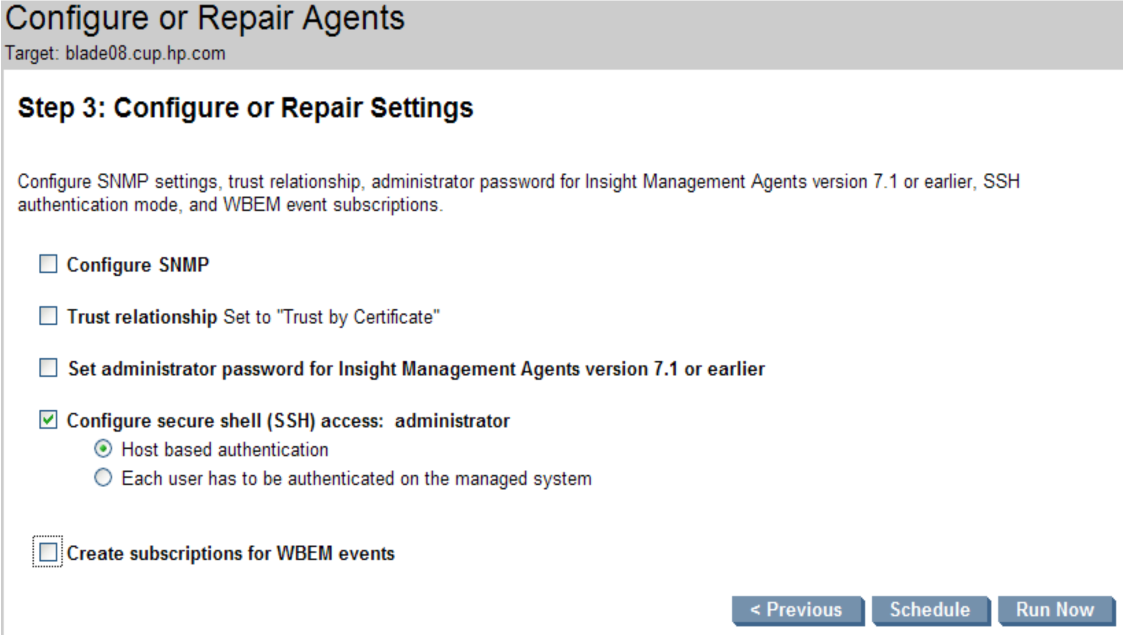
4. Does the `known_hosts` file have a different host key for the target system?

   A mismatched host key can be caused by reinstalling OpenSSH on the target system, or can indicate an imposter. By default, HP SIM does not validate host keys, but this can be enabled for more secure installations. You can remove a managed system from the HP SIM `known_hosts` file using the -r option of mxagentconfig:

   ```
   CMS> mxagentconfig -r -n blade08
   Successfully unregistered from localhost
   ```

5. Is OpenSSH configured to allow access from HP SIM?

Use the **Configure→Configure or Repair Agents** tool to configure SSH on the managed system. Check the box to configure SSH access.



Configure or Repair Agents

Target: blade08.cup.hp.com

Step 3: Configure or Repair Settings

Configure SNMP settings, trust relationship, administrator password for Insight Management Agents version 7.1 or earlier, SSH authentication mode, and WBEM event subscriptions.

□ Configure SNMP

□ Trust relationship Set to "Trust by Certificate"

□ Set administrator password for Insight Management Agents version 7.1 or earlier

☑ Configure secure shell (SSH) access: administrator

● Host based authentication

○ Each user has to be authenticated on the managed system

□ Create subscriptions for WBEM events

This tool sets up the passwd file and host or user public key authentication for the user name specified in this task. Continue with the following steps to verify its operation.

6. Is the `passwd` file correctly set up?

   If you failed to log in using ssh in step 3, check the passwd file. Use Notepad to open the passwd file in `C:\Program Files\OpenSSH\etc` and examine the contents. There should be an entry for the user name from step 1, and this should specify a valid home directory (either the user's real home directory if it exists, or hpsimssh). Note that domain users have a domain name specified:

   ```
   MyAdmin:unused_by_nt/2000/xp:500:513:U-BRIAN06\MyAdmin,S-1-5-21-
   1148942700-1292286586-3675345140-
   500:/home/Administrator:/bin/switch
   ```

   If the information is not correct, use sshuser to add the user and repeat the SSH test from step 3.

