Tivoli

Tivoli Cross-Site for Security™ Installation Guide

Version 1.1

October 21, 1999

Tivoli Cross-Site for Security^{TM} Installation Guide (October 1999)

Copyright Notice

Trademarks

Notice

References in this publication to Tivoli Systems or IBM products, programs, or services do not imply that they will be available in all countries in which Tivoli Systems or IBM operates. Any reference to these products, programs, or services is not intended to imply that only Tivoli Systems or IBM products, programs, or services can be used. Subject to Tivoli Systems' or IBM's valid intellectual property or other legally protectable right, any functionally equivalent product, program, or service can be used instead of the referenced product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by Tivoli Systems or IBM, are the responsibility of the user.

Tivoli Systems or IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York 10504-1785, U.S.A.

Contents

Preface..1

1 Requirements for the Cross-Site Server.......7

2 RDBMS Requirements 15

Oracle Configuration 16

DB2 Configuration..20

3 Requirements for the Web Server 25

4 Generating a License Key 29

Activating Your Support Account 30

Generating a New License Key 36

5 Installing the Cross-Site Server on NT........43

Contents of the CD-ROM 44

The 128-bit and 56-bit Versions of Cross-Site 46

Installing Locally Versus Remotely 46

Installing Intermixed Domains 47

Installing the Base Server 48

Installing Cross-Site for Security on the Server 53

Stopping and Restarting the Server 54

Verifying the Server's Installation...55

Verifying the Installation of the Database Tables..............................57

6 Installing the Cross-Site Server on AIX 59

Contents of the CD-ROM 60

The 128-bit and 56-bit Versions of Cross-Site 62

Installing Locally Versus Remotely..62

Installing Intermixed Domains 63

Installing the Management Server 64

Configuring the Management Server 67

Configuring the Base Server 67

Configuring Cross-Site for Security 76

Stopping and Restarting the Server 77

Verifying the Server’s Installation..78

Verifying the Installation of the Database Tables................................80

7 Installing the Cross-Site Server on Solaris 83

Contents of the CD-ROM 84

The 128-bit and 56-bit Versions of Cross-Site 86

Installing Locally Versus Remotely..86

Installing Intermixed Domains 87

Installing the Base Server 88

Installing Cross-Site for Security 100

Stopping and Restarting the Server 102

Verifying the Server’s Installation..103

Verifying the Installation of the Database Tables..............................105

8 Installing and Running the Console..........107

Requirements for the Console 107

Installing and Running the Console on Windows..............................111

Installing, Configuring, and Running the Console on AIX 117
Installing and Running the Console on Solaris 122

9 Installing the Security Agent...................... 129

Requirements for the Security Agent 129
Setting Up a User for the Agent 134
Installing on Windows NT 138
Installing and Configuring on AIX.. 144
Installing on Solaris... 149
Verifying the Agent's Installation... 154

10 Roadmap to Using Cross-Site.................. 157

A Frequently Asked Questions..................... 161

General (Installation).. 161
Web Server Requirements.. 163
RDBMS Requirements.. 164
Cross-Site Server Installation 165
Certificates 168
The Cross-Site Console.. 170
The Agents.. 171

B All About Certificates 173

An Overview of Keys and Certificates... 174
The Types of Certificates 176
Cross-Site and Certificates 179

Obtaining a Server Certificate 179
Supported Server Certificates 182
Generating a Key-pair File 184
Generating a Certificate Signing Request 188
Purchasing a Server Certificate...190
Generating an In-house Server Certificate 194
Enabling SSL Encryption on the Web Server..........................196
Importing an Unsupported Root Certificate 199
Obtaining a Signing Certificate...203
Supported Signing Certificates..206
Purchasing a Signing Certificate 209
Exporting the Certificate to a PKCS#12 File 213
Generating an In-house Signing Certificate 215
Importing an Unsupported Root Certificate 217
Importing a Signing Certificate into Cross-Site.........................220
References...222

C Regenerating Your License Key 225

Modifying Your License Key...226
Installing Your License Key...232

D Uninstalling Cross-Site 235

Uninstalling Cross-Site Agents..236
On Windows NT 236
On AIX 237
On Solaris...237
Uninstalling the Console 238
On Windows 95, 98, and NT 238
On AIX 239
On Solaris 239

Uninstalling the Cross-Site Server 240
On Windows NT 240
On AIX 241
On Solaris 242
Files and Directories Installed for the Cross-Site Server 246
On Windows NT 246
On AIX... 246
On Solaris 247
Files and Directories Installed for the Console 248
On Windows 95, 98, and NT 248
On AIX... 249
On Solaris 249
Files and Directories Installed for the Security Agent 250
On Windows NT 250
On AIX... 251
On Solaris 251

E Glossary...253

Index 277

Preface

Welcome to Cross-Site! Tivoli Cross-Site provides the first suite of e-commerce management products that enables you to collaborate with your online business partners to solve the unique problems arising from business-to-business e-commerce. The Cross-Site product suite includes the management server, which provides a set of core services, and the Cross-Site applications.

All Cross-Site applications leverage a set of core services that is provided with the Cross-Site server and agents. These services enable all communications, tasks, and security for Cross-Site. The Cross-Site services include:

- Authorization and authentication
- The event service
- The task manager
- The policy manager
- The channel manager
- The report generator

The Cross-Site for Security application provides intrusion detection for systems in your environment that might be vulnerable to attack. The Cross-Site for Security agent should be deployed wherever the administrative domain connects to the Internet. The Cross-Site for Security agent can do the following:

- Detect scans and floods
- Monitor IP traffic
- Monitor port services

- Detect DNS, mount service, and network file system requests and replies

- Detect portmapper service request and reply dumps

- Detect RStatd calls

- Detect requests for specific mapnames and file names

- Detect SMB-based attacks on PC file servers

- Detect Internet control message protocol

This preface identifies the audience for this guide, the related and prerequisite documentation, the typeface conventions used in the Cross-Site documentation, the Cross-Site icons, and instructions for obtaining customer support.

Who Should Read This Guide

The target audience for this guide is system or web administrators who are familiar with installing and upgrading operating systems, installing and administering web servers, database maintenance, and general information technology (IT) procedures. Specifically, users of the guide should have some knowledge of the following software:

- The Windows NT, AIX, or Solaris operating system

- The Netscape Enterprise Server, including the Administrative Server, and Web protocols such as HTTP and SSL; for secure web servers, you must also be familiar with digital certificates

- Oracle or DB2

- The Java environment

Prerequisite and Related Documents

The following documents are related to the Cross-Site product suite and are considered prerequisite reading before using Cross-Site:

- *Cross-Site for Security Release Notes*
  The release notes provide the most up-to-date information about known defects and their workarounds. Be sure to read this document before installing and using Cross-Site.

- *Cross-Site for Security User's Guide*
  This guide provides overview information about the product's features, instructions for using the console and performing tasks, reference information such as command line interfaces (CLIs), the Security agent's configuration files, and a glossary. The information in this book is available through the console's help system. You can also access this user's guide on the product CD-ROM or download it from the following URL:

  http://www.cross-site.com/support/docs

- *Guide to Cross-Site Integration with Tivoli Enterprise Applications*
  This guide describes how to use the features provided with Cross-Site for integration with Tivoli Enterprise applications. Specifically, Cross-Site provides integration with Tivoli Software Distribution, Tivoli User Administration, Tivoli Enterprise Console, and Tivoli NetView. You can download this user's guide from the following URL:

  http://www.cross-site.com/support/docs

Conventions Used in This Guide

This guide uses several typeface conventions for special terms and actions. These conventions have the following meaning:

Bold Command names and arguments, keywords, file names, World Wide Web addresses, or other information that you must use literally, appear in bold. Names of windows, dialogs, and other controls also appear in bold.

Italics Variables and values that you must provide appear in italics. Italics are also used to emphasize words or phrases.

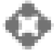
New terms appear in italics when they are defined in the text.

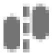
`Monospace` Code examples and commands appear in a monospace font.

Cross-Site Icons

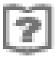
The following icons represent various Cross-Site resources:

Identifies the executable (EXE) files on Win32 platforms for the Cross-Site agent and console.

 Represents the Cross-Site suite; in particular, this icon represents a global view of all resources on the Cross-Site console.

 Represents the Cross-Site for Security application.

Represents Cross-Site's administrative services. For example, you can administer users, roles, events, and the event log.

 Represents the Cross-Site help system. The help system provides conceptual, procedural, and reference information about the Cross-Site services and applications.

Contacting Customer Support

Cross-Site documentation is available on the Cross-Site web site:

http://www.cross-site.com/support/docs/

Here, you can download copies of the installation guide and user's guide for each Cross-Site application. Additional supporting documents are also available. The web site is updated regularly with new documentation.

The Tivoli Cross-Site support team is committed to providing you with the best possible service. As a leading provider of Internet-based solutions, Tivoli believes the Web is the ideal venue for service. Therefore, you can obtain answers to critical questions on the Cross-Site web site (**http://www.cross-site.com/support/**). This support site contains the following information:

- Hot issues, which are immediate issues that are the most recently identified and the most frequently requested.
- A list of frequently asked questions (FAQs), which provides answers to basic questions that address issues that are important, but not necessarily urgent.
- Updated versions of the Cross-Site documentation.

Use the **Ask Support** form to submit a request for assistance. The URL for the form is as follows:

http://www.cross-site.com/support/asksupp/submitpmr

Tivoli is very interested in hearing from you about your experience with Cross-Site products and documentation.

For phone support inside the United States, contact Tivoli Cross-Site Support by calling 1-800-TIVOLI8. For support outside the United States, refer to your *Customer Support Handbook* for phone numbers in your country. The handbook is available online at the following URL:

http://www.support.tivoli.com

1

Requirements for the Cross-Site Server

This chapter provides important information about the hardware and software required to install the Cross-Site management server. If you do not adhere to these requirements, your installation might be needlessly prolonged. Tivoli strongly recommends that you read this information, as well as the information in the following two chapters, carefully. It will save you time when you are ready to install Cross-Site. After you install Cross-Site, Tivoli also recommends that you *review the user’s guide and online help* before using the product to manage your e-business.

You must install a web server on the same system where you intend to install the Cross-Site management server. The Cross-Site server and the web server must reside on the same system because the Cross-Site server relies on the web server to communicate with the Cross-Site clients. If you wish to use an existing web server to support the Cross-Site server, refer to “Requirements for the Web Server” on page 25 before assuming that you can use an existing web server, and before verifying that the existing web server’s system meets all of the requirements outlined in this chapter.

The following list describes the prerequisites and, where applicable, how to verify that you have the necessary resources. It is both a checklist and a work sheet; feel free to write down any values that you need to refer to during the installation.

1. Verify the version of the operating system on the machine where you intend to install the Cross-Site server. The following table outlines the supported platforms on which you can install the management server:

Requirement	Commands
Windows NT 4.0 service pack 4 or higher, on a Pentium 333 MHz class machine (or better), or	On Windows, select **Start -> Settings -> Control Panel**; double-click on **System** and review the **General** tab.
AIX 4.3.2, or	On AIX, enter **oslevel**.
Solaris 2.6 or 2.7 on Sun SPARC	On Solaris, to determine the version, enter **/usr/bin/uname -a**.

Note: *On AIX, the path to system commands is set by the path variable. Therefore, this table and subsequent ones identify the AIX command only, without its full path.*

2. Verify that the target system for the management server has enough disk space. The following table includes the disk space requirements for the Cross-Site management server:

Requirement	Commands
On Windows NT: 299 MB for the base server plus 192 KB for the Cross-Site for Security package	On Windows, double-click on **My Computer** and right-click on the drive where you intend to install the server. Select **Properties** and review the **General** tab.
On AIX: 269 MB for the base server plus 192 KB for the Cross-Site for Security package	On AIX, to determine the available disk space, enter **lsvg rootvg**. To determine the space allocated to the file systems, enter **df -k**.
On Solaris: 263 MB for the base server plus 192 KB for the Cross-Site for Security package	On Solaris, to determine the available disk space, enter **/usr/ucb/df -kl**.

3. Verify that the target system for the management server has enough memory, according to the requirement listed in the following table:

Requirement	Commands
256 MB on any supported platform	On NT, select **Start –> Programs –> Administrative Tools (Common) –> Windows NT Diagnostics**. Select the **Memory** tab and review the Physical Memory totals. On AIX, to determine the amount of available memory, enter **bootinfo -r**. AIX returns a value in KB. On Solaris, to determine the amount of available memory, enter **/usr/sbin/prtconf | head**.

4. Verify that the target system has enough swap space. This table includes the swap space requirements for the Cross-Site server:

Requirement	Commands
250 MB (300 MB recommended) on any supported platform	On NT, select **Start –> Programs –> Administrative Tools (Common) –> Windows NT Diagnostics**. Select the **Memory** tab and review the Pagefile Space totals. On AIX, to determine the amount of available swap space (paging space), enter **lsps -a**. On Solaris, to determine if a swap file is configured, enter **/usr/sbin/swap -l**. To determine the amount of available swap space, enter **/usr/sbin/swap -s**. Note the last number in the output.

5. *Solaris Only*
   Verify that the Solaris patches required to install the Java Development Kit (JDK) are installed on any workstation that you intend to include in your installation. You must install the patches prior to installing the JDK or the Cross-Site server.

Requirement	Commands
Patch 105284-05 and 105490-04 for Solaris 2.6	To list the patches installed on a Solaris system, enter **/usr/bin/showrev -p**.

You can download the latest patches from the following URLs:

http://access1.sun.com/cgi-bin/rpatch2html?README.105284-29
http://access1.sun.com/cgi-bin/rpatch2html?README.105490-07

Verify that your system functions properly after installing the patches.

6. *UNIX Only*
   Install the Java Development Kit (JDK), which provides a Java Virtual Machine (JVM). A JVM is required so that the Cross-Site server can connect to the web server. For NT, version 1.1.7 is bundled with the installation of the Cross-Site management server.

Requirement	Commands
For AIX, JDK version 1.1.6.2	On AIX, use this command to determine the level of the JDK: **lslpp -l Java.rte.bin**
For Solaris, JDK version 1.1.7 (rev 08 or higher)	To determine the version of JDK on Solaris, enter **java -fullversion**.

   If you have an older version of the JDK installed on Solaris, be sure to remove it before installing an updated version. You can use the following command to remove the installed JDK core packages:

```
pkgrm SUNWjvdem SUNWjvdev SUNWjvjit SUNWjvman SUNWjvrt
```

   You can download the JDK for AIX from the following site:
   http://service.software.ibm.com/support/rs6000/downloads

   You can download the JDK for Solaris from the following site:
   http://www.sun.com/solaris/java/index.html

   If you download the JDK 1.1.7_08 from this URL, you can also download the patches required for Solaris 2.6.

   Make note of the full path where the JDK is installed. You can enter it in the space below:

   _

7. If you intend to install the Cross-Site server on a UNIX system, obtain the **root** password for the system. If you intend to install it on a Windows NT system, obtain the **Administrator** password. Tivoli recommends that you do *not* record the password here.

8. *UNIX Only*
   Ensure that the following environment variables are *not* set in subshells: CLASSPATH and LIBPATH on AIX, and CLASSPATH and LD_LIBRARY_PATH on Solaris. Subshell environment variables are often set by files such as **.kshrc**, **.cshrc**, and **/etc/profile**. Cross-Site sets these environment variables and problems may arise if a shell script overrides them.

9. If you are using an HTTP proxy server, obtain the server's fully qualified host name and port number. You can write them in the space below:

   _

10. If you are using a SOCKS proxy server, obtain the server's fully qualified host name and port number. You can write them in the space below:

    _

11. Ensure that you can resolve the fully qualified and unqualified name of the system where you intend to install the Cross-Site server.

    On NT, use the **C:\Winnt\System32\nslookup** command.

    On AIX, use the **/usr/bin/nslookup** command.

    On Solaris, you can verify this using the **/usr/sbin/nslookup** command (if it is available on the server).

    You can record the fully qualified host name and the name of the administrative domain of the system where you are installing the Cross-Site server here:

    _

12. During installation of the Cross-Site server, you are prompted for the static IP address of the system where you are installing the Cross-Site server. Determine the IP address and enter it here for reference:

    _

13. You are prompted for the name of the X host where response windows can be displayed during installation of the Cross-Site server. If you intend to install the management server remotely, using an Xterm, for example, note the name of that system and ensure the two systems can connect to each other. You can write the name of the remote system here for reference:

    _

14. Back up the server and, if using a previously-installed database, back up the database. See your RDBMS documentation for more information.

    While no problems are expected as a result, you should make complete readable backups of the management server’s host before proceeding with the Cross-Site installation.

15. If Cross-Site 1.0 or 1.0.1 is installed, you must uninstall it before installing Cross-Site 1.1. See “Uninstalling Cross-Site” on page 235 for instructions. No upgrade or migration from version 1.0 or 1.0.1 is available yet.

16. If you have an IBM WebSphere Application Server 1.*x* installation, be aware that the Cross-Site server installation installs WebSphere 2.0.2. Either uninstall the 1.*x* installation or select another system to host the Cross-Site server. Do *not* overwrite 1.*x* with 2.0.2.

2

RDBMS Requirements

Tivoli Cross-Site supports Oracle, versions 8.0.4 and 8.0.5, and IBM DB2 5.2 as the relational database management systems (RDBMSes) that should be installed for use with Cross-Site.

Note: *Cross-Site supports and has tested Oracle for use only with a management server on Solaris or a Windows NT machine. DB2 is supported and has been tested only for use with an AIX management server. Other combinations are supported, though not tested. Contact Support if you wish to use an unsupported combination and encounter problems during their installation or use.*

Tivoli recommends that you observe the following table space estimates for one month of operational data. Space requirements may vary, however, depending on your environment and Cross-Site configuration.

- 50 MB for the management server
- 30 to 40 MB for each Security agent (this depends heavily on the agent's policy configuration, which dictates what the agent detects)

For Oracle, Cross-Site provides a sample script you can use to create 100 MB of table space. You can modify the script to create enough table space to meet your requirements. See step 6 on page 18 for this sample script. (The database dedicated to Cross-Site is referred to as the *management repository*.)

Tivoli recommends a rollback segment approximately half the size of the table space. The rollback segment should be auto-extensible and configured to have a large number of maximum extents. In addition, Tivoli recommends that you periodically shrink the rollback segment to conserve space on the file system where the database is installed. Remember, these estimates are for only one month of data. Consult your database administrator to determine values and procedures appropriate for your installation.

Oracle Configuration

After installing the RDBMS and reviewing the table space estimates for the Cross-Site management repository, complete the following steps to create a database for the Cross-Site management repository. These are overview steps only; refer to the Oracle installation guide for detailed instructions. If necessary, consult a database administrator for help.

If a database alias is defined in the **tnsnames.ora** file, you can refer to this alias during installation of the Cross-Site server. Otherwise, you are prompted for the database machine name, port number, and system identifier (SID).

1. Verify the version of the Oracle you have installed. You must have version 8.0.4 or 8.0.5; these are the only versions tested and supported by Tivoli.

2. Configure your RDBMS server to communicate with the Cross-Site server. If you install Oracle on a machine other than the Cross-Site server, install the Oracle client on the machine where the Cross-Site server will reside. See your database documentation for more information.

   Make note of the name of the machine on which you install Oracle, the name of the database, and the database SID. You are prompted for this information during the installation of the management server.

   ____

3. Verify that the Oracle listener is running. To do so, log in to the Oracle server using the Oracle account and enter the following commands:

```
cd $ORACLE_HOME
./bin/lsnrctl status
```

   The output of the **lsnrctl** command indicates whether the listener is running.

4. Determine which port the Oracle listener is using. To obtain the port number on which the listener is running, log in to the Oracle server using the Oracle account and enter the following command:

```
grep Port parameter_file
```

   where *parameter_file* is the path of the Listener Parameter File as indicated in the output of the **lsnrctl** command.

   Note that you are prompted for this port number during the installation of the management server. You can enter the port number here for reference:

   ____

5. Ensure that the ORACLE_HOME environment variable is set on the system where you intend to install the Cross-Site server.

   On NT, the default directory is **C:\oraNT\**.

   On AIX, the default home directory is in **/usr/lpp**.

   On Solaris, Oracle’s default home directory is *mount_point***/app/oracle/product/***version*, where *mount_point* is the base directory of the Oracle installation (there is no default) and *version* is the version of Oracle you have installed.

   Make note of the directory where Oracle is installed. You are prompted for this directory during the installation of the Cross-Site management server. You can enter the path here for reference:

   ____

6. Ensure that space is allocated in the database for the Cross-Site tables, which are created when the Cross-Site server is installed.

   The following is a sample SQL script that you can run to create the Cross-Site database table space and user for an Oracle database. Run this script as the Oracle **system** user. The script creates table space called **xtela_xsite_xx** and **xtela_temp_ts**, which totals 100 MB of space, and assumes that the Oracle installation directory is **/data/home/oracle/dbs**. The script also creates an Oracle user named **xsite**, with the password **xsite**.

   You might need to reevaluate the sizes in the script according to your environment and Cross-Site installation.

```
create tablespace xtela_xsite_xx
datafile ‘/data/home/oracle/dbs/xtela_xsite.dbf’ size 90M
default storage (
initial 100K
next 50K
minextents 2
maxextents 120)
offline;
commit;

create tablespace xtela_temp_ts
datafile ‘/data/home/oracle/dbs/xtela_temp.dbf’ size 10M
default storage (
initial 100K
next 50K
minextents 2
maxextents 20)
offline;
commit;

alter tablespace xtela_xsite_xx online;
commit;

alter tablespace xtela_temp_ts online;
commit;

create profile xsite_profile limit
sessions_per_user 50
cpu_per_session unlimited
cpu_per_call 6000
```

```
logical_reads_per_session unlimited
logical_reads_per_call 100
idle_time 30
connect_time 480;
commit;

create user xsite
identified by xsite
default tablespace xtela_xsite_xx
temporary tablespace xtela_temp_ts
quota unlimited on xtela_xsite_xx
profile xsite_profile;
commit;

GRANT CONNECT,RESOURCE,UNLIMITED TABLESPACE TO
xsite identified by xsite;
commit;
```

This is only an example, and the script you use depends on your environment. This script is not supported by Tivoli. See your database documentation for more information on creating table space and users in Oracle.

7. Create a database user that can be used by the Cross-Site server to access the database. This user must have sufficient privileges to create and edit tables.

   Make note of this information (do *not* write the password); you are prompted for it during the installation of the management server.

   ____

8. Install a Java database connectivity (JDBC) driver on the machine where the management server is installed.

   On NT, install version 8.0.*x* of the thin driver.

   On AIX and Solaris, install version 8.0.*x* of the OCI (type 2) or thin driver.

   You can download the latest drivers from the following URL: **http://technet.oracle.com/software/download.htm**

Make note of the class name of the driver, such as **oracle.jdbc.driver.OracleDriver** for Oracle 8. You are prompted for the class name during the installation of the management server.

_ _

Recall that Cross-Site currently supports Oracle for use only with a management server on Solaris or a Windows NT machine.

DB2 Configuration

After installing the IBM DB2 RDBMS server and reviewing the table space estimates for the Cross-Site management repository, complete the following steps to create a database for the Cross-Site management repository and to configure a connection from the Cross-Site server to the DB2 database. These are overview steps only; refer to the DB2 installation guide for detailed instructions. If necessary, consult a database administrator for help.

1. Verify the version of the DB2 you have installed. You must have version 5.2; this is the only version tested and supported by Tivoli.

2. If you choose, you can create a separate database in the DB2 RDBMS for Cross-Site's data, instead of using an existing database. The following command line example creates a database called **xsite**:

   ```
   db2 create database xsite with "Tivoli Cross Site
   database"
   ```

   This command creates a low maintenance, System Managed Space (SMS) table space. SMS table space is used for temporary tables created during database processing, and for user-defined tables and indexes. Also, this command creates the data files on the default drive, and the space needed for the tables is not allocated by the system until required.

For a large, high performance database, you may want to create a database with Database Managed Space (DMS) table spaces. Refer to the DB2 administration guide for more information.

Make note of the database name and installation directory. The default directory is **/usr/lpp/***version*. You are prompted for this information during the installation of the Cross-Site management server. You can enter it here for reference:

_ _

3. To configure the Cross-Site server to communicate with your RDBMS, you need to install and configure the DB2 Client Application Enabler (CAE) on the machine where Cross-Site will reside. The CAE must be the same version as the DB2 server.

   When installing and configuring the DB2 CAE, complete these items:

   - Ensure that there is no DB2 installation (either complete or partial) on the system. If there is, Tivoli recommends that you uninstall it.

   - Customize the options to select JDBC.

   - Ensure that ~2 MB are available in the selected home directory to accommodate the DB2 CAE.

   No matter if the DB2 CAE is running on a system or using a Network File System (NFS), you must source the **db2profile** file (for the Korn or Bourne shell) or **db2cshrc** file (for the C shell) to be able to run DB2 commands and utilities such as **catalog** and **connect**. These files are located in the home directory of the DB2 instance owner, under the **sqllib** subdirectory. Source the appropriate file in the **.profile** or **.cshrc** file of each account that needs to use the DB2 environment and tools.

4. To verify the setup of the RDBMS and CAE clients, ensure that the following environment variables are set correctly:

   - DB2DIR should point to the directory where the DB2 CAE is installed

   - DB2INSTANCE should be set to the database instance name. This is set during installation of the database.

   Make note of the DB2 instance name and home directory. You are prompted for this information during the installation of the management server.

---

5. Set up connectivity between the DB2 server and clients. The following command line example sets up node connectivity between the server, **ghost**, with the node name or alias **xs_db2**, which uses port 50000, and the client:

   ```
   db2 catalog tcpip node xs_db2 remote ghost server 50000
   ```

   Note: *The alias cannot be longer that 8 characters.*

   You must also set up the database connectivity. The following example sets up connectivity for the client to connect to the database named **xsitedev**, with the alias **xs_dev**:

   ```
   db2 catalog database xsitedev as xs_dev at node xs_db2
   ```

   To verify connectivity, enter a command similar to the following. This command verifies connectivity to the **xs_dev** database using the user name **xsite** and the password **connect2db**. This user name and password pair belongs to an account on the server; the server is set up for server authentication.

   ```
   db2 connect to xs_dev user xsite using connect2db
   ```

6. Install a DB2 Java database connectivity (JDBC) driver on any system where the CAE client is installed, including on the management server. The driver, which is installed using the **db2java.zip** file, is available in the **java** subdirectory of the CAE home directory. This is a type 2 driver that requires DB2 client shared libraries, which are available in the **lib** subdirectory of the CAE home directory.

   Install the driver in the *install_dir* **/java/** directory, where *install_dir* is the DB2's home directory.

   When you install the Cross-Site management server, you are prompted for the class name of the DB2 JDBC driver. You can enter it here for reference. (An example class name for the DB2 driver is **COM.ibm.db2.jdbc.app.DB2Driver**.)

   _

7. The Cross-Site management server requires that you install three user defined functions (UDFs) on the database server machine: **formatWeek**, **formatDay**, and **formatHour**. DB2 loads these functions in response to SQL queries issued by the management server. The management server installation executes CREATE FUNCTION statements to make the DB2 database aware of the location of the UDFs. However, you must copy the actual implementation of the UDFs to a location on a file system accessible to DB2 during run-time.

   On NT, copy the **formatDate.dll** file from the **db2\w32-ix86** directory on the Cross-Site CD-ROM to the **%DB2DIR%\function** directory on the DB2 server.

   On AIX, the UDFs are distributed as a shared library called **formatDate**. Copy the shared library to the DB2 instance home directory under **$DB2DIR/function** (on the DB2 server). This operation requires DB2 instance owner permissions. Tivoli provides the **setup_db2** script to help you perform this task. Run this script after copying the shared library. The script is located in the **db2/aix4-r3** directory on the Cross-Site CD-ROM.

You do not have to create a database user on DB2 because DB2 authenticates users by using an operating system account on AIX. When you are prompted for database user ID and password during the installation of the Cross-Site server, you can enter any valid AIX user ID and password.

3

Requirements for the Web Server

This chapter outlines the requirements and recommendations for the web server that is or will be installed for use with the Cross-Site management server. The web server and the Cross-Site server must reside on the same system because the Cross-Site server relies on the web server to communicate with the Cross-Site clients. Therefore, you must configure the web server before installing Cross-Site.

Because you are installing Cross-Site for Security, you must secure the web server with a server certificate. Obtain a server certificate, which enables you to convert the web server's protocol from HTTP to HTTPS, from a commercial vendor or in-house certificate source. See "Obtaining a Server Certificate" on page 179 for information about server certificates, and to review the list of supported certificates. (Tivoli recommends that you review the entire appendix regarding certificates if you are unfamiliar with them.) *DO NOT PROCEED WITH THE CROSS-SITE INSTALLATION UNTIL YOU OBTAIN AND INSTALL THE CERTIFICATE.*

After obtaining the server certificate, install it on the web server before installing Cross-Site, which is also described in "Obtaining a Server Certificate" on page 179.

Before completing the steps in this chapter, read and perform the steps in “Requirements for the Cross-Site Server” on page 7. By reading that chapter first, you ensure that the system on which the web server is installed meets the requirements for the Cross-Site server.

Complete the following steps before installing the Cross-Site server. Netscape Enterprise Server, version 3.6 Service Pack 2 (3.62), is the *only* web server supported by Cross-Site.

1. If you are installing a new web server, you can download the trial version of the Netscape Enterprise Server (NES) 3.62, from the following URL:

   http://www.iplanet.com/downloads/testdrive/detail_12_1.html

   If this link becomes outdated, go to **http://www.iplanet.com** and click the **Downloads** link, then the **Test Drive** link. Search the listed products for the Netscape Enterprise Server. After installing the trial version of NES, register and purchase the Enterprise Server.

2. If you choose to use an existing installation of NES, verify that the correct version (3.62) is installed. To do so, go to the Netscape Enterprise Server page, using a web browser. The URL for this page is *protocol*://*server*:*port*, where *protocol* is either HTTP or HTTPS, and *server* is the name of the Netscape Enterprise Server. The *port* variable is usually 80 if the protocol is HTTP or 443 if the protocol is HTTPS. (Recall that, because you are installing Cross-Site for Security, you must secure your web server. Therefore, the protocol should be HTTPS and the port may be 443.)

   If you must upgrade the web server, you can download NES 3.62 from the URL sited in step 1. You do not need to uninstall your current version; installing the newer version of NES overwrites the old one. Also, if you converted an existing web server to use HTTPS, you might suggest to your users that they change their bookmarked pages to refer to the web server’s new protocol (https://*URL* instead of http://*URL*). Finally, ensure that your firewall is configured for SSL.

3. Make note of the Netscape Administrative Server’s user name, password, and port. You can enter these values here, for reference later if you need to restart NES (do *not* write the password):

   _

   (The first time you use the Administrative Server’s page after installing the Cross-Site server, you are prompted to accept changes. You access the Administrative Server’s page by entering *protocol*://*server_name*:*admin_port* in the web browser. These changes are made by the installation of WebSphere, which is part of the Cross-Site server’s installation. Accept the changes.)

4. Make note of the Netscape Enterprise Server’s protocol and port. Enter these values here:

   _

5. Ensure that NES runs as any user other than as **root**. Although NES is installed as **root**, the NES installation script prompts you for the user that you want NES to run as. (The default is **nobody**.) Tivoli recommends that you create a user, such as **xsite**, that you can use to run NES. (If NES runs as **root**, the Cross-Site installation will fail due to permission problems.)

6. Avoid using the following ports when installing or configuring NES: 5282, 7727, 8000, 4444, 9527, and 7717. Cross-Site uses these ports to communicate with clients. (These ports do not need to be opened on the firewall for Cross-Site to work properly.)

7. Note the full path to the directory containing the NES **obj.conf** file. This file resides in the NES configuration directory.

   On NT, the default directory is as follows:
   C:\Netscape\SuiteSpot\https-*NESname***\config**

   On AIX, the default directory is as follows:
   /usr/netscape/suitespot/https-*NESname***/config**

On Solaris, the default directory is as follows:
/opt/netscape/suitespot/https-*NESname***/config**

Enter the path to your web server's **obj.conf** file below. You are prompted for it during the installation of the management server.

_ _

8. Note the Key File Password of the server certificate. This password is also referred to as the key-pair password; you set this password when you generated the key-pair. (Do *not* write the password here.)

9. If you installed a server certificate that is not supported by Cross-Site, you must you must create the **KeyRing.class** file. This is a special control file that contains the names of supported root certificates and to which you must import the root certificate of your server certificate. Create the **KeyRing.class** file as described in "Importing an Unsupported Root Certificate" on page 199. When you are done, note the path to the file here:

   _

10. Back up the **obj.conf** file and the **start** script before installing Cross-Site, which modifies both of these files.

11. Ensure that the web server is shut down before installing the Cross-Site *base* server. The base server provides the core services, web server plug-ins, and IBM's WebSphere. The base server's installation also creates the Cross-Site table space in the RDBMS. When the installation of the base server completes, it restarts the web server.

4

Generating a License Key

To use your Tivoli Cross-Site product, you need a customized license key. If you obtained Cross-Site through a business partner, contact that organization for a license key. If you purchased Cross-Site directly from Tivoli or IBM, you can generate a license key by completing the procedures in this chapter.

License management is a two-part process:

- Generating a license key using the Cross-Site Support system. (You must have an account on the Support site to generate a license key. If you do not have an account, you must first activate one.)
- Installing the license key on your Cross-Site management server, using a license servlet.

The Support system, which is hosted on the Cross-Site web site (**http://www.cross-site.com**), enables you to retrieve your purchase order for Cross-Site and generate a license key based on the number of clients you intend to deploy. For example, if you intend to deploy Cross-Site in a lab environment first, using a subset of the clients you purchased, you can create a license key for that test deployment. Later, when you decide to deploy Cross-Site in a production environment, you can regenerate the license key to include all of the Cross-Site clients you purchased. (Regenerating your license key is covered in “Regenerating Your License Key” on page 225.) Therefore, the Support system enables you to keep track of your configuration, in addition to creating licenses for you.

This chapter explains how to activate your Cross-Site Support account, which provides online access to the Cross-Site Support team and documentation. The chapter then demonstrates how to generate a license key. When the installation of the base server is complete, a web browser is displayed, which enables you to install the license key. (The base server is the first part of the Cross-Site management server’s installation and provides the Cross-Site framework services, RDBMS tables, and Cross-Site console.)

If you already have a license key, refer to “Regenerating Your License Key” on page 225 if you need to change your configuration and key. If you have trouble accessing the Cross-Site web site, please contact Tivoli Cross-Site Support by sending e-mail to **licensing@cross-site.com**.

Activating Your Support Account

Before you can use the Cross-Site Support system to generate license keys or access information, you must create an account for yourself. Complete the following steps to do so:

1. Gather your customer information, which you will need in order to obtain a license key.

   If you purchased Cross-Site from Tivoli, complete these steps:

   a. Find the Pick List document that came on the box with your Tivoli Cross-Site CD-ROM and documentation. This Pick List is located in a clear-label pouch that is affixed to an upper right-hand corner of the box. This document looks like a packing list, and it has the Tivoli logo and the text “Pick List” in bold at the top of the page.

      If you cannot find the Pick List document, contact Support using the Support contact information in the preface.

b. Locate the reference number and customer number on the Pick List. You will use these to log in to the Cross-Site license key web site. The reference number is located in the upper right-hand corner of the Pick List. It is usually a five-digit number.

c. Locate the customer number, which is located in the “First Ship To Customer Number” box on the right-hand side of the Pick List document. This number usually starts with the letter T, followed by six digits.

If you purchased Cross-Site from IBM, complete these steps:

a. Find the IBM Software Packing List document that came on the box with your Tivoli Cross-Site CD-ROM and documentation. This packing list has the IBM logo in the upper-left corner and a series of text boxes and bar codes printed on it. There is also a gray bar at the top of the document with “Software Packing List” printed on it.

   If you cannot find the Software Packing List, the information you need is also located on the mailing label and on other IBM documents shipped with your order.

b. Locate the IBM order number and customer number on the packing list. You will use these numbers to log in to the Cross-Site license key web site. The order number is located toward the middle of the packing list. It usually consists of six alphanumeric characters.

c. Locate the customer number, which is located in the upper right-hand corner of the packing list. This number is usually a seven-digit number.

If this information is not accurate, such as the names and locations of the numbers on the packing slip, refer to the following URL. It provides the most up-to-date information about obtaining a license key, which may have been updated since this document was created.

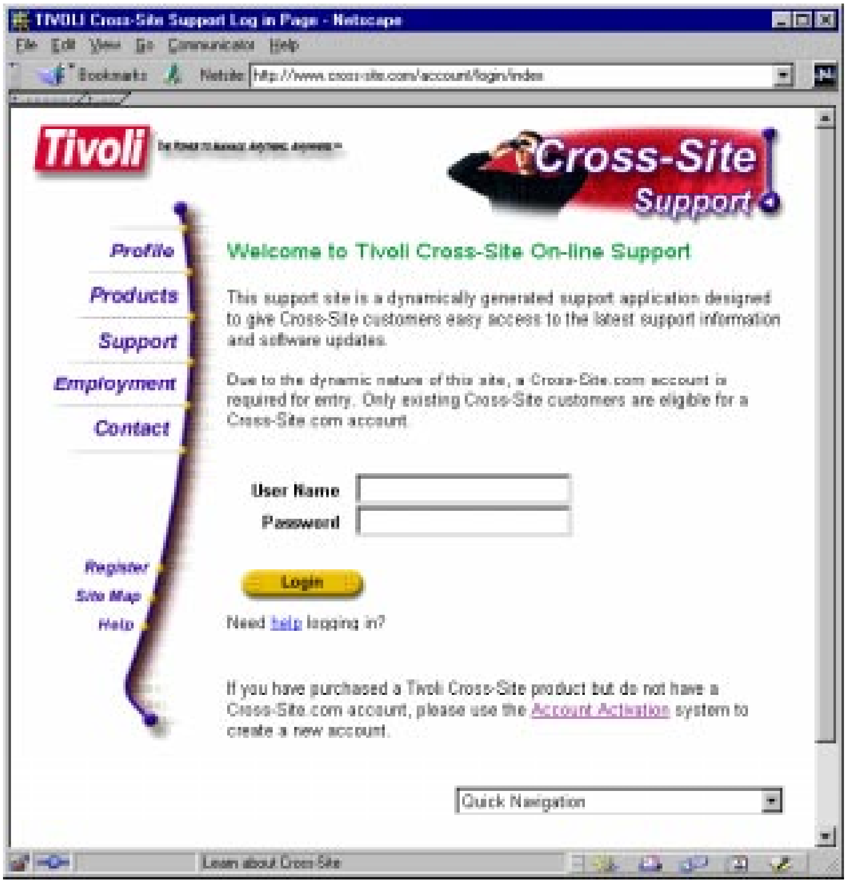
http://www.cross-site.com/support/licensing/

2. Access the Cross-Site Support web site by entering the following URL in a web browser:

   http://www.cross-site.com/support/

   You can also click the **Support** link on the home page of the Cross-Site web site (**http://www.cross-site.com**).

   The following page is displayed:



TIVOLI Cross-Site Support Log in Page - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: http://www.cross-site.com/account/login/index
Tivoli
Cross-Site Support
Profile
Products
Support
Employment
Contact
Register
Site Map
Help
Login
Quick Navigation
Learn about Cross-Site

Welcome to Tivoli Cross-Site On-line Support

This support site is a dynamically generated support application designed to give Cross-Site customers easy access to the latest support information and software updates.

Due to the dynamic nature of this site, a Cross-Site.com account is required for entry. Only existing Cross-Site customers are eligible for a Cross-Site.com account.

User Name

Password

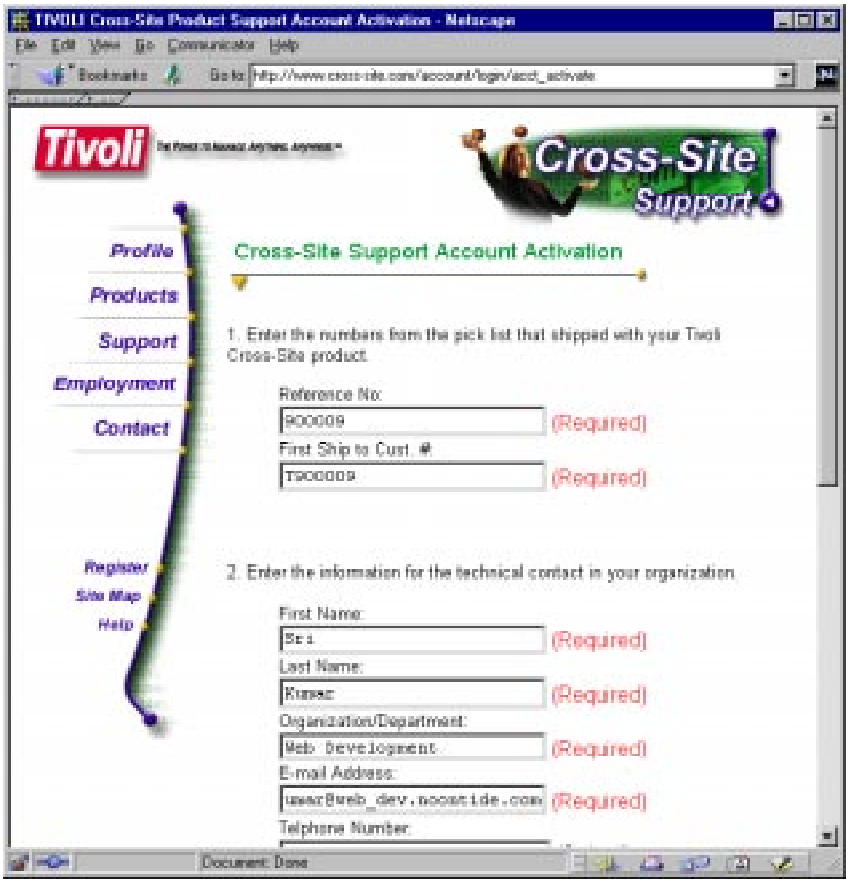
Need help logging in?

