



CHAPTER 1

Installing Cisco VSPT

The Cisco Voice Services Provisioning Tool (VSPT) provides an easy-to-use graphical tool to provision the Cisco PGW 2200 Softswitch running the Cisco MGC software.



Note

In the previous release the VSPT was known as the Cisco MGC Node Manager Provisioning Tool (MNM).

Individual releases of VSPT are designed to be used with specific releases of the Cisco MGC software. VSPT Release 2.6(1) is designed to be used with Cisco MGC Release 9.6(1). If you are using a different release of the Cisco MGC software, see the [“Determine the Correct Provisioning Tool Release”](#) section on page 1-1 to identify the release of VSPT that you need.

- [Installing VSPT Release 2.6\(1\), page 1-2](#)
 - [Planning and Setting Up for Backup and Restore, page 1-5](#)
 - [Installing SSH on VSPT, page 1-7](#)
- [Installing an Earlier Version of VSPT, page 1-9](#)
- [Upgrading VSPT, page 1-9](#)
- [Uninstalling VSPT, page 1-10](#)

Determine the Correct Provisioning Tool Release

You must install the provisioning tool release that is compatible with your Cisco MGC and BAMS software. Select the correct provisioning tool version by referring to [Table 1-1](#). The following versions are included on the Cisco MGC Node Manager CD. Check the applicable Release Notes for possible later patches.

Table 1-1 VSPT & Cisco MGC Software Version Compatibility

Provisioning Tool Software Version	Cisco MGC Software Release	BAMS Software Release
Provisioning Tool (VSPT) 2.6(1)	Cisco MGC Release 9.6(1)	BAMS Phase 3(3.13)
Provisioning Tool (VSPT) 2.5(2)	Cisco MGC Release 9.5(1)	BAMS Phase 3 (3.13)
MNM-Provisioning Tool (MNM-PT) 2.4(1)	Cisco MGC Release 9.4(1)	BAMS Phase 3 (3.12 and 3.13)

Table 1-1 VSPT & Cisco MGC Software Version Compatibility (continued)

Provisioning Tool Software Version	Cisco MGC Software Release	BAMS Software Release
Provisioning Tool (VSPT) 2.3(2)	Cisco MGC Release 9.3(2)	BAMs Phase 2, BAMS Phase 3 (3.10 and 3.12)
Provisioning Tool (VSPT) 2.2(2) and 2.2(2) patch 4	Cisco MGC Release 9.2(1.5-2)	BAMS Phase 2, BAMS Phase 3
Provisioning Tool (VSPT) 1.6(4) and 1.6(4) patch 3	Cisco MGC Release 7.4	BAMS Phase 1

Instructions for installing the Provisioning Tool are provided later in this chapter.

Installing VSPT Release 2.6(1)

Before installing VSPT Release 2.6(1), verify the following:

- You want to provision the Cisco PGW 2200 Softswitch running Cisco MGC software Release 9.6(1). If you are provisioning an earlier version, see the “[Determine the Correct Provisioning Tool Release](#)” section on page 1-1.
- You have met the workstation hardware and software requirements. See the “System Requirements” section of the associated release notes.
- You have established network connectivity between your workstation and the network elements.
- The network elements have the correct release of software installed.
- You have identified your desired installation configuration, one of the options described in the “[Determine the Correct Provisioning Tool Release](#)” section on page 1-1.
- You have decided if you are installing SSH for secure communications with SSH-enabled components.



Note

VSPT installation must be carried out from the VSPT server or a machine with X Window capability. Make sure you have root access on your Sun workstation.

Before you begin provisioning, you should have a list of components you want to provision, including the component names, IP addresses, properties, and other parameters. To create this list, use the instructions provided in the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/provisioning/guide/prvgde.html



Tip

In addition, descriptions of the properties and values contained in VSPT are included in Appendix A of the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* and [Table 1-2](#) of this document. Review this information before you begin provisioning, and keep it available for reference during provisioning.

To install VSPT Release 2.6(1), follow this procedure:

-
- Step 1** Verify that the requirements listed in the “[Determine the Correct Provisioning Tool Release](#)” section on [page 1-1](#) have been met.
- Step 2** Open an X terminal window.
- Step 3** If you are not already logged in as root, become the root user by entering the following command:
- ```
>su - root
```
- Step 4** Ensure that the X Windows display is set as follows:
- In csh or tcsh: `setenv DISPLAY <hostname>:0`
  - In sh or ksh: `DISPLAY=<hostname>:0 ; export $DISPLAY`
- Replace the value <hostname> with the hostname of your machine.
- Step 5** Download the VSPT tar file into the directory of your choice. The tar file is available at the following location:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/vspt>
- A valid login to the Cisco website is required for you to download the VSPT tar file from the preceding URL.
- Step 6** Navigate to the downloaded file.
- Step 7** Untar the downloaded file by entering `tar -xvf <filename>`
- Replace the value <filename> with the filename of the tar file.
- Step 8** Enter `./setup` to run the installation script.
- The VSPT InstallShield Wizard opens, displaying the Welcome window.
- Step 9** Click **Next**.
- The ReadMe Information window displays.
- Step 10** Click **Next**.
- The License Agreement window displays.
- Step 11** Accept the license agreement and click **Next**.
- The Destination Folder window displays, indicating the default destination directory.
- Step 12** Click **Next** to accept the default destination directory, or select **Change** to provide a different directory path. If you want to use a directory destination other than the default, enter the appropriate directory path and click **Next**.
- The Query Backup User Panel window displays.
- Step 13** Optional: Enter the Backup User ID (your backup server login ID), and click **Next**.



---

**Note** During installation you are asked to designate a Backup User ID. Only a user logged in with this ID can carry out backup and restore operations. See the “[Specify a Backup User ID During Installation](#)” section on [page 1-5](#) for more information. This is applicable only if you are conducting backup operations. All other features of VSPT function without the entering of a backup user ID.

---

The Ready to Install window displays.

- Step 14** Click **Install Now**.  
VSPT 2.6(1) installation take place and the Installation Summary window displays upon completion.
- Step 15** Click **Exit**.  
The VSPT InstallShield Wizard closes.
- Step 16** If you are using the VSPT Backup and Restore feature, enable TFTP on the backup server. See the [“Planning and Setting Up for Backup and Restore”](#) section on page 1-5.
- Step 17** If you are installing SSH for VSPT, see the [“Installing SSH on VSPT”](#) section on page 1-7.
- Step 18** Go on to the [“Starting VSPT”](#) section on page 1-8.

Table 1-2 defines the default VSPT files and directories.

**Table 1-2 Provisioning Tool Installation Files and Directories**

| File or Directory                          | Description                          |
|--------------------------------------------|--------------------------------------|
| <b>/opt/CSCOvsp26</b>                      |                                      |
| vspt                                       | Provisioning tool application script |
| /classes                                   | Class and property files             |
| /docs                                      |                                      |
| /help                                      | Online help files                    |
| /images                                    | Images or logos used in VSPT         |
| /jre/                                      | Java Runtime Environment             |
| /netscape                                  | Netscape web browser files           |
| /uninstall                                 | Uninstall script directory           |
| /utils                                     | Utilities for VSPT                   |
| /version                                   | Provisioning Tool version            |
| <b>/var/opt/CSCOvsp26 (home directory)</b> |                                      |
| /data                                      | Configuration files                  |
| /logs                                      | Log files                            |
| /etc                                       | XML files                            |



**Note**

The files and directories listed in Table 1-2 are for the most recent version of VSPT. Your directory structure may be different if you are using an older version.

## Planning and Setting Up for Backup and Restore

You typically use VSPT Backup to back up the configuration on a supported component, such as a Cisco PGW 2200, onto a different server (the backup host). The configuration can then be restored if needed on the original machine.

For example, if you are backing up a Cisco PGW 2200 host, VSPT logs in to the Cisco PGW 2200 host, copies the configuration, and the Cisco PGW 2200 transfers it to the backup host using TFTP. The backup host must have TFTP enabled.

If you are going to use Backup and Restore, you should do the following:

- [Specify a Backup User ID During Installation, page 1-5](#)
- [Select a Backup Host, page 1-6](#)
- [Enable TFTP on the Backup Host, page 1-6](#)

### Specify a Backup User ID During Installation

During VSPT installation, you are prompted for a Backup ID. The Backup ID is the UNIX ID of a user account authorized to use VSPT to perform configuration backups. Depending on your security policy, this might be the ID of a particular individual, or an ID created specifically for the purpose and usable by one or more individuals authorized to perform backups.

In order for a user to schedule backups or perform immediate backups, VSPT must be started from a UNIX shell with the backup ID, in either of two ways:

- If VSPT is launched from Cisco MGC Node Manager (Cisco MNM), the user must have started the Cisco EMF client with the Backup ID. If the user's normal ID is different from the backup ID, the user must start a new Cisco MNM session with the backup ID.
- From the command line in a UNIX shell opened with the backup ID.

### If You Reinstall VSPT with a Different Backup ID

If you reinstall VSPT and select a different backup ID, you must manually delete two files that are not automatically removed in reinstallation. (This is because the files are read-only and owned by root.)