7. Is the user configured for SSH access?

   Use mxagentconfig to configure the user name for remote access using user public key authentication. Use **mxagentconfig –c** to verify the configuration.

   ```
   CMS> mxagentconfig -c –n blade08 -u myadmin
   myadmin@blade08: success
   ```

   If this fails, check the `authorized_keys2` file on the managed system in the .ssh subdirectory of appropriate home directory for the specified user, as specified in the passwd file. It should contain the public key from the CMS. See the Diagnostic tool to check SSH setup section to diagnose errors from mxagentconfig. Complete the following steps to manually install user public keys:

   a. On a Windows CMS:
      i. Go to `C:\Program Files\HP\Systems Insight Manager\config\sshtools`.
      ii. Enter the following: `copy .dtfSshKey.pub authorized_keys2`.
      iii. Log into the remote system and change to the user name's home directory (as specified in the `passwd` file.

    iv. If not present, create an `.ssh` directory.
    v. Copy the `authorized_keys2` file from the CMS into the `.ssh` directory

b. On Linux and HP-UX – similar process as above, except as noted:

    i. Login as root on the CMS platform
    ii. Create an `authorized_keys2` file for copying to other systems by entering the command:

```
cp /etc/opt/mx/config/sshtools/.dtfSshkey.pub /<user’s
home directory>/.ssh/authorized_keys2
```

    iii. The above file is now manually copied to other systems into the `$HOME/.ssh` directory.
    Verify that the permissions on the `$HOME`, `$HOME/.ssh` directory, and the `authorized_keys2` file are owner write only and there are no write permissions for group or everyone.

As a work-around to public key authentication you can try password authentication. Configure the CMS with the password for this user:

```
CMS> mxnodesecurity -a -p ssh -n blade08 -c myadmin:mypwd
Credential added for node: "blade08"
```

8. Run an SSH task on the target system to verify correct operation:

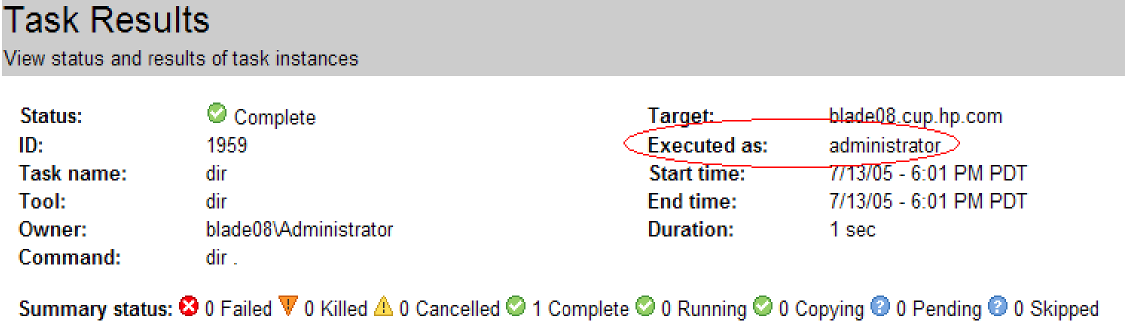
```
CMS> mxexec -t dir -A . -n blade08
Running tool dir with job id 2286.
Task Name       :defRunNowTaskId_1121366433279_3
Job ID          :2286
Tool Name       :dir
Job State       :Complete
User Name       :mydomain\bdh
Execute As User :myadmin
Start Time      :Thursday, July 14, 2005 11:40:33 AM PDT
End Time        :Thursday, July 14, 2005 11:40:34 AM PDT
Elapsed Time    :1 second 407 milliseconds
Node            :blade08
Status          :Complete
Exit Code       :0
STDOUT          :
 Volume in drive C has no label.
 Volume Serial Number is FC11-1248

 Directory of C:\Documents and Settings\Administrator

07/09/2005  07:53p      <DIR>          .
07/09/2005  07:53p      <DIR>          ..
05/10/2005  05:53p      <DIR>          .java
05/10/2005  05:53p      <DIR>          .jpi_cache
05/10/2005  06:06p               1,516 .plugin141_04.trace
07/12/2005  05:48p      <DIR>          .ssh
07/09/2005  07:51p      <DIR>          Desktop
04/07/2005  10:59a      <DIR>          Favorites
06/22/2005  02:16p      <DIR>          My Documents
05/10/2004  06:07p      <DIR>          Start Menu
               1 File(s)          1,516 bytes
               9 Dir(s)  50,392,518,656 bytes free
```

Checklist to debug SSH on Linux or HP-UX

The following checklist helps identify the cause of any problems you find with running SSH tasks on Linux or HP-UX. Note that it is important you are running with the latest version of HP SIM.