If you have purchased a Tivoli Cross-Site product but do not have a Cross-Site.com account, please use the Account Activation system to create a new account.

3. You must create an account for yourself in order to access the Support system. The account provides a user name and password, which you can use to log in to the Support site. To create an account,

click the **Account Activation** link at the bottom of the Login page. The **Cross-Site Support Account Activation** form is displayed.

4. Complete the form.



TIVOLI Cross-Site Product Support Account Activation - Netscape

Go to: http://www.cross-site.com/account/login/acct_activate

Cross-Site Support Account Activation

1. Enter the numbers from the pick list that shipped with your Tivoli Cross-Site product.

Reference No: 900009 (Required)

First Ship to Cust. #: T900009 (Required)

2. Enter the information for the technical contact in your organization.

First Name: Sri (Required)

Last Name: Kumar (Required)

Organization/Department: Web Development (Required)

E-mail Address: user@web_dev.crosside.com (Required)

Telphone Number:

Document: Done

5. Click the **Submit** button. When you submit the form, the Cross-Site Support system generates a password for the user name you specified in the **User Name** field (on the previous page). The system then sends your user name and password to you, using the e-mail account specified in the **E-mail Address** field.

An acknowledgment page is displayed. If you encounter an error instead, click the **Contact** link at the bottom of the page, to report the problem.

6. Retrieve your password from the e-mail sent to you by the Support system (**support@cross-site.com**). Recall that the e-mail is sent to the address specified on the Account Activation form.

   The e-mail will be similar to the following:

   ```
   A Cross-Site Online Support account has been created for
   you with the following username and automatically
   generated password:

   Username: skumar
   Password: q7wCosnK

   After you have used the above username and password to
   log in for the first time, we recommend you use the “Edit
   Profile” page to select a new password.

   Thank you for using Cross-Site Online Support.
   ```

7. Select the **Support** link on the left-hand side of the Account Activation page. The Login page is displayed again.

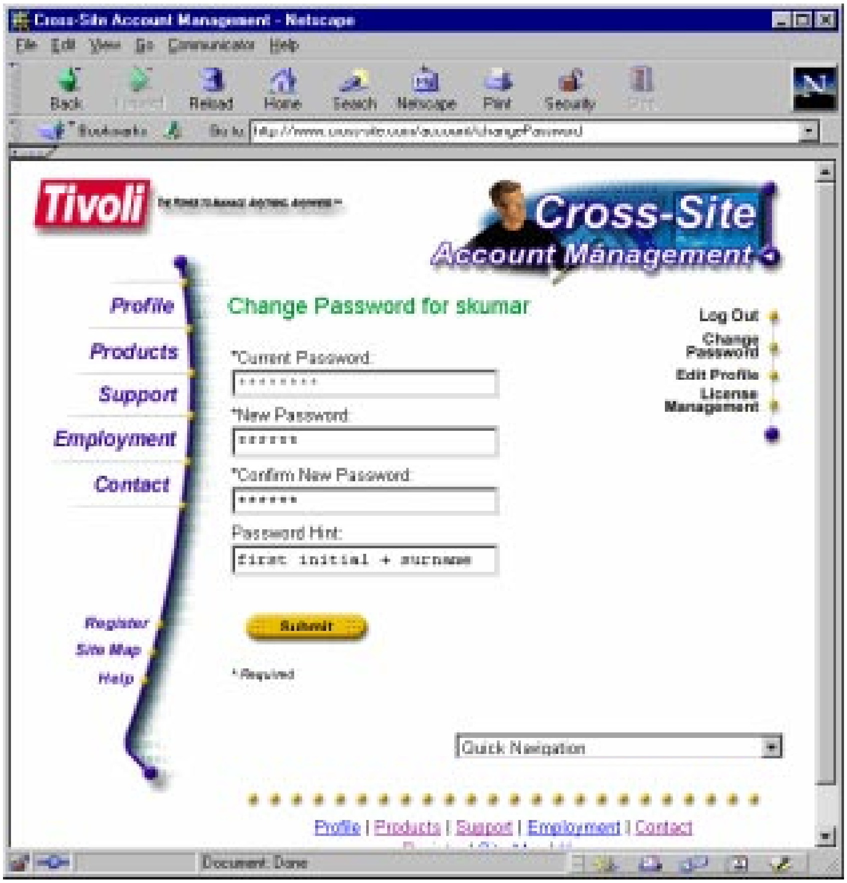
8. Enter your user name and password in the fields (as specified in the e-mail) and click the **Login** button. The Welcome page is displayed, which provides links to helpful information about Cross-Site and the Support system.

9. Tivoli recommends that you change your password as a first step in using the Support system. To do so, complete these steps:

   a. Click the **Account Management** link on the right-hand side of the page. The Account Management page is displayed.

   b. Click **Change Password** on the right-hand side of the page.

c. Complete the form that is displayed.



Cross-Site Account Management - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to: http://www.cross-site.com/account/changePassword
Tivoli
Cross-Site
Account Management
Profile
Products
Support
Employment
Contact
Register
Site Map
Help
Log Out
Change Password
Edit Profile
License Management
Quick Navigation
Profile | Products | Support | Employment | Contact
Document: Done

Change Password for skumar

*Current Password: ********

*New Password: ******

*Confirm New Password: ******

Password Hint: first initial + surname

Submit

* Required

If you specify a word or phrase in the **Password Hint** field, the Cross-Site Support system will e-mail this word or phrase to you if you request help when logging in.

d. Click **Submit**.

You can now log in to the Support system to generate your license key.

Generating a New License Key

Complete the following steps to generate the license key:

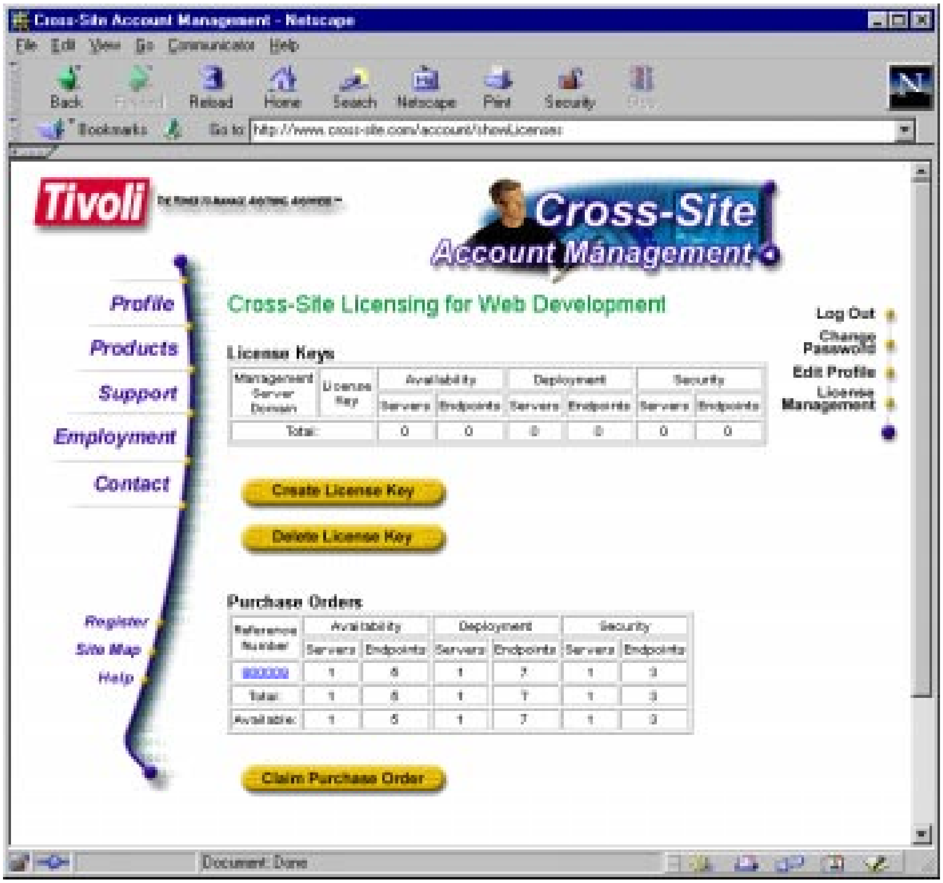
1. If necessary, log in to the Cross-Site Support system.

2. Enter the following URL in your web browser:

   http://www.cross-site.com/account/showLicenses

   You can also select the **Account Management** link on the Welcome page, then select the **License Management** link on the right-hand side of the Account Management page.

A page similar to the following is displayed:



Cross-Site Licensing for Web Development

License Keys

Management Server Domain	License Key	Availability		Deployment		Security	
		Servers	Endpoints	Servers	Endpoints	Servers	Endpoints
Total:		0	0	0	0	0	0

Purchase Orders

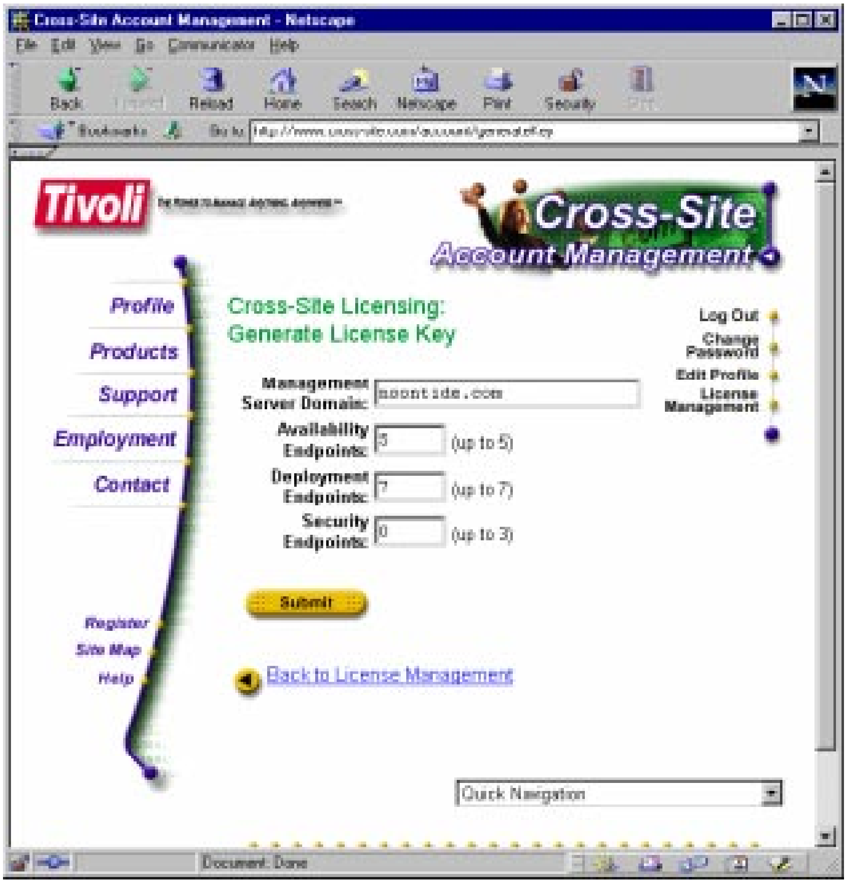
Reference Number	Availability		Deployment		Security	
	Servers	Endpoints	Servers	Endpoints	Servers	Endpoints
[illegible]	1	5	1	7	1	3
Total:	1	5	1	7	1	3
Available:	1	5	1	7	1	3

The first time you access the License Management page, your purchase order is listed in the Purchase Orders table. If your order is not listed, click the **Claim Purchase Order** button to retrieve your order from the system, then return to this page (by clicking the **Return** link on the Acknowledgment page). If your order is incorrectly listed, contact Support using the Support contact information in the preface.

3. Click the **Create License Key** button. The **Generate License Key** page is displayed.

4. Complete the form, specifying the clients that you want included in your license key. Licensing for your management server and its application components is implied by the types of clients you specify.

   Note: *The management server's domain name that you specify on this page must be the same as the administrative domain name you will specify when you install the management server.*



Cross-Site Licensing:
Generate License Key

Management Server Domain: acontide.com

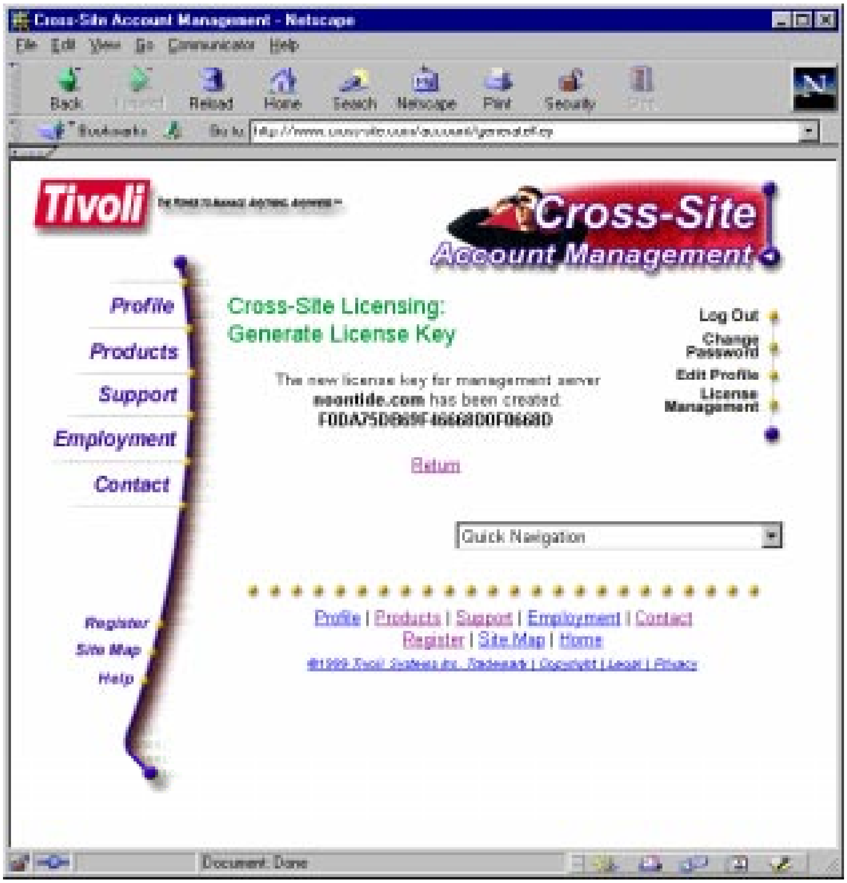
Availability Endpoints: 5 (up to 5)

Deployment Endpoints: 7 (up to 7)

Security Endpoints: 0 (up to 3)

The maximum number of endpoints (clients) you can specify is displayed next to each field. This information is based on your purchase order (or orders).

5. Click the **Submit** button to create the license key. A page with your new license key is displayed:

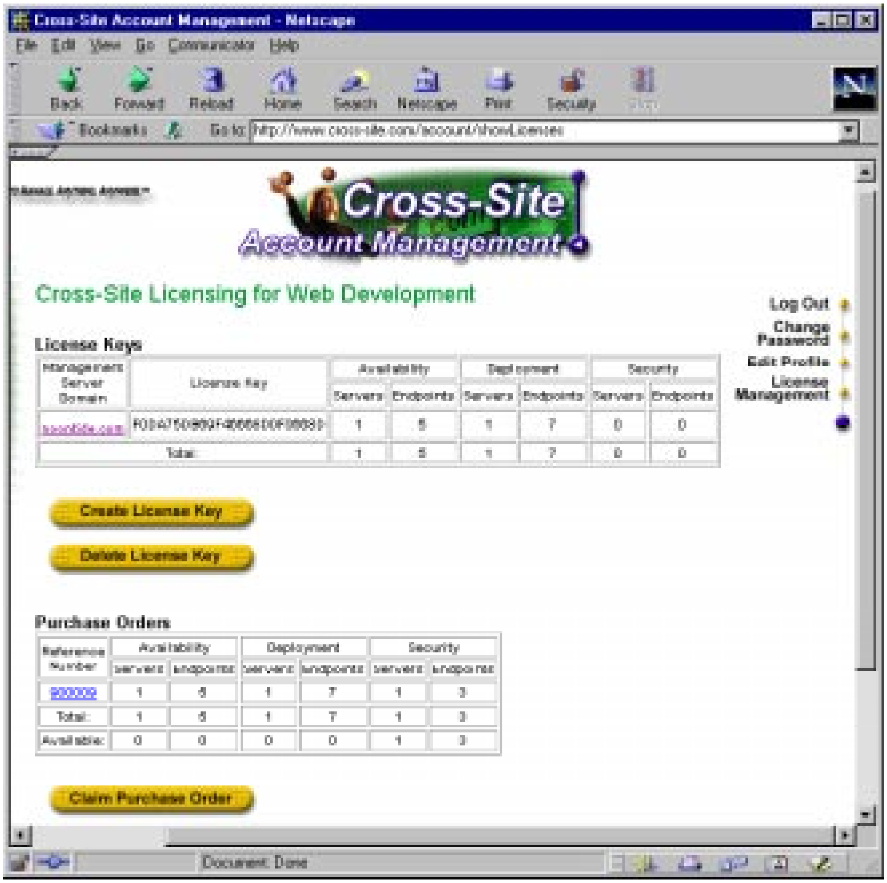


Cross-Site Account Management - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to:
Tivoli
Cross-Site Account Management
Profile
Products
Support
Employment
Contact
Register
Site Map
Help
Log Out
Change Password
Edit Profile
License Management
Return
Quick Navigation
Profile | Products | Support | Employment | Contact
Register | Site Map | Home
Document: Done

Cross-Site Licensing:
Generate License Key

The new license key for management server **neontide.com** has been created:
F0DA75D069F466680DF0668D

6. Click **Return** to display the License Management page.


Cross-Site Account Management - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to: http://www.cross-site.com/account/showLicenses
Cross-Site
Account Management
Log Out
Change Password
Edit Profile
License Management
Create License Key
Delete License Key
Claim Purchase Order
Document: Done

Cross-Site Licensing for Web Development

License Keys

Management Server Domain	License Key	Availability		Deployment		Security	
		Servers	Endpoints	Servers	Endpoints	Servers	Endpoints
boxedSite.com	F03475D89QF4666EDDF08693	1	5	1	7	0	0
Total:		1	5	1	7	0	0

Purchase Orders

Reference Number	Availability		Deployment		Security	
	Servers	Endpoints	Servers	Endpoints	Servers	Endpoints
900009	1	5	1	7	1	3
Total:	1	5	1	7	1	3
Available:	0	0	0	0	1	3

Note that the first table on the page displays the license key and lists the domain name and clients included in the key. The second table provides a count of the clients that have not been included in a license key yet.

7. Highlight the license key and copy it to your system's clipboard. If the browser will not allow you to highlight the key, print this page or make note of the key.

You can now proceed to the installation of the management server. If the installation can launch a web browser, it will display the Cross-Site License Manager, which will enable you to install your license key. If the installation cannot launch a browser, you need to install the key before installing any applications on the base server. See “Installing Your License Key” on page 232 for instructions.

5

Installing the Cross-Site Server on NT

This section describes the procedure for installing a Cross-Site management server on Windows NT. You *must* read and complete the steps in the following chapters before beginning the procedures in this one:

- “Requirements for the Cross-Site Server” on page 7.
- “RDBMS Requirements” on page 15.
- “Requirements for the Web Server” on page 25. And if you are using a DB2 RDBMS server, you must copy the **formatDate.dll** file to the DB2 server before beginning the installation. This is described in “DB2 Configuration” on page 20.
- If you installed a server certificate that is unsupported by Cross-Site on your web server, you must create the **KeyRing.class** file before installing the Cross-Site management server. This is described in “Importing an Unsupported Root Certificate” on page 199.
- Be sure to generate a license key before installing, as described in “Generating a License Key” on page 29.

Complete the steps in this chapter to install the base management server. The base server provides the core services, web server plug-ins, and IBM’s WebSphere. The base server’s installation also creates the Cross-Site table space in the RDBMS. When the installation of the base server completes, it restarts the web server. This chapter also describes how to install Cross-Site for Security on the management server.

Contents of the CD-ROM

The following directories are in the top-level directory of the Cross-Site CD-ROM:

aix4-r3 The directory that contains the AIX Cross-Site packages.

CARS The channel archive directory; this directory contains installation files for the management server if you are installing the management server using the CD-ROM (local/domestic installation). This directory is also provided in case you have problems installing your management server using the Tivoli fulfillment server, which is a server located at Tivoli from which your Cross-Site server downloads the most recent code.

db2 This directory contains the **w32-ix86** and **aix4-r3** subdirectories. The **w32-ix86** subdirectory contains the **formatDate.dll** file, which contains user defined functions required by the Cross-Site server.

DOCS The directory that contains the Cross-Site documentation in the Adobe PDF format. The free Adobe reader is available at the following URL:

http://www.adobe.com/prodindex/acrobat/readstep.html

solaris2 The directory that contains the Solaris Cross-Site packages.

TCI The directory that contains the installation files for the Tivoli Enterprise Module for Cross-Site.

UTIL The directory that contains a tool that you can use to add root certificates from unknown certificate authorities to the Cross-Site **KeyRing.class** file.

w32-ix86 The directory that contains the Windows packages.

The contents of the **w32-ix86** directory is as follows:

agent.EXE The installation program for installing the Cross-Site for Availability and Cross-Site for Deployment agents on Windows 95, 98, and NT systems.

availserver.EXE
The installation program for installing the Cross-Site for Availability server on the management server on NT.

console.EXE
The installation program for installing the Cross-Site console on Windows 95, 98, and NT systems.

Cross-Site for Security.EXE
The installation program for installing Cross-Site for Security on NT systems.

depserver.EXE
The installation program for installing the Cross-Site for Deployment server on the management server on NT.

mgtserver.EXE
The installation program for installing the base management server on NT.

secserver.EXE
The installation program for installing the Cross-Site for Security server on the management server on NT.

The 128-bit and 56-bit Versions of Cross-Site

If you are located in the United States or Canada, or if you qualify for 128-bit encryption outside of the U.S. or Canada, you were shipped the domestic version of the Cross-Site CD-ROM. This version provides 128-bit encryption. In general, if you are located outside of the U.S. or Canada, you received the export version of the Cross-Site CD-ROM. This version provides 56-bit encryption. (To verify which version of the CD-ROM you received, check the information printed on the CD-ROM.)

Installing Locally Versus Remotely

If you are installing Cross-Site from the domestic version of the CD-ROM, you *must* install the Cross-Site management server *locally*. (One of the installation prompts asks you to choose local or remote.) This means that the installation program will install the server using only the bits on the CD-ROM. This option enables you to install Cross-Site without contacting the Tivoli fulfillment server, which requires connectivity to the Internet. The fulfillment server is a server located at Tivoli headquarters that provides bits so that your Cross-Site server can download, versus relying solely on the CD-ROM.

If you are installing from the export version of Cross-Site, you may choose to install locally or remotely. If you install remotely, the installation program contacts the Tivoli fulfillment server to complete the installation. Tivoli *strongly* recommends that you install locally, no matter which version of the CD-ROM you received.

If you choose to install remotely, consider that installing Cross-Site involves downloading large files, sometimes up to 40–50 MB. This download estimate could impact you if bandwidth is an issue. In addition, verify that all routers, gateways, and firewalls are configured to allow HTTPS connections to **https://software.cross-site.com**.

Installing Intermixed Domains

It is possible that you install your Cross-Site domain using the domestic (128-bit) version of the CD-ROM and you or your e-business partner installs another (interconnected) Cross-Site domain using the export (56-bit) version, or vice versa. If this could potentially occur in your installations, you may want to consider the information in this section.

Most importantly, do not install the export version of Cross-Site agents against the domestic version of the Cross-Site server. Similarly, do not install the domestic version of Cross-Site agents against the export version of the Cross-Site server. If this configuration error occurs, the agent will download the incorrect binaries from the management server. Tivoli does not support these version mismatches. In addition, improper configuration may be a violation of U.S. Export regulations.

However, if intermixed domains are installed to work together, you should note the following: Cross-Site agents and consoles that were installed using the export media may not be able to communicate with a management server that was installed using the domestic version of the Cross-Site CD-ROM. Agents and consoles configured for 56-bit encryption cannot communicate with a management server that is configured for only 128-bit encryption. If an export agent or console attempts to contact a domestic server, the following error is displayed:

```
Server connection error: Failed to contact management
server.
```

To verify that it is an export-to-domestic problem, you can contact the management server by entering the following URL in the export version (56-bit) of the web browser:

protocol://*server_name*:*port***/servlet/CrossSiteServlet**

where *protocol*, *server_name*, and *port* are those values specified during the installation of the web server. For example, the following error message is displayed in the Netscape browser if there is a mismatch of encryption levels:

```
Netscape and this server cannot communicate securely because
they have no common encryption algorithm(s).
```

Installing the Base Server

Tivoli recommends that you close all Windows applications before beginning the installation. Also, ensure that the web server is shut down before installing the base server.

Note: *If you are reinstalling the management server or attempting to install again after a failed installation, ensure that all processes that were started by previous installations are stopped. See "Stopping and Restarting the Server" on page 54 for details.*

To install the Cross-Site management server on Windows NT, complete the following steps.

1. Log in to the Cross-Site server's host machine as **Administrator**, or as a user with Administrator privileges.

2. In the **w32-ix86** directory on the Cross-Site CD-ROM, double-click on the **mgtserver.EXE** file. The **Tivoli Cross-Site Management Server Welcome** dialog is displayed.

3. Click **Next**. The **Tivoli Cross-Site Management Server License Agreement** dialog is displayed. Depending upon your installation, this dialog displays either the Domestic or Export license agreement. Read the license agreement.

4. Click **Accept**. The **Choose Destination Location** dialog is displayed. The setup program will choose a installation directory for Cross-Site. The default drive and directory is **C:\Program Files\Tivoli\Cross-Site-Server** (and the **XSITsagt** directory is created under this path). If you wish to install in another location, use the **Browse** button to select that location.

   If you do not click **Accept**, the installation is cancelled.

5. Click **Next**. The **Fulfillment Server Usage** dialog is displayed. You must choose whether to perform a local or remote installation. By installing locally, you use the bits on the CD-ROM to install the management server. If you choose to install remotely, once the base server is installed, it contacts the Tivoli fulfillment server. It downloads bits from the fulfillment server to complete the installation. *TIVOLI STRONGLY RECOMMENDS THAT YOU CHOOSE LOCAL.*

   If you choose **Remote**, you must provide the protocol, name, and port number of the fulfillment server. The protocol is **HTTPS**, the host name for the Tivoli fulfillment server is **software.cross-site.com**, and the port number for the server is **443**. You must also specify the proxy and its port number, if your server must use a proxy server when contacting the Tivoli fulfillment server.

6. Click **Next**. The **Management Server Configuration** dialog is displayed.

   a. Select the protocol that will be used to access your new Cross-Site server. Select **HTTP** for an unsecure server. Select **HTTPS** for a server that will use the HTTPS protocol, which runs over SSL. (Cross-Site for Security must run on an HTTPS server.)

   The setup program fills in the **Management Server Host Name** field. The host name must be a fully qualified name. If this is not a fully qualified name, agents will not be able to resolve the host name of the server.

   b. Enter the IP address for your Cross-Site server.

   c. Enter the port number for your Cross-Site server.

   The setup program also fills in the **Admin Domain name** field.

7. Click **Next**. The **Alternate Certificate KeyRing** dialog is displayed if you selected HTTPS as the protocol of your server. If the management server needs to run with an alternate certificate, select **Yes** and enter the path to the **KeyRing.class** file. This implies that

you secured your web server using a server certificate that is not supported (by default) by Cross-Site. This also implies that you created the **KeyRing.class** file as described in “Importing an Unsupported Root Certificate” on page 199. Otherwise, select **No**.

8. Click **Next**. The **Management Server Extended Configuration** dialog is displayed. The setup program fills in the **Management Server Description** field. You must enter a collaboration password for the Cross-Site. This password will be used when collaborating with other Cross-Site servers. Tivoli recommends that, unless you are installing multiple management servers, you simply press Enter.

9. Click **Next**. The **Relational Database Configuration** dialog is displayed. Select the type of RDBMS that you plan to use with Cross-Site: **Oracle** or **IBM DB2**. Of course, this RDBMS must be configured as described in “RDBMS Requirements” on page 15.

   Note: *Recall that Tivoli has only tested the Oracle RDBMS server with an NT management server. Other combinations are supported, though not tested. Contact Support if you wish to use an unsupported combination and encounter problems during their installation or use.*

10. Click **Next**. The **Oracle Configuration** dialog or **IBM DB2 Configuration** dialog is displayed, depending on the database you are using. The setup program fills in the **Database Driver Type** and **Database JDBC Driver Type** fields.

    a. In the **Database User ID** field, enter a valid database user ID designated for Cross-Site.

    b. In the **Database Password** field, enter the password for the database user ID previously entered. You must reenter the password.

    c. In the **Database Host Name** field, enter the name of the machine on which the database is installed. This can be a local or remote machine.

d. *Oracle Only*
In the **Database Port** field, enter the port number of the listener on the machine where the database is installed.

e. *Oracle Only*
In the **Database SID** field, enter the database’s system identifier (SID).

f. *DB2 Only*
In the **Database Name** field, enter the name given to the database when it was created.

g. In the **Oracle Directory** or **IBM DB2 Directory** field, enter or browse for the installation directory of the database.

11. Click **Next**. The **Netscape Configuration** dialog is displayed. You must provide the path to the directory containing the **obj.conf** file for the Netscape Enterprise Server. By default, this file resides in the **C:\Netscape\SuiteSpot\https-***NESname***\config** directory.

12. Click **Next**. A dialog is displayed asking if you want to continue with the installation.

13. Click **Next** if you want to continue with the installation or **Cancel** if you want to stop and install the management server at another time. You can also click **Back** to review you installation settings.

The setup program installs the Cross-Server server, the Netscape plug-in, the JDK, and WebSphere. It installs the Cross-Site tables in the database and creates the **admin** and **install** users whose passwords are **admin** and **install**, respectively. (Tivoli recommends that you change the passwords for these users once you complete the console installation.)

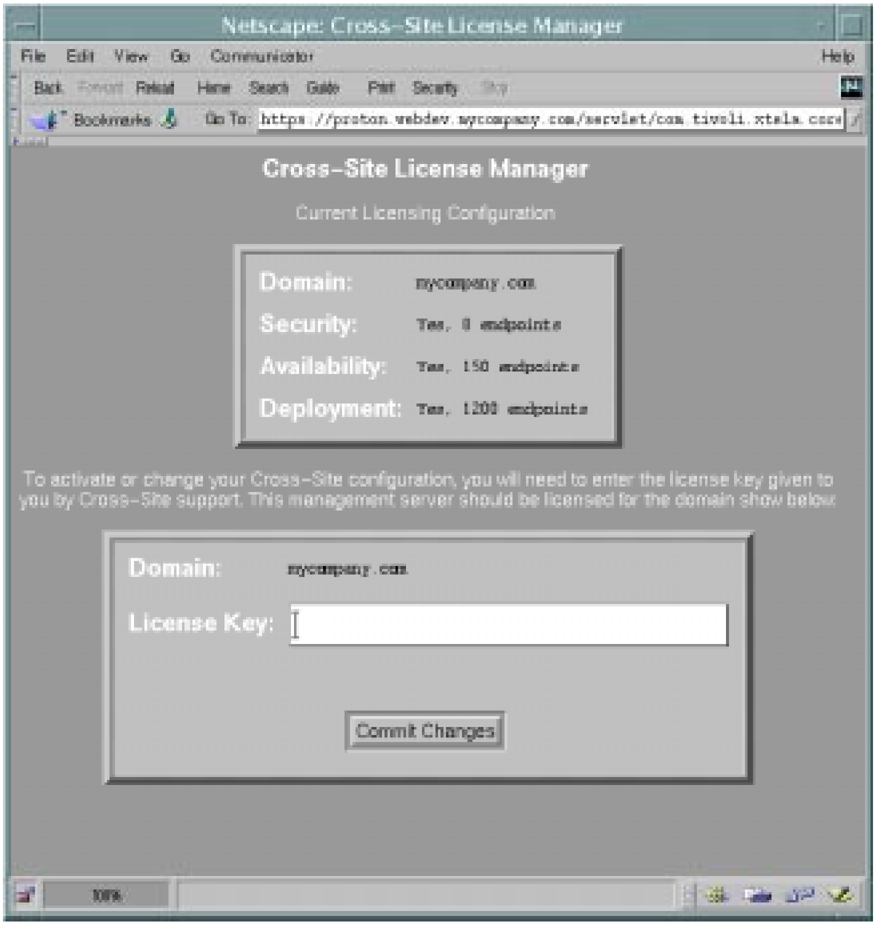
During the rest of the installation, several dialogs are displayed as the newly installed server tests connectivity to and initializes the RDBMS server. You may be prompted for the Key File Password, which is required to start the web server. Dialogs are also displayed when the management server starts and when it installs the Cross-Site channels. Click **Continue** in each of these dialogs to proceed with the installation.

The **Cross-Site License Manager** page is displayed in your default web browser. The URL for this page is as follows:

protocol://*server*/**servlet/com.tivoli.xtela.core.license.LicenseManagerServlet**

where *protocol* and *server* are those of the Cross-Site server you just installed. Be sure to install the license key, which must be installed in order for you to install the Cross-Site applications on the management server, and for you or your end users to install the Cross-Site agents.

The **Cross-Site License Manager** page is similar to the following:



Go To: https://proton.webdev.mycompany.com/servlet/com.tivoli.xtela.core

Cross-Site License Manager

Current Licensing Configuration

Domain:	mycompany.com
Security:	Yes, 0 endpoints
Availability:	Yes, 150 endpoints
Deployment:	Yes, 1200 endpoints

To activate or change your Cross-Site configuration, you will need to enter the license key given to you by Cross-Site support. This management server should be licensed for the domain show below.

Domain: mycompany.com

License Key:

Enter your license key in the **License Key** field and select the **Commit Changes** button. The **License Verified: Cross-Site Enabled** page is displayed to inform you that the installation of the license key succeeded.

After the installation, Tivoli recommends that perform the following:

- Change the password of the **admin** user for WebSphere. (WebSphere was installed as part of the base management server.) See **http://***server***:9527** for more information, where *server* is the host name of the management server. Log in as **admin** (the password is also **admin**) and select **Setup –>Administration** from the tree.

- Modify the NES mapping to the Cross-Site downloads page. To do so, go to the Netscape Server Administration page, using a web browser. The URL for the Netscape Server Administration UI is as follows:

  http://*server_name*:*admin_port***/admin-serv/bin/index**

  Select the Netscape Enterprise Server by clicking its button. Then, select **View Server Settings**. In the **Additional Documents Directory** section of the page, edit the **/Tivoli/Cross-Site** entry by clicking **Edit** and replacing the abbreviated paths with full paths.

Installing Cross-Site for Security on the Server

To install the Cross-Site for Security application on the management server, complete the following steps. If you have not done so, Tivoli recommends that you install a license key prior to completing these steps. See “Installing Your License Key” on page 232 for instructions. Also, Tivoli recommends that you start up your web server before configuring the Security application (though the installation of the base server should have restarted the web server).

1. Log in to the Cross-Site server’s host machine as **Administrator**, or as a user with Administrator privileges.

2. In the **w32-ix86** directory on the Cross-Site CD-ROM, double-click on the **secserver.EXE** file. The **Tivoli Cross-Site for Security Server Welcome** dialog is displayed.

3. Click **Next**. The **Tivoli Cross-Site for Security Server License Agreement** dialog is displayed. Depending upon your installation, this dialog displays either the Domestic or Export license agreement.

4. Read the license agreement and click **Accept**. The **Start Installation** dialog is displayed.

   If you do not click **Accept**, the installation is cancelled.

5. Click **Next**. The **Installation Complete** dialog is displayed.

6. Click **Finish** to close the **Installation Complete** dialog.

To verify that the Cross-Site for Security component installed successfully, look for the **secservice.jar** file in the *install_dir***\XSITsagt\lib** directory. The *install_dir* variable's value is that of the base server's installation drive and directory, as specified in step 4 on page 48. If this file exists, the installation was successful.

You need to stop and restart the Cross-Site server to make it aware of the newly-installed Security application component. See the next section for instructions.

Stopping and Restarting the Server

For troubleshooting, maintenance, or emergency recovery, you might need to restart the Cross-Site server.

To stop the Cross-Site server, select **Start -> Programs -> Tivoli Cross-Site -> Stop Cross-Site Server**. Follow the instructions provided. To restart the server, select **Start -> Programs -> Tivoli Cross-Site -> Start Cross-Site Server**. When you start the Cross-Site server, you are prompted for the Key File Password (also called the key-pair password) if the server is secure. Starting the Cross-Site server also starts the web server.

You can also perform the operations from the command line, using the following commands:

```
install_dir\XSITsagt\bin\stop_server.cmd
install_dir\XSITsagt\bin\start_server.cmd
```

where *install_dir* specifies the drive and directory in which the Cross-Site management server is installed.

The Cross-Site server is shut down and restarted automatically when you enter these commands. If you try to run the console immediately after restarting the server and it fails, wait a few minutes and try again. The web server may need time to complete its initialization.

Verifying the Server’s Installation

The following items will help you determine if the installation of the Cross-Site management server was successful.

- You can verify the accessibility of the server by entering the following URL in a web browser:

  protocol://*server_name*:*port***/servlet/CrossSiteServlet**

  where *server_name* and *port* are the values specified when the Cross-Site server was installed. This utility issues an HTTP request to the Cross-Site server.

  If the server is running, the URL displays a web page containing the following message:

  Cross-Site Management Server Status: ALIVE
  Version: *x* Build: *x*

- The installation creates several debugging files, which are located in the *install_dir* and *install_dir***\XSITsagt\support** directories, where *install_dir* is the destination directory you choose for the server. Review the **xs_install.log** file. It contains trace information about the management server’s installation.

- The channel manager service starts when the management server starts. To verify the processes running on the Cross-Site server, select **Settings –> Control Panel** from the **Start** menu. Double-click on the **Services** icon. Check that entries exist for the **Netscape Enterprise Server** and **WebSphere Servlet Service** and that their status is **Started**. The channel manager listens on port 5282.

- After installing the Cross-Site console on a system, ensure that it can connect to the management server without generating errors. See “Installing and Running the Console” on page 107 if you have not installed a console in your environment.

- The agent package, the console package, and the **index.html** file are in the *install_dir***\downloads\XSite** directory. This directory was created during the installation of the management server. This enables you to launch a web browser and load the *protocol*://*server*:*port***/Tivoli/Cross-Site** page, where *protocol* is that of the Cross-Site server, *server* is the name of the Cross-Site server, and *port* is its port number.

- A web browser can connect to the web server using the Cross-Site server’s name and port number. For example, if you enter **https://proton.webdev.mycompany.com:443/**, where **proton** is the Cross-Site server and **443** is its port, the **Netscape Enterprise Server** page is displayed.

- The first time you use the Netscape Administrative Server’s page after installing the Cross-Site server, you are prompted to accept changes. You access the Administrative Server’s page by entering *protocol*://*server_name*:*admin_port* in the web browser. The *protocol*, *server_name*, and *admin_port* variables’ values are that of the Netscape Administrative Server. These changes were made by the installation of WebSphere, which is part of the Cross-Site server’s installation. Accept the changes.

If you encounter problems with any of these items, restart the web server, which will start WebSphere. If the web server will not start, ensure that enough space is available on the disk partition of the management server’s host. Netscape might not be configured correctly for the management server. Also, refer to the web server’s release notes.

If you need to reinstall, be sure to uninstall Cross-Site (even if the installation failed) by following the instructions in “Uninstalling Cross-Site” on page 235.

Verifying the Installation of the Database Tables

To verify that the Cross-Site installation created its tables in the database, complete the following steps:

1. Log in to the database server.

2. If the RDBMS server is Oracle, complete these steps:

   a. Enter **sqlplus** and supply the user ID and password created to access Cross-Site’s database.

   b. At the SQLPLUS prompt, enter the following command:

   ```
   select * from cat;
   ```

   If this **select** command prints a list of catalog entries, the tables were created. If none are found, the installation of the database tables failed, which means that the Cross-Site server’s installation failed.

3. If the RDBMS server is DB2, complete these steps:

   a. Log in to the database server as user ID used to install the management server.

   b. Enter **db2**.

   c. At the DB2 prompt, enter the following command to connect to the database:

   ```
   connect to database
   ```

d. Enter the following command:

```
list tables
```

If the **list** command prints a list of table entries, the tables were created. If none are found, the installation of the database tables failed, which means that the Cross-Site server’s installation failed.

If you need to reinstall, be sure to uninstall Cross-Site (even if the installation failed) by following the instructions in “Uninstalling Cross-Site” on page 235.