- 
- Step 1** Log in as root.
- Step 2** Change to this directory:  
`/var/opt/CSCOVsp26/logs/`
- Step 3** Delete these two files:  
`now.log`  
`testValidTFTP`
-

## Select a Backup Host

The backup host to which configurations are copied can be any of the following:

- The same machine where Cisco MGC Node Manager is installed (and typically Cisco VSPT is also installed), referred to as the network management host
- The same machine where Cisco VSPT is installed, if this is different from the Cisco MGC Node Manager machine, and if this is not a Cisco PGW 2200 host
- A separate machine used for backups



### Note

Using a Cisco PGW 2200 host as a backup host is not recommended and is specifically not supported if you are using SSH.

## Enable TFTP on the Backup Host

VSPT uses Trivial File Transfer Protocol (TFTP) as the transfer utility to transfer configuration files from the Cisco PGW (or BAMS) to the backup host. Although UNIX systems include TFTP, by default it is not enabled. To be able to send configuration files to a backup host, you must first enable TFTP on that host.

Before you begin, be sure that you are using a Solaris or Solaris-like TFTP server. Unlike some TFTP servers, the Sun Solaris TFTP server allows a file to be written to the server using TFTP only if the file already exists on the system and is writable by the root user.

TFTP software that has the behavior of the Solaris TFTP software must be used (the file must exist and have write permissions by the root user before the TFTP transfer can be successful). This is because VSPT creates the file with root write permission before attempting to back up the file using TFTP. TFTP server implementations that require the file not to exist before the backup is attempted do not work.

### To Enable TFTP

- 
- Step 1** In the file `/etc/inetd.conf`, uncomment this line:
- ```
# tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```
- Thus:
- ```
tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```
- Step 2** Create the tftp user home directory:
- ```
# mkdir /tftpboot
# chown root /tftpboot
# chmod 777 /tftpboot
```
- Step 3** Restart inetd:
- ```
ps -ef | grep inetd*
kill -HUP <inetd-pid>
```
- Step 4** Verify that TFTP is working:
- ```
# cp /etc/hosts /tftpboot/.
# cd /tmp
```

```
# tftp <machine-name>
tftp> get hosts
```

Installing SSH on VSPT

VSPT 2.6(1) can be installed on both Solaris 8 and Solaris 10.

If you are installing VSPT 2.6(1) on Solaris 10 platform on which SSH is available, check if you have SSH installed. If you already have SSH installed, modify the `sshPath` variable in the configuration file as follows and ignore this section.

```
/opt/CSCOvsp26/classes/com/cisco/transpath/dart/editor/configEditor.properties
sshPath=/usr/bin
```

Where `/usr/bin` is the default location where `ssh` and `sftp` are installed.

If you are installing VSPT 2.6(1) on Solaris 8, the SSH security package used for VSPT is the same CSCOk9000 package used on the Cisco PGW 2200, BAMS, and HSI server. To install this package on VSPT, use the same procedure as for those devices. In addition, you need to modify a variable if the base path of `ssh` and `sftp` is not the default.

Before you begin, VSPT should have software Release 2.6(1) installed.



Note

We recommend installing SSH on VSPT (and Cisco MGC Node Manager) before you install it on the Cisco PGW, so that you can use the element managers to monitor the installation process on the PGW and other managed components.

Step 1 Download the security package, CSCOk9000. You must first secure authorization.



Note

There are U.S. Government restrictions on the exporting of cryptographic technology. The Secure Shell (SSH) program falls under the umbrella of those restrictions. The security package (CSCOk9000) is registered and located in a restricted area from which only authorized customers can download.

Step 2 Stop VSPT.

If VSPT is a co-resident on the Cisco PGW server and CSCOk9000 is already installed, go on to Step 4. If not, go on to Step 3.

Step 3 Install the CSCOk9000 package on the VSPT server machine. For instructions, refer to the steps in *Cisco PGW 2200 Security Enhancements*, “Installing CSCOk9000 on the Cisco PGW 2200 Host.”

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/software/SW2/SecEnh.html

Step 4 If the base path of `ssh` and `sftp` is not the default `/opt/ssh/bin`, modify the `sshPath` variable in the configuration file:

```
/opt/CSCOvsp26/classes/com/cisco/transpath/dart/editor/configEditor.properties
sshPath=/usr/local/bin
```

Where `/usr/local/bin` is the location where `ssh` and `sftp` are installed.

After you install the CSCOk9000 package, both secure and nonsecure utilities are enabled. Users can use Telnet or ssh, FTP or sftp. If you want to disable nonsecure utilities, go on to Step 5.

Step 5 (Optional) To disable nonsecure utilities, use the following toggles:



Note The scripts `toggle_telnet.sh` and `toggle_ftp.sh`, are located in the `/opt/sun_install` directory.