1. What user name are tasks to run as?

   This is a key question to answer, as this user needs to be configured for SSH access on the target managed system. The user can be specified in the tool that is to be run, although some tools run as the user signed into HP SIM. The user is displayed on the **Task Results** page.



Task Results

View status and results of task instances

Status:	✓ Complete	**Target:**	blade08.cup.hp.com
ID:	1959	**Executed as:**	administrator
Task name:	dir	**Start time:**	7/13/05 - 6:01 PM PDT
Tool:	dir	**End time:**	7/13/05 - 6:01 PM PDT
Owner:	blade08\Administrator	**Duration:**	1 sec
Command:	dir .		

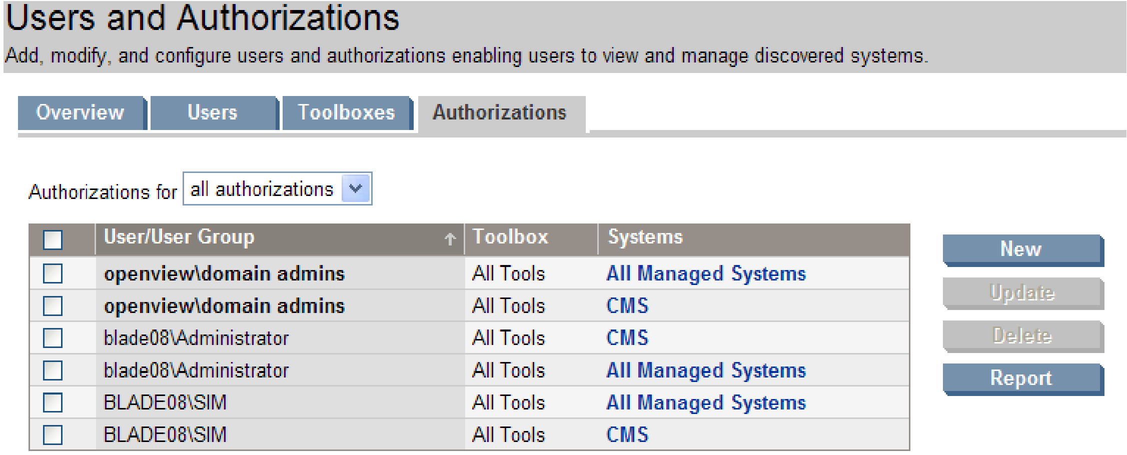
Summary status: 0 Failed 0 Killed 0 Cancelled 1 Complete 0 Running 0 Copying 0 Pending 0 Skipped

   Tools supplied by HP SIM to run on Unix systems specify the root user. The tools must be modified if a different account is to be used. See Modifying the HP SIM tools.

2. Is this user name valid?

   Check the operating system to ensure that the user from the step 1 is a valid Unix account that can log into the target system.

   Some tools supplied by HP SIM must run other tools as part of their operation. To do this, the user must be a valid HP SIM user with authorizations for the target systems. Check the HP SIM authorizations to ensure that this user is a valid HP SIM user and has authorizations to run tools on the CMS.



Users and Authorizations

Add, modify, and configure users and authorizations enabling users to view and manage discovered systems.

Authorizations for: all authorizations

□	User/User Group	Toolbox	Systems
□	**openview\domain admins**	All Tools	**All Managed Systems**
□	**openview\domain admins**	All Tools	**CMS**
□	blade08\Administrator	All Tools	**CMS**
□	blade08\Administrator	All Tools	**All Managed Systems**
□	BLADE08\SIM	All Tools	**All Managed Systems**
□	BLADE08\SIM	All Tools	**CMS**

3. Is the OpenSSH server installed and working correctly?

   Verify that OpenSSH is installed on the target system and that the sshd daemon is running.