6

Installing the Cross-Site Server on AIX

This section describes the procedure for installing a Cross-Site management server on AIX. You *must* read and complete the steps in the following chapters before beginning the procedures in this one:

- “Requirements for the Cross-Site Server” on page 7.
- “RDBMS Requirements” on page 15.
- “Requirements for the Web Server” on page 25.
- “Requirements for the Web Server” on page 25. And if you are using a DB2 RDBMS server, you must install the user defined functions (UDFs) as described in “DB2 Configuration” on page 20.
- If you installed a server certificate that is unsupported by Cross-Site on your web server, you must create the **KeyRing.class** file before installing the Cross-Site management server. This is described in “Importing an Unsupported Root Certificate” on page 199.
- Be sure to generate a license key before installing, as described in “Generating a License Key” on page 29.

Complete the steps in this chapter to install the base management server. The base server provides the core services, web server plug-ins, and IBM’s WebSphere. The base server’s installation also creates the Cross-Site table space in the RDBMS. When the installation of the base server completes, it restarts the web server. This chapter also describes how to install Cross-Site for Security on the management server.

Contents of the CD-ROM

The following directories are in the top-level directory of the Cross-Site CD-ROM:

aix4-r3 The directory that contains the AIX Cross-Site packages.

CARS The channel archive directory; this directory contains installation files for the management server if you are installing the management server using the CD-ROM (local/domestic installation). This directory is also provided in case you encounter problems installing your management server using the Tivoli fulfillment server, which is a server located at Tivoli from which your Cross-Site server downloads the most recent code to complete its installation.

db2 The directory that contains the **w32-ix86** and **aix4-r3** subdirectories. The **aix4-r3** subdirectory contains the **setup_db2** script, which helps you copy these files to the DB2 instance home directory.

DOCS The directory that contains the Cross-Site documentation in the Adobe PDF format. A free Adobe reader is available at the following URL:

http://www.adobe.com/prodindex/acrobat/readstep.html

solaris2 The directory that contains the Solaris Cross-Site packages.

TCI The directory that contains the media for the Tivoli Enterprise Module for Cross-Site.

UTIL The directory that contains a tool that you can use to add root certificates from unknown certificate authorities to the Cross-Site **KeyRing.class** file.

w32-ix86 The directory that contains the Cross-Site Windows packages.

The contents of the **aix4-r3** directory is as follows on the domestic and export versions of the Cross-Site product CD-ROM:

.toc The table of contents file that is read by AIX and that lists all of the prerequisites and corequisites for the software in the directory.

IBMWebAS.base.bff
This file contains the AIX installation image for the IBM WebSphere Application Server. Components of this package are required by the Cross-Site management server.

IBMWebAS.en_US.bff
This file contains the AIX installation image for the English messages for the IBM WebSphere Application Server.

xsite.avlserver_dom.bff or **xsite.avlserver_exp.bff**
This file contains the AIX installation image for the Cross-Site for Availability component of the Cross-Site server.

xsite.console_dom.bff or **xsite.console_exp.bff**
This file contains the AIX installation image for the Cross-Site console.

xsite.depagent_dom.bff or **xsite.depagent_exp.bff**
This file contains the AIX installation image for the Cross-Site for Deployment agent.

xsite.depserver_dom.bff or **xsite.depserver_exp.bff**

This file contains the AIX installation image for the Cross-Site for Deployment component of the Cross-Site server.

xsite.mgmtserver_dom.bff or **xsite.mgmtserver_exp.bff**

This file contains the AIX installation image for the Cross-Site (base) management server.

xsite.secagent_dom.bff or **xsite.secagent_exp.bff**

This file contains the AIX installation image for the Cross-Site for Security agent.

xsite.secserver.bff

This file contains the AIX installation image for the Cross-Site for Security component of the management server.

The 128-bit and 56-bit Versions of Cross-Site

If you are located in the United States or Canada, or if you qualify for 128-bit encryption outside of the U.S. or Canada, you were shipped the domestic version of the Cross-Site CD-ROM. This version provides 128-bit encryption. In general, if you are located outside of the U.S. or Canada, you received the export version of the Cross-Site CD-ROM. This version provides 56-bit encryption. (To verify which version of the CD-ROM you received, check the information printed on the CD-ROM.)

Installing Locally Versus Remotely

If you are installing Cross-Site from the domestic version of the CD-ROM, you *must* install the Cross-Site management server *locally*. (One of the installation prompts asks you to choose local or remote.) This means that the installation program will install the server using only the bits on the CD-ROM. This option enables you to install Cross-Site without contacting the Tivoli fulfillment server, which requires connectivity to the Internet. The fulfillment server is a server located at Tivoli headquarters that provides bits so that your Cross-Site server can download, versus relying solely on the CD-ROM.

If you are installing from the export version of Cross-Site, you may choose to install locally or remotely. If you install remotely, the installation program contacts the Tivoli fulfillment server to complete the installation. Tivoli *strongly* recommends that you install locally, no matter which version of the CD-ROM you received.

If you choose to install remotely, consider that installing Cross-Site involves downloading large files, sometimes up to 40–50 MB. This download estimate could impact you if bandwidth is an issue. In addition, verify that all routers, gateways, and firewalls are configured to allow HTTPS connections to **https://software.cross-site.com**.

Installing Intermixed Domains

It is possible that you install your Cross-Site domain using the domestic (128-bit) version of the CD-ROM and you or your e-business partner installs another (interconnected) Cross-Site domain using the export (56-bit) version, or vice versa. If this could potentially occur in your installations, you may want to consider the information in this section.

Most importantly, do not install the export version of Cross-Site agents against the domestic version of the Cross-Site server. Similarly, do not install the domestic version of Cross-Site agents against the export version of the Cross-Site server. If this configuration error occurs, the agent will download the incorrect binaries from the management server. Tivoli does not support these version mismatches. In addition, improper configuration may be a violation of U.S. Export regulations.

However, if intermixed domains are installed to work together, you should note the following: Cross-Site agents and consoles that were installed using the export media may not be able to communicate with a management server that was installed using the domestic version of the

Cross-Site CD-ROM. Agents and consoles configured for 56-bit encryption cannot communicate with a management server that is configured for only 128-bit encryption. If an export agent or console attempts to contact a domestic server, the following error is displayed:

```
Server connection error: Failed to contact management
server.
```

To verify that it is an export-to-domestic problem, you can contact the management server by entering the following URL in the export version (56-bit) of the web browser:

protocol://*server_name*:*port***/servlet/CrossSiteServlet**

where *protocol*, *server_name*, and *port* are those values specified during the installation of the web server. For example, the following error message is displayed in the Netscape browser if there is a mismatch of encryption levels:

```
Netscape and this server cannot communicate securely because
they have no common encryption algorithm(s).
```

Installing the Management Server

To install the Cross-Site management server on AIX, you must install the base management server and the Cross-Site for Security component. Though you can use the System Management Interface Tool (SMIT) to install them separately, this procedure demonstrates installing the base management server and Cross-Site for Security together.

Complete the following steps to do so:

1. Log in to the Cross-Site server’s host machine as **root**. You must have superuser privileges to install the Cross-Site server. Also, you must log in as **root**, rather than using the **su** command.

2. To log trace information about the installation, create the **/tmp/XSITsagt.debug** directory prior to installing the management server. Enter the following command to do so:

```
mkdir -pm 777 /tmp/XSITsagt.debug
```

The **/tmp/XSITsagt.install** file is created during the installation as the result of this command. Be aware that this file will contain unencrypted passwords (those entered during the installation).

3. As part of the Cross-Site management server installation, the IBM WebSphere Application Server is also installed. To ensure that WebSphere is properly installed and configured, you must set two environment variables before beginning the installation process.

   - Set the JAVA_HOME environment variable to the directory where the Java Development Kit (JDK) is installed. For IBM's AIX Java application, set JAVA_HOME as follows (using the Korn shell):

     ```
     export JAVA_HOME=/usr/jdk_base
     ```

   - Set the NS35_CONFIG_PATH environment variable to the path to the Netscape web server's **obj.conf** file. By default, this path is **/usr/netscape/suitespot/https-***NESname***/config**. For example, you could set NS35_CONFIG_PATH as follows:

     ```
     export NS35_CONFIG_PATH=
     /usr/netscape/suitespot/https-myserver/config
     ```

     where NES is installed in **/usr/netscape/suitespot** and your web server is named **myserver**.

4. To install the Cross-Site server on AIX using the System Management Interface Tool (SMIT), complete the following steps:

   a. Insert the CD-ROM into the drive and mount the drive, as follows:

      mount -v cdrfs -r */dev/cd0 /mnt*

      where */dev/cd0* is your CD-ROM and */mnt* is the mount point.

   b. Display the **SMIT Install and Update from Latest Available Software** menu using the following command:

      ```
      /usr/bin/smit install_latest
      ```

c. In the **INPUT device/directory for software** field, enter the following:

   /_mnt_**/aix4-r3**

   where _/mnt_ is the directory where you mounted your CD-ROM.

d. Press **Enter**. The dialog is updated with a new list of entry fields.

e. In the **SOFTWARE to install** field, select the following WebSphere filesets:

   IBMWebAS Base Release
   IBMWebAS Plugins - Netscape 3.5.1 Plugin

   In addition, select the Tivoli Cross-Site components you want to install. This should include the Cross-Site management server and any other component you want to install. For example, you might want to select the Cross-Site console for installation.

f. Once you complete your selection, press **Enter**.

g. If you wish to change any of the default values for other entry fields on the **Install and Update from Latest Available Software** menu, do so before continuing.

h. When you are ready to install, press **Enter** to continue. You are prompted with an **ARE YOU SURE** popup dialog. Press **Enter** again to continue with the installation.

After the installation is complete, consult the installation summary at the bottom of your SMIT output to verify that the installation completed successfully. Then, exit SMIT.

Continue with the configuration of your Cross-Site server by first configuring the management server and then configuring any additional Cross-Site components that you install.

Configuring the Management Server

This section describes how to configure each component of the Cross-Site management server. After you install the base server and application components, you must configure them.

Note: *If you are reinstalling the management server or attempting to install again after a failed installation, ensure that all processes that were started by previous installations are stopped. See "Stopping and Restarting the Server" on page 77 for details.*

Configuring the Base Server

Before beginning this procedure, ensure that the web server is shut down. Configure the management server using the following command (you must have superuser privileges to configure the Cross-Site server):

```
/usr/Tivoli/XSite/XSITsagt/install/sagtconfig
```

This command prompts you for configuration information. Answer each prompt with a value, as follows:

1. Please specify the directory containing the **obj.conf** file for the Netscape Enterprise Server. This file resides in the Netscape configuration directory. By default, the path to this directory is **/usr/netscape/suitespot/https-***NESname***/config**.

2.
   ```
   The installation of the Cross-Site server contacts a
   fulfillment server, which is located at Tivoli and
   provides the most up-to-date installation media (in the
   form of channels). The fulfillment server provides
   these channels, which are downloaded by your Cross-Site
   server and initialized.

   If you do NOT wish to rely on the fulfillment server,
   enter local. This option is available if you are in an
   isolated environment such as a test lab. The
   installation will proceed, using the channels that are
   provided on the Cross-Site CD-ROM. If you would like to
   ```

```
download channels from the fulfillment server, which is
recommended, enter remote.
```

```
Enter the installation method used to install and
initialize the Cross-Site channels.
```

Enter **local** if you wish to install Cross-Site from the CD-ROM. *TIVOLI STRONGLY RECOMMENDS THAT YOU CHOOSE LOCAL.* The following prompt is then displayed:

```
Enter path to the Cross-Site CD-ROM image.
```

Enter the full path to the mounted CD-ROM. You simply need to enter the top-level directory of the CD-ROM, such as **/cdrom**.

If you enter **remote**, you must provide the protocol, name, and port number of the fulfillment server. The protocol is **HTTPS**, the host name for the Tivoli fulfillment server is **software.cross-site.com**, and the port number for the server is **443**. You must also specify the proxy and its port number, if your server must use a proxy server when contacting the Tivoli fulfillment server.

3.
   ```
   Enter the protocol that will be used to access your new
   Cross-Site server.
   ```

   This protocol is the same as the installed web server. Enter **https** for a server that will use the HTTPS protocol, which runs over SSL. (Cross-Site for Security must run on an HTTPS server.) Enter **http** for an unsecure server.

4.
   ```
   Enter the fully-qualified host name for your Cross-Site
   server.
   ```

   You *must* enter a fully qualified name, such as **host.dept.company.com**. Cross-Site agents that reside outside of your firewall or domain receive and use this fully qualified name to communicate with the Cross-Site server. If you do not specify a fully qualified name, agents will not be able to resolve the host name of the server.

5.
   ```
   Enter the port number of your Cross-Site server.
   ```

   Enter the Cross-Site server’s port number. This is the port number of the web server (NES).

6. If you are installing a secure Cross-Site server, the following prompts are displayed:

   a.
   ```
   Enter the HTTPS Key File Password for your Cross-Site
   server.
   ```

   This is the password you are prompted for when you start a web server running HTTPS.

   b.
   ```
   Enter the HTTPS Key File Password again.
   ```

   Reenter the Key File Password to verify that you entered it correctly the first time.

   c.
   ```
   If your Cross-Site server does not use a supported
   Certificate Authority for authentication, enter the
   full path of the directory containing an alternate
   KeyRing.class file here. Otherwise, enter "none".
   ```

   Enter **none** unless you created the **KeyRing.class** file for the unsupported CA prior to this installation. (If you used an unsupported server certificate to secure the web server, you should have created the **KeyRing.class** file as described in “Importing an Unsupported Root Certificate” on page 199.) If you have the file, enter the full path to the directory where it resides.

7.
   ```
   Enter the name of the administrative domain name for
   your Cross-Site server. To ensure uniqueness, it is
   recommended that you use a name within your DNS domain
   or the name of the DNS domain itself.
   ```

   Enter the name of the domain where your Cross-Site server will reside.

8. `Enter a name for your Cross-Site server.`

   Enter a meaningful name for the server. This is the name that end users and other console users will use to contact your server.

9. `Enter the IP address of your Cross-Site server.`

   Enter the system’s IP address here. The server must have a static IP address; the dynamic host configuration protocol (DHCP) is not supported for the Cross-Site server.

10. `Enter a description for your Cross-Site server.`

    Enter a description for the server. This is for your information only.

11. `Enter the password that will be used by other Cross-Site servers to collaborate with your Cross-Site server.`

    Enter a password for your Cross-Site server. This is different than the **admin** user’s password provided by Tivoli. The password you enter at this prompt will be used when collaborating with other Cross-Site servers. Tivoli recommends that, unless you are installing multiple management servers, you simply press **Enter**.

12. `Enter the collaboration password again.`

    Reenter the password to verify that you entered it correctly the first time.

13. `Enter the directory on your Cross-Site server where you want to store the console and agent packages. To allow users to download these packages, the Web server must have access to this directory.`

    Enter the full path to a directory where the console and agent packages will be installed. By default, the installation creates the *base_dir*/**downloads** directory, where *base_dir* is the installation directory for the management server, such as **/usr/Tivoli/XSite/XSITsagt**. If you specify a directory that does not exist, you are prompted to create it.

14. `Enter the type of database that your Cross-Site server will use.`

    Enter the type of database that you plan to use. Enter **DB2** or **Oracle8**.

    Note: *Recall that Tivoli has only tested the DB2 RDBMS server with an AIX management server. Other combinations are supported, though not tested. Contact Support if you wish to use an unsupported combination and encounter problems during their installation or use.*

    If you enter **DB2**, the following prompts are displayed. (If you enter **Oracle8**, go to step a on page 72.)

    a. `Enter the DB2 database installation directory.`

       Enter the installation directory of the database.

    b. `Enter the DB2 instance name.`

       Enter the instance name of the DB2 database.

    c. `Enter the DB2 instance home directory.`

       Enter the home directory of the DB2 database.

    d. `Enter the database driver.`

       Enter the class name of the JDBC driver that you installed prior to running this script. For example, the class name may be **COM.ibm.db2.jdbc.app.DB2Driver**.

    e. `Enter the user ID that your Cross-Site server will use to access the database.`

       Enter a valid database user ID designated for Cross-Site. This can be any valid AIX user ID; DB2 does not require that you create a separate database user ID.

f. `Enter the database user’s password.`

   Enter the password for the user ID previously entered.

g. `Enter the database user’s password again.`

   Enter the database password again to verify that you entered it correctly the first time.

h. `Enter the DB2 database name.`

   Enter the name of the database.

Continue the installation with step 15 on page 74.

If you enter **Oracle8** as the type of database that your server will use, the following prompts are displayed:

a. `Enter the Oracle8 database installation directory.`

   Enter the installation directory of the database.

b. `Enter the database driver.`

   Enter the class name of the JDBC driver that you installed prior to running this script, for example, **oracle.jdbc.driver.OracleDriver** for the Oracle8 database.

c. `Enter the user ID that your Cross-Site server will use to access the database.`

   Enter a valid database user ID designated for Cross-Site.

d. `Enter the database user’s password.`

   Enter the password for the database user ID previously entered.

e. `Enter the database user’s password again.`

   Enter the database password again to verify that you entered it correctly the first time.

f. `Have you set up the Oracle environment on your Cross-Site server and inserted the name of your database workspace in the tnsnames.ora file?`

   Enter **y** if you are using Oracle 8.0 and the **tnsnames.ora** file contains an entry for the database server. Otherwise, enter **n**.

   If you enter **y**, the following prompt is displayed:

   ```
   Enter the database name.
   ```

   Enter the name of the database, which is the name of the Oracle instance.

   If you enter **n**, these prompts are displayed:

   1. `Enter the JDBC driver type (e.g., oci8, thin).`

      Enter a JDBC driver type. Possible values for the driver include **oci8** and **thin**, which correspond to your version of Oracle.

   2. `Enter the Oracle database host name.`

      Enter the name of the system where the database is installed. You can enter a fully qualified name or simply the name of the system, if the name can be resolved.

   3. `Enter the Oracle database port number.`

      Enter the port number of the listener on the machine where the database is installed.

   4. `Enter the Oracle database SID.`

      Enter the database’s system identifier (SID).

15. `Enter the machine name or IP address of your X Server.`

    Enter the name or IP address of the system if you are viewing the installation on a remote display. The installation script needs this information because it displays several dialogs after the installation. Before entering the host name here, ensure that you can connect to the host's display. (The DISPLAY variable should be set and you may wish to use the **xhost** command to enable the connection.)

16. `Enter the full path of the Web browser you will use to install the Cross-Site license key. If you do not want to install a license key at the end of the installation or you do not have a local Web browser, enter "none".`

    Enter the path to the web browser that will be displayed at the end of the installation so that you can install a license key. If you enter **none**, you can install a license key later.

17. `Do you want to review your answers?`

    To review all of the prompts and your responses, enter **y**. Tivoli recommends that you review your responses to ensure that you did not enter something incorrectly, which could cause the installation to fail. You can change your answers as you review them. Enter **n** to continue with the installation without reviewing your responses. Enter **q** to exit the installation without completing it.

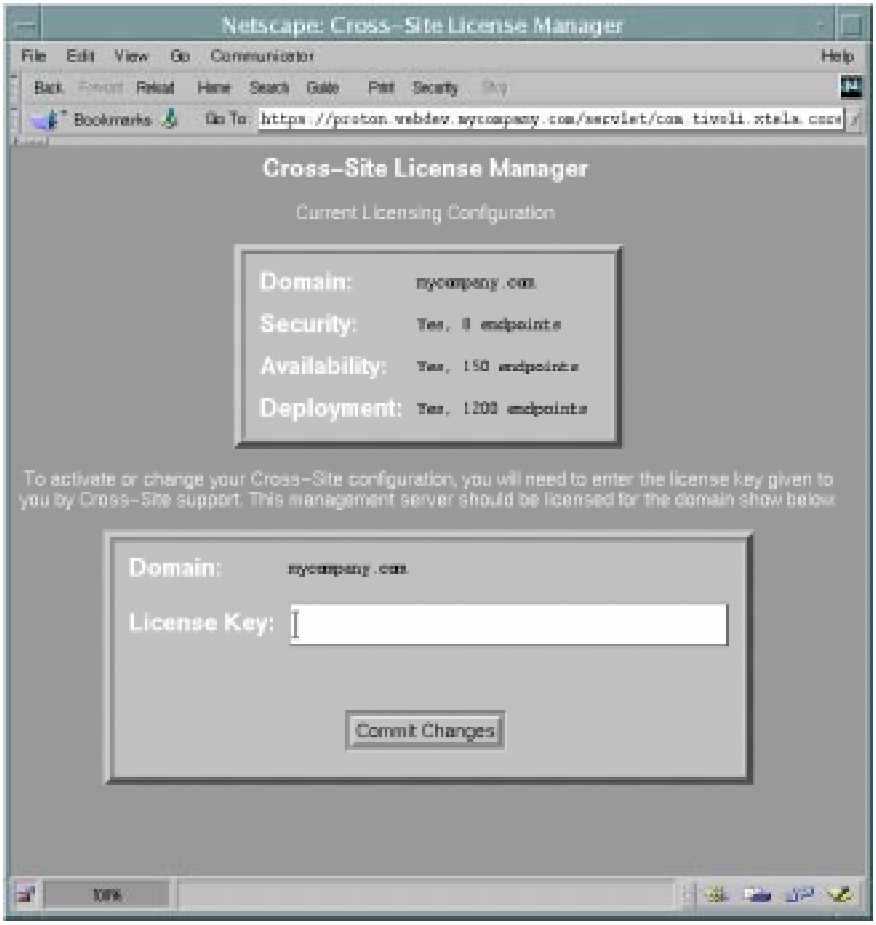
The **sagtconfig** command installs the Cross-Site server, Netscape plug-in, and WebSphere. It also installs the Cross-Site tables in the database and creates the **admin** and **install** users, whose passwords are **admin** and **install**, respectively. (Tivoli recommends that you change these passwords once you complete the console installation.)

If you specified a path to a web browser in step 16 on page 74, the **Cross-Site License Manager** page is displayed. The URL for this page is as follows:

protocol:**//***server***/servlet/com.tivoli.xtela.core.license.**
LicenseManagerServlet

where *protocol* and *server* are those of the Cross-Site server you just installed. Be sure to install the license key, which must be installed in order for you to install the Cross-Site applications on the management server, and for you or your end users to install the Cross-Site agents.

The **Cross-Site License Manager** page is similar to the following:


Netscape: Cross-Site License Manager
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks
Commit Changes
100%

Go To: https://proton.webdev.mycompany.com/servlet/com.tivoli.xtela.core

Cross-Site License Manager

Current Licensing Configuration

Domain: mycompany.com
Security: Yes, 0 endpoints
Availability: Yes, 150 endpoints
Deployment: Yes, 1200 endpoints

To activate or change your Cross-Site configuration, you will need to enter the license key given to you by Cross-Site support. This management server should be licensed for the domain show below.

Domain: mycompany.com
License Key:

Enter your license key in the **License Key** field and select the **Commit Changes** button. The **License Verified: Cross-Site Enabled** page is displayed to inform you that the installation of the license key succeeded.

After the installation, Tivoli recommends that you change the password of the **admin** user for WebSphere. (WebSphere was installed as part of the base management server.) See **http://***server***:9527** for more information, where *server* is the host name of the management server. Log in as **admin** (the password is also **admin**) and select **Setup –>Administration** from the tree.

Configuring Cross-Site for Security

To configure the Cross-Site for Security application on the management server, complete the following steps. If you have not done so, Tivoli recommends that you install a license key prior to completing these steps. See “Installing Your License Key” on page 232 for instructions. Also, Tivoli recommends that you start up your web server before configuring the Security application (though the configuration of the base server should have restarted the web server).

1. Enter the following command to configure the Security application (you must have superuser privileges to configure the Cross-Site server):

   ```
   /usr/Tivoli/XSite/XSITsagt/install/secsconfig
   ```

2. Upon completion of the configuration, the command displays the following message:

   ```
   Please restart your Netscape server by executing the
   Netscape “stop” and “start” scripts:

   install_dir/netscape/suitespot/https-server/stop
   install_dir/netscape/suitespot/https-server/start
   ```

   Despite this message, you should restart the web server (and Cross-Site server) by following the instructions in the following section.

Stopping and Restarting the Server

For troubleshooting, maintenance, or emergency recovery, you might need to restart the Cross-Site server. You can restart the Cross-Site server on AIX by restarting the web server itself. (The Cross-Site server restarts automatically every time you restart the web server.)

Note: *Restarting the web server not only affects the Cross-Site server but also any other applications that rely on the web server.*

Before restarting the Cross-Site server, obtain the user name, password, port number, and the Key File Password (also called the key-pair password) for the web server.

To restart the web server from the command line (thereby restarting the Cross-Site server), complete the following steps:

1. To stop the Netscape web server, enter the following command:

   ```
   install_dir/https-server/stop
   ```

   where *install_dir* is the directory path to the web server's installation directory. By default, NES is installed in **/usr/netscape/suitespot** on AIX. The *server* variable specifies the name of the web server. Wait several minutes to ensure that the web server shuts down properly.

2. Verify that all processes related to Cross-Site were shutdown with the web server. Enter the following command:

   ```
   /bin/ps -ef | grep user
   ```

   where *user* is that of the Netscape Enterprise Server.

3. If processes are listed that are owned by the Netscape user, enter the following command to stop each process:

   ```
   kill -9 process
   ```

   You need to ensure that the **tuner.sh**, **native_threads/jre**, and (Java) **OutOfProcEngine** processes are stopped.

4. Restart the web server by entering the following command:

   ```
   install_dir/https-server/start
   ```

   where *install_dir* is the directory path to the web server's installation directory. By default, the Netscape Enterprise Server is installed in **/usr/netscape/suitespot** on AIX. The *server* variable specifies the name of the web server. Enter the Key File Password if prompted.

The Cross-Site server is shut down and restarted automatically when you enter these commands. If you try to run the console immediately after restarting the server and it fails, wait a few minutes and try again. The web server may need time to complete its initialization.

Verifying the Server's Installation

The following items will help you determine if the installation of the Cross-Site management server was successful:

- You can verify the accessibility of the server by entering the following URL in a web browser:

  protocol://*server_name*:*port***/servlet/CrossSiteServlet**

  where *server_name* and *port* are the values specified when the Cross-Site server was installed. This utility issues an HTTP request to the Cross-Site server.

  If the server is running, the URL displays a web page containing the following message:

  Cross-Site Management Server Status: ALIVE
  Version: *x* Build: *x*

- If you created the **/tmp/XSITsagt.debug** directory prior to installing the management server, the **/tmp/XSITsagt.install** file was created during the installation. It contains trace information about the management server’s installation. You can also run the **tail -f /tmp/XSITsagt.install** command, which enables you to list the processes as they occur, and helps you identify if a process is hung.

- The channel manager service starts when the management server starts. To list the processes running on the Cross-Site server, enter the following command:

  ```
  /bin/ps -ef | egrep "netsc|java|jre"; echo; netstat -a |
  grep 5282
  ```

  The channel manager listens on port 5282.

- After installing the Cross-Site console on a system, ensure that it can connect to the management server without generating errors. See “Installing and Running the Console” on page 107 if you have not installed a console in your environment.

- The agent packages, the console package, and the **index.html** file are in the **downloads/XSite** directory. This directory was created during the installation of the management server. This enables you to launch a web browser and load the *protocol*://*Server*:*Port***/Tivoli/Cross-Site** page, where *protocol* is that of the Cross-Site server, *Server* is the name of the Cross-Site server, and *Port* is its port number.

- A web browser can connect to the web server using the Cross-Site server’s name and port number. For example, if you enter **https://proton.webdev.mycompany.com:443/**, where **proton** is the Cross-Site server and **443** is its port, the **Netscape Enterprise Server** page is displayed.

- The first time you use the Netscape Administrative Server’s page after installing the Cross-Site server, you are prompted to accept changes. You access the Administrative Server’s page by entering *protocol*://*server_name*:*admin_port* in the web browser. The *protocol*, *server_name*, and *admin_port* variables’ values are that of the Netscape Administrative Server. These changes were made by the installation of WebSphere, which is part of the Cross-Site server’s installation. Accept the changes.

If you encounter problems with any of these items, restart the web server, which will start WebSphere. If the web server will not start, ensure that enough space is available on the disk partition of the management server’s host. Netscape might not be configured correctly for the management server. Also, refer to the web server’s release notes.

If you need to reinstall, be sure to uninstall Cross-Site (even if the installation failed) by following the instructions in “Uninstalling Cross-Site” on page 235.

Verifying the Installation of the Database Tables

To verify that the Cross-Site installation created its tables in the database, complete the following steps:

1. Log in to the database server.

2. If the RDBMS server is Oracle, complete these steps:

    a. Enter **sqlplus** and supply the user ID and password created to access Cross-Site’s database.

    b. At the SQLPLUS prompt, enter the following command:

    ```
    select * from cat;
    ```

    If this **select** command prints a list of catalog entries, the tables were created. If none are found, the installation of the database tables failed, which means that the Cross-Site server’s installation failed.

3. If the RDBMS server is DB2, complete these steps:

    a. Log in to the database server as user ID used to install the management server.

    b. Enter **db2**.

c. At the DB2 prompt, enter the following command to connect to the database:

```
connect to database
```

where *database* is the name of the database

d. Enter the following command:

```
list tables
```

If the **list** command prints a list of table entries, the tables were created. If none are found, the installation of the database tables failed, which means that the Cross-Site server's installation failed.

If you need to reinstall, be sure to uninstall Cross-Site (even if the installation failed) by following the instructions in "Uninstalling Cross-Site" on page 235.

7

Installing the Cross-Site Server on Solaris

This section describes the procedure for installing a Cross-Site management server on Solaris.You *must* read and complete the steps in the following chapters before beginning the procedures in this one:

- "Requirements for the Cross-Site Server" on page 7.
- "RDBMS Requirements" on page 15.
- "Requirements for the Web Server" on page 25.
- If you installed a server certificate that is unsupported by Cross-Site on your web server, you must create the **KeyRing.class** file before installing the Cross-Site management server. This is described in "Importing an Unsupported Root Certificate" on page 199.
- Be sure to generate a license key before installing, as described in "Generating a License Key" on page 29.

Complete the steps in this chapter to install the base management server. The base server provides the core services, web server plug-ins, and IBM's WebSphere. The base server's installation also creates the Cross-Site table space in the RDBMS. When the installation of the base server completes, it restarts the web server. This chapter also describes how to install Cross-Site for Security on the management server.

Contents of the CD-ROM

The following directories are in the top-level directory of the Cross-Site CD-ROM:

aix4-r3 The directory that contains the AIX Cross-Site packages.

CARS The channel archive directory; this directory contains installation files for the management server if you are installing the management server using the CD-ROM (local/domestic installation). This directory is also provided in case you have problems installing your management server using the Tivoli fulfillment server, which is a server located at Tivoli from which your Cross-Site server downloads the most recent code.

db2 The directory that contains the **w32-ix86** and **aix4-r3** subdirectories. These subdirectories contain files for configuring a DB2 RDBMS server, for use with Cross-Site.

DOCS The directory that contains the Cross-Site documentation in the Adobe PDF format. A free Adobe reader is available at the following URL:

http://www.adobe.com/prodindex/acrobat/readstep.html

solaris2 The directory that contains the Solaris Cross-Site packages.

TCI The directory that contains the media for the Tivoli Enterprise Module for Cross-Site.

UTIL The directory that contains a tool that you can use to add root certificates from unknown certificate authorities to the Cross-Site **KeyRing.class** file.

w32-ix86 The directory that contains the Cross-Site Windows packages.

The contents of the **solaris2** directory is as follows:

XSiteAvlSvrPkg.solaris2.tar.Z
When uncompressed and untarred, this file contains the **XSITavls** Solaris package, which installs Cross-Site for Availability on the Cross-Site server, and the **install_avlsvr** installation script.

XSiteConsolePkg.solaris2.tar.Z
When uncompressed and untarred, this file contains the **XSITcons** Solaris package, which installs the Cross-Site console for the Cross-Site server.

XSiteDepAgtPkg.solaris2.tar.Z
When uncompressed and untarred, this file contains the **XSITdagt** Solaris package, which installs the Cross-Site for Deployment agent component of the Cross-Site agent, and the **install_depagt** script.

XSiteDepSvrPkg.solaris2.tar.Z
When uncompressed and untarred, this file contains the **XSITsdep** package, which installs Deployment on the Cross-Site server, and the **install_depsvr** script.

XSiteSecAgtPkg.solaris2.tar.Z
When uncompressed and untarred, this file contains the **XSITids** Solaris package, which installs the Cross-Site for Security agent.

XSiteSecSvrPkg.solaris2.tar.Z
When uncompressed and untarred, this file contains the **XSITsecs** Solaris package, which installs Cross-Site for Security on the Cross-Site server, and the **install_secsvr** script.

XSiteSvrPkg.solaris2.tar.Z
When uncompressed and untarred, this file contains the **IBMWebAS**, **SENs351**, **SERSCSEN**, and **XSITsagt** packages, which install the Cross-Site base server. This file also contains the **install_mgtsvr** script.

The 128-bit and 56-bit Versions of Cross-Site

If you are located in the United States or Canada, or if you qualify for 128-bit encryption outside of the U.S. or Canada, you were shipped the domestic version of the Cross-Site CD-ROM. This version provides 128-bit encryption. In general, if you are located outside of the U.S. or Canada, you received the export version of the Cross-Site CD-ROM. This version provides 56-bit encryption. (To verify which version of the CD-ROM you received, check the information printed on the CD-ROM.)

Installing Locally Versus Remotely

If you are installing Cross-Site from the domestic version of the CD-ROM, you *must* install the Cross-Site management server *locally*. (One of the installation prompts asks you to choose local or remote.) This means that the installation program will install the server using only the bits on the CD-ROM. This option enables you to install Cross-Site without contacting the Tivoli fulfillment server, which requires connectivity to the Internet. The fulfillment server is a server located at Tivoli headquarters that provides bits so that your Cross-Site server can download, versus relying solely on the CD-ROM.

If you are installing from the export version of Cross-Site, you may choose to install locally or remotely. If you install remotely, the installation program contacts the Tivoli fulfillment server to complete the installation. Tivoli *strongly* recommends that you install locally, no matter which version of the CD-ROM you received.

If you choose to install remotely, consider that installing Cross-Site involves downloading large files, sometimes up to 40–50 MB. This download estimate could impact you if bandwidth is an issue. In addition, verify that all routers, gateways, and firewalls are configured to allow HTTPS connections to **https://software.cross-site.com**.

Installing Intermixed Domains

It is possible that you install your Cross-Site domain using the domestic (128-bit) version of the CD-ROM and you or your e-business partner installs another (interconnected) Cross-Site domain using the export (56-bit) version, or vice versa. If this could potentially occur in your installations, you may want to consider the information in this section.

Most importantly, do not install the export version of Cross-Site agents against the domestic version of the Cross-Site server. Similarly, do not install the domestic version of Cross-Site agents against the export version of the Cross-Site server. If this configuration error occurs, the agent will download the incorrect binaries from the management server. Tivoli does not support these version mismatches. In addition, improper configuration may be a violation of U.S. Export regulations.

However, if intermixed domains are installed to work together, you should note the following: Cross-Site agents and consoles that were installed using the export media may not be able to communicate with a management server that was installed using the domestic version of the Cross-Site CD-ROM. Agents and consoles configured for 56-bit encryption cannot communicate with a management server that is configured for only 128-bit encryption. If an export agent or console attempts to contact a domestic server, the following error is displayed:

```
Server connection error: Failed to contact management
server.
```

To verify that it is an export-to-domestic problem, you can contact the management server by entering the following URL in the export version (56-bit) of the web browser:

protocol://*server_name*:*port***/servlet/CrossSiteServlet**

where *protocol*, *server_name*, and *port* are those values specified during the installation of the web server. For example, the following error message is displayed in the Netscape browser if there is a mismatch of encryption levels:

```
Netscape and this server cannot communicate securely because
they have no common encryption algorithm(s).
```

Installing the Base Server

The following procedure provides steps for installing the base management server on a Solaris system. This system must meet the requirements outlined in “Requirements for the Cross-Site Server.” Also, ensure that the web server is shut down before beginning this procedure.

Note: *If you are reinstalling the management server or attempting to install again after a failed installation, ensure that all processes that were started by previous installations are stopped. See “Stopping and Restarting the Server” on page 102 for details.*

Complete the following steps to install the Cross-Site management server:

1. Log in to the Cross-Site server’s host machine as **root**. You must have superuser privileges to install the Cross-Site server. Also, you must log in as **root**, rather than using the **su** command.

2. Uncompress and untar the **XSiteSvrPkg.solaris2.tar.Z** file, which resides in the **solaris2** directory on the CD-ROM. Complete the following steps to do so:

   a. Create a directory where you can unpackage the installation package.

   ```
   mkdir XSiteSvr
   ```

   b. Change to the newly created directory.

   ```
   cd XSiteSvr
   ```

   c. Copy the **XSiteSvrPkg.solaris2.tar.Z** file from the CD-ROM.

   ```
   cp /cdrom_mnt_pt/solaris2/XSiteSvrPkg.solaris2.tar.Z .
   ```

   d. Uncompress the file using the following command. This command removes the **.Z** from the end of the file name.

   ```
   uncompress XSiteSvrPkg.solaris2.tar.Z
   ```

e. Extract, or untar, the contents of the file using the following command.

```
tar xvf XSiteSvrPkg.solaris2.tar
```

When complete, the **IBMWebAS**, **SENs351**, **SERSCSEN**, and **XSITsagt** packages, and the **install_mgtsvr** script are listed in the directory.

3. To log trace information about the installation, create the **/tmp/XSITsagt.debug** directory prior to installing the management server. Enter the following command to do so:

```
mkdir -pm 777 /tmp/XSITsagt.debug
```

The **/tmp/XSITsagt.install** file is created during the installation as the result of this command. Be aware that this file will contain unencrypted passwords (those entered during the installation).

4. Run the **install_mgtsvr** script using the following command:

```
./install_mgtsvr -d ‘pwd‘
```

where the **-d** option specifies a source directory for the installation.

5. The script prompts you for configuration settings. Answer each prompt with a value, as follows:

a.

```
************************************************
* Where is your java home?
*
* If your java home is not installed please
* type q, and install the correct version of the
* jdk before continuing
************************************************
JavaHome:
```

Enter the path to the JDK directory. By default, the JDK is installed in **/usr/java1.1**.

b.
```
Do you want to continue with the installation of
<IBMWebAS> [y,n?]
```

Enter **y** to install WebSphere, which is installed in **/opt/IBMWebAS**. If you enter **y** and the installation script encounters a conflict with previously installed packages, the script will prompt you to again continue the installation. If you answer **n**, the installation stops.

If you have an IBM WebSphere Application Server 1.*x* installation, be aware that the Cross-Site server installation will upgrade the WebSphere installation to version 2.0. Either uninstall the 1.*x* installation or select another system to host the Cross-Site server.

c.
```
************************************************
* Please specify the directory containing the
* obj.conf file for the Netscape Webserver V3.5
*
* Type q to skip auto-configuration of the
* obj.conf file.
*************************************************
Netscape V3.5 config path:
```

Enter the path to the directory containing this file. The **obj.conf** file is provided by the Netscape web server. By default, this path is **/opt/netscape/suitespot/https-***NESname***/config**.

Though this prompt states that you must enter the path for Netscape 3.5, Tivoli supports only Netscape 3.6. This has been tested and is officially support by Tivoli.

d.
```
Do you want to continue with the installation of
<SENs351> [y,n,?]
```

Enter **y** to install the Netscape plug-in. If you enter **y** and the installation script encounters a conflict with previously installed packages, the script will prompt you to again continue the installation. If you answer **n**, the installation stops.

e.
```
By default, the /opt/Tivoli installation base
directory is created. The Cross-Site server is then
installed in /opt/Tivoli/XSITsagt.

If you would like the software installed in a
different base directory, enter the directory path
now. Otherwise, press Enter.
```

   Enter an installation directory for Cross-Site. Or, simply press **Enter** to install Cross-Site in the default directory. The installation creates the **XSITsagt** directory under the specified directory.

f.
```
The installation of the Cross-Site server contacts a
fulfillment server, which is located at Tivoli and
provides the most up-to-date installation media (in
the form of channels). The fulfillment server
provides these channels, which are downloaded by
your Cross-Site server and initialized.

If you do NOT wish to rely on the fulfillment server,
enter local. This option is available if you are in
an isolated environment such as a test lab. The
installation will proceed, using the channels that
are provided on the Cross-Site CD-ROM. If you would
like to download channels from the fulfillment
server, which is recommended, enter remote.

Enter the installation method used to install and
initialize the Cross-Site channels.
```

   Enter **local** if you wish to install Cross-Site from the CD-ROM. *TIVOLI STRONGLY RECOMMENDS THAT YOU CHOOSE LOCAL.* The following prompt is then displayed:

```
Enter path to the Cross-Site CD-ROM image.
```

   Enter the full path to the mounted CD-ROM. You simply need to enter the top-level directory of the CD-ROM, such as **/data/tmp**.