- To disable FTP (making only sftp available):
`/opt/sun_install/toggle_ftp disable`
- To reenable FTP (making both FTP and sftp available):
`/opt/sun_install/toggle_ftp enable`

Uninstalling SSH on VSPT

- If you need to uninstall SSH, use the procedure described in *Cisco PGW 2200 Security Enhancements*, “Fallback Procedures” at http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/software/SW2/SecEnh.html

This reenables FTP and Telnet and uninstalls the CSCOk9000 package.

Starting VSPT

You can start VSPT standalone from the operating system or you can start it from Cisco MGC Node Manager.



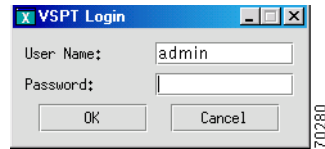
Note See the *Cisco Media Gateway Controller Software Version 9 Installation and Configuration Guide* for information on setting up user privileges and access rights.

Perform the following steps to start the VSPT:

Step 1 Do one of the following:

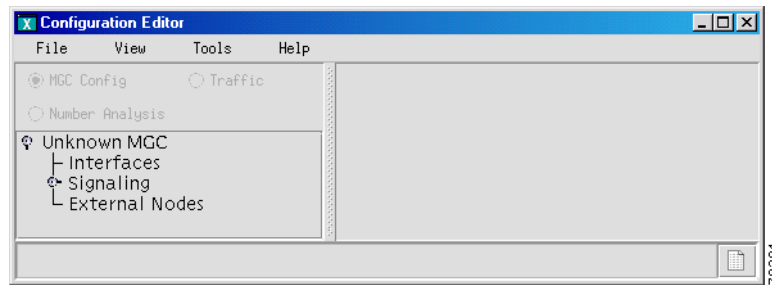
- Start VSPT standalone:
 - Log in to the VSPT server or access it from a machine with X window capability.
 - In a terminal window, change to the default directory, typically:
 - `>cd /opt/CSCOvsp26`
 - Enter the following command to start VSPT:
 - `>./vspt`
- Start VSPT from Cisco MGC Node Manager:
 - Before starting Cisco MGC Node Manager, log in as root.
 - In the Map Viewer, choose **Tools > Provisioning Tool**.

The login screen shown in [Figure 1-1](#) appears.

Figure 1-1 Login Window

Step 2 Enter your user name and password, and click **OK**.

The default user name is admin, and the password is also admin. The Welcome screen is displayed briefly during the login process, and the main window appears (see [Figure 1-2](#)).

Figure 1-2 Main VSPT Window

Exiting the VSPT

You can exit the VSPT at any time by performing one of these actions:

- Click **File > Exit**. Click **OK** at the resulting prompt.
- Click the close box in the upper right of the VSPT window. Click **OK** at the prompt.

Installing an Earlier Version of VSPT

Follow the procedure described in [“Installing VSPT Release 2.6\(1\)”](#) by selecting the version you want to install. You must install the base version before installing a patch.

Upgrading VSPT

To upgrade VSPT, you install the new version as described in the [“Installing VSPT Release 2.6\(1\)”](#) section. Depending on the version you are upgrading from, you may need to take some steps beforehand:

- Because two versions of VSPT (such as VSPT 2.3(2) and 2.6(1)) can exist on the same system, when you are upgrading, the older version is not automatically removed. If you do not want to use both versions, you can manually uninstall the older version. See the [“Uninstalling VSPT”](#) section. (However, keeping the old version is harmless.) Uninstall removes the software, but not the configuration data files.

- If you want to use configuration files created in a previous version, you must copy them. Of course, the configuration will not include components new in the 9.6(1) release.

Uninstalling VSPT

If you upgrade to VSPT Release 2.6(1) and no longer need an earlier version, follow these procedures to uninstall an earlier version.

The uninstallation process removes the `/var/opt/<CSCOvsp2x>` directory (where `2x` is the VSPT release, such as 26 for Release 2.6(1)) created by the installation process. If a directory contains a file that was not created during the installation process, it is not removed and is logged in the `uninstall.log` file. This might occur in the data and logs directories. All application data stored in the `/var/opt/<CSCOvsp2x>` directory is retained.

**Note**

Since the uninstall directory and files are removed during uninstall, *do not* change to the `/opt/CSCOvsp2x` directory to run the uninstall script.

Step 1 Enter the following commands:

```
>su -root
```

```
>cd /
```

```
>/opt/CSCOvsp2x/uninstall/uninstall
```

Step 2 Proceed with the new VSPT software installation (see the [“Installing VSPT Release 2.6\(1\)”](#) section).

**Note**

If your next installation specifies a different backup ID, you must manually delete certain files. See the [“If You Reinstall VSPT with a Different Backup ID”](#) section on page 1-5.