   You can verify operation of the SSH server using the SSH command line utility. This is shipped with OpenSSH and enables interactive login using SSH. Try to log in using the user name from step 1.

```
CMS> ssh root@mysystem
Password: ****
Last login: Thu Jul 14 16:31:49 2005 from mysystem.hp.com
root@cupux30$
```

   You can run SSH with the -v to produce verbose output, which might help diagnose any problems.

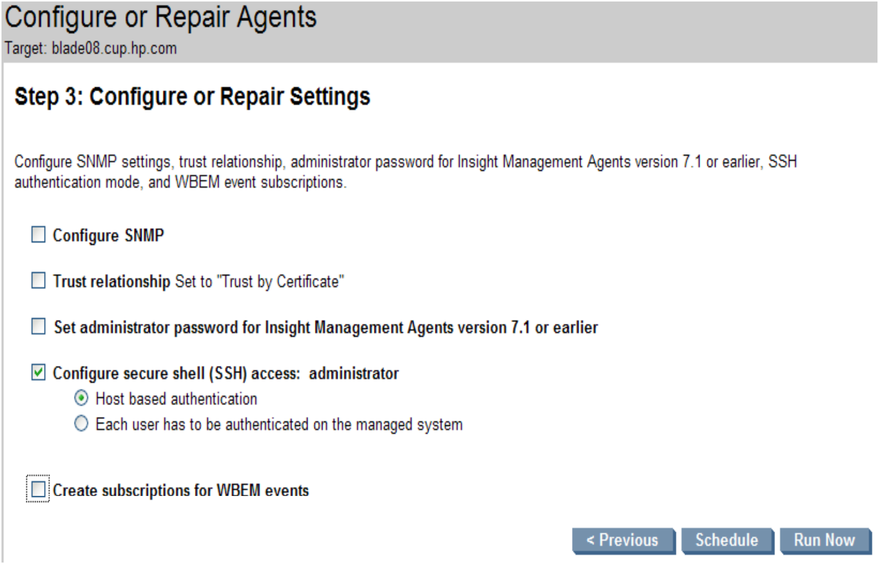
4. Does the `known_hosts` file have a different host key for the target system?

A mismatched host key can be caused by reinstalling OpenSSH on the target system, or can indicate an imposter. By default HP SIM does not validate host keys, but this can be enabled for more secure installations. You can remove a managed system from the HP SIM known_hosts file using the -r option of mxagentconfig:

```
CMS> mxagentconfig -r -n blade08
Successfully unregistered from localhost
```

5. Is OpenSSH configured to allow access from HP SIM?

   Use the **Configure→Configure or Repair Agents** tool to configure SSH on the managed system. Check the box to configure SSH access.



Configure or Repair Agents
Target: blade08.cup.hp.com

Step 3: Configure or Repair Settings

Configure SNMP settings, trust relationship, administrator password for Insight Management Agents version 7.1 or earlier, SSH authentication mode, and WBEM event subscriptions.

□ Configure SNMP

□ Trust relationship Set to "Trust by Certificate"

□ Set administrator password for Insight Management Agents version 7.1 or earlier

☑ Configure secure shell (SSH) access: administrator
● Host based authentication
○ Each user has to be authenticated on the managed system

□ Create subscriptions for WBEM events

   This tool sets up the passwd file and host or user public key authentication for the user name specified in this task. Continue with the following steps to verify its operation.

6. Is the user configured for SSH access?

   Use mxagentconfig to configure the user name for remote access using user public key authentication. Use **mxagentconfig –c** to verify the configuration.

```
CMS> mxagentconfig -c –n blade08 -u myadmin
myadmin@blade08: success
```

   If this fails, check the `authorized_keys2` file on the managed system in the `.ssh` subdirectory of appropriate home directory for the specified user, as specified in the `passwd` file; it should contain the public key from the CMS. See mxagentconfig errors. You can take the following steps to manually install user public keys:

   a. On a Windows CMS:
      i. Go to `C:\Program Files\HP\Systems Insight Manager\config\sshtools`.
      ii. Enter the following: `copy .dtfSshKey.pub authorized_keys2`
      iii. Log into the remote system and change to the user name's home directory (as specified in the `passwd` file)
      iv. If not present, create an `.ssh` directory.
      v. Copy the `authorized_keys2` file from the CMS into the `.ssh` directory
   b. On Linux and HP-UX – similar process as above, except as noted:
      i. Login as root on the CMS platform

ii. Create an `authorized_keys2` file for copying to other systems by entering the command:

```
cp /etc/opt/mx/config/sshtools/.dtfSshkey.pub /<user’s
home directory>/.ssh/authorized_keys2
```

iii. The above file is now manually copied to other systems into the `$HOME/.ssh` directory.