   If you enter **remote**, you must provide the protocol, name, and port number of the fulfillment server. The protocol is **HTTPS**, the host name for the Tivoli fulfillment server is **software.cross-site.com**, and the port number for the server is **443**. You must also specify the proxy and its port number, if your server must use a proxy server when contacting the Tivoli fulfillment server.

g. `Enter the protocol that will be used to access your new Cross-Site server.`

   This protocol is the same as the installed web server. Enter **http** for an unsecure server. Enter **https** for a server that will use the HTTPS protocol, which runs over SSL. (Cross-Site for Security must run on an HTTPS server.)

h. `Enter the fully-qualified host name for your Cross-Site server.`

   You *must* enter a fully qualified name, such as **host.dept.company.com**. Cross-Site agents that reside outside of your firewall or domain receive and use this fully qualified name to communicate with the Cross-Site server. If you do not specify a fully qualified name, agents will not be able to resolve the host name of the server.

i. `Enter the port number of your Cross-Site server.`

   Enter the Cross-Site server’s port number.

j. If you are installing a secure Cross-Site server, the following prompts are displayed:

   1. `Enter the HTTPS Key File Password for your Cross-Site server.`

      This is the password you are prompted for when you start a web server running HTTPS.

2. `Enter the HTTPS Key File Password again.`

   Reenter the Key File Password to verify that you entered it correctly the first time.

3. `If your Cross-Site server does not use a supported Certificate Authority for authentication, enter the full path of the directory containing the KeyRing.class file here. Otherwise, "enter none".`

   Enter **none** unless you created the **KeyRing.class** file for the unsupported CA prior to this installation. (If you used an unsupported server certificate to secure the web server, you should have created the **KeyRing.class** file as described in “Importing an Unsupported Root Certificate” on page 199.) If you have the file, enter the full path to the directory where it resides.

k. `Enter the name of the administrative domain name for your Cross-Site server. To ensure uniqueness, it is recommended that you use a name within your DNS domain or the name of the DNS domain itself.`

   Enter the name of the domain where your Cross-Site server will reside.

l. `Enter a name for your Cross-Site server.`

   Enter a meaningful name for the server. This is the name that end users and other console users will use to contact your server.

m. `Enter the IP address of your Cross-Site server.`

   Enter the system’s IP address here. The server must have a static IP address; the dynamic host configuration protocol (DHCP) is not supported for the Cross-Site server.

n. `Enter a description for your Cross-Site server.`

   Enter a description for the server. This is for your information only.

o. `Enter the password that will be used by other Cross-Site servers to collaborate with your Cross-Site server.`

Enter a password for your Cross-Site server. This is different than the **admin** user’s password provided by Tivoli. The password you enter at this prompt will be used when collaborating with other Cross-Site servers. Tivoli recommends that unless you are installing multiple management servers, you simply press **Enter**.

p. `Enter the collaboration password again.`

Reenter the password to verify that you entered it correctly the first time.

q. `Enter the directory on your Cross-Site server where you want to store the console and agent packages. To allow users to download these packages, the Web server must have access to this directory.`

Enter the full path to a directory where the console and agent packages will be installed. By default, the installation creates the *base_dir***/downloads** directory, where *base_dir* is the installation directory for the management server, such as **/opt/Tivoli/XSite/XSITsagt**. If you specify a directory that does not exist, you are prompted to create it.

r. `Enter the type of database that your Cross-Site server will use.`

Enter the type of database that you plan to use. Enter **Oracle8** or **DB2**.

Note: *Recall that Tivoli has only tested the Oracle RDBMS server with a Solaris management server. Other combinations are supported, though not tested. Contact Support if you wish to use an unsupported combination and encounter problems during their installation or use.*

If you enter **Oracle8**, the following prompts are displayed (if you enter **DB2**, go to step 1 on page 96):

1.
   ```
   Enter the Oracle8 database installation
   directory.
   ```

   Enter the installation directory of the database.

2.
   ```
   Enter the database driver.
   ```

   Enter the class name of the JDBC driver that you installed prior to running this script, for example, **oracle.jdbc.driver.OracleDriver** for the Oracle 8 database.

3.
   ```
   Enter the user ID that your Cross-Site server
   will use to access the database.
   ```

   Enter a valid database user ID designated for Cross-Site.

4.
   ```
   Enter the database user’s password.
   ```

   Enter the password for the database user ID previously entered.

5.
   ```
   Enter the database user’s password again.
   ```

   Enter the password again to verify you entered it correctly.

6.
   ```
   Have you set up the Oracle environment on your
   Cross-Site server and inserted the name of your
   database workspace in the tnsnames.ora file?
   ```

   Enter **y** if you are using Oracle 8.0 and the **tnsnames.ora** file contains an entry for the database server. Otherwise, enter **n**.

   If you enter **y**, the following prompt is displayed:

   ```
   Enter the Oracle database name.
   ```

   Enter the name of the database, which is the name of the Oracle instance.

If you enter **n**, you are prompted for the JDBC driver type, which is either **oci8** and **thin** and corresponds to your version of Oracle. You are also prompted for the name of the system where the database is installed, the port number of the listener on the machine where the database is installed, and the database's system identifier (SID).

Continue the installation at step s on page 97.

If you entered **DB2** as the database your server will use (in step r on page 94), the following prompts are displayed:

1. `Enter the DB2 database installation directory`.

   Enter the installation directory of the database.

2. `Enter the DB2 instance name.`

   Enter the instance name of the DB2 database.

3. `Enter the database driver`.

   Enter the class name of the JDBC driver that you installed prior to running this script, for example, **COM.ibm.db2.jdbc.app.DB2Driver** for the DB2 database.

4. `Enter the user ID that your Cross-Site server will use to access the database`.

   Enter a valid database user ID designated for Cross-Site.

5. `Enter the database user’s password`.

   Enter the password for the database user ID previously entered.

6. `Enter the database user’s password again.`

   Enter the database password again to verify that you entered it correctly.

7. `Enter the DB2 database name.`

Enter the name of the database.

s. `Enter the machine name or IP address of your X Server.`

Enter the name or IP address of the system if you are viewing the installation on a remote display. The installation script needs this information because it displays several dialogs after the installation. Before entering the host name here, ensure that you can connect to the host’s display. (The DISPLAY variable should be set and you may wish to use the **xhost** command to enable the connection.)

t. `Enter the full path of the Web browser you will use to install the Cross-Site license key. If you do not want to install a license key at the end of the installation or you do not have a local Web browser, enter “none”.`

Enter the path to the web browser that will be displayed at the end of the installation so that you can install a license key. If you enter **none**, you can install a license key later.

u. `Do you want to review your answers?`

To review all of the prompts and your responses, enter **y**. Tivoli recommends that you review your responses to ensure that you did not enter something incorrectly, which could cause the installation to fail. You can change your answers as you review them. Enter **n** to continue with the installation without reviewing your responses. Enter **q** to exit the installation without completing it.

v. `Do you want to continue with the installation of <XSITsagt> [y,n,?]`

   Enter **y** to continue the installation of the Cross-Site server. If you enter **y** and the installation script encounters a conflict with a previously installed package, the script will prompt you to continue the installation. To cancel the installation, enter **n**.

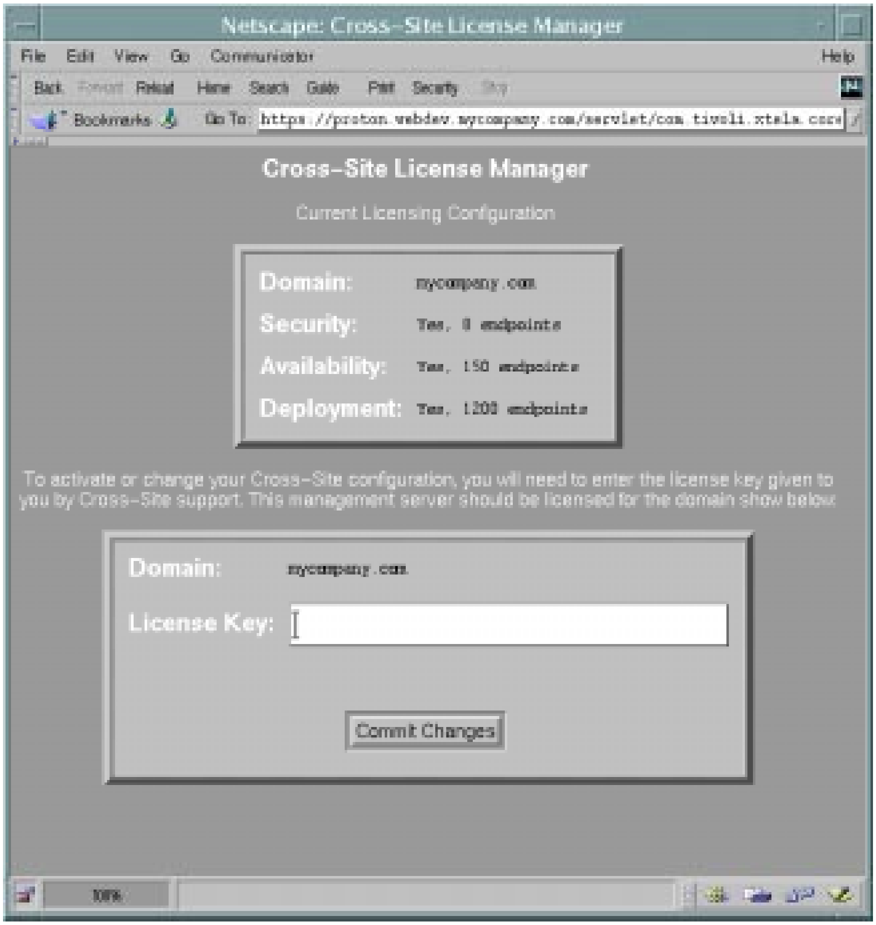
The script installs the Cross-Site server, Netscape plug-in, and WebSphere. It installs the Cross-Site tables in the database and creates the **admin** and **install** users, whose passwords are **admin** and **install**, respectively. (Tivoli recommends that you change these passwords once you complete the console installation.)

6. If you specified a path to a web browser in step t on page 97, the **Cross-Site License Manager** page is displayed in the browser. The URL for this page is as follows:

   *protocol***://***server***/servlet/com.tivoli.xtela.core.license.LicenseManagerServlet**

   where *protocol* and *server* are those of the Cross-Site server you just installed. Be sure to install the license key, which must be installed in order for you to install the Cross-Site applications on the management server, and for you or your end users to install the Cross-Site agents.

The **Cross-Site License Manager** page is similar to the following:


Netscape: Cross–Site License Manager
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks
Go To:
100%

https://proton.webdev.mycompany.com/servlet/com.tivoli.xtela.core

Cross–Site License Manager

Current Licensing Configuration

Domain:	mycompany.com
Security:	Yes, 0 endpoints
Availability:	Yes, 150 endpoints
Deployment:	Yes, 1200 endpoints

To activate or change your Cross–Site configuration, you will need to enter the license key given to you by Cross–Site support. This management server should be licensed for the domain show below.

Domain: mycompany.com

License Key:

Commit Changes

Enter your license key in the **License Key** field and select the **Commit Changes** button. The **License Verified: Cross-Site Enabled** page is displayed to inform you that the installation of the license key succeeded.

After the installation, Tivoli recommends that you change the password of the **admin** user for WebSphere. (WebSphere was installed as part of the base management server.) See **http://***server***:9527** for more information, where *server* is the host name of the management server. Log in as **admin** (the password is also **admin**) and select **Setup –>Administration** from the tree.

Installing Cross-Site for Security

To install the Cross-Site for Security application on the management server, complete the following steps. If you have not done so, Tivoli recommends that you install a license key prior to completing these steps. See step 6 on page 98 for instructions. Also, Tivoli recommends that you start up your web server before configuring the Security application (though the installation of the base server should have restarted the web server).

1. Untar and uncompress the **XSiteSecSvrPkg.solaris2.tar.Z** file, which is located in the **solaris2** of the Cross-Site CD-ROM. Complete the following steps to do so:

   a. Create a directory where you can unpackage the installation package.

   ```
   mkdir Security
   ```

   b. Change to the newly created directory.

   ```
   cd Security
   ```

   c. Copy the **XSiteSecSvrPkg.solaris2.tar.Z** file from the CD-ROM.

   ```
   cp /cdrom_mntpt/solaris2/XSiteSecSvrPkg.solaris2.tar.Z .
   ```

   d. Uncompress the file using the following command. This command removes the **.Z** from the end of the file name.

   ```
   uncompress XSiteSecSvrPkg.solaris2.tar.Z
   ```

   e. Extract, or untar, the contents of the file using the following command.

```
tar xvf XSiteSecSvrPkg.solaris2.tar
```

When complete, the **XSITsecs** package and the **install_secsvr** script are listed in the directory.

2. Run the **install_secsvr** script using the following command (you must have superuser privileges to install Cross-Site for Security):

```
./install_secsvr -d ‘pwd‘
```

where the **-d** option specifies a source directory for the installation.

3. The script prompts you for configuration settings. Answer each prompt with a value, as follows:

a.
```
Please enter the directory where IBM WebSphere is
installed:
```

When you installed the management server, WebSphere was installed in **/opt/IBMWebAS**. Enter this directory.

b.
```
Do you want to continue with the installation of
<XSITsecs> [y,n,?]
```

Enter **y** to continue the installation of Cross-Site for Security on the server. (**XSITsecs** is the name of the Security package.) If you enter **y** and the installation script encounters a conflict with a previously installed (Solaris) package, the script will prompt you to continue the installation.

To cancel the installation, enter **n**.

c.
```
Please restart your Netscape server by executing the
Netscape "stop" and "start" scripts:

install_dir/netscape/suitespot/https-server/stop
install_dir/netscape/suitespot/https-server/start
```

Despite this message, you should restart the web server (and Cross-Site server) by following the instructions in the following section. You must restart the web server so that it can pick up the new Solaris package that was added during the installation. However, you can wait to restart the web server if you intend to install other Cross-Site applications.

Cross-Site for Security is installed on the Cross-Site management server in the *base_dir*/**XSITsagt** directory. The *base_dir* variable's value is that of the base server's installation directory, as specified in step e on page 91.

Stopping and Restarting the Server

For troubleshooting, maintenance, or emergency recovery, you might need to restart the Cross-Site server. You can restart the Cross-Site server on Solaris by restarting the web server itself. (The Cross-Site server restarts automatically every time you restart the web server.)

Note: *Restarting the web server not only affects the Cross-Site server but also any other applications that rely on the web server.*

Before restarting the Cross-Site server, obtain the user name, password, port number, and the Key File Password (also called the key-pair password) for the web server.

To restart the web server from the command line (thereby restarting the Cross-Site server), complete the following steps:

1. To stop the Netscape web server, enter the following command:

   ```
   install_dir/https-server/stop
   ```

   where *install_dir* is the directory path to the web server's installation directory. By default, the Netscape Enterprise Server is installed in **/opt/netscape/suitespot** on Solaris. The *server* variable specifies the name of the web server. Wait several minutes to ensure that the web server shuts down completely.

2. Verify that all processes related to Cross-Site were shutdown with the web server. Enter the following command:

   ```
   /usr/ucb/ps -auxlww | grep user
   ```

   where *user* is the user used when the Netscape Enterprise Server was installed.

3. If processes are listed that are owned by the Netscape user, enter the following command to stop each process:

   ```
   kill -9 process
   ```

   You need to ensure that the **tuner.sh** and **native_threads/jre** processes are stopped.

4. Restart the web server by entering the following command:

   ```
   install_dir/https-server/start
   ```

   where *install_dir* is the directory path to the web server's installation directory. By default, the Netscape Enterprise Server is installed in **/opt/netscape/suitespot** on Solaris. The *server* variable specifies the name of the web server. Enter the Key File Password if prompted.

The Cross-Site server is shut down and restarted automatically when you enter these commands. If you try to run the console immediately after restarting the server and it fails, wait a few minutes and try again. The web server may need time to complete its initialization.

Verifying the Server's Installation

The following items will help you determine if the installation of the Cross-Site management server was successful:

- You can verify the accessibility of the server by entering the following URL in a web browser:

  protocol://*server_name*:*port*/**servlet/CrossSiteServlet** where *server_name* and *port* are the values specified when the Cross-Site server was installed. This utility issues an HTTP request to the Cross-Site server.

If the server is running, the URL displays a web page containing the following message:

Cross-Site Management Server Status: ALIVE
Version: *x* Build: *x*

- If you created the **/tmp/XSITsagt.debug** directory prior to installing the management server, the **/tmp/XSITsagt.install** file was created during the installation. It contains trace information about the management server's installation. You can also run the **tail -f /tmp/XSITsagt.install** command, which enables you to list the processes as they occur, and helps you identify if a process is hung.

- The channel manager service starts when the management server starts. To list the processes running on the Cross-Site server, enter the following command:

  ```
  /bin/ps -ef | egrep "netsc|java|jre"; echo; netstat -a |
  grep 5282
  ```

  The channel manager listens on port 5282.

- After installing the Cross-Site console on a system, ensure that it can connect to the management server without generating errors. See "Installing and Running the Console" on page 107 if you have not installed a console in your environment.

- The agent packages, the console package, and the **index.html** file are in the **downloads/XSite** directory. This directory was created during the installation of the management server. This enables you to launch a web browser and load the *protocol*://*Server*:*Port***/Tivoli/Cross-Site** page, where *protocol* is that of the Cross-Site server, *Server* is the name of the Cross-Site server, and *Port* is its port number.

- A web browser can connect to the web server using the Cross-Site server's name and port number. For example, if you enter **https://proton.webdev.mycompany.com:443/**, where **proton** is the Cross-Site server and **443** is its port, the **Netscape Enterprise Server** page is displayed.

- The first time you use the Netscape Administrative Server's page after installing the Cross-Site server, you are prompted to accept changes. You access the Administrative Server's page by entering *protocol*://*server_name*:*admin_port* in the web browser. The *protocol*, *server_name*, and *admin_port* variables' values are that of the Netscape Administrative Server. These changes were made by the installation of WebSphere, which is part of the Cross-Site server's installation. Accept the changes.

If you encounter problems with any of these items, restart the web server, which will start WebSphere. If the web server will not start, ensure that enough space is available on the disk partition of the management server's host. Netscape might not be configured correctly for the management server. Also, refer to the web server's release notes.

If you need to reinstall, be sure to uninstall Cross-Site (even if the installation failed) by following the instructions in "Uninstalling Cross-Site" on page 235.

Verifying the Installation of the Database Tables

To verify that the Cross-Site installation created its tables in the database, complete the following steps:

1. Log in to the Oracle RDBMS server.

2. Enter **sqlplus** and supply the user ID and password created to access Cross-Site's database.

3. At the SQLPLUS prompt, enter the following command:

   ```
   select * from cat;
   ```

   If this **select** command prints a list of catalog entries, the tables were created. If none are found, the installation of the database tables failed, which means that the Cross-Site server's installation failed.

4. If the RDBMS server is DB2, complete these steps:

   a. Log in to the database server as user ID used to install the management server.

   b. Enter **db2**.

   c. At the DB2 prompt, enter the following command to connect to the database:

      ```
      connect to database
      ```

      where *database* is the name of the database

   d. Enter the following command:

      ```
      list tables
      ```

   If the **list** command prints a list of table entries, the tables were created. If none are found, the installation of the database tables failed, which means that the Cross-Site server's installation failed.

If you need to reinstall, be sure to uninstall Cross-Site (even if the installation failed) by following the instructions in "Uninstalling Cross-Site" on page 235.

8

Installing and Running the Console

You must install the Cross-Site console in order to access Cross-Site management information. The console is Cross-Site's desktop. Installing consoles throughout your network and on your partners' sites enables you to share information and administrative duties. This chapter includes instructions for installing the console on Windows 95, 98, NT, AIX, and Solaris systems. It also provides instructions for running the console.

If a **KeyRing.class** file was created before the installation of the management server, you need to ensure that a copy of the same **KeyRing.class** file was saved on each client machine where you intend to install the console. The console installation prompts you for the path to the file on the client machine. After the installation, ensure that it was copied to in the *install_dir*/**lib** directory.

Requirements for the Console

The following list describes the prerequisites for the Cross-Site console and, where applicable, how to verify that you have the necessary resources. It is both a checklist and a work sheet; feel free to write down any values that you need to refer to during the installation.

1. Verify the version of the operating system on the machine where you intend to install the Cross-Site console. The following table outlines the supported platforms on which you can install the console:

Requirement	Commands
Windows 95, or Windows 98, or Windows NT 4.0 service pack 4 or higher, on a Pentium 333 MHz class machine (or better), or	On Windows, select **Start -> Settings -> Control Panel**; double-click on **System** and review the **General** tab.
AIX 4.3.2, or	On AIX, enter **oslevel**.
Solaris 2.6 or 2.7 on Sun SPARC	On Solaris, to determine the version, enter **/usr/bin/uname -a**.

Note: *On AIX, the path to system commands is set by the path variable. Therefore, this table and subsequent ones identify the AIX command only, without its full path.*

2. Verify that the target system for the console has enough disk space. The following table includes the disk space requirements for the Cross-Site console:

Requirement	Commands
24 MB on all Windows platforms	On Windows, double-click on **My Computer** and right-click on the drive where you intend to install the console. Select **Properties** and review the **General** tab.
17 MB on AIX	On AIX, to determine the available disk space, enter **lsvg rootvg**. To determine the space allocated to the file systems, enter **df -k**.
17 MB on Solaris	On Solaris, to determine the available disk space, enter **/usr/ucb/df -kl**.

3. Verify that the target system for the console has enough memory, according to the requirement listed in the following table:

Requirement	Commands
32 MB on all Windows platforms	On Windows, select **Start -> Settings -> Control Panel**; double-click on **System** and review the **General** tab.
23 MB on AIX	On AIX, to determine the amount of available memory, enter **bootinfo -r**. AIX returns a value in KB.
27 MB on Solaris	On Solaris, to determine the amount of available memory, enter **/usr/sbin/prtconf | head**.

4. *Solaris Only*
Verify that the Solaris patches that are required to install the Java Development Kit (JDK) are installed on any Solaris workstation that you intend to include in your installation. You must install the patches prior to installing the JDK or the console (according to the Solaris installation documentation).

Requirement	Commands
Patch 105284-05 and 105490-04 for Solaris 2.6	To list the patches installed on a Solaris system, enter **/usr/bin/showrev -p**.

You can download the latest patches from the following URLs:

http://access1.sun.com/cgi-bin/rpatch2html?README.105284-29

http://access1.sun.com/cgi-bin/rpatch2html?README.105490-07

Verify that your system functions properly after installing the patches.

5. *UNIX Only*
Install the JDK, which provides a Java Virtual Machine (JVM). For Windows, version 1.1.7 is bundled with the installation of the console.

Requirement	Commands
For AIX, JDK version 1.1.6.0	On AIX, use this command to determine the level of the JDK: **lslpp -l Java.rte.bin**
For Solaris, JDK version 1.1.7 (rev 08 or higher)	To determine the version of JDK on Solaris, enter **java -fullversion**.

If you have an older version of the JDK installed on Solaris, be sure to remove it before installing an updated version.You can use the following command to remove the installed JDK core packages:

```
pkgrm SUNWjvdem SUNWjvdev SUNWjvjit SUNWjvman SUNWjvrt
```

You can download the JDK for AIX from the following site: **http://service.software.ibm.com/support/rs6000/downloads**

You can download the JDK for Solaris from the following site: **http://www.sun.com/solaris/java/index.html**

If you download the JDK 1.1.7_08 from this URL, you can also download the patches required for Solaris 2.6.

Make note of the full path where the JDK is installed below:

_ _

6. If a **KeyRing.class** file was created before the installation of the management server, you need to ensure that a copy of the same **KeyRing.class** file was saved on each client machine where you intend to install an console. The console installation prompts you for the path to the file on the client machine. You can write it here:

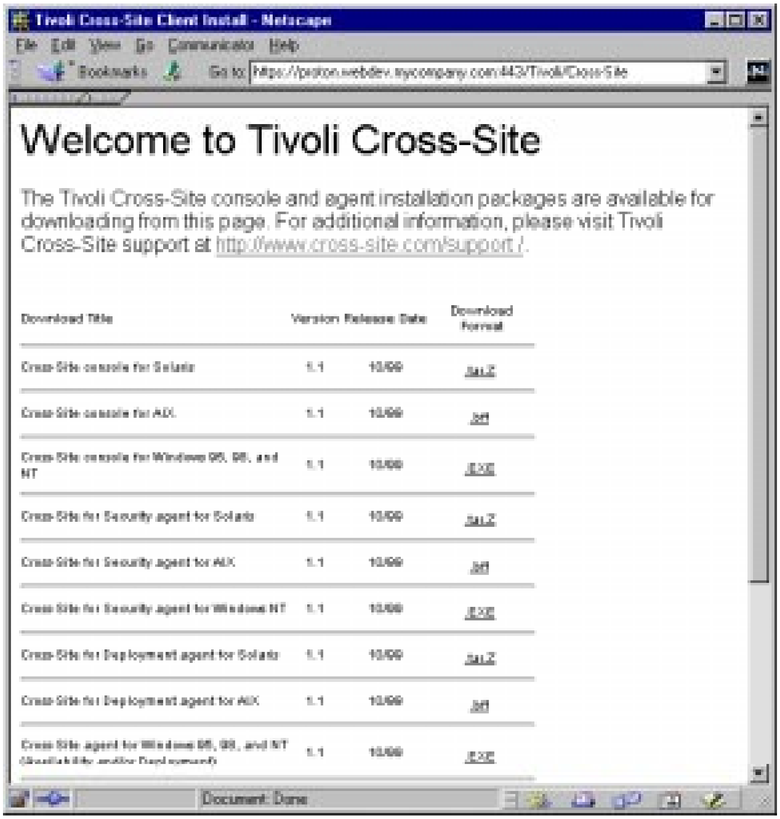
_ _

Installing and Running the Console on Windows

Complete the following steps to install the console on a Windows 95, 98, or NT system. This procedure runs the **console.EXE** installation program, which is located in the **w32-ix86** directory of the Cross-Site CD-ROM. It is also available on the Cross-Site server for downloading. If you wish to install from the CD-ROM, skip to step 4 on page 112. Otherwise, begin with step 1.

1. Launch a web browser and load the Cross-Site download page. The URL for the page is *protocol*://*Server:Port***/Tivoli/Cross-Site**, where *protocol* is the protocol of the Cross-Site server, *Server* is the name of the Cross-Site server, and *Port* is its port number.

The download page is similar to the following:



Tivoli Cross-Site Client Install - Netscape

Go to: https://proton.webdev.mycompany.com:443/Tivoli/Cross-Site

Welcome to Tivoli Cross-Site

The Tivoli Cross-Site console and agent installation packages are available for downloading from this page. For additional information, please visit Tivoli Cross-Site support at http://www.cross-site.com/support/.

Download Title	Version	Release Date	Download Format
Cross-Site console for Solaris	1.1	10/99	.tar.Z
Cross-Site console for AIX	1.1	10/99	.tar
Cross-Site console for Windows 95, 98, and NT	1.1	10/99	.EXE
Cross-Site for Security agent for Solaris	1.1	10/99	.tar.Z
Cross-Site for Security agent for AIX	1.1	10/99	.tar
Cross-Site for Security agent for Windows NT	1.1	10/99	.EXE
Cross-Site for Deployment agent for Solaris	1.1	10/99	.tar.Z
Cross-Site for Deployment agent for AIX	1.1	10/99	.tar
Cross-Site agent for Windows 95, 98, and NT (Availability and/or Deployment)	1.1	10/99	.EXE

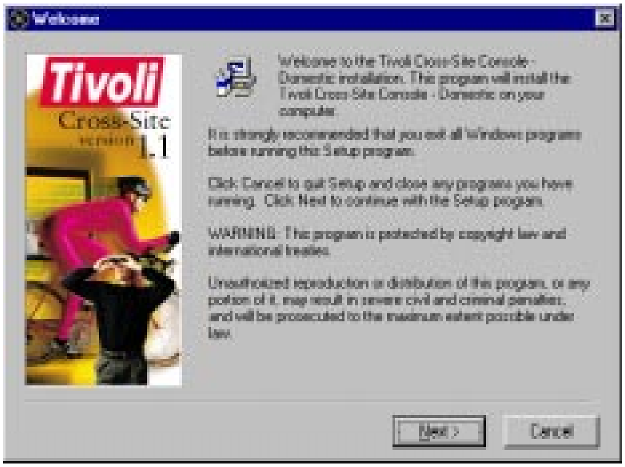
Document: Done

2. Select the **.EXE** link for the console.

3. Choose to save the file and select a location for the **console.EXE** file. Keep in mind that this also serves as the program’s staging directory during the installation.

4. Run the installation program. You can run it by selecting **Start –> Run** and entering a path to the **console.EXE** file, or you can double-click on the file in the **Explorer** window. You can also run it from the command prompt.

The installation program displays a **Welcome** dialog:



Welcome to the Tivoli Cross-Site Console - Domestic installation. This program will install the Tivoli Cross-Site Console - Domestic on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

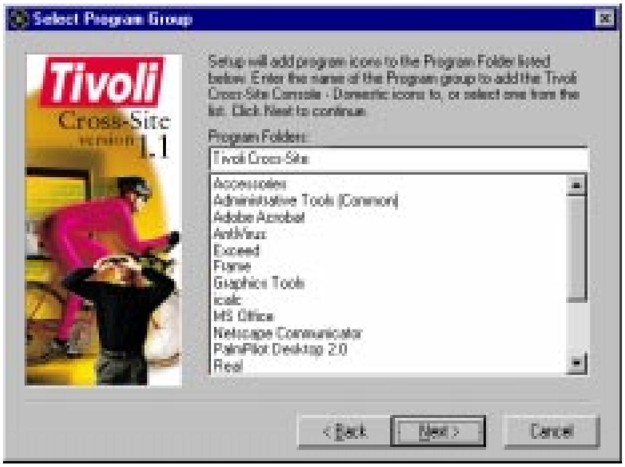
5. Click **Next** and follow the instructions on each of the following dialogs:

   a. In the **Tivoli Cross-Site Console - Domestic/Export License Agreement** dialog, read the license agreement and click **Accept** if you understand and accept the terms of the installation.

   b. In the **Choose Destination Location** dialog, select or browse for a destination folder for the Cross-Site console and click **Next**.

   c. In the **Backup Replaced Files** dialog, select **Yes** if you wish to backup changed files and browse for a folder where the backup files will be stored. You can also accept the default folder. Click **Next** to proceed.

d. In the **Select Program Group** dialog, select or enter the name of a program folder for the **Cross-Site Console** entry and click **Next**.



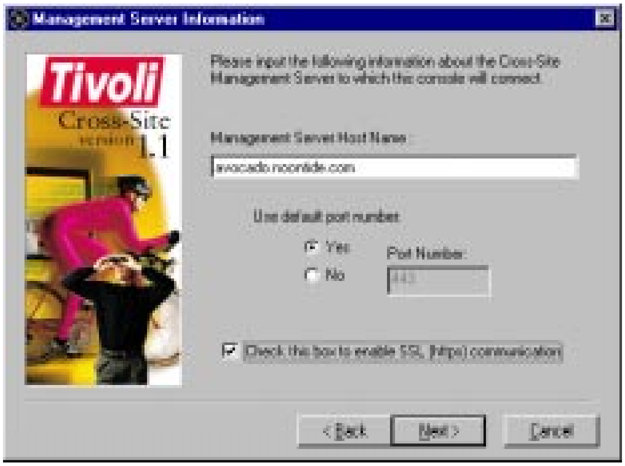
Setup will add program icons to the Program Folder listed below. Enter the name of the Program group to add the Tivoli Cross-Site Console - Domestic icons to, or select one from the list. Click Next to continue.

Program Folders:

Tivoli Cross-Site

Accessories
Administrative Tools (Common)
Adobe Acrobat
AntiVirus
Exceed
Frame
Graphics Tools
icalc
MS Office
Netscape Communicator
PalmPilot Desktop 2.0
Real

e. In the **Management Server Information** dialog, enter the Cross-Site management server’s host name and specify the server’s port. If the Cross-Site server uses HTTPS, select the check box. This enables SSL communication between the console you are installing and the Cross-Site server. Click **Next**.



Please input the following information about the Cross-Site Management Server to which the console will connect.

Management Server Host Name:

avocado.noontide.com

Use default port number

● Yes

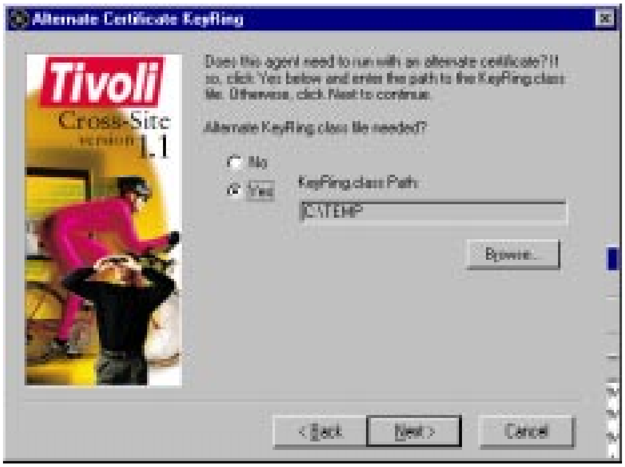
○ No

Port Number:

443

☑ Check this box to enable SSL (https) communication

f. If you selected the check box on the **Management Server Information** dialog, the **Alternate Certificate KeyRing** dialog is displayed. If the digital certificate was not issued by one of the supported certification authorities (CAs), select **Yes**. Enter the full path to the **KeyRing.class** file on the client where you are installing the console. (You must have already edited the KeyRing, as discussed in “Importing an Unsupported Root Certificate” on page 199.) Click **Next** to proceed.



Alternate Certificate KeyRing

Does this agent need to run with an alternate certificate? If so, click Yes below and enter the path to the KeyRing.class file. Otherwise, click Next to continue.

Alternate KeyRing.class file needed?

○ No
● Yes

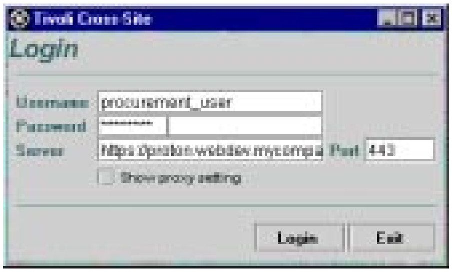
KeyRing.class Path:
C:\TEMP

The installation copies the specified file to the *install_dir*/**lib** directory, where *install_dir* is the directory specified in step b on page 113.

g. In the **Start Installation** dialog, verify your entries and click **Next**.

h. The **Installation Complete** dialog is displayed. Click **Finish**.

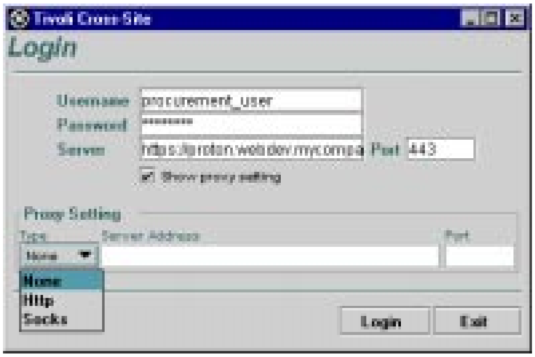
When complete, a menu item is added to the **Start** menu. By default, the **Start –> Programs –> Tivoli Cross-Site –> Cross-Site Console** entry is added to the current user’s menu (the top section of the **Programs** menu). Select this menu item to start the console. When you start the console, a dialog similar to the following is displayed:



Username procurement_user
Password **********
Server https://proton.webdev.mycompa Port 443
□ Show proxy setting

Enter a Cross-Site user’s name and password. (The first time you log in, use **admin** as the username and the **admin** as the password.) To connect to a different management server, specify the server’s name and port in the fields, respectively.

If you wish to use a proxy server when connecting to the Cross-Site server, select the **Show proxy setting** check box. Note that this check box is available only when you log in to a console installed on a Windows client. The login dialog is expanded as follows:

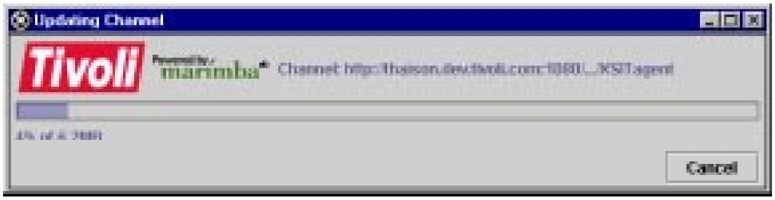


Username procurement_user
Password *********
Server https://proton.webdev.mycompa Port 443
☑ Show proxy setting

Proxy Setting
Type None
Server Address
Port

Select the type of proxy from the drop-down list and enter the proxy server’s name and port. When you click the **Login** button, the console uses the specified proxy server to contact the Cross-Site server.

The first time you run the console, it downloads a channel from the management server’s channel manager. The console’s channel contains all of the latest binaries and necessary files.The **Updating Channel** dialog is displayed while the console downloads its channel.



Channel: http://thaison.dev.tivoli.com:5880/...XSIT.agent

[illegible]

It may take a few minutes to download the channel the first time you log in.

Tivoli recommends that you change the password of the **admin** user (resource) the first time you log in. The default password is **admin**. For instructions, refer to the section regarding access control and user configuration in the online help or in the user's guide.

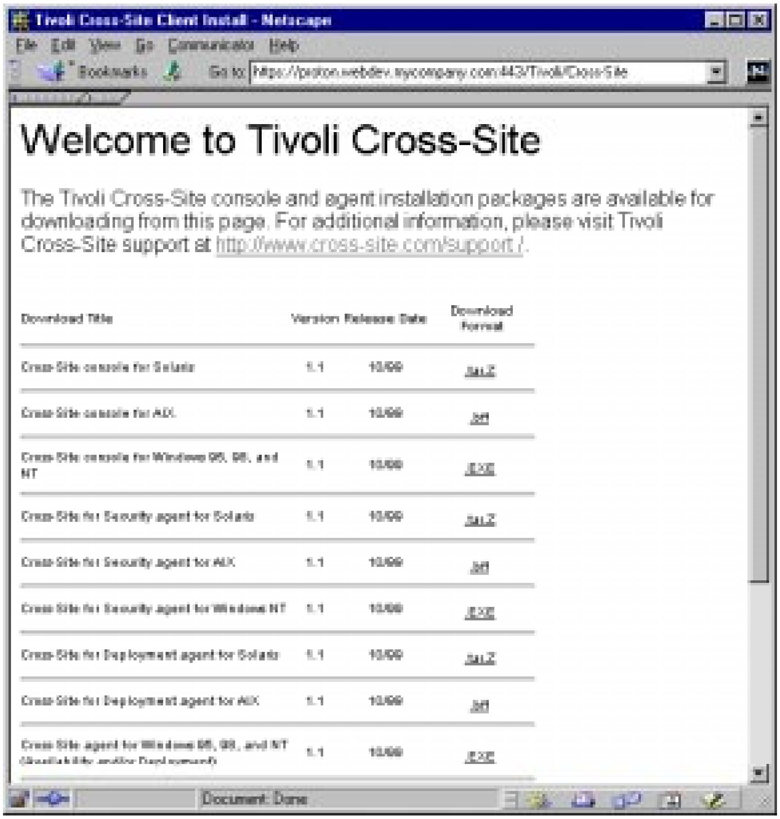
To close the Cross-Site console, simply close the console's window.

Installing, Configuring, and Running the Console on AIX

To install and configure the Cross-Site console on AIX using the System Management Interface Tool (SMIT), complete the following steps. This procedure installs the **xsite.console.bff** file. This file can be found in the **aix4-r3** directory on the CD-ROM, and can also be downloaded from the Cross-Site server. If you wish to install from the CD-ROM, skip to step 6 on page 119. Otherwise, begin with step 1.

1. Launch a web browser and load the Cross-Site download page. The URL for the page is *protocol*://*Server:Port***/Tivoli/Cross-Site**, where *protocol* is the protocol of the Cross-Site server, *Server* is the name of the Cross-Site server, and *Port* is its port number.

The download page is similar to the following:


Tivoli Cross-Site Client Install - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: https://proton.webdev.mycompany.com:443/Tivoli/Cross-Site
Document: Done

Welcome to Tivoli Cross-Site

The Tivoli Cross-Site console and agent installation packages are available for downloading from this page. For additional information, please visit Tivoli Cross-Site support at http://www.cross-site.com/support/.

Download Title	Version	Release Date	Download Format
Cross-Site console for Solaris	1.1	10/99	.tar.Z
Cross-Site console for AIX	1.1	10/99	.bff
Cross-Site console for Windows 95, 98, and NT	1.1	10/99	.EXE
Cross-Site for Security agent for Solaris	1.1	10/99	.tar.Z
Cross-Site for Security agent for AIX	1.1	10/99	.bff
Cross-Site for Security agent for Windows NT	1.1	10/99	.EXE
Cross-Site for Deployment agent for Solaris	1.1	10/99	.tar.Z
Cross-Site for Deployment agent for AIX	1.1	10/99	.bff
Cross-Site agent for Windows 95, 98, and NT (Availability and/or Deployment)	1.1	10/99	.EXE

2. Create a directory where you can download the console's **.bff** file.

   ```
   mkdir /usr/Tivoli/console
   ```

3. Change to the newly-created directory.

   ```
   cd /usr/Tivoli/console
   ```

4. Download the **xsite.console.bff** file by selecting the **.bff** link on the download page. Save it in the current directory.