Verify that the permissions on the `$HOME, $HOME/.ssh` directory, and the `authorized_keys2` file are owner write only and there are no write permissions for group or everyone.

As a work-around to public key authentication you can try password authentication. Configure the CMS with the password for this user:

```
CMS> mxnodesecurity -a -p ssh -n blade08 -c myadmin:mypwd
Credential added for node: "blade08"
```

7. Run an SSH task on the target system to verify correct operation:

```
CMS> mxexec -t ls -A . -n blade08
Running tool ls with job id 2353.
Task Name       :defRunNowTaskId_1121379737441_4
Job ID          :2353
Tool Name       :ls
Job State       :Complete
User Name       :mydomain\myuser
Execute As User :root
Start Time      :Thursday, July 14, 2005 3:22:18 PM PDT
End Time        :Thursday, July 14, 2005 3:22:19 PM PDT
Elapsed Time    :1 second 266 milliseconds
Node            :blade06
Status          :Complete
Exit Code       :0
STDOUT          :
bin
core
dev
etc
```

mxagentconfig errors

Problem: mxagentconfig –c failed

```
CMS> mxagentconfig -c -n blade08 -u administrator
administrator@harrison.cup.hp.com: failed
Completed with errors.
```

This return indicates that the SSH server cannot be contacted on the target system, or the specified user has not been configured for SSH access from this system.

- Verify OpenSSH is running on the target system
- Run **mxagentconfig –a** to add the user.

```
CMS> mxagentconfig -a -n blade08 -u administrator
```

Problem: “There was a problem connecting to the HP SIM server”

```
CMS> mxagentconfig -c -n blade08 -u administrator
```

```
There was a problem connecting to the HP SIM server. Make sure
that:
```

1. Your user name has been added to HP SIM.
2. Your user name and password, if specified, are correctly spelled.
3. HP SIM is running.
4. You used '--' for any long options and double quotes if your user name includes a domain.

```
For example: <commandname> --user "mydomain\myusername" --pass
mypassword
```

This error message normally indicates that HP SIM is not running on the CMS, or that the user running the command is not an administrator of the CMS.

- Verify that the HP SIM service is running
- For a Windows CMS, verify that the user logged in to Windows is a member of the Administrators group
- Verify that the logged in user is an authorized HP SIM user

Problem: mxagentconfig Password Authentication Failed

```
CMS> mxagentconfig -a -n blade08 -u administrator
Password: ******
Failed to register as an agent to: harrison.cup.hp.com
Error: Configuration failed to complete due to the following
exception:
    Ssh Operation failed for node:harrison. password authentication
failed:FAILED
Completed with errors.
```

This return is expected if the user or password supplied is not valid on the target system; user administrator on system blade08 in the example above. Verify that the correct user name and password have been supplied.

This return can also indicate that the specified user has not been added to the passwd file on Windows. Verify that the specified user is listed in the passwd file on the target system (`C:\Program Files\OpenSSH\etc\passwd`); use **sshuser** on the managed system to add the user if necessary.

```
sshuser –u administrator –f "C:\Program Files\OpenSSH\etc\passwd"
```

Problem: mxagentconfiug returns 'SSH Channel Failure'

```
CMS> mxagentconfig -a -n blade08 -u mydomain\myuser
Password: ****
Failed to register as an agent to: harrison.cup.hp.com
Error: Configuration failed to complete due to the following
exception:
    Ssh Operation failed for node:harrison. SSH_CHANNEL_FAILUREnull
Completed with errors.
```

This return is expected if the user specified does not have sufficient privileges on the target system, user's group ID does not exist in the SSH group file or both.

If you can log into the SSH server through the SSH command line:

```
CMS> ssh Mydomain\MyUser@targethost

Mydomain\MyUser@targethost's Password:****
```

because you do not have sufficient privileges. Be sure that the specified user is a direct member of the Administrators group on the target system and remember that membership of a domain group is not sufficient for OpenSSH. This can be achieved by running following command on the target system:

```
net localgroup administrators MyDomain\MyUser /add
```

If the SSH command gives following error message:

```
setgid: Invalid argument
```

This is caused by the group id of the user is not in SSH server's group file. In most situations, this is caused by domain groups not added to the group file. Log in to the target system with an account that has domain access and run following command to add the domain groups into the SSH server's group file:

```
mkgroup –d >> <openssh install dir>\etc\group
```

Problem: mxagentconfig fails to authenticate with Suse Linux Enterprise Server 9

```
Ssh Operation failed for node:harrison. password authentication
failed:FAILED
Completed with errors.
```

SuSE Linux Enterprise Server 9 ships with SSH configured to use PAM authentication instead of password authentication. **mxagentconfig** requires password authentication. To enable password authentication, modify the following lines in `/etc/ssh/sshd_config` of the target system:

```
PasswordAuthentication yes
#UsePAM yes
```

Then retrieve the sshd's pid from file `/var/run/sshd.pid` and restart sshd by using following command:

```
kill -SIGHUP <sshd'spid>
```

sshuser errors

Problem: no output from sshuser

Running sshuser for a domain user should return an entry that can be added to the passwd file:

```
> sshuser -d mydomain -u myuser
mydomain\myuser:unused_by_nt/2000/xp:9159:513:WMI,U-OPENVIEW\wmi,S-1-5-
21-27163274-143742939-1512734326-9159:/cygdrive/C/Documents and
Settings/hpsimssh:/bin/switch
```

No output is returned if you do not have sufficient rights to access the domain, used by sshuser to obtain the user's SID. You should log in to the managed system as a domain account and re-run sshuser.

Errors running tasks

When you have a problem executing a task, one of the following might be the cause:

- The SSH server on the managed system on which you are trying the command is not available
- The user running the command is not authorized to login through SSH to the managed system
- The user trying to run the command does not have the HP SIM authorizations to run this tool on that managed system

Follow the checklist given earlier to debug the SSH connection to the target system. Most importantly, make sure the user trying to run the command is the correct user. Sometimes the tool is designed to be run by a particular user such as root or Administrator. Other tools are designed to be run by the user who is logged into the CMS.

Problem: An MxAuthenticationException is generated when a tool is run, either from the GUI or the command line interface.

Solution: Follow the steps listed in Checklist to debug SSH on Windows or Checklist to debug SSH on Linux or HP-UX sections

Problem: When executing a task, the message *Unknown OS* is displayed.

Solution: The installation might not have been completed properly.

1. If you are trying to execute a task on a Windows system, make sure that it was rebooted after installation of SSH. A reboot is required to complete the installation.
2. Enable DMI, WBEM, or SNMP on the system so the type of operating system can be determined, then run data collection to update the HP SIM database.
3. Make sure that commands to determine the operating system are working.

   For Windows, type: **ver**

   For HP-UX and Linux, type: **uname**

Problem: Standard Windows tools run on the CMS fail with authentication error.

Solution: The Administrator account might not be correctly configured on the CMS to run SSH tools.

1. Verify the name of the user account to be used for Windows tools. This is 'Administrator' by default, but this account may have been renamed pr an alternative account may be used. The account may be specified by setting the global property "WindowsAdminUserName" on the CMS:

   ```
   mxglobalsettings -s WindowsAdminUserName=MyDomain\MyAdmin
   ```

2. Verify the passwd file to ensure that this user account has been added. Use sshuser on the target system to add the user if needed.

   ```
   sshuser –u MyAdmin –d MyDomain –f "C:\Program
   Files\OpenSSH\etc\passwd"
   ```

3. Run mxagentconfig on the CMS to configure this user account

   ```
   mxagentconfig –a –u MyDomain\MyAdmin –n <cms machine name>
   ```

Problem: Linux or HP-UX CMS unable to run tools on Windows systems

Solution: The Windows tools are configured to run as Administrator by default. If the Administrator account has been renamed or disabled then an alternate account must be used. This can be done by setting the *WindowsAdminUserName* property. See the steps above.

Problem: mxagentconfig or command execution fails after reinstalling the openSSH server.