5. Create a **.toc** file in the current directory by running the following command:

   ```
   /usr/sbin/inutoc
   ```

6. If installing from CD-ROM, insert the CD-ROM into the drive and mount the drive, as follows:

   ```
   mount -v cdrfs -r /dev/cd0 /mnt
   ```

   where */dev/cd0* is your CD-ROM device and */mnt* is the mount point.

7. Use SMIT to install the file, as follows:

   a. Display the **SMIT Install and Update from Latest Available Software** menu using the following command:

   ```
   /usr/bin/smit install_latest
   ```

   b. In the **INPUT device/directory for software** field, enter one of the following commands:

   ```
   /mnt/aix4-r3
   ```

   ```
   /usr/Tivoli/console
   ```

   where */mnt* is the directory where you mounted your CD-ROM and **/usr/Tivoli/console** is where you downloaded the **.bff** file.

   c. Press **Enter**. The dialog is updated with a new list of entry fields.

   d. In the **SOFTWARE to install** field, select **Tivoli Cross-Site Console**.

   If you wish to change any of the default values for other entry fields on the **Install and Update from Latest Available Software** menu, do so before continuing.

   e. When you are ready to install, press **Enter** to continue. You are prompted with an **ARE YOU SURE** popup dialog. Press **Enter** again to continue with the installation.

After the installation is complete, consult the installation summary at the bottom of your SMIT output to verify that the installation completed successfully. Exit SMIT when you are finished.

8. Configure the console for AIX by using the following command:

   ```
   /usr/Tivoli/XSite/XSITconsl/install/conslconfig
   ```

   This command prompts you for configuration information. Answer each prompt with a value, as follows:

   a. `Enter the fully-qualified host name for your Cross-Site management server.`

      Enter the fully-qualified domain name of the Cross-Site server.

   b. `Enter the protocol that will be used to access your Cross-Site server.`

      Enter the protocol of the Cross-Site server you intend to access using the console (either HTTP or HTTPS).

   c. `Enter the port number of your Cross-Site server.`

      Enter the port number of the Cross-Site server.

   d. If you are installing a console that will connect to a secure Cross-Site server, the following prompt is displayed:

      ```
      If your Cross-Site server does not use a supported
      Certificate Authority for authentication, enter the
      full path of the directory containing an alternate
      KeyRing.class file. Otherwise, enter "none".
      ```

      Enter **none** unless you created the **KeyRing.class** file for the unsupported CA prior to this installation. (If you used an unsupported server certificate to secure the web server, you should have created the **KeyRing.class** file as described in “Importing an Unsupported Root Certificate” on page 199.) If you have the file, enter the full path to the directory where it resides.

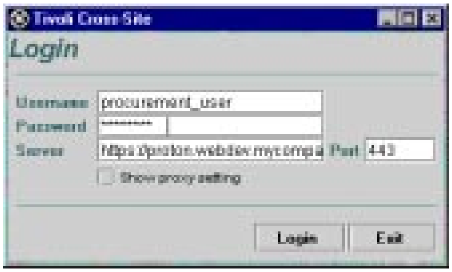
To run the console on AIX, enter the following command:

```
base_dir/XSITconsl/bin/xs_console
```

where *base_dir* is the directory in which you installed the Cross-Site console, such as **/usr/Tivoli/XSite**.

The Cross-Site console runs as a stand-alone application on the desktop. To ensure that you always have the latest version of the console, Cross-Site enables you to receive automatic updates to the console when available. If you want to enable this auto-update feature on UNIX, you also need to run the console as **root**. The NT version of the console always runs in this auto-update mode.

When you start the console, a dialog similar to the following is displayed, which enables you to log in to the Cross-Site server:



Tivoli Cross-Site

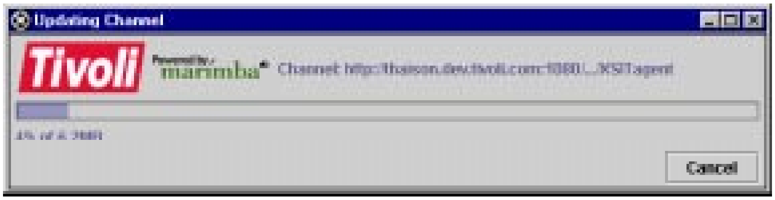
Login

Username: procurement_user
Password: ********
Server: https://proton.webdev.mycompa
Port: 443

□ Show proxy setting

Enter a Cross-Site user’s name and password. (The first time you log in, use **admin** as the username and the **admin** as the password.) To connect to a different management server, specify the server’s name and port in the **Server** and **Port** fields, respectively. Click the **Login** button to display the console.

The first time you run the **xs_console** command, the console downloads a channel from the management server’s channel manager. The console’s channel contains all of the latest binaries and necessary files.The **Updating Channel** dialog is displayed while the console downloads its channel.



It may take a few minutes to download the channel the first time you log in.

Tivoli recommends that you change the password of the **admin** user (resource) the first time you log in. The default password is **admin**. For instructions, refer to the section regarding access control and user configuration in the online help or in the user’s guide.

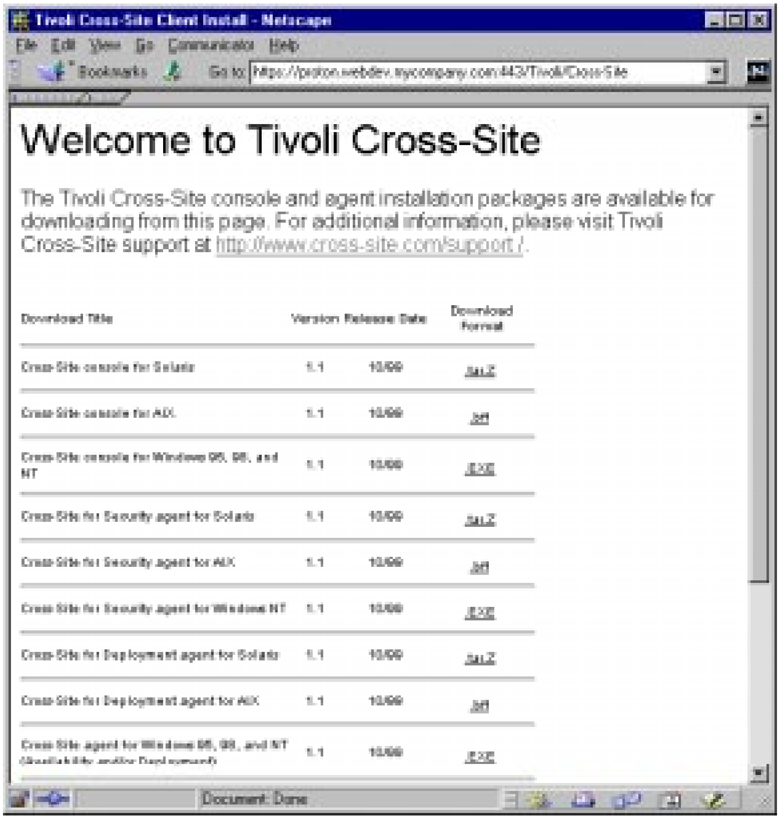
To close the Cross-Site console, simply close the console’s window.

Installing and Running the Console on Solaris

Complete the following steps to install the console on a Solaris system. This procedure runs the **pkgadd** installation script, which is packaged in the **XSiteConsolePkg.solaris2.tar.Z** file. This file can be found in the **solaris2** directory on the CD-ROM, and can also be downloaded from the Cross-Site server. If you wish to install from the CD-ROM, skip to step 7 on page 124. Otherwise, begin with step 1.

1. Launch a web browser and load the Cross-Site download page. The URL for the page is *protocol*://*Server:Port***/Tivoli/Cross-Site**, where *protocol* is the protocol of the Cross-Site server, *Server* is the name of the Cross-Site server, and *Port* is its port number.

The download page is similar to the following:


Tivoli Cross-Site Client Install - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: https://proton.webdev.mycompany.com:443/Tivoli/Cross-Site
Document: Done

Welcome to Tivoli Cross-Site

The Tivoli Cross-Site console and agent installation packages are available for downloading from this page. For additional information, please visit Tivoli Cross-Site support at http://www.cross-site.com/support/.

Download Title	Version	Release Date	Download Format
Cross-Site console for Solaris	1.1	10/99	tar.Z
Cross-Site console for AIX	1.1	10/99	.bff
Cross-Site console for Windows 95, 98, and NT	1.1	10/99	.EXE
Cross-Site for Security agent for Solaris	1.1	10/99	tar.Z
Cross-Site for Security agent for AIX	1.1	10/99	.bff
Cross-Site for Security agent for Windows NT	1.1	10/99	.EXE
Cross-Site for Deployment agent for Solaris	1.1	10/99	tar.Z
Cross-Site for Deployment agent for AIX	1.1	10/99	.bff
Cross-Site agent for Windows 95, 98, and NT (Availability and/or Deployment)	1.1	10/99	.EXE

2. Create a directory where you can download and unpackage the installation package.

   ```
   mkdir /data/opt/Tivoli/console
   ```

3. Change to the newly-created directory.

   ```
   cd /data/opt/Tivoli/console
   ```

4. Download the **XSiteConsolePkg.solaris2.tar.Z** file by selecting the **tar.Z** link on the download page.

5. Uncompress the file using the following command. This command removes the **.Z** from the end of the file name.

   ```
   uncompress XSiteConsolePkg.solaris2.tar.Z
   ```

6. Extract the contents of the file using the following command:

   ```
   tar xvf XSiteConsolePkg.solaris2.tar
   ```

7. Run the following **pkgadd** script:

   ```
   ./pkgadd -d ‘pwd‘
   ```

8. The script prompts you for configuration settings. Answer each prompt with a value, as follows:

   a. ```
      By default, the /opt/Tivoli installation base
      directory is created. The Cross-Site console is then
      installed in /opt/Tivoli/XSITcons.

      If you would like the software installed in a
      different base directory, enter the directory path
      now. Otherwise, click Enter.
      ```

      Enter an installation directory for the Cross-Site console. To install Cross-Site in the default directory, click **Enter** without entering a directory. The installation creates the **XSITcons** directory under the specified directory.

   b. ```
      Enter path to the Java home directory.
      ```

      Enter the path to the directory where the Java Development Kit (JDK) is installed. By default, the JDK is installed in **/usr/java1.1**.

   c. ```
      Enter the fully-qualified host name for your
      Cross-Site management server.
      ```

      Enter the fully-qualified domain name of the Cross-Site server.
      ```

d.
```
Enter the protocol that will be used to access your
Cross-Site server.
```

Enter the protocol of the Cross-Site server you intend to access using the console.

e.
```
Enter the port number of your Cross-Site server.
```

Enter the port number of the Cross-Site server.

f. If you are installing a console that will connect to a secure Cross-Site server, the following prompt is displayed:

```
If your Cross-Site server does not use a supported
Certificate Authority for authentication, enter the
full path of the directory containing an alternate
KeyRing.class file. Otherwise, enter "none".
```

Enter **none** unless you created the **KeyRing.class** file for the unsupported CA prior to this installation. (If you used an unsupported server certificate to secure the web server, you should have created the **KeyRing.class** file as described in “Importing an Unsupported Root Certificate” on page 199.) If you have the file, enter the full path to the directory where it resides.

g. If the specified installation directory does not exist, you are prompted to create it.

```
The selected base directory x must exist before
installation is attempted.

Do you want this directory created now?
```

Enter **y** to create the directory.

h. `This package contains scripts which will be executed with super-user permission during the process of installing this package.`

```
Do you want to continue with the installation of
<XSITcons> [y,n,?]
```

Enter **y** to continue the installation of the Cross-Site console. If you enter **y** and the installation script encounters a conflict with a previously installed package, the script prompts you to continue the installation. To cancel the installation, enter **n**.

When complete, the installation program starts the console and displays the **Login** dialog.

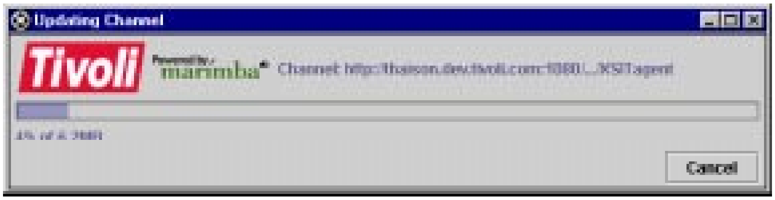
To run the console on Solaris, enter the following command:

```
base_dir/XSITcons/bin/xs_console
```

where *base_dir* is the directory in which you installed the Cross-Site console, such as **/opt/Tivoli/XSite**.

The Cross-Site console runs as a stand-alone application on the desktop. To ensure that you always have the latest version of the console, Cross-Site enables you to receive automatic updates to the console when available. If you want to enable this auto-update feature on UNIX, you also need to run the console as **root**. The NT version of the console always runs in this auto-update mode.

The first time you run the **xs_console** command, the console downloads a channel from the management server's channel manager. The console's channel contains all of the latest binaries and necessary files.The **Updating Channel** dialog is displayed while the console downloads its channel.



Channel: http://thaison.dev.tivoli.com:5080/...XSITagent

[illegible]

It may take a few minutes to download the channel the first time you log in.

Tivoli recommends that you change the password of the **admin** user (resource) the first time you log in. The default password is **admin**. For instructions, refer to the section regarding access control and user configuration in the online help or in the user's guide.

To close the Cross-Site console, simply close the console's window.

9

Installing the Security Agent

You can install agents on Windows NT, AIX, and Solaris systems. The agent is responsible for monitoring your network for intrusion attempts. It is intended to be installed on key systems, such as firewall machines.

If a **KeyRing.class** file was created before the installation of the management server, you need to ensure that a copy of the same **KeyRing.class** file was saved on each client machine where you intend to install the agent. The agent installation prompts you for the path to the file on the client machine. After the installation, ensure that it was copied to in the *install_dir***/lib** directory.

Requirements for the Security Agent

The following list describes the prerequisites for the agent and, where applicable, how to verify that you have the necessary resources. It is both a checklist and a work sheet; feel free to write down any values that you need to refer to during the installation.

1. Verify the version of the operating system on the machine where you intend to install the Security agent. The following table outlines the supported platforms on which you can install the agent:

Requirement	Commands
Windows NT 4.0 service pack 4 or higher, on a Pentium 333 MHz class machine (or better), or	On Windows, select **Start -> Settings -> Control Panel**; double-click on **System** and review the **General** tab.
AIX 4.3.2, or	On AIX, enter **oslevel**.
Solaris 2.6 or 2.7 on Sun SPARC	On Solaris, to determine the version, enter **/usr/bin/uname -a**.

Note: *On AIX, the path to system commands is set by the path variable. Therefore, this table and subsequent ones identify the AIX command only, without its full path.*

2. Verify that the target system for the Security agent has enough disk space. The following table includes the disk space requirements:

Requirement	Commands
11 MB on Windows NT	On NT, double-click on **My Computer** and right-click on the drive where you intend to install the agent. Select **Properties** and review the **General** tab.
8 MB on AIX	On AIX, to determine the available disk space, enter **lsvg rootvg**. To determine the space allocated to the file systems, enter **df -k**.
8 MB on Solaris	On Solaris, to determine the available disk space, enter **/usr/ucb/df -kl**.

3. Verify that the target system for the agent has enough memory, according to the requirement listed in the following table:

Requirement	Commands
11 MB on Windows NT	On NT, select **Start –> Programs –> Administrative Tools (Common) –> Windows NT Diagnostics**. Select the **Memory** tab and review the Physical Memory totals.
12 MB on AIX	On AIX, to determine the amount of available memory, enter **bootinfo -r**. AIX returns a value in KB.
13 MB on Solaris	On Solaris, to determine the amount of available memory, enter **/usr/sbin/prtconf | head**.

4. *Solaris Only*
   Verify that the Solaris patches that are required to install the Java Development Kit (JDK) are installed on any Solaris workstation that you intend to include in your installation. You must install the patches prior to installing the JDK or the agent (according to the Solaris installation documentation).

Requirement	Commands
Patch 105284-05 and 105490-04 for Solaris 2.6	To list the patches installed on a Solaris system, enter **/usr/bin/showrev -p**.

You can download the latest patches from the following URLs:

http://access1.sun.com/cgi-bin/rpatch2html?README.105284-29

http://access1.sun.com/cgi-bin/rpatch2html?README.105490-07

Verify that your system functions properly after installing the patches.

5. *UNIX Only*
   Install the JDK, which provides a Java Virtual Machine (JVM). For NT, version 1.1.7 is bundled with the installation of the Cross-Site for Security agent.

Requirement	Commands
For AIX, JDK version 1.1.6.0	On AIX, use this command to determine the level of the JDK: **lslpp -l Java.rte.bin**
For Solaris, JDK version 1.1.7 (rev 08 or higher)	To determine the version of JDK on Solaris, enter **java -fullversion**.

   If you have an older version of the JDK installed on Solaris, be sure to remove it before installing an updated version. You can use the following command to remove the installed JDK core packages:

```
pkgrm SUNWjvdem SUNWjvdev SUNWjvjit SUNWjvman SUNWjvrt
```

   You can download the JDK for AIX from the following site:
   http://service.software.ibm.com/support/rs6000/downloads

   You can download the JDK for Solaris from the following site:
   http://www.sun.com/solaris/java/index.html

   If you download the JDK 1.1.7_08 from this URL, you can also download the patches required for Solaris 2.6.

   Make note of the full path where the JDK is installed. You can enter it in the space below.

   _

6. *AIX Only*
   Verify that the **bos.net.tcp.server** package is present on the system before installing the agent by entering the following command:

```
lslpp -l bos.net.tcp.server
```

7. If you intend to install the Security agent on a UNIX system, obtain the **root** password for the system. If you intend to install it on a Windows NT system, obtain the **Administrator** password. Tivoli recommends that you do *not* record the password here.

8. Ensure that any NT system where you intend to install the Security agent is assigned a static IP address; Tivoli Cross-Site for Security does not support the Dynamic Host Configuration Protocol (DHCP).

9. If a **KeyRing.class** file was created before the installation of the management server, you need to ensure that a copy of the same **KeyRing.class** file was saved on each client machine where you intend to install an agent. The agent installation prompts you for the path to the file on the client machine. You can write it here for reference:

   _

10. Ensure that each machine on which you want to install an agent can access the Cross-Site management server. You can record the management server's host name and port number here for reference; you are prompted for this information during installation:

    _

Review “Security Configurations” in the *Tivoli Cross-Site for Security User’s Guide*, if you have not already done so. This chapter provides information about positioning Security agents on your network.

Setting Up a User for the Agent

During the installation of the Security agent, you must supply a user name and password. This user name and password corresponds to a Cross-Site user resource, which is stored in the management repository and displayed on the Cross-Site console. (Refer to the *Cross-Site for Security User's Guide* for information on user resources.) To install the Security agent, the user resource whose name and password you supply must be assigned the **install** role.

Before installing the agent, decide which user resource you want the agent to use. Create a new user resource or use an existing one. You have several options to consider when determining the user resource to use during the agent's installation:

- You can create a unique user resource for each agent. This provides the finest degree of granularity, enabling you to manage each end user's access to data.
- You can create a user resource that can be used by a group of end users to install the agent. This provides less granularity but can be useful if you have a large number of end users that share common responsibilities.
- You can use either the **install** or **admin** user resource, which were created when the management server was installed. You can use these, again, for a group of end users installing the agent. This is the least secure option, but it makes the installation easier because you do not have to create users. Tivoli recommends that you use the **install** user if you choose this installation option.

Remember, though, that the user resource must be assigned the **install** role. The agent uses the user's name and password only once, immediately after the installation, to be authenticated and authorized. The agent is then registered with the management server.

If you choose to use either the **install** or **admin** user, skip the following procedure. To create a new user, complete the following steps:

1. Start the Cross-Site console and log in as the **admin** user.

   To start the console on a Windows NT system, select **Start –> Programs –> Tivoli Cross-Site –> Cross-Site Console**.

   To start the console on AIX, enter the following:

   ```
   base_dir/XSITconsl/bin/xs_console
   ```

   where *base_dir* is the directory in which you installed the console, such as **/usr/Tivoli/XSite**

   To start the console on Solaris, enter the following:

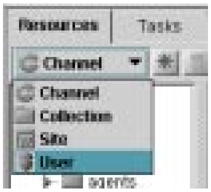
   ```
   base_dir/XSITcons/bin/xs_console
   ```

   where *base_dir* is the directory in which you installed the console, such as **/opt/Tivoli/XSite**.

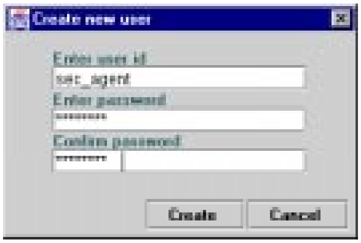
2. Select the **Global** icon at the top of the console to display the Global view.

3. Select the **Resources** tab in the Global view. (This tab is selected by default.)

4. Select **User** from the drop-down list below the **Resources** tab.



5. Click the **New** button, which is to the right of the drop-down list. The **Create new user** dialog is displayed.



Create new user

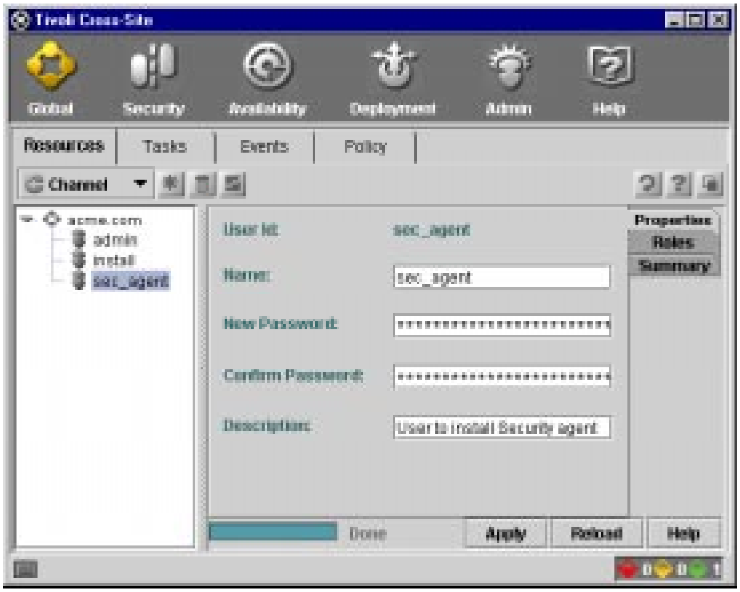
Enter user id: sec_agent

Enter password: ********

Confirm password: ********

6. Enter a name and password for the user and click **Create**. The new user is displayed in the tree, under your server's domain.

7. To change the user's properties, select the **Properties** tab (on the right side of the console).



Tivoli Cross-Site

User Id: sec_agent

Name: sec_agent

New Password: ************************

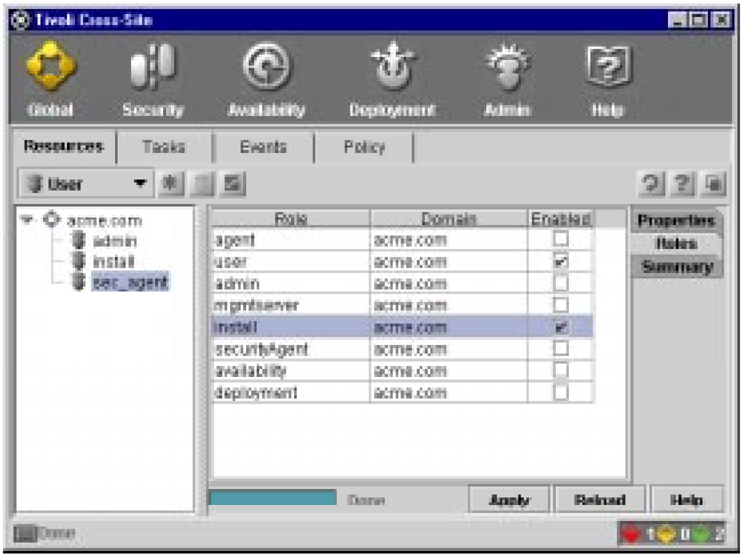
Confirm Password: ************************

Description: User to install Security agent

8. Specify a name, password, and description.

9. Select the **Roles** tab to specify a role for the user.

10. Select the **install** role. The **user** role is selected by default. You can select other roles, but these roles are required to install the Security agent.



Role	Domain	Enabled
agent	acme.com	☐
user	acme.com	☑
admin	acme.com	☐
mgmtserver	acme.com	☐
install	acme.com	☑
securityAgent	acme.com	☐
availability	acme.com	☐
deployment	acme.com	☐

11. Click the **Apply** button to create the user resource.

You can now specify this user when installing the Security agent. See the section regarding users and access control in the *Tivoli Cross-Site for Security User’s Guide* for a full description of users and roles.

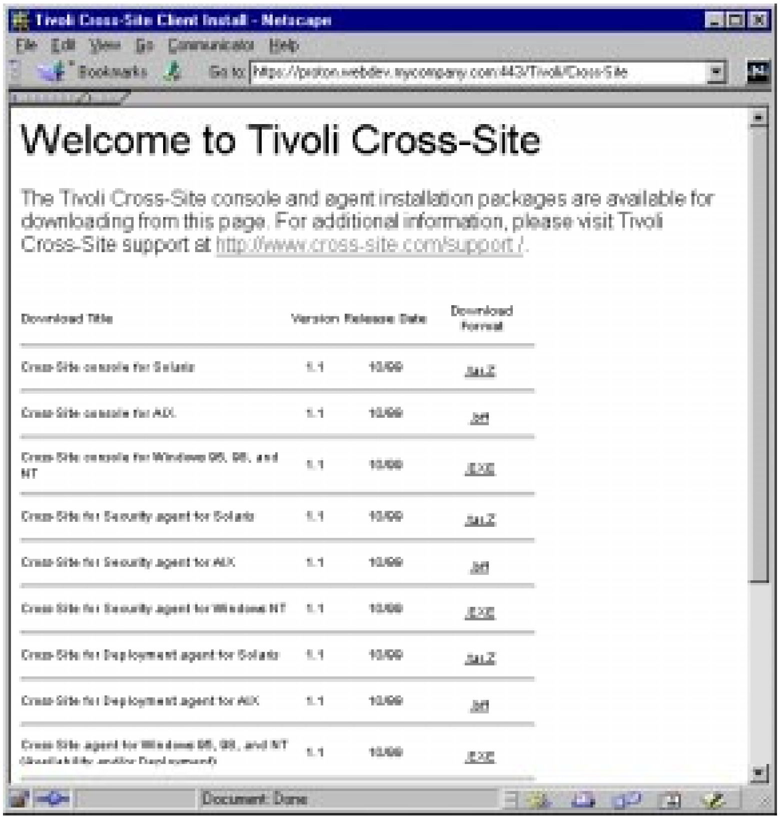
Installing on Windows NT

This procedure runs the **Cross-Site for Security.EXE** installation program, which is located in the **w32-ix86** directory on the Cross-Site CD-ROM. It is also available on the Cross-Site server for downloading. If you wish to install from the CD-ROM, skip to step 4 on page 139. Otherwise, begin with step 1.

Complete the following steps to install the Cross-Site for Security agent on a Windows NT system:

1. Launch a web browser and load the Cross-Site download page. The URL for the page is *protocol*://*Server:Port***/Tivoli/Cross-Site**, where *protocol* is the protocol of the Cross-Site server, *Server* is the name of the Cross-Site server, and *Port* is its port number.

The download page is similar to the following:



Tivoli Cross-Site Client Install - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: https://proton.webdev.mycompany.com/443/Tivoli/Cross-Site
Document: Done

Welcome to Tivoli Cross-Site

The Tivoli Cross-Site console and agent installation packages are available for downloading from this page. For additional information, please visit Tivoli Cross-Site support at http://www.cross-site.com/support/.

Download Title	Version	Release Date	Download Format
Cross-Site console for Solaris	1.1	10/00	.tar.Z
Cross-Site console for AIX	1.1	10/00	.bff
Cross-Site console for Windows 95, 98, and NT	1.1	10/00	.EXE
Cross-Site for Security agent for Solaris	1.1	10/00	.tar.Z
Cross-Site for Security agent for AIX	1.1	10/00	.bff
Cross-Site for Security agent for Windows NT	1.1	10/00	.EXE
Cross-Site for Deployment agent for Solaris	1.1	10/00	.tar.Z
Cross-Site for Deployment agent for AIX	1.1	10/00	.bff
Cross-Site agent for Windows 95, 98, and NT (Availability and/or Deployment)	1.1	10/00	.EXE

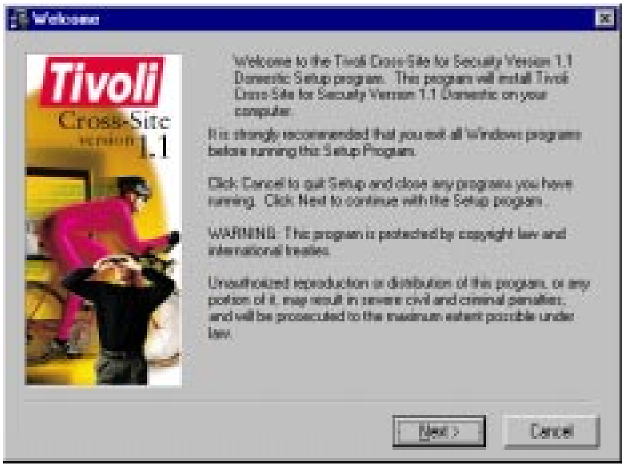
2. Select the **.EXE** link for the Security agent.

3. Choose to save the file and select a location for the **Cross-Site for Security.EXE** file. Keep in mind that this also serves as the program’s staging directory during the installation.

4. Run the installation program. You can run it by selecting **Start –> Run** and entering a path to the **.EXE** file, or you can double-click on the **Cross-Site for Security.EXE** file in the **Explorer** window. You can also run it from the command prompt.

   Note: *You must have Administrator privileges to install the agent.*

The installation program displays a **Welcome** dialog:



Welcome to the Tivoli Cross-Site for Security Version 1.1 Domestic Setup program. This program will install Tivoli Cross-Site for Security Version 1.1 Domestic on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup Program.

Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

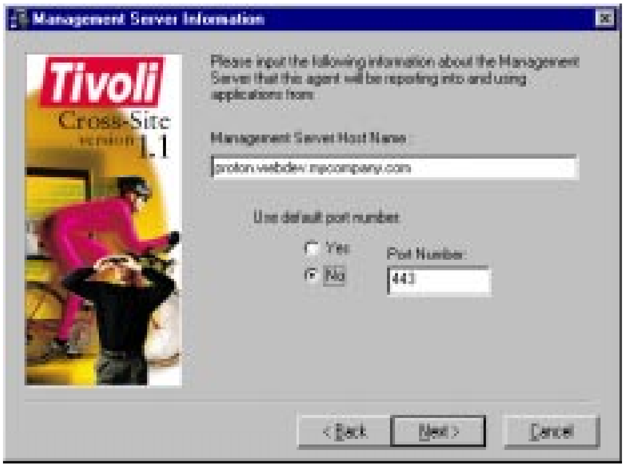
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

5. Click **Next** and follow the instructions on each of the following dialogs:

    a. In the **Tivoli Cross-Site for Security - Domestic/Export License Agreement** dialog, read the license agreement and press **Accept** if you understand and accept the terms of the installation.

    b. In the **Choose Destination Location** dialog, select or browse for a destination folder for the Security agent. By default, the destination directory is **C:\Program Files\Tivoli\Cross-Site for Security**. Click **Next**.

c. In the **Management Server Information** dialog, enter the Cross-Site management server’s host name and specify the server’s port. Click **Next**.



Management Server Information

Please input the following information about the Management Server that this agent will be reporting into and using applications from

Management Server Host Name:

proton.webdev.mycompany.com

Use default port number

○ Yes

● No

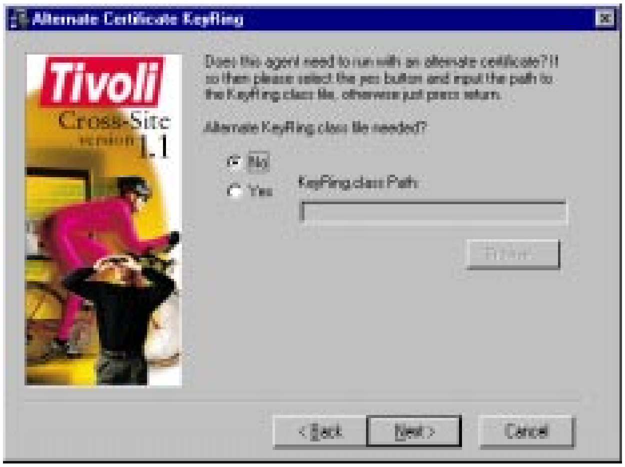
Port Number:

443

d. In the **Provide Agent Name** dialog, enter a name for the agent in the field and click **Next**.

e. In the **Alternate Certificate KeyRing** dialog, if the digital certificate was not issued by one of the supported certification authorities (CAs), select **Yes**. Use the **Browse** button to select a path to the **KeyRing.class** file on the PC where you are installing the agent.

The dialog is similar to the following:



Alternate Certificate KeyRing

Does this agent need to run with an alternate certificate? If so then please select the yes button and input the path to the KeyRing class file, otherwise just press return.

Alternate KeyRing class file needed?

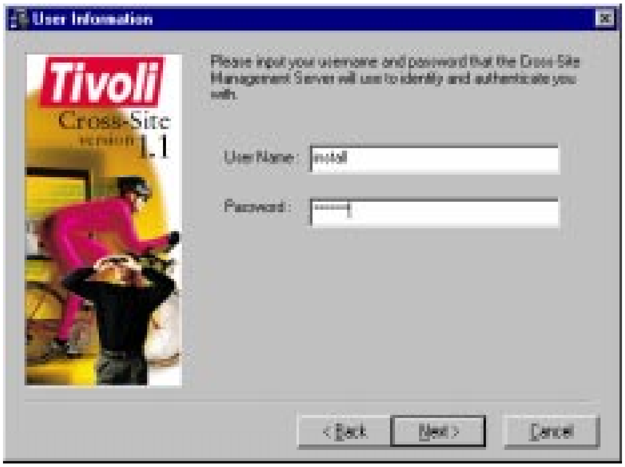
● No

○ Yes

KeyRing class Path:

The installation copies the specified file to the *install_dir***\lib** directory, where *install_dir* is the directory specified in step b on page 140. Click **Next** to continue.

f. In the **User Information** dialog, enter a user name and password that the agent can use to register itself with the server. Click **Next**. “Setting Up a User for the Agent” on page 134 provides more information about this user.



User Information

Please input your username and password that the Cross Site Management Server will use to identify and authenticate you with.

User Name: install

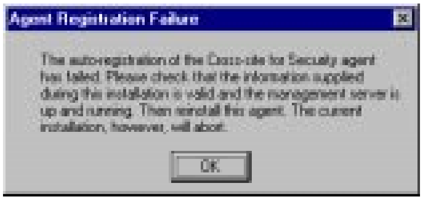
Password: ******

g. In the **Start Installation** dialog, verify your entries and click **Next**.

h. The **Management Server Installation** dialog is displayed. Click **Continue** to finish installing the agent.

i. After the installation finishes, the **Installation Complete** dialog is displayed. If it was installed correctly, the Security agent starts running in the background.

   If the installation program encountered problems, an error message is displayed, which indicates that the agent could not register itself. You may have entered the user name and password incorrectly. Also, ensure that the NT system on which you are installing the Security agent has a static IP address.



The auto-registration of the Cross-site for Security agent has failed. Please check that the information supplied during this installation is valid and the management server is up and running. Then reinstall this agent. The current installation, however, will abort.

To verify that the installation was successful, see “Verifying the Agent’s Installation” on page 154.

When a Cross-Site for Security agent starts, it registers itself with its Cross-Site server as *machine_name* **- Security**. When you run the console, the agent’s icon is displayed in the Global and Security views, on the Resources explorer.

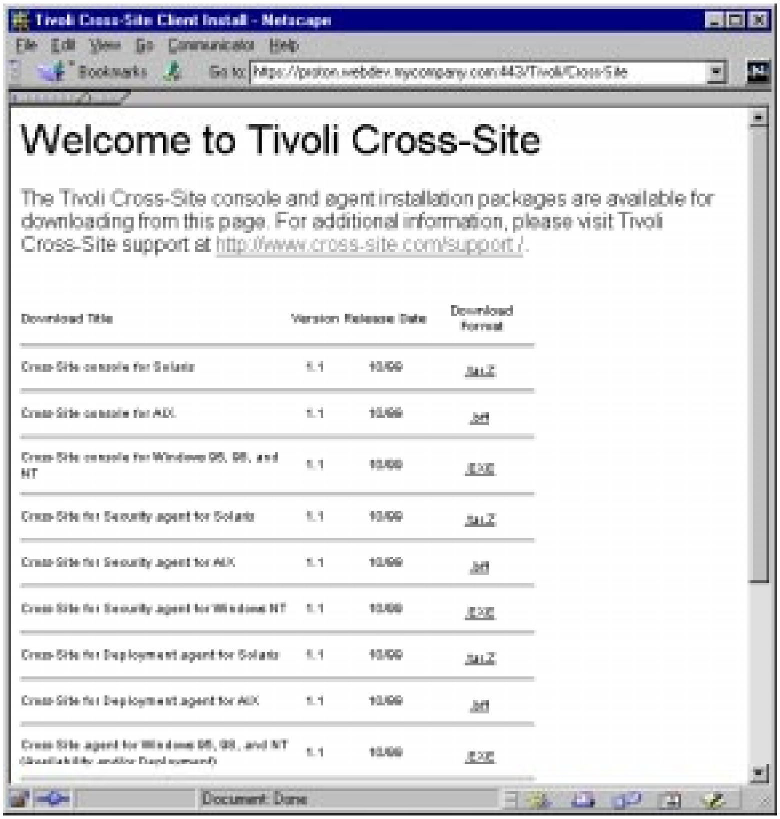
Installing and Configuring on AIX

Before installing the Security agent on an AIX system, ensure that the Java Development Kit (JDK), as described in “Requirements for the Security Agent” on page 129, is installed. You must log in to the system as **root** to run the installation program and have access to the root environment. Tivoli recommends that you log in as **root** instead of using the **su** command.

To install and configure the Security agent on AIX using the System Management Interface Tool (SMIT), complete the following steps. This procedure installs the **xsite.secagent.bff** file. This file can be found in the **aix4-r3** directory on the CD-ROM, and can also be downloaded from the Cross-Site server. If you wish to install from the CD-ROM, skip to step 6 on page 146. Otherwise, begin with step 1.

1. Launch a web browser and load the Cross-Site download page. The URL for the page is *protocol*://*Server:Port***/Tivoli/Cross-Site**, where *protocol* is the protocol of the Cross-Site server, *Server* is the name of the Cross-Site server, and *Port* is its port number.

The download page is similar to the following:



Tivoli Cross-Site Client Install - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: https://proton.webdev.mycompany.com:443/Tivoli/CrossSite
Document: Done

Welcome to Tivoli Cross-Site

The Tivoli Cross-Site console and agent installation packages are available for downloading from this page. For additional information, please visit Tivoli Cross-Site support at http://www.cross-site.com/support/.

Download Title	Version	Release Date	Download Format
Cross-Site console for Solaris	1.1	10/00	.tar.Z
Cross-Site console for AIX	1.1	10/00	.bff
Cross-Site console for Windows 95, 98, and NT	1.1	10/00	.EXE
Cross-Site for Security agent for Solaris	1.1	10/00	.tar.Z
Cross-Site for Security agent for AIX	1.1	10/00	.bff
Cross-Site for Security agent for Windows NT	1.1	10/00	.EXE
Cross-Site for Deployment agent for Solaris	1.1	10/00	.tar.Z
Cross-Site for Deployment agent for AIX	1.1	10/00	.bff
Cross-Site agent for Windows 95, 98, and NT (Availability and/or Deployment)	1.1	10/00	.EXE

2. Create a directory where you can download the agent’s **.bff** file.

   ```
   mkdir /usr/Tivoli/agent
   ```

3. Change to the newly-created directory.

   ```
   cd /usr/Tivoli/agent
   ```

4. Download the **xsite.secagent.bff** file by selecting the **.bff** link on the download page. Save it in the current directory.

5. Create a **.toc** file in the current directory by running the following command:

   ```
   /usr/sbin/inutoc
   ```

6. If installing from CD-ROM, insert the CD-ROM into the drive and mount the drive, as follows:

   ```
   mount -v cdrfs -r /dev/cd0 /mnt
   ```

   where */dev/cd0* is your CD-ROM device and */mnt* is the mount point.

7. Use SMIT to install the file, as follows:

   a. Display the **SMIT Install and Update from Latest Available Software** menu using the following command:

      ```
      /usr/bin/smit install_latest
      ```

   b. In the **INPUT device/directory for software** field, enter one of the following:

      ```
      /mnt/aix4-r3
      ```

      ```
      /usr/Tivoli/agent
      ```

      where */mnt* is the directory where you mounted your CD-ROM and **/usr/Tivoli/agent** is where you downloaded the **.bff** file.

   c. Press **Enter**. The dialog is updated with a new list of entry fields.

   d. In the **SOFTWARE to install** field, select **Tivoli Cross-Site Security Agent**.

      If you wish to change any of the default values for other entry fields on the **Install and Update from Latest Available Software** menu, do so before continuing.

   e. When you are ready to install, press **Enter**. You are prompted with an **ARE YOU SURE** popup dialog. Press **Enter** again to continue with the installation.