Solution: If SSH key checking is enabled, then the `known_hosts` file might have an incorrect key for the target system. Remove the key using the -r option of **mxagentconfig**:

```
CMS> mxagentconfig -r -n blade08
Successfully unregistered from localhost
```

Problem: Unable to execute custom commands

Solution: Custom commands use SSH to execute on the CMS with the user name of the user logged into HP SIM. SSH must be configured correctly for this user name for custom commands to execute. On a Windows CMS:

- The user name must be a member of the Administrators group
- The user name must be added to the passwd file:
  ```
  sshuser –u joe –d MyDomain –f "C:\Program Files\OpenSSH\etc\passwd"
  ```
- The user name must be configured for user or host based authentication:
  ```
  mxagentconfig –a –u mydomain\joe –n localhost
  ```

Appendix A: Changes in HP SIM 5.x

HP SIM 5.x includes a number of improvements to SSH handling:

- Improved error reporting to make troubleshooting easier
- Support for host-based and password authentication, in addition to user-based authentication
- A new utility, **sshuser**, for Windows systems replaces the mkpasswd tool.
    - This new tool resolves issues with domain users (the domain name is now included as part of the user name).
    - It also supports users who have not logged into a system, as a special home directory is used.
- The Configure or Repair Agents tool now includes SSH configuration for Windows, Linux, and Unix systems.
- The mxagent CMS process is no longer used.
- Changes were made to the handling of SSH keys with the `known_hosts` file
    - By default, HP SIM no longer verifies that a managed system's SSH key matches the key in the `known_hosts` file.
    - A new user interface allows the SSH key checking to be changed, and enables keys to be deleted from the `known_hosts` file.
    - The `known_hosts` file now lists system by name rather than IP address.
- The SSH Bypass mechanism is now used on all CMS platforms when running a tool locally.

Appendix B: Tool examples

This section provides examples of MSA and SSA tools available in HP SIM.

MSA tools

Category	Tool Name	Description
Command Line Tools	PostgreSQL DB Backup	Back up the Systems Insight Manager PostgreSQL database.
Configuration Tool	Subscribe to WBEM Events, Unsubscribe to WBEM Events	Configure a managed system to send WBEM indications to HP SIM.
Resource Management	Process Resource Manager Console	Run the Process Resource Manager for managing system resources.

SSA tools

Category	Tool Name	Description
Configure	Configure DMI Access	Set DMI access on selected systems.
Configure	Configure SNMP Access	Set SNMP access on selected systems.
General Tools	Install Package	Install RPM Package Manager package(s.)
General Tools	Query Package	Query installed RPM Package Manager package(s) version.
General Tools	Uninstall Package	Uninstall RPM Package Manager package(s.)
General Tools	Verify Package	Verify installed RPM Package Manager package(s.)
General Tools	bdf	Report free disk space on files or filesystems.
General Tools	cat	Display the contents of a file.
General Tools	copy	Copy one or more files to another location.
General Tools	cp	Copy file or files to a destination file or directory.
General Tools	del	Delete one or more files (or all files in specified directories.)
General Tools	df	Report free disk space on files or filesystems.
General Tools	dir	Display list of files and subdirectories in a directory.
General Tools	find	Recursively descend a directory hierarchy.
General Tools	ls	List files or directories.
General Tools	mv	Move file or files to a destination.
General Tools	net	Display Windows System and Network information.
General Tools	netstat	Display active network connections.
General Tools	ps	List system processes.
General Tools	rm	Remove files or directory trees.
General Tools	rmdir	Remove a directory and all its contents.
General Tools	type	Display the contents of one or more text files.
Partition Management	Create Partition	Start the Create Partition dialog on the selected system in the complex.