After the installation is complete, consult the installation summary at the bottom of your SMIT output to verify that the installation completed successfully. Exit SMIT when you are finished.

8. Configure the Tivoli Cross-Site for Security agent for AIX by using the following command:

   ```
   /usr/Tivoli/XSite/XSITids/idsconfig
   ```

   This command prompts you for configuration information. Answer each prompt with a value, as follows:

   a. `Please enter the Tivoli Cross-Site management server’s hostname:`

      Enter the fully qualified domain name of your Cross-Site server.

   b. `Please enter the port number of the management server:`

      Enter the port number of your Cross-Site server.

   c. `Please enter the login ID for the administrator on the management server:`

      Enter a user ID that has the **install** role. If you enter an invalid user ID, the installation will fail and you will have to remove and reinstall the **XSITids** package.

   d. `Please enter the password for the administrator on the management server:`

      Enter the password for the user. If you enter an invalid password, the installation will fail and you will have to remove and reinstall the **XSITids** package.

   e. `Please re-enter the password:`

      Enter the password again.

f. `Currently the name of the agent is as follows: "machine_name". If you would like the agent to have a different name enter the name below. Otherwise, press Enter.`

   Enter a name for the agent. Press **Enter** if the name listed is sufficient.

g. `Currently the default display that will be used is on host: "machine_name". If you would like the display to appear on a different host, enter the hostname below. Otherwise, press Enter.`

   Enter the name of the system if you are viewing the installation on a remote display. The installation script needs this name to display a dialog after the installation. Before entering the host name here, ensure that you can connect to the host's display.

h. `If there is an alternate KeyRing.class file that should be used for this agent, enter the path to that file below. Otherwise, press Enter.`

   Enter **none** unless you created the **KeyRing.class** file for the unsupported CA prior to this installation. (If you used an unsupported server certificate to secure the web server, you should have created the **KeyRing.class** file as described in "Importing an Unsupported Root Certificate" on page 199.) If you have the file, enter the full path to the directory where it resides.

The configuration script configures the Security agent and registers it with the Cross-Site server. The following message is displayed:

```
Registering the agent with the Cross-Site management
server ... please wait
Registration complete ... the agent is installed.

*** Tivoli Cross-Site for Security started and running
*** connected to management server: server
*** on port number: x
```

To verify that the installation was successful, see “Verifying the Agent’s Installation” on page 154. The agent, by default, is installed in **/usr/Tivoli/XSite/XSITids**.

When the Cross-Site for Security agent starts, it registers itself with its Cross-Site server as *machine_name* **- Security**. When you run the console, the agent’s icon is displayed in the Global and Security views, on the Resources explorer.

Installing on Solaris

Before installing the Security agent on a Solaris system, ensure that the Solaris patches and the Java Development Kit (JDK), as described in “Requirements for the Security Agent” on page 129, are installed.

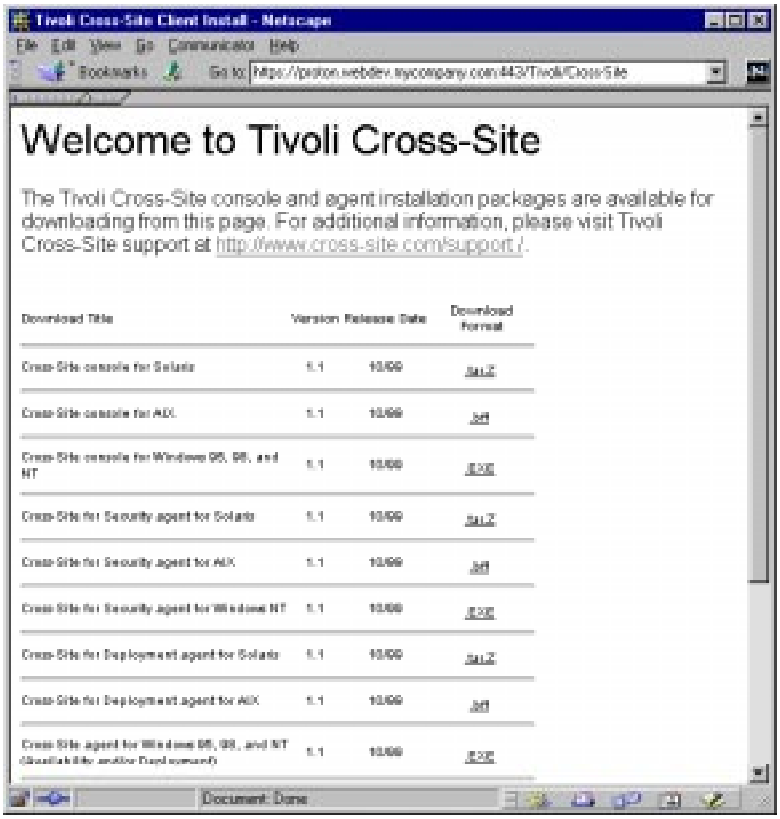
You must log in to the system as **root** to run the installation program. Tivoli recommends that you log in as **root** instead of using the **su** command.

This procedure runs the **pkgadd** command for the **XSITids** package. The **XSiteSecAgtPkg.solaris2.tar.Z** package is located in the **solaris2** directory on the Cross-Site CD-ROM. It is also available on the Cross-Site server for downloading. If you wish to install from the CD-ROM, skip to step 6 on page 151. Otherwise, begin with step 1.

Complete the following steps to install the Cross-Site for Security agent on Solaris:

1. Launch a web browser and load the Cross-Site download page. The URL for the page is *protocol*://*Server:Port***/Tivoli/Cross-Site**, where *protocol* is the protocol of the Cross-Site server, *Server* is the name of the Cross-Site server, and *Port* is its port number.

The download page is similar to the following:


Tivoli Cross-Site Client Install - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: https://proton.webdev.mycompany.com:443/Tivoli/Cross-Site
Document: Done

Welcome to Tivoli Cross-Site

The Tivoli Cross-Site console and agent installation packages are available for downloading from this page. For additional information, please visit Tivoli Cross-Site support at http://www.cross-site.com/support/.

Download Title	Version	Release Date	Download Format
Cross-Site console for Solaris	1.1	10/99	tar.Z
Cross-Site console for AIX	1.1	10/99	.bff
Cross-Site console for Windows 95, 98, and NT	1.1	10/99	.EXE
Cross-Site for Security agent for Solaris	1.1	10/99	tar.Z
Cross-Site for Security agent for AIX	1.1	10/99	.bff
Cross-Site for Security agent for Windows NT	1.1	10/99	.EXE
Cross-Site for Deployment agent for Solaris	1.1	10/99	tar.Z
Cross-Site for Deployment agent for AIX	1.1	10/99	.bff
Cross-Site agent for Windows 95, 98, and NT (Availability and/or Deployment)	1.1	10/99	.EXE

2. Create a directory in which you can download and unpackage the Security agent's installation package.

   ```
   mkdir XSITsec_agt
   ```

3. Change to the newly-created directory.

   ```
   cd XSITsec_agt
   ```

4. On the Cross-Site web page, select the **tar.Z** link for the Security agent.

5. Choose to save the file. Specify to save the **XSiteSecAgtPkg.solaris2.tar.Z** file in the newly created directory.

6. Uncompress the file using the following command. This command strips the **.Z** from the end of the file name.

   ```
   uncompress XSiteSecAgtPkg.solaris2.tar.Z
   ```

7. Unpackage (untar) the **XSiteSecAgtPkg.solaris2.tar** file using the following command:

   ```
   tar xvf XSiteSecAgtPkg.solaris2.tar
   ```

8. Run the **pkgadd** command to install the Security agent, as follows:

   ```
   pkgadd -d ‘pwd‘ XSITids
   ```

   where the **-d** option specifies a temporary staging directory for the installation. This command registers the agent package with Solaris.

9. The script prompts you as follows:

   a.
   ```
   If you would like the software installed in a
   different base directory, enter the directory below.
   Otherwise, press Enter.
   ```

   Specify a directory in which you want to install the Cross-Site for Security agent, or press **Enter** to install it in the default directory. The installation creates a subdirectory named **XSITids** within the directory you specify.

   b.
   ```
   Please enter the Tivoli Cross-Site management
   server’s hostname:
   ```

   Enter the fully-qualified domain name of your Cross-Site server.

   c.
   ```
   Please enter the port number of the management
   server:
   ```

   Enter the port number of your Cross-Site server.

d. `Please enter the login ID for the administrator on the management server:`

Enter a user ID that has the **install** role. If you enter an invalid user ID, the installation will fail and you will have to remove and reinstall the **XSITids** package.

e. `Please enter the password for the administrator on the management server:`

Again, enter the password for the user. If you enter an invalid password, the installation will fail and you will have to remove and reinstall the **XSITids** package.

f. `Reenter the password.`

Reenter the password for the administrator to confirm that you entered it correctly the first time.

g. `If you would like the agent to have a different name, enter the name below. Otherwise, press Enter.`

Enter a name for the agent. Press **Enter** if the name listed is sufficient.

h. `If you would like the display to appear on a different host, enter the hostname below. Otherwise, press Enter.`

Enter the name of the system where you are viewing the installation. The installation script needs this name to display a dialog after the installation. Before entering the host name here, ensure that you can connect to the host’s display. (The DISPLAY variable should be set and you may wish to use the **xhost** command to enable the connection.)

i. `Please enter the installation path for the Sun Java Development Kit (JDK). This should already be installed on the machine and is a prerequisite to run this agent. If the path is something other than /usr/java1.1, enter the path below. Otherwise, press Enter.`

   Enter the path to the JDK directory. By default, the JDK is installed in **/usr/java1.1**.

j. `If there is an alternate KeyRing.class file that should be used for this agent, enter the path to that file below. Otherwise, press Enter.`

   Enter **none** unless you created the **KeyRing.class** file for the unsupported CA prior to this installation. (If you used an unsupported server certificate to secure the web server, you should have created the **KeyRing.class** file as described in “Importing an Unsupported Root Certificate” on page 199.) If you have the file, enter the full path to the directory where it resides.

k. `Do you want to continue with the installation of <XSITids>?`

   Enter **y** to continue with the installation. If you enter **n**, the installation exits. If you enter **?**, Solaris provides you with help.

The installation script installs the Security agent and registers it with the Cross-Site server. The following message is displayed:

```
Registering the agent with the Cross-Site management
server ... please wait
Registration complete ... the agent is installed.

Installation of <XSITids> was successful.
*** Tivoli Cross-Site for Security started and running
*** connected to management server: server
*** on port number: x
```

To verify that the installation was successful, see the following section.

When the Cross-Site for Security agent starts, it registers itself with its Cross-Site server as *machine_name* **- Security**. When you run the console, the agent's icon is displayed in the Global and Security views, on the Resources explorer.

Verifying the Agent's Installation

On all platforms, if the **KeyRing.class** file was used when installing the agent, ensure that it was copied to in the *install_dir***/lib** directory during the agent's installation.

To verify that the installation of a Security agent was successful on Windows NT, review the files listed in the base installation directory, which, by default, is the following:

C:\Program Files\Tivoli\Cross-Site for Security

If the **ids.cfg**, **ids.msg**, and **ids.rules** files are present, the agent was installed correctly and is running.

To confirm that the Security agent is running as a process, complete the following steps. You must be **Administrator** to stop and start the Security agent.

1. Select **Settings –> Control Panel** from the **Start** menu on the system running the Cross-Site agent.

2. Double-click on **Services**.

3. Ensure that the **Tivoli Cross-Site for Security** process is running.

4. If the agent is not running, select **Tivoli Cross-Site for Security** in the list and click the **Start** button.

To start the Security agent on AIX, enter the following commands. You must be **root** to restart the agent.

```
/etc/Tivoli/XSite/XSITids/ids stop

/etc/Tivoli/XSite/XSITids/ids start
```

```
or

/etc/Tivoli/XSite/XSITids/ids restart
```

To start the Security agent on Solaris, enter the following commands. You must be **root** to start the agent.

```
/etc/init.d/ids stop
/etc/init.d/ids start
```

or

```
/etc/init.d/ids restart
```

10

Roadmap to Using Cross-Site

The following steps describe what you need to do to get your Cross-Site management server and agents up and running. They provide an overview of the procedures you will have to perform to use Cross-Site.

1. Tivoli recommends that you change the **admin** and **install** users' passwords, if you have not already done so. When you install Cross-Site, these users (user resources on the console, that is) are created. Changing their passwords provides more security for your system. For information about how to change a user's password, see the section regarding configuring user resources in the user's guide (provided on the CD-ROM and web site) and the online help.

2. Create users for administrators who need to use the Cross-Site console. Assign the **admin** role to each user; administrators who intend to log in to the console must be assigned at least the **admin** role. For more information, see the section regarding configuring user resources in the user's guide and the online help.

3. Configure the event service by specifying the polling interval, the number of events in the event log, and event-forwarding directions. For information about setting the polling interval and configuring the event log, see the section about viewing events on the console. For

information about forwarding events, see the section about managing events. Both of these topics are in the user's guide and the online help.

After installation, the Security agents automatically start monitoring the network. Using the default policy, the agents generate incidents and send critical alerts to the Cross-Site console. You can view the alerts as events on the console or forward them to another administrator for further processing. The following steps describe how to get started with Cross-Site for Security:

1. Create a task to upload alert data from the Security agents. (By default, critical alerts are sent to the console and are displayed as events in the event log.) To view other alerts generated by Security agents, you must create an upload task. This task uploads all the alerts generated by Security incidents to the management server.

2. Evaluate the events generated by the Security agents and decide if you need to alter their policy. You alter policy by editing the Security configuration and rules files. These files are called **ids.cfg** and **ids.rules,** and must be edited manually in a text editor. Use the Policy explorer in the Security view to edit alert messages. Here you determine the priority and text of Security alerts.

3. If you changed a Security agent's policy, reevaluate the current settings based on the events generated.

4. Continue steps 3 and 4 until the management server receives only pertinent events. You may want to create different policies for agents installed in the "demilitarized zone" (DMZ), or the area between firewalls, and agents installed on your intranet.

5. Configure Security agent resources. You can edit the agent name and intrusion detection policy assigned to the agent. You make these changes by selecting the agent you want to configure from the Resources explorer.

When you complete these steps, Cross-Site for Security begins logging incidents based on the intrusion signatures that you have specified. See the *Tivoli Cross-Site for Security User’s Guide* for procedures and conceptual information.

A

Frequently Asked Questions

These frequently asked questions (FAQs) are provided to help clarify any confusing aspects of the Tivoli Cross-Site installation. For the most current FAQs, please visit the Cross-Site support page of FAQs. The URL for the FAQ is as follows:

http://www.cross-site.com/support/faqs/

Customer support and development contributed to the following list, in hopes of addressing common questions and obstacles.

General (Installation)

Is there any particular order I should follow when installing the prerequisite software and the Cross-Site server?

Yes. For best results, install and configure your Netscape server and Java Developer Kit (JDK) first. Then, check your available disk space before installing a Cross-Site management server. For complete information regarding prerequisites and the installation, see “Requirements for the Cross-Site Server.”

What are the system prerequisites for Cross-Site? How much disk space, memory, and CPU power is required for a Cross-Site system?

Cross-Site is an integrated environment composed of hardware, system software, memory disk, and network resources. These requirements must be met to ensure a reliable, fully-operational system.

To answer the question here, the documentation specifies that you need about 300 MB of disk space for the Cross-Site server. You need 256 MB of real memory and 300 MB of swap space.

What does a typical Cross-Site installation look like?

Tivoli has prepared a collection of system overview diagrams to help you get a good idea of the many parts to the Cross-Site suite and how they interact. We suggest that network administrators, system administrators, implementors, and system users study these diagrams carefully in order to understand how the various parts work together. Note, however, that it is impossible to document every possible permutation of a Cross-Site domain. To review the Cross-Site system diagrams, visit the following URL:

http://www.cross-site.com/support

and select the **System Overview** link. Keep the connectivity and system load issues in mind if you are considering alternatives to a typical installation.

Is DNS a requirement for installing and running Cross-Site?

Yes. Cross-Site complements the existing e-business infrastructure, which relies on DNS to provide user-friendly Internet addressing. Attempting to run a collaborative management system on a numeric address scheme in dynamic network environments is theoretically possible. However, it is impractical and unsupported.

Web Server Requirements

Is HTTPS (SSL) a requirement for running Cross-Site?

Yes, but only if you plan to install the Cross-Site for Security application, or if you wish to secure transactions between the Cross-Site server and Cross-Site clients (agents and consoles). This means that the web server must be secure.

Note that you cannot “upgrade” the Cross-Site installation from HTTP to HTTPS. To “upgrade” to HTTPS, you must uninstall your Cross-Site server, enable encryption on your Netscape web server with a secure server certificate and SSL, then reinstall the Cross-Site management server (specifying HTTPS during the installation). You will also have to reinstall your agents. Therefore, before installing Cross-Site, be sure that you will never need a secure web server.

See “All About Certificates” for more information. You can also refer to your Netscape documentation for enabling SSL encryption.

Does the Cross-Site management server have to reside on the same system as the Netscape web server?

Yes. The Cross-Site server relies on the web server for its transactions with clients, such as agents and consoles.

What TCP ports does Cross-Site use?

The Cross-Site management server uses the same HTTP port as your web server (typically 80 for HTTP and 443 for HTTPS). The web server’s port is the only one that needs to be opened on your firewall. The Cross-Site server also uses the following ports:

- 7727 and 5282 for the Channel manager
- 8000 and 4444 for the Certificate manager
- 7717 for the management server’s tuner port
- 9527 for WebSphere’s port

These are internal ports and you do not need to open them on the firewall. When the server needs to “talk” to an agent or console, it uses the web server’s port.

If the Netscape web server stops, does my Cross-Site server continue to run?

No. The Cross-Site management server depends on the Netscape Enterprise server for much of its functionality. It starts and stops with your web server and will not run properly without it. For procedural information about restarting the web server, see the section on restarting the Cross-Site server in the appropriate installation chapter.

RDBMS Requirements

Does the Cross-Site management server have to reside on the same system as the RDBMS?

No. Cross-Site can be configured to connect to a remote RDBMS server listening on a TCP port. The connection must be functional and efficient for the whole system to work, however. You may wish to refer to “RDBMS Requirements” for detailed information.

Where can I find and download the Oracle JDBC drivers?

Visit the Oracle JDBC driver page at the following URL:
http://www.oracle.com/java/jdbc

You can download the drivers here:
http://technet.oracle.com/software/download.htm

You might also want to read the JDBC FAQ, which is provided on this page:
http://www.oracle.com/java/jdbc/faq.htm

Note that there are two types of drivers: thin type 4 and OCI type 2. We recommend that you use the OCI drivers. You must use OCI drivers if you plan to run a secure (SSL) server or the Security agent.

Cross-Site Server Installation

What is the fulfillment server?

The fulfillment server is located at the Tivoli headquarters and provides the most up-to-date installation media (in the form of channels) for the Cross-Site server you are installing. When the management server installation reaches a certain point, it contacts the fulfillment server to download channels that contain the remaining binaries for the server. Your management server is also configured to receive future updates from the fulfillment server.

Note that only the installation for the export version of Cross-Site (outside of US and Canada; 56-bit encryption) will contact the fulfillment server. If you are installing the domestic version of Cross-Site, the installation is performed using only the media provided on the CD-ROM. If you are installing the export version of Cross-Site, ensure that the systems you intend to include in the Cross-Site installation have HTTP and HTTPS connectivity to the Internet. In either case, Tivoli recommends that you install locally, by relying solely on the CD-ROM for the installation.

What is IBM WebSphere and why do I need it?

The IBM WebSphere Application Server (WebSphere) is a Java-based application environment for building, deploying, and managing Internet and intranet applications. It is bundled with the Cross-Site management server and provides the interface between the Cross-Site server and the web server. For more information, visit the following URL:

http://www.software.ibm.com/webservers/appserv/

What is the difference between a local and a remote management server installation?

If you are located in the United States or Canada, or if you qualify for 128-bit encryption outside of the US and Canada, you were shipped the domestic version of the Cross-Site CD-ROM. You must perform a “local” installation; that is, you must install your management server entirely from the CD-ROM media. When prompted during the installation whether to install the local or remote version of Cross-Site, you must enter **local**. If you enter **remote**, the installation will fail.

In general, if you are located outside of the US or Canada, you received the export version of the Cross-Site CD-ROM, which provides 56-bit encryption. You can choose to install Cross-Site remotely. The final binaries will be downloaded from the Tivoli fulfillment server, which is located at Tivoli. (The binaries are downloaded in channels.)

You can choose to enter **local** if you do not want to contact the fulfillment server during the installation, such as if you are installing in a lab environment or if you have a slow connection to the Internet. If you install from the CD-ROM, the management server will download the updates on the fulfillment server the next time they are available.

What is the Key File Password?

The Key File Password is the password for the web server's key file, which secures the server. This password is chosen when you generate a key-pair, which you must supply when purchasing a certificate from a certificate authority (CA). The Key File Password is also needed when you start the (secure) web server. If you are installing a secure Cross-Site server, which is implied if the web server is secure, you must supply the Key File Password during the installation of the Cross-Site server.

For more information, refer to "All About Certificates" on page 173. Or, see the Netscape online help by clicking Help on the Netscape Server Administration UI (in the top right corner). The URL for the Netscape Server Administration UI is as follows:

*protocol***://***server***:***port***/admin-serv/bin/index**

where *protocol*, *server*, and *port* are the values of your web server. Read the section regarding encryption and SSL in the *Netscape Administration Server: Managing Netscape Servers* book.

What is the KeyRing.class file? When do I need to modify it?

If your web server is secured by a certificate that was issued by an unsupported certificate authority (CA), you must add the CA's root certificate to the **KeyRing.class** file. (Unsupported CAs and, therefore, their certificates are not included in Cross-Site's **KeyRing.class** file.) The **KeyRing.class** file is a special control file that contains the names of supported sites and CAs that are trusted and authorized for access.

To edit the **KeyRing.class** file, use the **xs_editkeyring** command that is provided by Cross-Site. This command is located in the management server's **bin** subdirectory and on the Cross-Site CD-ROM. After you create the custom **KeyRing.class** file, it is located in the management server's **lib/local** subdirectory. The command is documented in "Importing an Unsupported Root Certificate" on page 199.

How do I update my license to include another Cross-Site application?

If you wish to install an additional Cross-Site application on an existing Cross-Site server, you must update your license before installing the new application. You then install the new application on the server and clients, and install the new license key. For complete steps to generate a new license key, install it, and restart Cross-Site, see "Regenerating Your License Key" on page 225.

How do I exit Cross-Site (shutdown the Cross-Site server)?

This is covered in each installation chapter for the management server, under restarting the server. Follow those detailed instructions for best results. The following is an overview of shutting down the server:

1. Stop the console by closing its window.
2. Stop all Cross-Site agents by right-clicking on each agent's icon in the system tray and selecting **Exit**.
3. Stop your management server by stopping the web server.

In general, you shutdown and start the Cross-Site server by shutting down and starting the web server.

Certificates

What is a secure server certificate and how do I get one?

A secure server certificate is required to run a secure (HTTPS) web server. The process of obtaining and installing a secure certificate, and of enabling encryption on your web server, is documented in the certificates section in the Netscape server's online help. You can also refer to "All About Certificates" on page 173, which describes certificates, how to obtain them, and lists the supported certificate authorities (CAs).

What types of certificate does Cross-Site use and when does Cross-Site use them?

Cross-Site uses two types of certificates: server certificates and signing certificates. If you are installing Cross-Site for Security or wish to secure transactions (using HTTPS) between the Cross-Site server and clients, you need a server certificate. If you are installing Cross-Site for Deployment and wish to sign channels, you need a signing certificate. Refer to "All About Certificates" on page 173 for complete information on Cross-Site and certificates.

Cross-Site indirectly uses a server certificate for securing the Cross-Site management server. It is an indirect use because the certificate is installed on the web server, which the Cross-Site server relies on for transactions with its clients. A server certificate enables the Cross-Site server and clients to "talk" to each other over a secure (HTTPS) connection.

Cross-Site uses signing certificates to authenticate and sign Cross-Site Deployment channels. You can sign a Deployment channel with a personal, publisher, or signing certificate. You must sign channels that require access to a client machine, such as if the channel copies data to the machine's hard drive.

Can I use the server certificate that was purchased for our Microsoft Internet Information Server (IIS) to secure the Netscape Enterprise Server that is required by Cross-Site?

No. IIS stores its private key, which is part of the secure certificate, in a proprietary format. Though you can use the Microsoft Cryptography API (CAPI) to “extract” the private key from IIS, Netscape does not offer an import facility for private keys. Also, some private keys may be stored and used only in hardware. And the certificate import facility in both IIS and Netscape only accepts the signed public key.

Essentially, there is no way to “migrate” the secure certificate because each web server stores the private key in a proprietary format. You must generate a new private key (on the Netscape server) and purchase a server certificate for the Netscape web server, if you intend to enable SSL on it.

What certificate is my Netscape server using to authenticate itself?

Complete these steps to find out:

1. Log in to the Netscape Server Administration UI, using a web browser. The URL for the Netscape Server Administration UI is as follows:

   *protocol***://***server***:***port***/admin-serv/bin/index**

   where *protocol*, *server*, and *port* are the values of your Netscape Administration server.

2. Click on button that corresponds to the Netscape Enterprise server and your Cross-Site server.

3. Click the **Server Preferences** button at the top of the administration page that is displayed.

4. Select **View Server Settings** in the list of links on the left of the page.

5. Review the technical setting, which describe the active certificate.

The Cross-Site Console

What is the console?

The console is Cross-Site's desktop. It is the user interface where basic operations to manage the Cross-Site environment are performed. The console displays and organizes the resources, policies, tasks, events, and reports of the different Cross-Site applications. It is installed on the management server and can be installed on other systems that meet the requirements. See "Installing and Running the Console" for complete information.

How much memory is required to run the console?

You can run the Cross-Site console on any Windows 95, 98, NT, Solaris, or AIX system with about 30 MB of available memory.

Can I run a console on my laptop and monitor Cross-Site from home or a remote site?

Yes. Provided that your system meets all system requirements and you have established a PPP or SLIP link to your management server, you should be able to run a remote console on a laptop. You can install a remote console on any Windows NT or UNIX machine by downloading the installation executable from the Cross-Site download page.

How do I close the Cross-Site console?

The is no specific "quit" button for the console. Simply close the console's window.

The Agents

What is the base agent?

The Deployment and Availability agents have one part in common, which is called the base agent. When you install an agent on a remote system, you install the base agent. The application component, either Availability or Deployment, is downloaded by the base agent, once its installation completes, from your management server. Providing a base agent is more efficient than duplicating the same code in both agents; the memory required for an agent that provides Availability and Deployment functions is less because of the shared code. (Note that the Security agent does not share this base agent code.)

How much memory does the Cross-Site agent require to run?

You can run the Cross-Site for Availability agent on any Windows 95, 98, or NT system with 40 MB of available memory. You can run the Cross-Site for Deployment agent on any Windows 95, 98, NT, Solaris, or AIX system 25 MB of available memory. You can run the Cross-Site for Security agent with 12 MB of available memory.

Where can I install the Cross-Site agent?

Regarding platforms, you can install the Cross-Site for Availability agent on a Windows 95, 98, or NT machine. You can install the Cross-Site for Deployment agent on a Windows 95, 98, NT, Solaris, or AIX system. You can install the Security agent on Windows NT, Solaris, or AIX system. Of course, all of the client machines on which you intend to install an agent must meet the minimum system requirements.

You can install any Cross-Site agent on a client system within your enterprise or outside of your firewall. Unlike the Tivoli Management Agent (TMA), the agent can communicate with its server outside of the enterprise. The Cross-Site agent receives and transmits information using HTTP, or HTTPS if it is enabled on the management server.

Can I perform a “silent” installation of the Cross-Site agent?

Yes, for all Availability and Deployment agents on Windows 95, 98, and NT. You can create a response file, called **CUSTDATA.INI**, that you can use when installing the agents. (Note that the Security agent’s installation does not support this feature.) For more information, see the section about creating a response file in the agent chapter.

Can one agent connect to multiple management servers?

Yes and no. If Cross-Site for Deployment is installed and you created a foreign domain and role on the management server to represent a foreign server, a Deployment agent can connect to the foreign domain and download channels. However, all Cross-Site agents are registered and controlled by the management server that was specified when they were installed. The agent sends and receives information only to and from that management server.

For more information on foreign domains and enabling Deployment agents to access foreign channels, see the section about managing foreign roles in the *Cross-Site for Deployment User’s Guide* or the online help.

B

All About Certificates

A digital certificate, or *certificate*, is a digital document obtained from a *certificate authority (CA)*. A certificate enables you to sign, or encrypt, data. For example, you can install a server certificate on a web server, to enable Secure Sockets Layer (SSL). That certificate enables the web server to encrypt, or secure, transactions to clients (such as web browsers). A certificate contains the following data, which is encrypted:

- The owner’s name, company (if applicable), and address
- The owner’s public key
- The certificate’s serial number
- The validity dates for the certificate (indicating when the certificate will expire)
- The certificate authority’s public key
- The certificate authority’s digital signature

A certificate authority is a trusted, third-party organization that issues and signs certificates. When you request a certificate from a CA, the CA authenticates your identity and the services that you are authorized to use. It also issues and renews certificates, and revokes certificates belonging to users who are no longer authorized to use them. A certificate authority signs certificates that it issues with its root certificate. This signifies that, because the CA is a trusted organization, the certificate that it issued (and its holder) can also be trusted.

This document provides an overview of certificates and how Cross-Site uses them. It also provides the procedures you need to perform to obtain and use certificates with Cross-Site. In short, if you are installing Cross-Site and wish to secure the transactions between the server and clients, you need a server certificate. If you are installing Cross-Site for Deployment, you may need a signing certificate. Review this document for all of the details.

An Overview of Keys and Certificates

As mentioned above, a certificate contains the public key of the owner and the CA. Keys are used to enable encryption. Two keys are used: a *public key* and a *private key*. You create this pair of keys using the web server. Specifically, you generate a key-pair file, which contains the private and public key. The private key remains on the server, and the server sends the public key to requesting clients. When the server sends data to a client, the server first uses its private key to encrypt the data. When the client receives the data, it uses the public key to decrypt the message. For example, if the web server sends data to a web browser, it encrypts the data with its private key. When the browser receives the data, it decrypts the data with the public key.

Keys are also used when generating certificates. If you wish to obtain a server certificate, you first generate a key-pair. You then generate a certificate signing request (CSR), which contains the public key (from the key-pair) and the name of your organization. You then send the CSR to the CA from which you are requesting the certificate. The CA signs your public key with their private key, which it includes along with the signature in the certificate. The certificate also includes other information about your organization.

The following are the high-level steps that describe how servers and clients use certificates and keys:

1. A client connects to the server, requesting data.

2. The server digitally signs its certificate and sends it to the client. The server signs the certificate using its private key.

3. Using the public key included in the certificate, the client verifies that the owner of the certificate is the same one who signed it.

4. If the client “knows” the certificate’s CA, it accepts the certificate. If not, the client informs its user that the certificate was issued by an unknown CA and gives the user the choice to accept or refuse the connection.

5. The client compares the information in the certificate to the information it just received about the server. If all the information matches, the client accepts the site as authenticated, or trusted.

These steps outline server authentication. Client authentication is very similar. You can obtain a client-side certificate that you can use for signing content, such as e-mail. Once the certificate is installed on the client, the client sends the certificate to the server in a transaction. Using the client’s public key that is included in the certificate, the server verifies that the owner of the certificate is the same as the sender. If it is, the client is authenticated to the server.

As an overview, certificates are used for the following reasons:

- To verify that the owner is truly the entity identifying itself in a transaction. Certificates are used to digitally sign a message so that the recipient knows that a message really came from the sender.

- To ensure the integrity of the message sent in the transaction. A certificate encrypts the message so that the intended recipient can decrypt and read the message contents and attachments. A certificate also guarantees that the content of the message and the transaction were protected from tampering, impersonation, and eavesdropping while en route to the recipient.

- To establish a trust relationship between the sender and the recipient. Each party in the transaction must hold a key-pair file. A key-pair file contains the private and public keys. Those keys were used in creating the certificate and are used to encrypt and decrypt messages that are signed with the certificate.

Cross-Site uses certificates for two purposes: to secure transactions between the Cross-Site server and its clients, and to sign Cross-Site for Deployment channels. See “Cross-Site and Certificates” on page 179 for more information.

The Types of Certificates

Certificate authorities offer an array of certificates. In general, you can use a certificate for any of the following purposes:

- To secure web transactions between web servers and web browsers. These transactions are secured through the following measures:
    - Web server authentication and content confidentiality, by enabling Secure Socket Layer (SSL) and Transport Layer Security transactions
    - Browser (client-side) authentication and secure form submissions using a client-side certificate (the certificates are implemented in the browsers)
    - Digital signature verification of distributed code, such as signed applets, ActiveX components, and so on
- To secure e-mail, as implemented by QUALCOMM Eudora, Netscape Messenger, Microsoft Outlook, and other Simple Mail Transfer Protocol (SMTP) servers.
- To secure online financial settlements and Secure Electronic Transactions (SET).
- To secure networks, virtual private networks (VPNs), IP Security Protocol (IPSEC), IPv6, and products such as Point-to-Point

Tunneling Protocol (PPTP), Windows 2000, Network Associates, Data Fellows, and so on.

- To secure custom applications, such as Entrust PKI-based applications, Baltimore PKI-based applications, E-Lock, or any public key infrastructure (PKI) vendor that offers an API toolkit.

You can purchase different types of certificates based on your needs. The following list describes the certificates you can purchase from a CA:

ConsoleRoot certificate

Identifies a certification authority as an issuer of certificates. These are often self-signed and are used to validate other kinds of certificates. A CA may use different root certificates for different certificate applications to signify that different criteria were used to approve different certificates. Often, “root certificate” and “root authority” are used synonymously.

Server certificate

Identifies a server and includes a digitally signed version of the server’s public key, Internet host name, the name of the organization that owns the server, and the public key of the issuing certification authority. Use a server certificate to secure a web server, by enabling SSL. This certificate validates the server to the client and establishes an encrypted session with the client. A server certificate is sometimes referred to as a site certificate or an SSL certificate.

Personal certificate

Identifies a person and includes a digitally signed version of the person’s name, organization, and public key. These certificates come in a variety of security levels based on the security policy used to obtain them. The level of trust granted to a certificate varies by the security policy of each secure server.

Software publisher certificate

Identifies a software developer and includes a digitally signed version of his or her name, organization, and public key within the code. A developer uses this certificate to sign a software application for Internet distribution.

Content signing certificate

Identifies the owner of the content and includes a digitally signed version of the owner's name, organization, and public key in the content. Use this certificate to sign content that is distributed, such as channels. This certificate authenticates the owner of the content to the end user who subscribes to the content.

In addition to the different types of certificates, certificate authorities issue different levels of certificates based on how thoroughly they investigate the requestor. While the name of the security levels can vary among CAs, the purpose and function of levels is the same. For example, VeriSign's certificate levels are as follows.

Class 1 VeriSign checks to see that the user can receive e-mail at the given address and that no other certificate has been issued for that e-mail address.

Class 2 VeriSign checks a user's identity by checking personal information against information stored in online databases.

Class 3 VeriSign validates the identity of the user who is applying for the certificate by using background checks and investigative services.

Class 4 VeriSign validates the user's identity though a stringent investigation and, sometimes, a personal interview.

Cross-Site supports a variety of certificate types and levels. See "Supported Server Certificates" on page 182 and "Supported Signing Certificates" on page 206 for more information.

Cross-Site and Certificates

Cross-Site indirectly uses a server certificate for securing the Cross-Site management server. It is an indirect use because the certificate is installed on the web server, which the Cross-Site server relies on for transactions with its clients. The server certificate enables you to “turn on” SSL encryption, thereby implementing HTTPS as the transaction protocol. Therefore, a server certificate enables the Cross-Site server and clients to “talk” to each other over a secure connection.

The section below describes server certificates a bit further and outlines the certificates that are supported. It also provides procedures for obtaining and installing a server certificate.

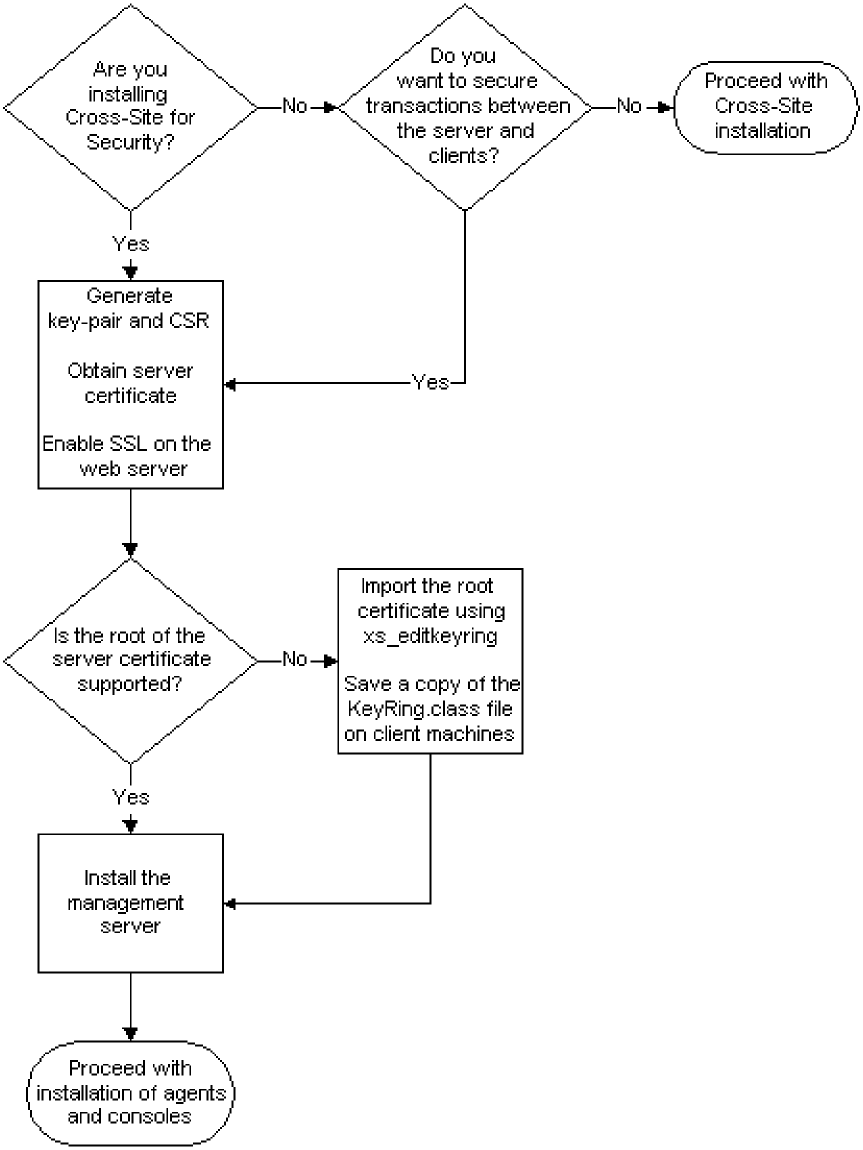
Cross-Site also uses certificates to authenticate and sign channels. You can sign a Cross-Site for Deployment channel with a personal, publisher, or content signing certificate. You must sign channels that require access to a client machine, such as if the channel copies data to the machine’s hard drive. See “Obtaining a Signing Certificate” on page 203 for a list of supported certificates, procedures for obtaining signing certificates, and procedures for importing them into Cross-Site.

Obtaining a Server Certificate

A server certificate is issued by a certificate authority (CA) and signed by a root certificate. The server certificate identifies the web server on which it is installed. It includes an encrypted version of the server’s public key, Internet host name, the name of the organization that owns the server, and the public key of the issuing certification authority. Use a server certificate to enable SSL on a web server, thereby securing transactions to and from the web server, using the HTTPS protocol. Server certificates are also referred to as site certificates and SSL certificates.

If you intend to install Cross-Site for Security, or if you want to enable SSL so that transactions between the Cross-Site server and clients (consoles and agents) are secure, you must obtain a server certificate. You can obtain a server certificate from a commercial vendor or in-house certificate source. After obtaining the server certificate, install it on the Netscape Enterprise Server (NES) before installing Cross-Site.

The following flowchart provides a decision tree to help you determine the steps you need to take to obtain and install a server certificate. Each of the actions listed in the boxes corresponds to a procedure included in this section.


Are you installing Cross-Site for Security?
No
Do you want to secure transactions between the server and clients?
No
Proceed with Cross-Site installation
Yes
Generate key-pair and CSR
Obtain server certificate
Enable SSL on the web server
Yes
Is the root of the server certificate supported?
No
Import the root certificate using xs_editkeyring
Save a copy of the KeyRing.class file on client machines
Yes
Install the management server
Proceed with installation of agents and consoles

All About Certificates

This section demonstrates how you can use the Netscape Enterprise Server, version 3.6, which must be installed before beginning any of the procedures. Netscape Communicator, version 4.5, is also used. These products are used because the Cross-Site server must be installed with a Netscape server. Therefore, it makes sense to demonstrate the Netscape products because, on the server, they are readily available. In “Generating an In-house Server Certificate” on page 194, the Microsoft Certificate Server is used to illustrate generating a certificate. This product was chosen because it is commonly used in e-business environments. Please note, however, that this section provides examples and you are free to use any software, unless a particular product is needed, such as NES. Refer to the Cross-Site release notes for supported products and their versions.

Supported Server Certificates

The following list provides the root certificates that Cross-Site supports for issuing server certificates:

- AT&T Certificate Services
- AT&T Directory Services
- BBN Certificate Services
- BelSign Secure Server CA
- Entrust PKI Demonstration Certificates
- GTE CyberTrust Trial Root
- GTE CyberTrust Global Root
- GTE CyberTrust Root
- GTE SureServer CA
- IBM World Registry
- Keywitness Canada Inc.
- Microsoft Root Authority
- Thawte Server CA

- Thawte Premium Server CA
- VeriSign Commercial Certificate Authority, RSA Data Security, Inc.
- VeriSign Secure Server CA, RSA Data Security, Inc.
- VeriSign Test Secure Server ID (TestCPS)
- VeriSign OnSite for Server Certificates

If you have a server certificate that was issued by any of these root certificates, you can use that server certificate to secure the Netscape server that the Cross-Site server uses. However, not all of these root certificates provide server certificates to the general public.

If you need to purchase a server certificate to secure the Cross-Site server, choose from the following list of CAs and their products. If you choose to download a test (or trial) certificate, be aware that it will expire sooner than a purchased certificate. Tivoli recommends that you use test certificates in a lab or test environment only. Also, if your company uses Microsoft Internet Information Server (IIS) and you purchased a server certificate for IIS, you cannot use the same server certificate for Netscape Enterprise Server (NES), which Cross-Site requires. You must purchase another server certificate to secure NES.

You can purchase any one of the following certificate products to install on NES, for use with Cross-Site. If you are an international customer, verify with the certificate vendor that you can purchase any of these certificates.

- BelSign Secure Server Certificate
  http://www.belsign.be/en/services/webmaster/index.html
- Entrust PKI Demonstration Certificate
  http://freecerts.entrust.com/webcerts/index.htm or
  http://freecerts.entrust.com/webcerts/ag_server_req.htm
- GTE CyberTrust
  - SureServer Certificate
    http://www.cybertrust.com/cybertrust/products_services/products/sureserver/buy.html

    - SureServer Test Certificate
      http://www.cybertrust.com/cybertrust/products_services/products/sureserver/test_cert.html

- Thawte SSL Server Certificate
  http://www.thawte.com/certs/server/contents.html

- VeriSign, Inc.

    - Secure Site
      http://www.verisign.com/server/ or
      http://digitalid.verisign.com/server/enrollIntro.htm

    - Secure Site Plus
      http://www.verisign.com/server/ or
      http://digitalid.verisign.com/server/enrollIntro.htm

    - Global Site
      http://www.verisign.com/server/ or
      http://www.verisign.com/server/prd/preq.html

    - Global Site Plus
      http://www.verisign.com/server/ or
      http://www.verisign.com/server/prd/preq.html

    - Test Secure Server ID
      http://digitalid.verisign.com/server/trial/index.html

In addition to these server certificates, you can use a server certificate that is generated using an in-house certificate server. See “Generating an In-house Server Certificate” on page 194 for instructions.

Generating a Key-pair File

In public-key encryption, you use two keys: the public key and the private key. If the public key encrypts a message, the private key must be used to decrypt it. To obtain a set of private and public keys, you must generate a key-pair. A key-pair file contains both the public and private keys of the web server. You use the key-pair file when you request and install a certificate.

This procedure demonstrates the steps to generate a key-pair in the following environment:

- On a Netscape Enterprise Server (NES), version 3.6, that is installed on a Solaris system named avocado. This is also the server on which the Cross-Site server will be installed.
- Using Netscape Communicator, version 4.5, on a Windows NT 4.0 machine. (If you use another browser, the steps may vary.)
- Using a telnet session to avocado.noontide.com (the machine on which the Netscape server is installed).

Also, to help you better understand the steps in obtaining and installing a server certificate, a fictitious company called NoonTide is used to provide a scenario for the procedures. NoonTide develops, markets, and sells electronic products. They have many organizational departments, one of which is Web Development. One of the web administrators at NoonTide, Harper Smith, will install and use Cross-Site to monitor the NoonTide web site, as well as partner sites.

Complete the following steps to generate a key-pair file, which you can use to request or generate a root certificate.

1. Log on to the Netscape Enterprise Server, as follows:

   ```
   telnet avocado.noontide.com
   ```

   Once logged in, you may need to log in as **root** (on UNIX only). The directory in which the key-pair is saved is owned and writable by **root**.

2. Change to the **/data/app/netscape/suitespot/bin/admin/admin/bin** directory, where **/data/app** is the root directory of the Netscape server.

3. Enter the following command to run the **sec-key** utility:

   ```
   ./sec-key
   ```

If NES is installed on an NT system, run the **sec-key.exe** command from the Command Prompt or by double-clicking on its icon. The command on NT is located in the same directory as on UNIX.

4. Answer each prompt. The prompts are as follows:

   a.
   ```
   ---------------------------------------------------
   |       Netscape Communications Corporation       |
   |           Key Pair File Generation              |
   ---------------------------------------------------

   This program generates a key-pair file that your
   servers use in encrypted communications. The
   key-pair file is also needed when requesting a
   certificate.

   Enter a unique alias to use as part of the file name
   for the key-pair file. An alias can have any
   characters except white space. For example, if the
   alias is ‘mail’, then the key-pair file name is
   mail-key.db. This file is stored in the directory
   <server-root>/alias.

   Alias: avocado
   ```

   Enter an alias for the key-pair file. Tivoli recommends that you enter the name of your Cross-Site server. Do not use spaces in the alias name. You can use symbols that your operating system allows in file names (such as underscores). By default, the key-pair file is stored in *NES_install_dir*<b>/netscape/suitespot/alias/</b>*alias*<b>-key.db</b>, where *alias* is the alias you enter here.

   b.
   ```
   The key-pair will be placed in
   /data/app/netscape/suitespot/alias/avocado-key.db.
   Press enter to continue:
   ```

   Simply press the **Enter** key.

c.

```
To create a key-pair file, this program needs to
generate a random number. One of the easiest ways to
create a random number is to count the amount of time
between keystrokes on a keyboard.

To begin, type keys on the keyboard until this
program meter is full. DO NOT USE THE AUTOREPEAT
FUNCTION ON YOUR KEYBOARD!

|-
Continue typing until the progress meter is full:
```

Type randomly at different speeds until the progress meter is full. The time between each keystroke is used to generate a random number for the unique key-pair file.

```
|************************************************|
Continue typing until the progress meter is full:
Great! Press enter to continue:
```

Press the **Enter** key.

d.

```
The random number generated successfully. Enter a
for the key-pair file. You need to enter this  when
starting or stopping your server.

The  must be at least 8 characters long, and must
contain at least one non-alphabetic character.

:
```

Enter a comprised of eight or more alphanumeric characters. The must have at least one non-alphabetical character. For the **avocado** key-pair, enter the **2clever4you**.

Note: *Memorize or make note of this ! You will need this when enabling SSL on the web server, when logging in to the web server once SSL is enabled, and when installing the Cross-Site server.*

e. `Re-enter the  for verification:`

Enter the again.

If the key-pair file was successfully generated, your new key-pair is saved as *alias***-key.db**, in the *NES_install_dir***/netscape/suitespot/alias** directory. The key-pair file must reside in this directory in order for NES to use it. In this example, the **avocado-key.db** file was saved to the **/data/app/netscape/suitespot/alias** directory.

5. Change the owner of the *alias***-key.db** file to the NES user. Use the following command to change the owner to the NES user for the **avocado-key.db** file on the Solaris system. On avocado, the NES user's ID is **xsite**.

```
chown xsite avocado-key.db
```

The key-pair file resides on the web server where it was generated, and the private key is encrypted using the you specified when generating it.

Generating a Certificate Signing Request

No matter if you are purchasing a server certificate or generating one using an in-house certificate server, you must generate a certificate signing request (CSR). A CSR is an encrypted file that contains your organization's public key, name, locality, and URL. You generate a CSR on the web server. You then send the CSR to the certificate authority, which signs your public key with their private key.

This procedure demonstrates how Harper Smith, the NoonTide web administrator, can generate a CSR in NoonTide's environment:

■ On a Netscape Enterprise Server (NES), version 3.6, that is installed on a Solaris system and named avocado.

■ Using Netscape Communicator, version 4.5, on a Windows NT 4.0 machine. (If you use another browser, the steps may vary.)

To generate the CSR in this example environment, complete the following steps:

1. Go to the Netscape Server Administration page, using a web browser. The URL for the Netscape Server Administration UI on avocado is as follows:

   http://avocado.noontide.com:9344/admin-serv/bin/index

2. Click the **Keys & Certificates** button.

3. Click **Request Certificate** in the left-hand column of the page.

4. Complete the **Request a Server Certificate** form as follows:

   a. Click the **New certificate** option.

   b. Under **Submit to Certificate Authority via**, click either option and fill the field in accordingly. If the CA enables you to submit the certificate request automatically, the CA may post the e-mail address or URL on its home or services page. If the CA does not accept requests through e-mail or as a URL, send the certificate request to yourself. You can later copy and paste the request when purchasing or generating a certificate.

      In this example, choose the **CA Email Address** option and enter **harper.smith@web_dev.noontide.com**. Harper will copy and paste the certificate request when obtaining the certificate.

   c. Select **avocado** from the **Alias** pull-down list. This was the alias used to create the key-pair.

   d. In the **Key Pair File** field, enter the specified when creating the key-pair, which was **2clever4you**.

   e. Fill in the **Requestor name** and **Telephone number** fields with your contact information.

f. In the **Common name** field, enter the fully qualified domain name for the server. For avocado, enter **avocado.noontide.com**.

g. Fill in the **Email address**, **Organization**, **Organizational Unit**, **Locality**, **State or Province**, and **Country** fields appropriately.

h. Click **OK** to submit the information and generate the certificate request.

The certificate request is then displayed in your browser. It is also sent to the e-mail address specified in the **Email address** field.

Purchasing a Server Certificate

You can purchase a server certificate from a CA to enable SSL encryption on the Netscape Enterprise Server, thus securing it. The most common method of purchasing a certificate is using the CA's web site. The following procedure demonstrates the general steps for purchasing a server certificate from VeriSign, Inc. Use this procedure to get an idea of the steps you perform to purchase a server certificate from any of the supported vendors. All of the CA's procedures are very similar. For a complete list of server certificates that Cross-Site supports, see "Supported Server Certificates" on page 182.

Before beginning the procedure to purchase a certificate, gather the following information. You will be prompted for it.

- The certificate signing request (CSR). To generate a CSR, you must first generate a key-pair, as documented on page 184. Then, you can generate a CSR, as documented on page 188.

- Your organization's D-U-N-S number. You must submit documentation that demonstrates your right to use the corporate name specified in the request. The D-U-N-S number is an internationally recognized, company identifier that is provided by Dun & Bradstreet. The following URL enables you to obtain this information:

  https://www.dnb.com/product/eupdate/update.htm

If you are located outside of the United States, use the following URL instead of the first one listed above:

http://www.dnb.com/global/menu.htm

- Your company's registered domain name. The following URL enables you to verify that your company's domain name is registered:

  http://www.networksolutions.com/cgi-bin/whois/whois

  If your domain name is not registered, you must register it before proceeding with obtaining a server certificate. You can purchase a domain name by entering the following URL in the browser:

  http://www.networksolutions.com/purchase/

- The technical contact's name, address, e-mail address, phone number, and title. Presumably, this information is yours but if you are not the technical contact, collect this information.
- The billing contact's name, address, e-mail address, phone number, and title. This contact is the person responsible for payment, such as your organization's accountant or a financial support representative. This person is also responsible for notifying the certificate authority of any billing changes.
- The type of server certificate you wish to purchase from the CA. For example, VeriSign offers the Secure Server, Secure Server Plus, Global Server, and Global Server Plus products. Cross-Site supports all of these. Decide which certificate, and the services offered with it, best fits your needs.
- The payment information. If you choose to pay with a credit card, you will need the card type, number, expiration date, and name on the card. VeriSign also allows you to pay by purchase order, check, and wire transfer. Obtain the payment information.

The following steps illustrate how Harper Smith can purchase a server certificate from VeriSign, Inc., using Netscape Communicator, version 4.5. (If you use another browser, the steps may vary.) Recall that Harper is the web administrator for NoonTide, which is a fictitious company provided to create a scenario that you can follow through the procedures. The VeriSign enrollment process gives you the option to use a wizard to purchase a server certificate. These steps follow the standard process, to illustrate what you need to do without a wizard's assistance.

1. Go to the VeriSign product page by entering the following URL in the browser:

   http://www.verisign.com/products/index.html

2. Click the **Server IDs** link. The **Web Site Security** page is displayed.

3. Click the **Buy Now** button next for the Secure Site (Standard SSL) product.

4. Review the prerequisites before beginning the enrollment process. Namely, ensure that you can connect to a secure server outside of your firewall. You must also have the Netscape server installed before beginning.

5. Copy and paste the CSR on the appropriate VeriSign enrollment page. (See "Generating a Certificate Signing Request" on page 188 if you have not generated a CSR.) When you generate the CSR, it is displayed in the web browser, by highlighting it and pressing **Ctrl**+**C**. The following is an example of what you should copy:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgY4xCzAJBgNVBAYTAlVTMQ4wDAYDVQQI
EwVUZXhhczEPMA0GA1UEBxMGXVzdGluMR0wGwYDVQQKEx
RUaXZvbGkgU3lzdGVtcywgSW5jLjEbMBkGA1UECxMSQ3Jvc3Mt
c2l0ZSBTdXBwb3J0MSIwIAYDVQQDExlzaWxseWdvb3NlLmRldi5
0aXZvbGkuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
BgQDsWMvy9ECFzR7aoqeLzDzhjL5LLjvL7vC3G2jwfTWm65VCE
gcBUss0YxOYI28gG9vhmXUwDfsUYBnNbI0GoqI4lBhOZBnAqpml
BtYEW65MkIGIbUQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYE
AP2CD3f52oB4ieWAQi8PEk7Op65v+xAECvEr4woILH/1jG/8DolDv
HR5XWfzyIwA/Z4CrcK7tHMenFgHQHXg58GdwfIwM7or7iZ2Uax6h
cutamQvzo8IadTxn2M69+sqHWZgB/xBLM6OITufwz6SDlBVPPII=
-----END NEW CERTIFICATE REQUEST-----
```

Note: *You must include the -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST----- lines when copying the key.*

Paste the CSR by pressing **Ctrl**+**V**.

6. Complete the certificate application, which includes these steps:

   a. Verify your company's information. The information was extracted from the CSR. If any of this information is incorrect, you must generate and submit a new CSR that contains the correct information.

   b. Select **Netscape** as the vendor of your web server.

   c. Enter your contact information if you are the technical contact. If not, enter the name and information for the technical contact.

   d. Enter the contact information of the person in your organization who is responsible for the server ID, such as your manager, and for payment.

   e. Enter the credit card information to which the purchase will be charged. Often, you can also choose to use a purchase order, pay by check, or pay by wire transfer.

   f. Enter your D-U-N-S number.

   g. Read and accept the purchasing agreement.

7. Wait to receive your server ID. VeriSign will send you a signed certificate file, which contains the information you need to secure your Netscape Enterprise Server. Other certificate vendors might deliver your server ID by e-mail or courier.

8. When you receive the server ID, install it on the Netscape server. See "Enabling SSL Encryption on the Web Server" on page 196 for instructions.

Tivoli recommends that you back up the key-pair file and certificate and store the backups in a secure location.

Generating an In-house Server Certificate

Instead of purchasing a certificate, you can use a certificate server to generate one. Often, large companies or companies that deploy web applications have installed an in-house certificate server as an inexpensive and easily accessible way to obtain certificates. If your company has its own certificate server (and is, therefore, its own CA), you can request a certificate from the department that runs the certificate server. Or, if you have access to the server, you can generate a server certificate.

This procedure demonstrates how Harper Smith can generate a secure certificate in the following environment:

- Using Netscape Communicator, version 4.5, on a Windows NT 4.0 machine. (If you use another browser, the steps may vary.)
- Using the Microsoft Certificate Server on an NT machine named diamond.

Recall that Harper is the web administrator for NoonTide, which is a fictitious company provided to create a scenario that you can follow through the procedures.

In addition to the Microsoft Certificate Server, you can use another vendor’s certificate server to generate in-house certificates. See “References” on page 222 for a list of public key infrastructure (PKI) vendors, though the list is not comprehensive.

To generate the certificate, complete the following steps:

1. Generate a key-pair, as described in “Generating a Key-pair File” on page 184.
2. Generate a CSR, as documented in “Generating a Certificate Signing Request” on page 188.

   The certificate request key is then displayed in your browser. It is also sent to the e-mail address specified in the **Email address** field.

3. Copy the CSR, which is displayed in the web browser, by highlighting it and pressing **Ctrl**+**C**. The following is an example of what you should copy:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgY4xCzAJBgNVBAYTAlVTMQ4wDAYDVQQI
EwVUZXhhczEPMA0GA1UEBxMGXVzdGluMR0wGwYDVQQKEx
RUaXZvbGkgU3lzdGVtcywgSW5jLjEbMBkGA1UECxMSQ3Jvc3Mt
c2l0ZSBTdXBwb3J0MSIwIAYDVQQDExlzaWxseWdvb3NlLmRldi5
0aXZvbGkuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
BgQDsWMvy9ECFzR7aoqeLzDzhjL5LLjvL7vC3G2jwfTYNdWkusT
WDUfrLmzKfw9Gk9tTEoC+t+VyqjakDzN5hHCWjdtumlWo3gAQzg
Wm65VCEgcBUss0YxOYI28gG9vhmXUwDfsUYBnNbI0GoqI4lBhO
ZBnAqpmlBtYEW65MkIGIbUQIDAQABoAAwDQYJKoZIhvcNAQEE
BQADgYEAP2CD3f52oB4ieWAQi8PEk7Op65v+xAECvEr4woILH/1
jG/8DolDvHR5XWfzyIwA/Z4CrcK7tHMenFgHQHXg58GdwfIwM7or
7iZ2Uax6hcutamQvzo8IadTxn2M69+sqHWZgB/xBLM6OITufwDII=
-----END NEW CERTIFICATE REQUEST-----
```

Note: *You must include the -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST----- lines when copying the key.*

4. Enter the following URL in the web browser:

   http://diamond.noontide.com/certSrv

   where **diamond** is the Windows NT server on which the Microsoft Certificate Server is installed.

5. Click the **Certificate Enrollment Tools** link.

6. Click **Process a Certificate Request**.

7. On the **Web Server Enrollment** page, paste the key in the field by pressing **Ctrl**+**V**, and click the **Submit Request** button.

8. On the **Certificate Download** page, click **Download** and save the certificate to a file on your local disk. In this example, save the certificate to **C:\keysNcerts\avocado.cer**.

   You can view the certificate using any text editor.

9. Install the certificate on the Netscape Enterprise Server to enable SSL. Complete the steps described in “Enabling SSL Encryption on the Web Server” on page 196 to do so.

Tivoli recommends that you back up the key-pair and certificate and store the backup in a secure location.

Enabling SSL Encryption on the Web Server

This procedure presents the steps to install a secure certificate, thereby enabling SSL encryption on the Netscape Enterprise Server (NES) and converting the server to use HTTPS. The procedure installs the certificate that Harper Smith obtained on the web server named avocado. It is demonstrated in NoonTide’s environment, as follows:

- On a Netscape Enterprise Server (NES), version 3.6, that is installed on a Solaris system and named avocado.

- Using Netscape Communicator, version 4.5, on a Windows NT 4.0 machine. (If you use another browser, the steps may vary.)

To enable encryption on NES, complete the following steps:

1. Copy the certificate by opening **avocado.cer** in a text editor, highlighting it, and pressing **Ctrl**+**C**. The following is an example of what you should copy:

```
-----BEGIN CERTIFICATE-----
MIIEVDCCA8GgAwIBAgIIBbHhGgAAAFowCQYFKw4DAh0FADB6
MQswCQYDVQQGEwJVUzEOMAwGA1UECBMFVGV4YXMxDzA
NBgNVBAcTBkF1c3RpbjEXMBUGA1UEChMOVGl2b2xpIFN5c3Rl
bXMxDDAKBgNVBAsTA0lCVTEjMCEGA1UEAxMaVGl2b2xpIElCV
SBUcnVzdCBBdXRob3JpdHkwHhcNOTkwODA1MTcxNjU3WhcNM
DAwODA1MTcxNjU3WjCBlzELMAkGA1UEBhMCVVMxDjAMBgNV
```

```
BAgTBVRleGFzMQ8wDQYDVQQHEwZBdXN0aW4xFzAVBgNVBA
oTDlRpdm9saSBTeXN0ZW1zMQ0wCwYDVQQKEwRJbmMuMRs
wGQYDVQQLExJDcm9zcy1zaXRlIFN1cHBvcnQxIjAgBgNVBAMT
GXNpbGx5Z29vc2UuZGV2LnRpdm9saS5jb20wgZ8wDQYJKoZIhv
cNAQEBBQADgY0AMIGJAoGBANPaXCo8CjuzzhVuG3LJh+1kVG
wefGzJCBGZS8N6x0d71taIfJeI58BfMvhEwZBdXN0aW4xFzAVBg
NVBAoTDlRpdm9saSBTeXN0ZW1zMQwwCgYDVQQLEwNJQlUxI
zAhBgNVBAMTGlRpdm9saSBJQlUgVHJ1c3QgQXV0aG9yaXR5gh
BhVHlPwADolhHTAZit2J0wMIGdBgNVHR8EgZUwgZIwRqBEoEK
GQGh0dHA6Ly9UQUdBTUVUL0NlcnRTcnYvQ2VydEVucm9sbC9U
aXZvbGkgSUJVIFRydXN0IEF1dGhvcml0eS5jcmwwSKBGoESGQ
mZpbGU6Ly9cXFRBR0FNRVRcQ2VydFNydlxDZXJ0RW5yb2xsXF
Rpdm9saSBJQlUgVHJ1c3QgQXV0aG9yaXR5LmNybDAJBgNVHR
MEAjAAMGQGCCsGAQUFBwEBBFgwVjBUBggrBgEFBQcwAoZIa
HR0cDovL1RBR0FNRVQvQ2VydFNydi9DZXJ0RW5yb2xsL1RBR0
BSsOAwIdBQADgYEAxJtOiCcHt6wO//dSg0b+IZ6mcm2dqaPSfzTA
ax1XKSPTeGe0zV7bfecb9HD4dBWZ9w6+TUMNDBa1alAUBzYtG/
n6DDxANVesw+wPxiSh0eMCZvHhM2tSV/PhTMinh47x2JQ/yZ4dQ
k6Jza7jaxBGPXaT6elPN73sAuPpEVP9bnU=
-----END CERTIFICATE-----
```

Note: *You must include -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines when copying the certificate.*

2. Go to the Netscape Server Administration page, using a web browser. The URL for the Netscape Server Administration UI on avocado is as follows:

   http://avocado.noontide.com:9344/admin-serv/bin/index

3. Click the **Keys & Certificates** button.

4. Click **Install Certificate** in the left-hand column of the page.

5. Complete the **Install a Server Certificate** form as follows:

   a. Select the **This Server** option.

   b. Select the **Message text (with headers)** option and paste the certificate text in the field by pressing **Ctrl**+**V**.

c. Select **avocado** from the **Alias** pull-down list.

d. Click **OK**.

6. On the Netscape Server Administration UI, click the **avocado** button to view the server settings for avocado.

7. Click **Encryption On/Off** in the left-hand column of the page.

8. Fill in the **Encryption On/Off** form, as follows:

   a. Select the **On** option under **Encryption**.

   b. Specify a port number. Tivoli recommends you use **443**, which is the standard port number for secure servers. However, you can use any port number that is available.

   c. Select **avocado** from the **Alias** pull-down list.

   d. Click **OK**.

   e. When prompted, enter the key-pair , which was **2clever4you**.

To complete this procedure, you must restart the web server. To restart avocado, return to the Netscape Server Administration page, click the toggle button next to the **avocado** button, which should change the button’s label to **OFF**. Click the toggle button again to restart the server. (You are prompted again for the key-pair when logging into the secure server.)

To verify that SSL is enabled, access the web server by entering **https://avocado** in the browser. The **Netscape Enterprise Server** page should be displayed in the browser. If you used a certificate that you obtained from an unknown CA (such as one generated in-house), you will be prompted to accept the certificate. Also, if the Netscape server is used for other purposes, such as hosting intranet web pages, be sure to notify users that the protocol of the server has changed. Let them know that they must change their bookmark to refer to **https://avocado**, not **http://avocado**.

Importing an Unsupported Root Certificate

Cross-Site ships with a list of supported root certificates, which are trusted and authorized for use with Cross-Site. The list of supported root certificates is in “Supported Server Certificates” on page 182. If you enabled SSL on the web server with a server certificate that was signed by an unsupported root certificate, such as one you generated in-house, you must create the **KeyRing.class** file. This is a special control file that contains the names of supported root certificates and to which you must import the root certificate of your server certificate.

Before installing the Cross-Site server, use the **xs_editkeyring** command to launch the keyman tool, which enables you to create the **KeyRing.class** file. This command is located in the **Util/KeyRing** directory on the Cross-Site CD-ROM. After Cross-Site is installed, this command is located in the **bin** subdirectory of the Cross-Site server’s installation directory.

Note: *SSL must be enabled on the web server and the web server must be running in order for you to use this command and import the certificate.*

You must edit the **KeyRing.class** file (after installing the Cross-Site server) if you intend to connect to another Cross-Site server, contact that server’s administrator and obtain the list of root certificates that he or she added to that server’s **KeyRing.class** file. Add those certificates to your server’s **KeyRing.class** file using the following procedure. The Cross-Site servers will then be able communicate securely and without problems.

This procedure demonstrates how Harper Smith, NoonTide’s web administrator, creates the **KeyRing.class** file and imports the root of her server certificate:

1. Log in to the system on which the Netscape Enterprise Server (NES) is installed, and on which you will install the Cross-Site management server. Log in as **root** on UNIX, **Administrator** on NT, the NES user, or a user with equivalent privileges. The directory in which the **KeyRing.class** file is saved is owned and writable by the NES user.

   Harper logs in to avocado as **root**, which is a Solaris system.

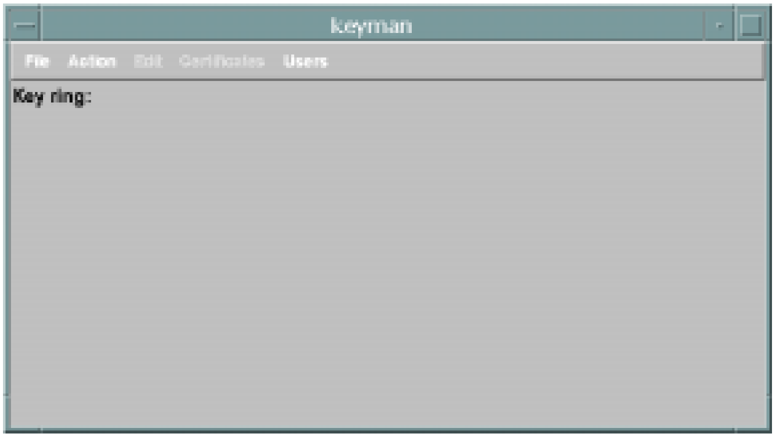
Note: *If you log in to the system remotely, ensure that the DISPLAY environment variable is set to the machine you are using and that the machine can connect to the server.*

2. On the command line, enter the following command:

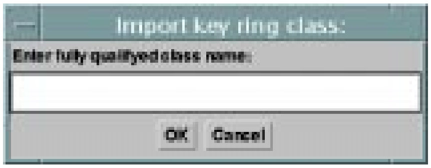
```
/cdrom/cdrom0/UTIL/KeyRing/xs_editkeyring
```

   where **/cdrom/cdrom0/** is the path to the mounted CD-ROM. If the server is installed on an NT system, run this command from the Command Prompt.

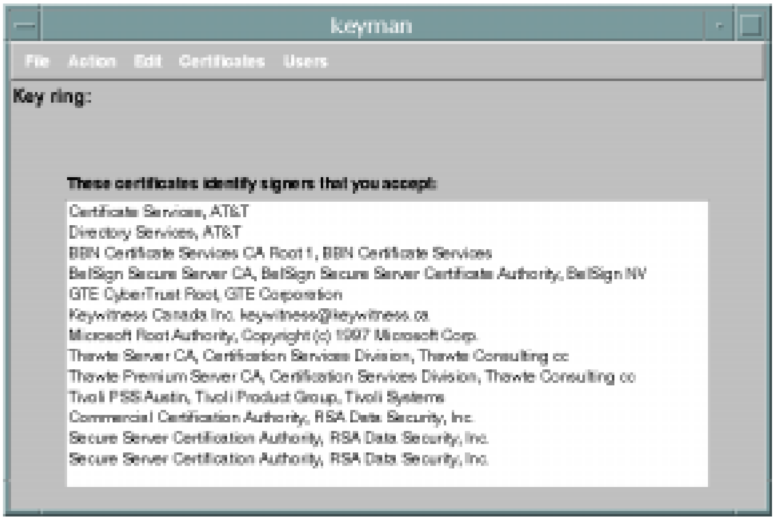
   The **keyman** window is displayed:



3. Select **File –> Import class**. The following dialog is displayed:



4. Enter **KeyRing** in the field and click **OK**. KeyRing is the class name that is defined by Cross-Site. The keyman tool obtains this file from the CD-ROM or Cross-Site management server. A list of root certificates is displayed in the **keyman** window.

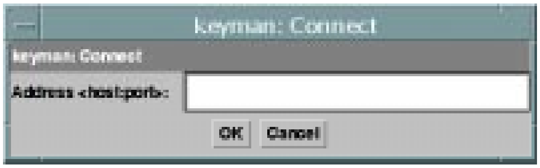


Key ring:

These certificates identify signers that you accept:

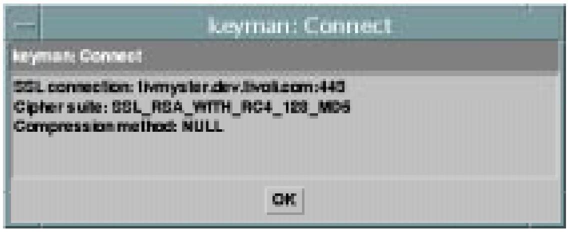
Certificate Services, AT&T
Directory Services, AT&T
BBN Certificate Services CA Root 1, BBN Certificate Services
BelSign Secure Server CA, BelSign Secure Server Certificate Authority, BelSign NV
GTE CyberTrust Root, GTE Corporation
Keywitness Canada Inc. keywitness@keywitness.ca
Microsoft Root Authority, Copyright (c) 1997 Microsoft Corp.
Thawte Server CA, Certification Services Division, Thawte Consulting cc
Thawte Premium Server CA, Certification Services Division, Thawte Consulting cc
Tivoli PSS Austin, Tivoli Product Group, Tivoli Systems
Commercial Certification Authority, RSA Data Security, Inc.
Secure Server Certification Authority, RSA Data Security, Inc.
Secure Server Certification Authority, RSA Data Security, Inc.

5. Select **Action –> Connect**. The **keyman:Connect** dialog is displayed.



6. Enter the host name and port number of the web server that is, or will be, associated with the Cross-Site management server. and click **OK**. For example, if the web server is installed on avocado and uses port 443, enter **avocado.noontide.com:443**. The keyman tool attempts to connect to the server over SSL.

If the connection was successful, the **keyman:Connection** dialog is displayed.



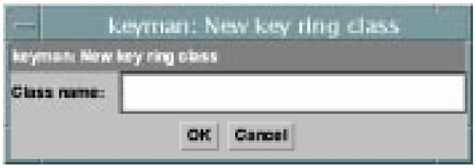
SSL connection: livmyster.dev.tivoli.com:443
Cipher suite: SSL_RSA_WITH_RC4_128_MD5
Compression method: NULL

7. Click the **OK** button to dismiss the **keyman:Connection** dialog The certificate chain is displayed in the **keyman** window. The certificate chain can include the server certificate, the root certificate, and user.

8. Select your root certificate, which is either the only one or the last one listed, from the certificate chain and select **Edit -> Import as signer certificate** to import the certificate into the KeyRing.

9. To confirm that the keyman tool imported your certificate, select **Certificates -> Signers**. Scroll down to the bottom of the list, which is where new certificates are added.

10. Select **File -> Save as class**. The following dialog is displayed:



11. Enter **KeyRing** and click **OK**. A browser dialog is displayed.

12. Enter a directory in the field at the top of the dialog; choose any directory you like. Click **Update** on UNIX, or click **Save** on NT.

13. Enter **KeyRing.class** file in the field at the bottom of the dialog and click **OK**. When the Cross-Site server is installed, it refers to the **KeyRing.class** file and copies it to the *base_dir***/XSITsagt/lib/local** directory, where *base_dir* is the installation directory of the Cross-Site server.

14. Select **File –> Exit** to exit the **keyman** window and the **xs_editkeyring** command.

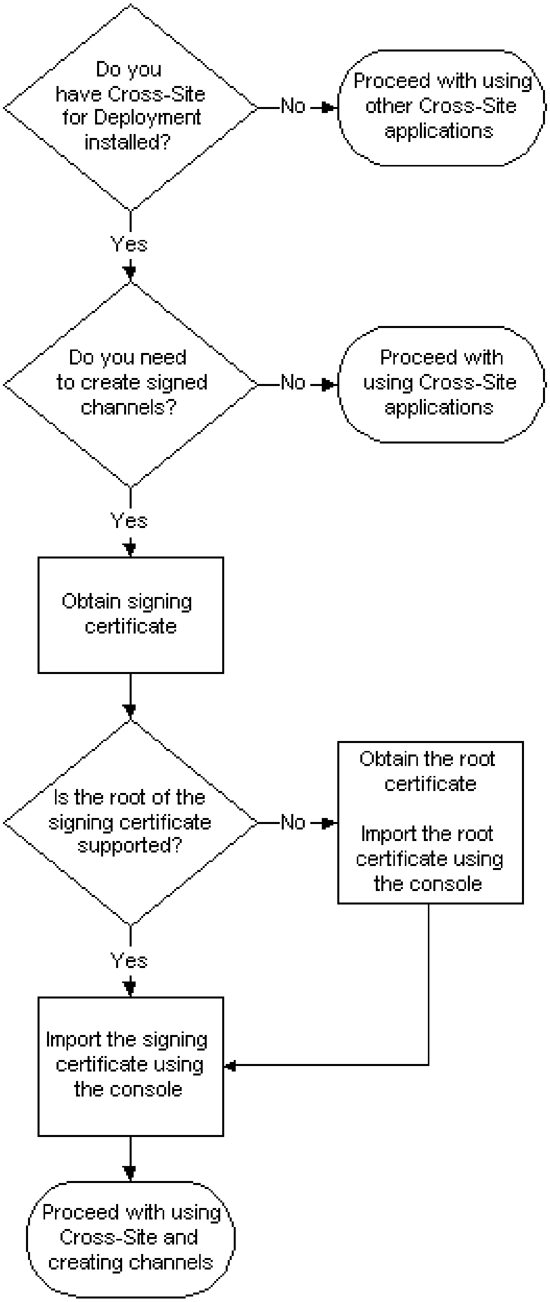
If you performed this procedure after the Cross-Site server was installed, restart the Cross-Site server, which requires that you restart the web server. See the section on restarting the server in the installation guide for instructions.

You must save a copy of the **KeyRing.class** file (using FTP, for example) on each client machine where you intend to install an agent or console. Copy the file as a binary file. The agent and console installation programs prompt you for the path of the file on the client machine. After installing the console or agent, ensure that the **KeyRing.class** file is located in the *install_dir***/lib** directory.

Obtaining a Signing Certificate

A content signing certificate, or simply “signing certificate,” identifies the owner of the content and includes a digitally signed version of the owner’s name, organization, and public key in the content. It enables you to digitally sign your applets or other Java code, JavaScript scripts, plug-ins, or any kind of file. In Cross-Site, you can sign Cross-Site for Deployment channels with a signing certificate. Signing certificates are also referred to as developer certificates, digital IDs, and publisher certificates. A signing certificate is different than a server certificate and they cannot be used interchangeably.

If you intend to sign a Deployment channel, you must obtain a signing certificate and import it into Cross-Site.You need to sign any channel that requires write access on the client machine, such as if the channel will copy files to the client’s file system. When you sign a channel with a certificate, end users are assured that no one has tampered with the content in the channel. The channel can then install data and programs on users' systems and is permitted to use all of the users' system resources.


Do you have Cross-Site for Deployment installed?
No
Proceed with using other Cross-Site applications
Yes
Do you need to create signed channels?
No
Proceed with using Cross-Site applications
Yes
Obtain signing certificate
Is the root of the signing certificate supported?
No
Obtain the root certificate
Import the root certificate using the console
Yes
Import the signing certificate using the console
Proceed with using Cross-Site and creating channels

The procedures in this section demonstrate using Netscape Communicator, version 4.5, and Internet Explorer, version 5. These products are used because they are readily available on most Windows machines. In “Generating an In-house Signing Certificate” on page 215, the Microsoft Certificate Server is used to illustrate generating a signing certificate. This product was chosen because it is commonly used in e-business environments. Please note, however, that this section provides examples and you are free to use any software you choose, unless a specific product is needed, such as NES.

Supported Signing Certificates

The following list provides the root certificates that Cross-Site supports for issuing signing certificates. Some CAs refer to signing certificates as developer certificates.

- BelSign Secure Server CA
- BelSign Class1 CA
- BelSign Class 2 CA
- BelSign Class 3 CA
- BelSign Object Publishing CA
- Entrust Demo Web Certification Authority
- Marimba Root CA
- Thawte Server CA
- RSA Data Security, Inc. Secure Server Certificate Authority
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 2 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority

- VeriSign Class 4 Public Primary Certification Authority
- VeriSign Class 3 Commercial Content/Software Publisher CA
- VeriSign Object Signing CA - Class 3 Organization
- VeriSign Trust Network
- VeriSign Test Secure Server ID (TestCPS)

If you have a signing certificate that was signed by any of these root certificates *and* you can export the certificate to a PKCS#12 file, you can use that certificate to sign Cross-Site channels. See "Exporting the Certificate to a PKCS#12 File" on page 213 for more information on the file format.

If you need to purchase a signing certificate, the following list provides the certificate authorities and their signing products that Cross-Site supports. Choose any one of the listed certificates to purchase. After you purchase the certificate, you must import it into the applicable tool and export it as a PKCS#12 file. For example, if you purchase VeriSign's Netscape Object Signing certificate, you must import it then export it from the Netscape browser. Therefore, the most important thing to keep in mind before purchasing a signing certificate is the tool that you have that will enable you to export the certificate.

A URL is provided for each CA so that you can access their web site to purchase a certificate. If you choose to download a trial signing certificate, such as the trial version of VeriSign's Personal Digital ID, Tivoli recommends that you only use this certificate with Cross-Site in a test or lab environment. Also, if you are an international customer, verify with the certificate vendor that you can purchase any of these certificates.

- Thawte Certification
  http://www.thawte.com/certs/developer/contents.html
  - Developer Certificate for Microsoft Authenticode
    (Import this certificate into the Microsoft registry and export it using Microsoft's pvkimport tool.)

  - Developer Certificate for Microsoft Office 2000 / VBA
    (Request this certificate using the Internet Explorer 5.0 or higher. Export it using the Internet Explorer, also.)

  - Developer Certificate for Netscape Object Signing
    (Request this certificate using the Netscape Communicator 4.0 or higher, which installs the certificate in the Netscape certificate database. Export it using the Netscape Communicator, also.)

  - Marimba Channel Signing
    (Import and export this certificate using the Marimba Certificate Manager, which you can access using the Marimba Tuner or Publisher.)

- VeriSign, Inc.
  http://www.verisign.com/developer/index.html

  - Channel Signing ID for Marimba Castanet
    (Import and export this certificate using the Marimba Certificate Manager, which you can access using the Marimba Tuner or Publisher.)

  - Software Developer ID for Microsoft Authenticode
    (Import this certificate into the Microsoft registry and export it using Microsoft’s pvkimport tool.)

  - Software Developer ID for Netscape Object Signing
    (Request this certificate using the Netscape Communicator 4.0 or higher, which installs the certificate in the Netscape certificate database. Export it using the Netscape Communicator, also.)

  - Software Developer ID for Microsoft Office 2000 and Visual Basic
    (Request this certificate using the Internet Explorer 5.0 or higher. Export it using the Internet Explorer, also.)

  - Personal Digital ID, including the trial version
    (When you purchase this certificate, it is automatically installed in the browser. Export it from the browser for use in Cross-Site.)

For more information about exporting the certificate, see “Exporting the Certificate to a PKCS#12 File” on page 213 for more information.

In addition to signing certificates listed above, you can use a certificate that you generate using an in-house certificate server. See “Generating an In-house Signing Certificate” on page 215 for instructions.

Purchasing a Signing Certificate

The following procedure demonstrates the general steps for purchasing a certificate from Thawte Certification, which you can use to sign Cross-Site for Deployment channels. Use this procedure to get an idea of the steps you perform to purchase a signing certificate. All of the CAs have similar procedures. For a complete list of signing certificates that you can purchase to use when signing Deployment channels, see “Supported Signing Certificates” on page 206.