Category	Tool Name	Description
Partition Management	Partition Manager	Start the Partition Manager graphical user interface on the selected system in the complex.
Partition Management	Show Complex Details	Start the Show Complex Details dialog on the selected system in the complex.
Partition Management	View Partition Manager Log	Start the Log Viewer dialog on the selected system in the complex.
Resource Management	Display Resource Usage	Display the current Process Resource Manager resource usage.
Resource Management	Event Monitoring Service	Configure and view resource monitoring requests on the managed system.
Resource Management	List Resource Availability	List Process Resource Manager resources available.
Software Management	CLI List Software	Example tool that runs Software Distributor (SD) swlist command on each system.
Software Management	CLI Preview Install	Example tool that runs Software Distributor (SD) swinstall -x match_target=true command on each system.
Software Management	CLI Verify Software	Example tool that runs swverify command on each system.
Software Management	Set SD Access	Set Software Distributor (SD) access to the target system by way of the appropriate SD access control lists (ACLs.)
Software Management	Software Distributor Daemon Log	Display the tail end of the Software Distributor (SD) daemon log.
Software Management	View Depot Software	Start the Software Distributor (SD) graphical user interface to view depot software and depot logfile.
Software Management	View Installed Software	Start the Software Distributor (SD) graphical user interface to view installed software and agent logfile.
Software Management	View Software Distributor Agent Log	Display the tail end of the Software Distributor (SD) agent log.
System Administration	Accounts for Users and Groups	Start the HP-UX SAM Accounts for Users and Groups functional area.
System Administration	Auditing	Start the HP-UX SAM Auditing functional area.
System Administration	Disks and File Systems	Start the HP-UX SAM Disks and File Systems functional area.
System Administration	Kernel Configuration	Start the HP-UX SAM Kernel Configuration functional area.
System Administration	Peripheral Devices	Start the HP-UX SAM Peripheral Devices functional area.
System Administration	Printers and Plotters	Start the HP-UX SAM Printers and Plotters functional area.
System Administration	System Properties	Start the HP-UX SAM System Properties functional area.
System Administration	System Security Policies	Start the HP-UX SAM System Security Policies functional area.
System Administration	Verified Commands	Start the HP-UX SAM Verified Commands functional area.

Category	Tool Name	Description
System Administration	View SAM Log	Start the HP-UX SAM Log Viewer X application.

Appendix C: Glossary

API — application programming interface. An interface provided for programs to execute services provided by a piece of software, versus a human executing those services by way of the command line or a GUI.

CMS — central management server. The system on which HP Systems Insight Manager is installed.

Cygwin — a UNIX compatibility layer that is used to port some UNIX utilities to Windows.

DSA — digital signature algorithm. A public key algorithm used by SSH.

GUI — graphical user interface. For example, the Web-based portal interface to HP SIM.

Host key — the public key that proves the identity of a particular host.

IETF — Internet Engineering Task Force. From the IETF Web page: "The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet."

Managed system — any system on the network being managed by HP SIM, including the CMS itself.

Mount point — maps a physical file system name to a logical name, which can then be used for convenience.

MSA tool — multi-system aware tool. This is a tool that executed on a certain system called the execution system, and then performs tasks against the target systems. Target systems are provided to the tool by an environment variable.

OpenBSD — a free, Berkeley Software Division (BSD) 4.4–based UNIX-like operating system. Their implementation of the SSH protocol is OpenSSH.

OpenSSH — a free version of the SSH protocol suite, implemented and supported by the OpenBSD project.

Private key — the private half of a public and private key pair. The private key is stored in and owner read-only file (for example, only the owner can view it) on a particular system. The private key is never transmitted to another system.

Public key — the public half of a public and private key pair. The public key can be freely distributed without fear that it can be used to impersonate the user. It can only be used for authentication in conjunction with a private key.

Remote task — a task initiated on the CMS, and executed on a managed system.

RSA — Rivest-Shamir-Adleman. A public key algorithm used by SSH.

SFTP — Secure File Transfer Protocol. It is the part of the SSH protocol used to transfer files between systems. This protocol is performed with the same server as command execution.

SSA Tool —single-system aware tool. This type of tool is executed by way of SSH on the target system.

SSH — Secure Shell. An IETF recommendation. There are two protocols: the original SSH version 1 protocol (SSH-1) and the current SSH version 2 (SSH-2.) Whenever SSH is mentioned in this document, it refers to the SSH-2 protocol.

SSH client— connects to SSH servers to perform remote task execution and file copy.

SSH server — listens for and services requests coming in on the proper TCP/IP port, usually port 22.

Target system — the system selected for a tool to run on.

TDEF — tool definition file. It defines parameters of a tool, its execution user, toolbox, and so on in XML format.

For more information

- **HP Systems Insight Manager**

www.hp.com/go/hpsim

- **IETF secsh working group home page**

www.ietf.org/html.charters/secsh-charter.html

- **OpenSSH**

www.openssh.org

5982-4832EN, 01/2007