Before beginning the procedure to purchase a signing certificate, gather the following information. You will be prompted for it.

- The type of certificate you wish to purchase from the CA. For example, Thawte offers developer certificates for the Marimba Castanet, Microsoft Authenticode, Microsoft Office 2000 / VBA, and Netscape Object Signing products. Cross-Site supports all of these. Decide which certificate best fits your needs.

- Your company’s registered domain name. The following URL enables you to verify your company’s domain name:

  http://www.networksolutions.com/cgi-bin/whois/whois

  If your domain name is not registered, you must register it before proceeding with obtaining a server certificate. You can purchase a domain name by entering the following URL in the browser:

  http://www.networksolutions.com/purchase/

- Your organization’s D-U-N-S number. You must submit documentation that demonstrates your right to use the corporate name specified in the request. The D-U-N-S number is an internationally-recognized, company identifier that is provided by Dun & Bradstreet. The following URL enables you to obtain this information:

https://www.dnb.com/product/eupdate/update.htm

If you are located outside of the United States, use the following URL instead of the first one listed above:

http://www.dnb.com/global/menu.htm

- The payment information. If you choose to pay with a credit card, you will need the card type, number, expirations date, and name on the card. Thawte also allows you to pay by check, bank draft, wire transfer, stronghold bundle, and through an enterprise account. Obtain the payment information.
- The authorizing contact's name, title, e-mail address, and international phone number. This contact is the person responsible for authorizing the use of your company's name.
- The technical contact's name, e-mail address, phone number, and title. Presumably, this information is yours but if you are not the technical contact, collect this information.

As in the procedures in "Obtaining a Server Certificate" on page 179, a fictitious company called NoonTide is used to provide a scenario for the procedures in this section. NoonTide develops, markets, and sells electronic products. They have many organizational departments, one of which is Web Development. One of the web administrators at NoonTide, Harper Smith, installed and uses Cross-Site to monitor the NoonTide web site, as well as partner sites. She also intends to create signed Deployment channels.

To purchase a certificate (for Microsoft Authenticode) from Thawte, complete the following steps. Note that you must use the Microsoft Internet Explorer (IE) to purchase a Microsoft Authenticode certificate; this procedure illustrates the steps using IE 5.0.

1. Go to the Thawte developer certificates page by entering the following URL in the browser:

   https://www.thawte.com/cgi/server/step1.exe?zone=devel

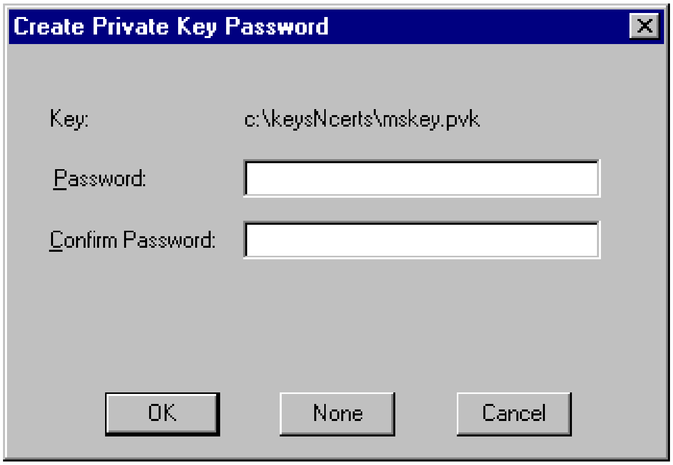
   You can also access the developer certificates by entering the following URL in your web browser:

   http://www.thawte.com/certs/developer/contents.html

2. Select a certificate, such as the Microsoft Authenticode Certificate.

3. On the first form, enter your company’s name and location when prompted. Choose where to store the private key (for the certificate). Choose to store it as a file. This process will create a private key and store it in the designated location. For this example, choose **C:\keysNcerts\mskey.pvk**.

4. When prompted by the following dialog, choose a for the private key.



Key: c:\keysNcerts\mskey.pvk

Password:

Confirm Password:

When you import the certificate in “Exporting the Certificate to a PKCS#12 File” on page 213, you must specify this .

5. On the second form, verify your company’s information. Enter the D-U-N-S number, and enter the authorizing and technical contacts’ names. Enter the payment information.

6. Gather your letter of authorization. You must prove that your company “owns” its name. For example, if your company is a partnership, you must obtain a copy of some form of verifiable proof of the partnership name. For this example, because NoonTide is incorporated, gather a copy of the certificate of incorporation.

   Print the letter on your company’s letterhead. Send the documentation to Thawte by faxing it to your local representative. For a list of representatives, see the following URL:

   http://www.thawte.com/contact.html

7. If a **Security Warning** dialog is displayed, prompting you to install and run a specific Microsoft component, click **Yes**.

8. You can check the status of your certificate order here. To do so, return to the enrollment page by entering the following URL in the browser:

   https://www.thawte.com/certs/developer/contents.html

9. To pick up your certificate, retrieve it by going to the URL sent in the confirmation e-mail (from Thawte). Follow the instructions on the site, including selecting the appropriate format.

Now that you have the certificate, you must import it into the Microsoft registry and export it as a PKCS#12 file. This will then enable you to sign Cross-Site channels. See the following section to export the certificate in the PKCS#12 format.

Exporting the Certificate to a PKCS#12 File

The PKCS#12 file format is a standard format that contains both the signing public and private key. By containing both keys, you can “move” the certificate from one application to another, to secure the content produced by the application. Before you can use a certificate to sign a Cross-Site channel, you must import it into the applicable tool and export the certificate as a PKCS#12 file. For example, if you purchased a developer ID for Microsoft Authenticode from VeriSign, you must import it into the Microsoft registry and export it using Microsoft’s pvkimport tool. See “Supported Signing Certificates” on page 206 for a list of supported certificates and the tools you must use to import and export the certificate.

Note: *If you export the certificate from the NT registry, you can copy it to the AIX or Solaris system on which the Cross-Site server is installed. Likewise, you can copy a certificate from a UNIX system to an NT system. A certificate file is a binary file and can be used on both platform types.*

Continuing with the example in “Purchasing a Signing Certificate” on page 209, this procedure demonstrates how Harper Smith can import the certificate that she purchases from Thawte into the Microsoft registry on a Windows NT 4.0 system. This procedure also illustrates how she can export it using Internet Explorer, version 5.0. (If you use another browser, the steps may vary.)

1. To import the signing certificate into the Windows NT registry, you must download the pvkimport tool. Enter the following URL in the browser:

   http://msdn.microsoft.com/vba/technical/pvk.asp

   Microsoft’s **PVK Digital Certificate Files Importer** page is displayed.

2. Click the **Download the pvkimprt.exe** link at the bottom of the page. When prompted, save it to a directory, such as **C:\Program Files\Microsoft**.

3. On the Windows Explorer, navigate to the **C:\Program Files\Microsoft** directory and double-click on the **pvkimprt.exe** file. When prompted, begin the installation of the pvkimprt tool.

4. When prompted, read and accept the license agreement, then select a location in which the tool will be installed. The default location is **C:\WINNT**.

5. When the installation completes, run the pvkimprt tool by entering the following command in a Command Prompt window (from the **C:\** directory). You cannot double-click on the **Pvkimprt.exe** file; you must run it from the command line and provide the arguments.

   ```
   winnt\pvkimprt “c:\keysNcerts\signing.spc”
   “c:\keysNcerts\signing.pvk”
   ```

   where **signing.spc** and **signing.pvk** are the files provided to you by the CA when you purchased the signing certificate.

6. To verify that the files were imported into the registry, select **Internet Options** from the **Tools** menu on Internet Explorer.

7. On the **Content** tab, click the **Certificates** button. The **Certificate Manager** dialog is displayed.

8. Choose the **Personal** tab to view the certificates for which you have the private key.

9. Select the certificate in the list and click **Export**. The **Certificate Manager Export Wizard** is displayed.

10. Follow the prompts. Be sure to export the private keys and select the PKCS format, when prompted. When complete, close the dialogs.

    The browser stores the PKCS#12 file in the specified location, such as **C:\keysNcerts\signing.pfx**.

If you wish to export the certificate from a Netscape browser, you can do so by clicking the **Security** icon below the menu. Then, select **Yours** on the left side of the window that is displayed.

After you export the certificate as a file, use the **Certificates** explorer on the Cross-Site console to install the certificate on your Cross-Site server. The “Importing a Signing Certificate into Cross-Site” on page 220 section describes how to install a certificate in Cross-Site.

Generating an In-house Signing Certificate

Instead of purchasing a signing certificate, you can use a certificate server to generate one. If your company has installed an in-house certificate server, you can request a certificate from the department that runs the certificate server. Often, large companies or companies involved heavily in e-commerce have installed an in-house certificate server, to easily and inexpensively obtain certificates. If you have access to the server, you can generate a signing certificate.

This procedure demonstrates how Harper Smith can generate a signing certificate in NoonTide’s environment, as follows:

- Using Netscape Communicator, version 4.5, on a Windows NT 4.0 machine. (If you use another browser, the steps may vary.)
- On the Microsoft Certificate Server on an NT machine.

Recall that Harper is the web administrator for NoonTide, which is a fictitious company provided to create a scenario that you can follow through the procedures.

In addition to the Microsoft Certificate Server, you can use another vendor’s certificate server to generate in-house certificates. See “References” on page 222 for a list of public key infrastructure (PKI) vendors, though the list is not comprehensive.

To generate the signing certificate, complete the following steps:

1. Enter the following URL in the web browser:

   http://diamond.noontide.com/certSrv

   where **diamond** is the Windows NT server on which the Microsoft Certificate Server is installed.

2. Click the **Certificate Enrollment Tools** link.

3. Click **Request a Client Authentication Certificate**.

4. Select your browser type, **Netscape**, from the list and click **Submit**.

5. On the **Certificate Enrollment** page, fill in the fields. For key strength, Tivoli recommends that you choose a strength that is consistent with the your corporate security policy and export requirements. Click **Submit**.

   Note: *If you are not prompted to generate a private key, your browser may be incompatible with the certificate server. Refer to the server's documentation and, if necessary, launch a different browser.*

6. On the **Generate A Private Key** dialog, click **OK** to generate a private key for the certificate.

7. Enter a for the key. For this example, enter **12345678.** Enter it a second time to confirm. Click **OK**. The **New User Certificate** dialog is displayed.

8. Scroll down to the bottom of the dialog and uncheck the option; you do not want this certificate used as the default in the browser. Click **OK** to install the certificate in the browser. The **Save User Certificate** dialog is displayed.

9. Click the **Save As** button. The **Entry** dialog is displayed.

10. Enter **12345678** (the key's) in the field and click **OK**. Another **Entry** dialog is displayed.

11. Enter a to protect the key, such as **flybyn1te**, and click **OK**. When prompted, reenter it and click **OK** again. The **File Name to Export** dialog is displayed.

12. Select a location and name for the certificate and click **Save**. The file is saved in the PKCS#12 format. For this example, save the file as **C:\keysNcerts\signing.p12**.

13. To verify that the signing certificate was generated and installed successfully, click the **Security** icon below the menu on the Netscape browser. The Security Info page is displayed.

14. Click the **Yours** link. Your certificate should be in the list.

Because you saved the certificate as a PKCS#12 file, you do not need to export the certificate from the browser, for use by Cross-Site. You can now launch the Cross-Site console and import the certificate, as described in “Importing a Signing Certificate into Cross-Site” on page 220.

Importing an Unsupported Root Certificate

If the signing certificate is signed by a root certificate other than one listed in “Supported Signing Certificates” on page 206, you must add the root certificate to the Cross-Site management repository. This list of root certificates is maintained in a table in the Cross-Site server’s management repository. It contains metadata about each certificate such as the name, issuer, and expiration date; the certificates table does not contain the actual certificates. The list of supported certificates is also passed to the Cross-Site agents when they are installed.

Importing the root certificate on the Cross-Site server adds the certificate to the management repository. To synchronize the agent’s certificate list with the newly modified one in the management repository, a channel is provided on the agent. This channel is called **XSiteRootCertsImport** and, by default, is hidden. When this channel runs, which is every third day at 5:30 AM (by default) or when the agent restarts, the agent’s certificate list is updated. (End users cannot download a signed channel whose root certificate was just imported until the certificates list is synchronized.) To view the **XSiteRootCertsImport** channel on the agent’s desktop, select the **Channels** tab on the agent’s desktop and select the option in the bottom right-hand corner. This channel, as well as several others used for agent maintenance, is displayed.

This procedure demonstrates how Harper Smith, NoonTide’s web administrator, can import a root certificate in the following environment:

- Using Internet Explorer (IE), version 5.0, on a Windows NT 4.0 machine. (If you use another browser, the steps may vary.)

- On the Microsoft Certificate Server on an NT machine.
- On the Cross-Site management server (and console) that is installed on a Solaris system named avocado.

This example demonstrates obtaining a root certificate from the Microsoft Certificate Server, which was used to generate the in-house signing certificate on page 215. It is possible to obtain a commercially available signing certificate from a certificate vendor that is not supported by Cross-Site. In that case, contact the vendor to obtain the root certificate.

To import the unsupported root certificate into the certificate database, complete these steps:

1. For the in-house generated certificate **signing.p12**, obtain a root certificate from the Microsoft Certificate Server. To do so, enter the following URL in the web browser:

   http://diamond.noontide.com/certSrv/

   where **diamond** is the system on which the Microsoft Certificate Server is installed.

2. Click **Certificate Enrollment Tools**.

3. Click **Install Certificate Authority Certificates**.

4. Right-click on the **MSIE Users: Certificate for DIAMOND\NoonTide Trust Authority** link and select **Save Target As** from the pop-up menu.

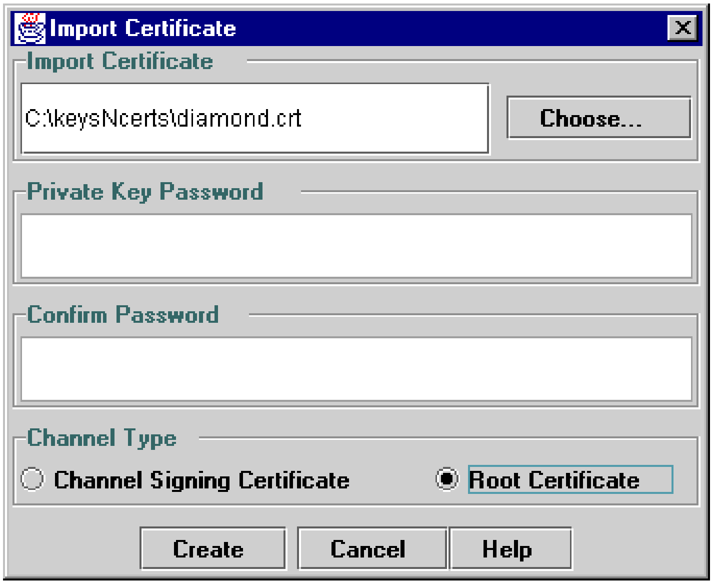
5. When prompted, save the certificate file to on your system, such as **C:\keysNcerts\diamond.crt**. The format of this file is PKCS#7.

6. Run the Cross-Site console.

7. In the Admin view, select the **Certificates** tab.

8. Click the **New Certificate** button. The **Import Certificate** panel is displayed.

9. Enter the path to the root certificate in the **Import Certificate** field and select the **Root Certificate** option. Do not enter a . (You enter a only when importing a signing certificate.)



Import Certificate

Import Certificate: C:\keys\certs\diamond.crt

Private Key Password:

Confirm Password:

Channel Type: ○ Channel Signing Certificate ● Root Certificate

10. Click **Create**. The **NoonTide Trust Authority** certificate is displayed in the tree on the Certificates explorer.

Now that the root certificate has been imported into Cross-Site, the root certificate is no longer considered unsupported or foreign. You can import signing certificates signed by the root certificate, as described below.

Importing a Signing Certificate into Cross-Site

To import the signing certificate into Cross-Site, which enables you to sign Cross-Site for Deployment channels, follow the steps below. The procedure demonstrates how Harper Smith can import the signing certificate that was generated by NoonTide's certificate server. If your certificate is signed by an unsupported root certificate, such as one generated by an in-house certificate server, you must first import the root certificate as described in above.

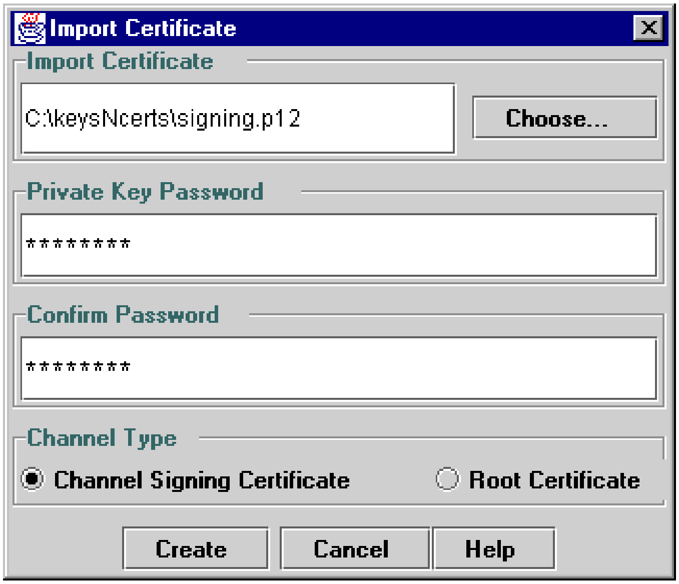
1. Ensure that the console has read access to the certificate file.

2. Run the console.

3. In the Admin view, select the **Certificates** tab.

4. Click the **New Certificate** button. The **Import Certificate** panel is displayed.

5. Complete the fields on the panel. For the , enter the key for the certificate. You chose this when you generated the certificate, or when you exported a purchased certificate. For the signing.p12 certificate, enter **12345678** as the . Select the **Channel Signing Certificate** option.



Import Certificate

Import Certificate: C:\keysNcerts\signing.p12

Private Key Password: ********

Confirm Password: ********

Channel Type: ● Channel Signing Certificate ○ Root Certificate

6. Click the **Create** button. Your certificate is added to the tree on the left. Its name is the name that you specified when you generated or requested the certificate.

After you complete these procedures, the signing certificate is available for signing Cross-Site for Deployment channels.

References

If you wish to find out more about certificates and the public key infrastructure (PKI), refer to the following organizations, standards, and PKI vendors:

Organizations

- American National Standards Institute (ANSI)
  www.x9.org
- Institute of Electronic and Electrical Engineers (IEEE)
  www.standards.ieee.org
- Internet Engineering Task Force (IETF)
  www.ietf.org
- International Standards Organization (ISO)
  www.iso.ch
- International Telecommunications Union (ITU)
  www.itu.org

Standards

- Public Key Cryptography Standards (PKCS), developed by RSA Data Security
  http://www.rsa.com/rsalabs/pubs/PKCS/
- IETF Public Key Infrastructure and Interoperability (PKIX)
  http://www.ietf.org/html.charters/pkix-charter.html
- Secure Sockets Layer (SSL) 3.0, developed by Netscape Communications
  http://home.netscape.com/eng/ssl3/
- TLS 1.0 (SSL 3.0 in standards form)
  http://www.ietf.org/html.charters/tls-charter.html

- X.509
http://www.itu.int/plweb-cgi/fastweb?getdoc+view1+itudoc+7897+0++X.509

PKI Vendors of Commercial CA Software

- Netscape Certificate Management System (part of SuiteSpot)
http://www.iplanet.com/products/infrastructure/dir_security/cert_sys/index.html

- Microsoft Certificate Server (included in Windows NT Option Pack 4; formerly included in Microsoft BackOffice)
http://www.microsoft.com/ntserver/web/exec/overview/WebFeat.asp

PKI Vendors of Enterprise CA Software

- Entrust Technologies
http://www.entrust.com/

- Baltimore Technologies
http://www.baltimore.com/

- GTE CyberTrust Enterprise CA
http://www.cybertrust.com/cybertrust/products_services/products/enterprise/enterprise.html

- Entegrity Solutions
http://www.entegrity.com/

- CertCo
http://www.certco.com/

- E-Lock
http://www.e-lock.com/

You can also refer to the online help provided with the Netscape Enterprise Server. Click **Help** on the Netscape Server Administration UI and review the chapter on encryption and SSL in the *Netscape Administration Server: Managing Netscape Servers* book.

C

Regenerating Your License Key

You must regenerate your Cross-Site license key in the following scenarios:

- You purchased and wish to install an additional Cross-Site application on an existing Cross-Site server. For example, if you are currently using Cross-Site for Deployment and your company has decided to purchase Cross-Site for Availability, you must regenerate your license key to include the new application's server and clients.

- You intend to install additional clients (agents) for an application you already have installed. For example, if you installed Cross-Site in a lab environment using a subset of the clients you purchased, you must regenerate your license key to include the additional clients that you intend to install in the production environment.

- You wish to change the configuration of your Cross-Site installation. For example, say you created your license key based on having two Cross-Site applications installed on the same management server. Now, if you want to install each application on its own management server, you must regenerate the existing license key and generate a new license key for the second server.

In any of these scenarios, you must update your license key before installing the new application or clients.

The Support system, which is hosted on the Cross-Site web site (www.cross-site.com), enables you to retrieve your purchase order for Cross-Site and generate a license key based on the number of clients you intend to deploy. The Support system enables you to keep track of your configuration, in addition to creating licenses for you.

Modifying Your License Key

Complete the following steps to modify your license key:

1. Enter the following URL in your web browser:

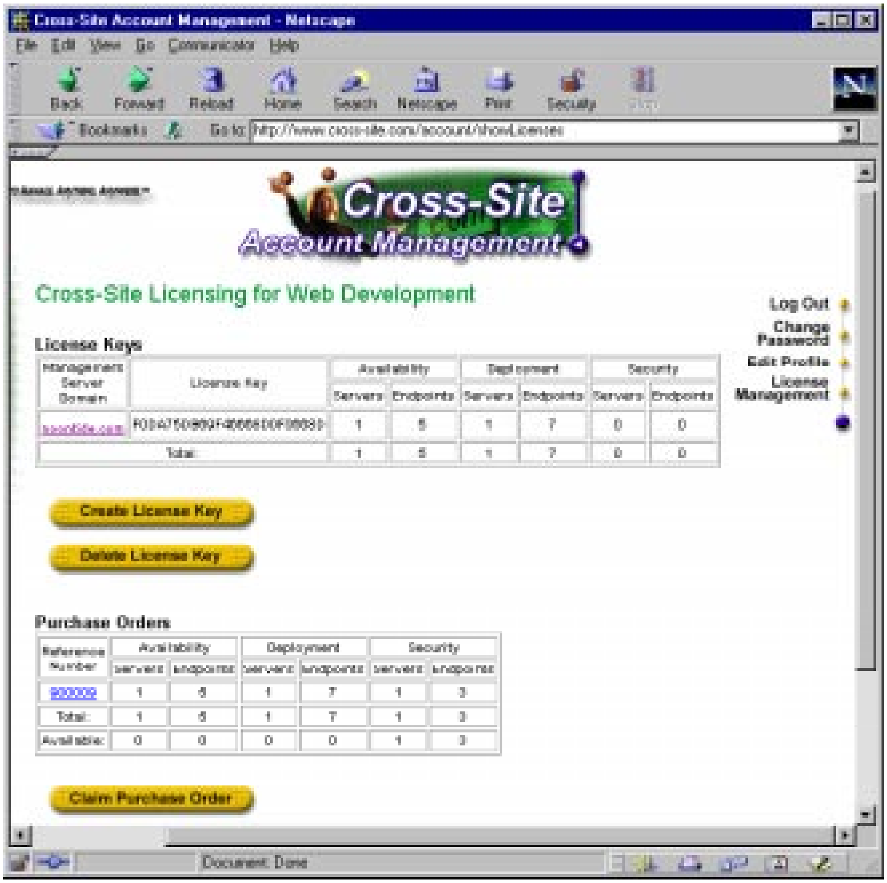
   http://www.cross-site.com/support

2. Log in. If you are already logged in to the Cross-Site Support system, you can simply enter the following URL in your web browser and skip to step 5.

   http://www.cross-site.com/account/showLicenses

3. Click **Account Management** on the right-hand side of the page.

4. Click **License Management** on the right-hand side of the page. The License Management page is displayed, which displays your current license.



Cross-Site Account Management - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security
Bookmarks Go to: http://www.cross-site.com/account/showLicenses
Cross-Site
Account Management
Log Out
Change Password
Edit Profile
License Management
Document: Done

Cross-Site Licensing for Web Development

License Keys

Management Server Domain	License Key	Availability		Deployment		Security	
		Servers	Endpoints	Servers	Endpoints	Servers	Endpoints
[illegible]	F03A75D9B9F46666D0F09893	1	5	1	7	0	0
Total:		1	5	1	7	0	0

Create License Key

Delete License Key

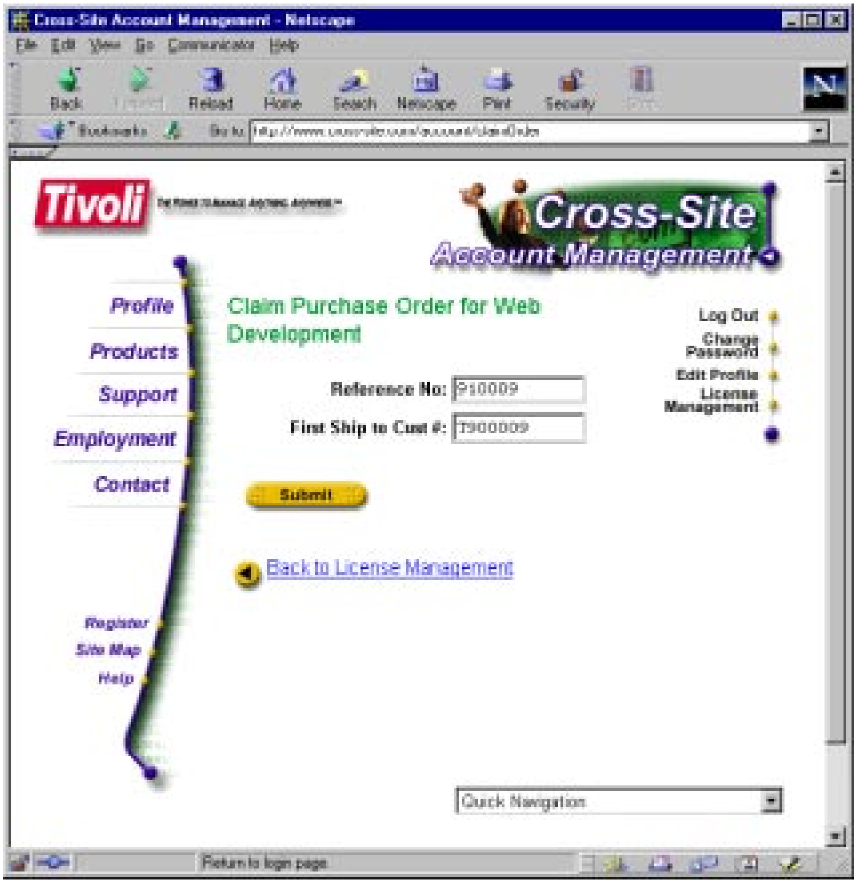
Purchase Orders

Reference Number	Availability		Deployment		Security	
	servers	endpoints	servers	endpoints	servers	endpoints
[illegible]	1	5	1	7	1	3
Total:	1	5	1	7	1	3
Available:	0	0	0	0	1	3

Claim Purchase Order

5. Click the **Claim Purchase Order** button. If you previously claimed a purchase order, you may need to reload the page to update the displayed information.

6. On the **Claim Purchase Order** page, fill in the fields with values found on the packing slip that was shipped with the application you wish to install.


Cross-Site Account Management - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to: http://www.cross-site.com/account/claimOrder
Tivoli
Cross-Site Account Management
Profile
Products
Support
Employment
Contact
Register
Site Map
Help
Log Out
Change Password
Edit Profile
License Management
Submit
Back to License Management
Quick Navigation
Return to login page

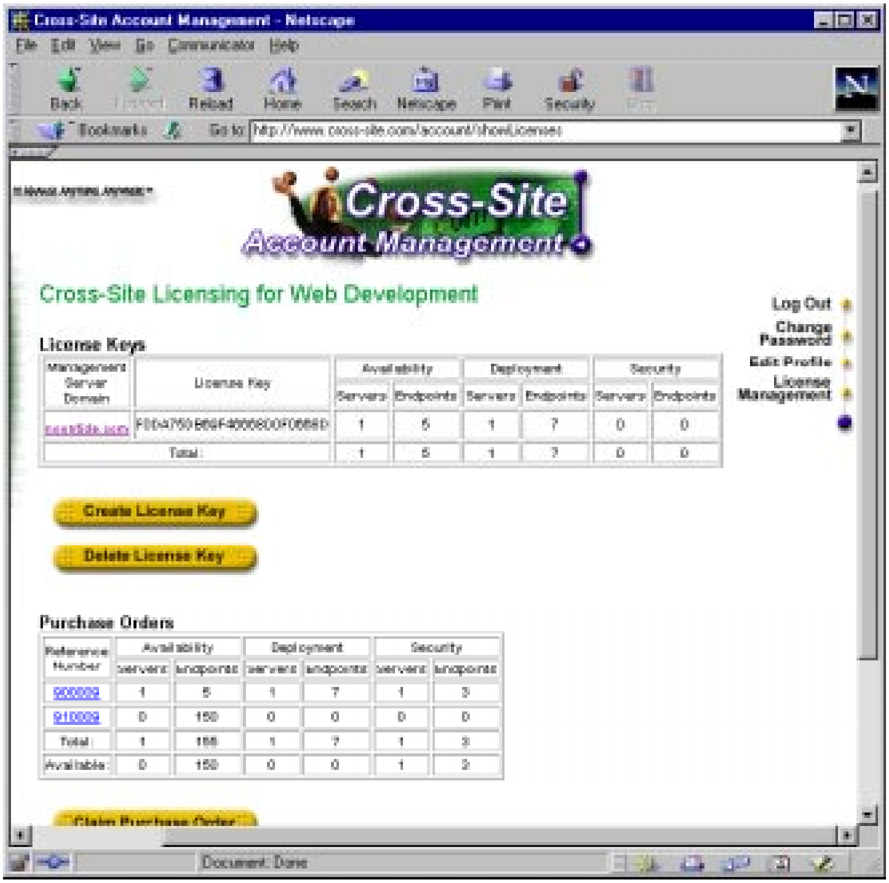
Claim Purchase Order for Web Development

Reference No: 910009

First Ship to Cust #: T900009

7. Click **Submit**. An acknowledgment page is displayed.

8. Click the **Return** link. You may need to reload the page to update the information that is displayed. Your new purchase order is displayed in the second table.



Cross-Site Licensing for Web Development

License Keys

Management Server Domain	License Key	Availability		Deployment		Security	
		Servers	Endpoints	Servers	Endpoints	Servers	Endpoints
crossSite.com	[illegible]	1	5	1	7	0	0
Total:		1	5	1	7	0	0

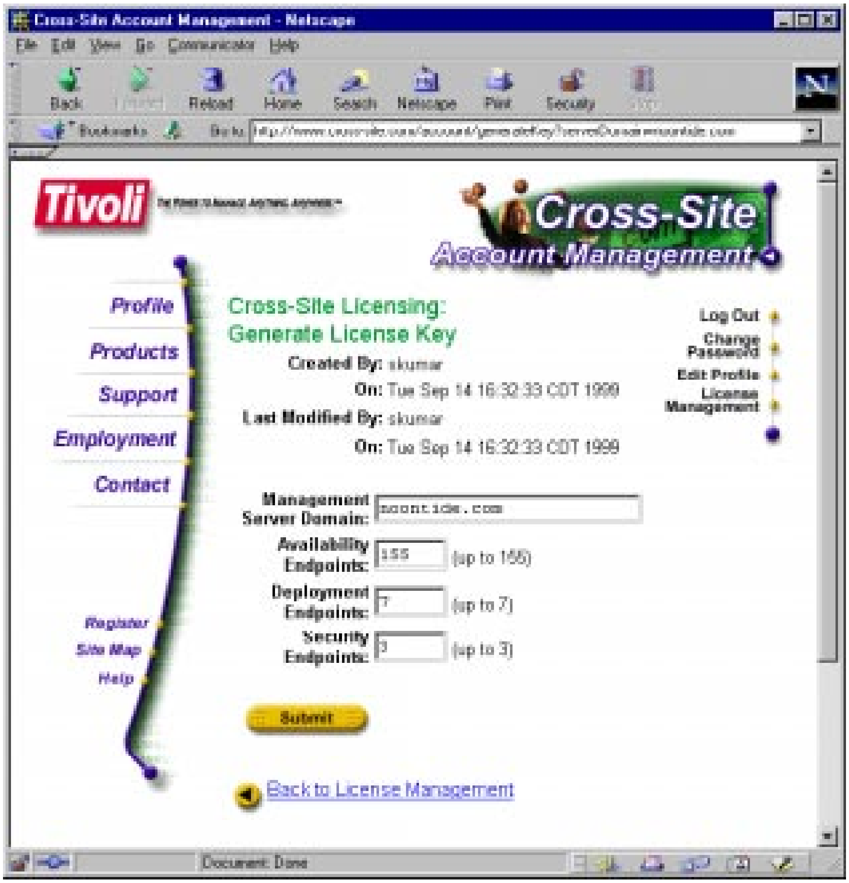
Purchase Orders

Reference Number	Availability		Deployment		Security	
	servers	endpoints	servers	endpoints	servers	endpoints
900009	1	5	1	7	1	3
910009	0	150	0	0	0	0
Total:	1	155	1	7	1	3
Available:	0	150	0	0	1	3

Cross-Site Account Management - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to: http://www.cross-site.com/account/showLicenses
Cross-Site
Account Management
Log Out
Change Password
Edit Profile
License Management
Create License Key
Delete License Key
Claim Purchase Order
Document: Done

9. To modify your existing license key, click your domain name in the table. A page is displayed that shows your existing configuration. If the numbers next to the fields have not increased to include your new purchase order, you need to reload the page.

10. Fill in the fields according to the number of clients you purchased. Be sure to include the existing clients in addition to the new ones.


Cross-Site Account Management - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to:
Tivoli
Cross-Site Account Management
Profile
Products
Support
Employment
Contact
Register
Site Map
Help
Log Out
Change Password
Edit Profile
License Management
Submit
Back to License Management
Document: Done

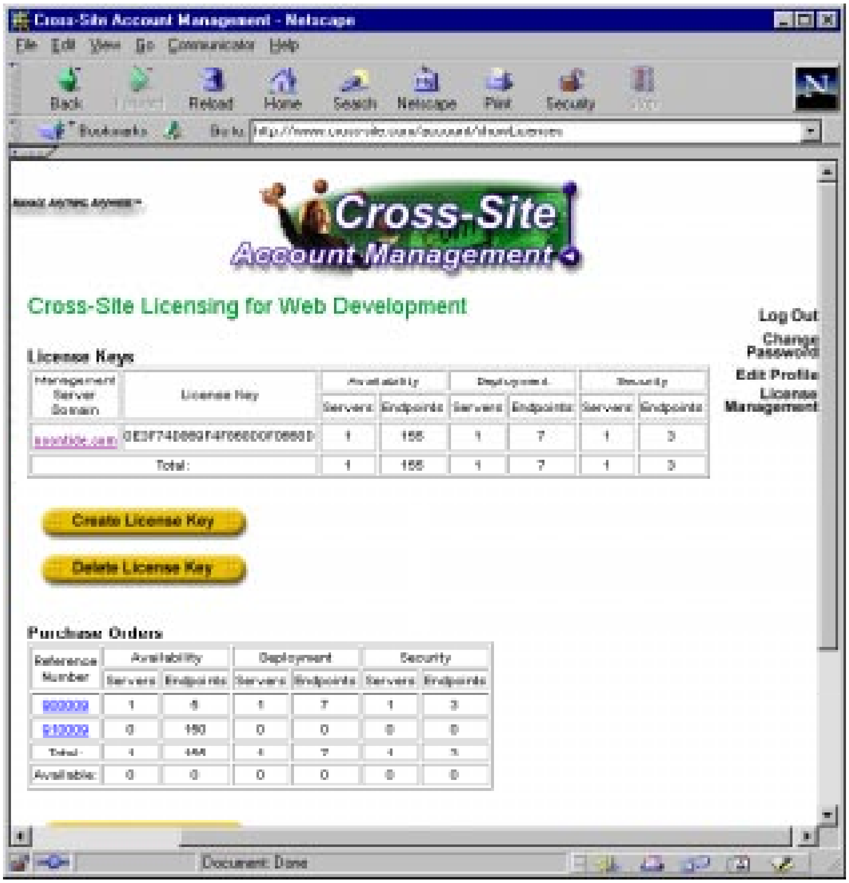
Cross-Site Licensing:
Generate License Key

Created By: skumar
On: Tue Sep 14 16:32:33 CDT 1999
Last Modified By: skumar
On: Tue Sep 14 16:32:33 CDT 1999

Management Server Domain: moontide.com
Availability Endpoints: 155 (up to 155)
Deployment Endpoints: 7 (up to 7)
Security Endpoints: 3 (up to 3)

11. Click **Submit**. The system processes your new configuration and displays a page with a new license key listed.

12. Click the **Return** link. The License Management page is displayed and the new license key is displayed in the first table.



Cross-Site Account Management - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to: http://www.crosssite.com/account/showLicenses
Cross-Site Account Management
Log Out
Change Password
Edit Profile
License Management
Create License Key
Delete License Key
Document: Done

Cross-Site Licensing for Web Development

License Keys

Management Server Domain	License Key	Availability		Deployment		Security	
		Servers	Endpoints	Servers	Endpoints	Servers	Endpoints
[illegible]	0E3F74D8B9F4F068D0F08881	1	155	1	7	1	3
Total:		1	155	1	7	1	3

Purchase Orders

Reference Number	Availability		Deployment		Security	
	Servers	Endpoints	Servers	Endpoints	Servers	Endpoints
[illegible]	1	5	1	7	1	3
[illegible]	0	150	0	0	0	0
Total:	1	155	1	7	1	3
Available:	0	0	0	0	0	0

13. Highlight the license key and copy it to your system’s clipboard, so that you can install it on your management server. If the browser will not allow you to highlight the license key, print this page or make note of the key.

You can now install the new license key on your Cross-Site server. Complete the steps in the following section to do so.

Installing Your License Key

You must install the license key on the management server before installing the additional application on the server, and before installing any additional agents. Install the license key on your Cross-Site management server by completing these steps:

1. Go to the following URL:

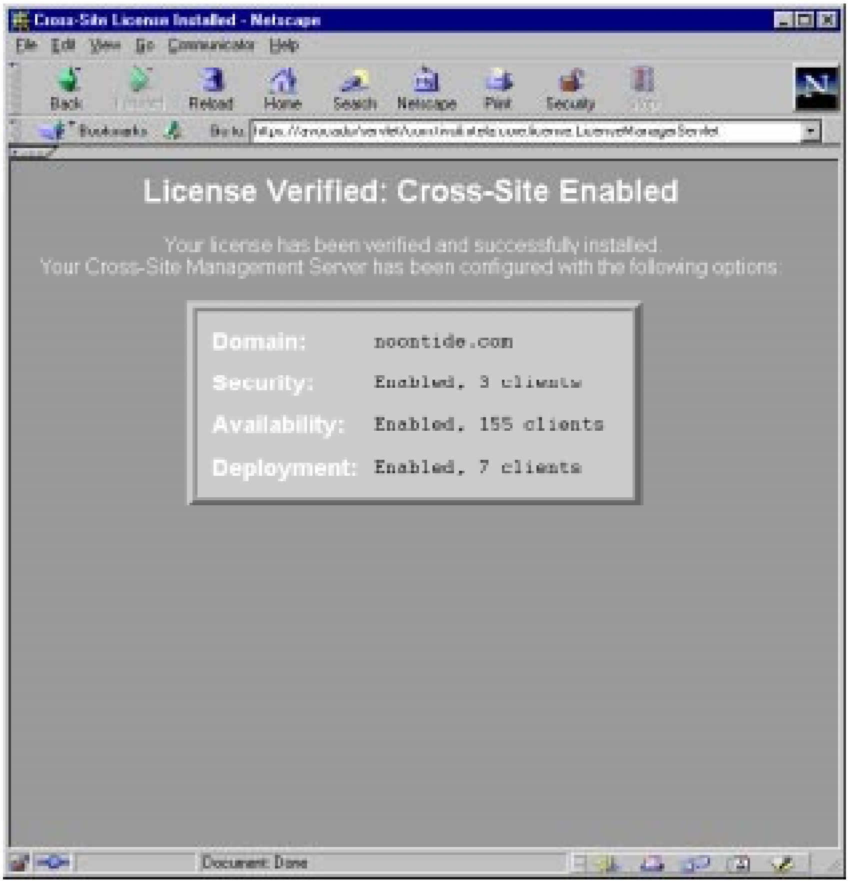
   *protocol***://***server***/servlet/**
   com.tivoli.xtela.core.license.LicenseManagerServlet

   where *protocol* and *server* are the values for your Cross-Site server.

   You are prompted to log in to the web server that is used by the Cross-Site server. After you log in, a page is displayed that lists the current domain name and clients, which are included in the currently installed license key.

2. Enter your new license key in the field.

3. Click **Commit Changes**. A page similar to the following is displayed:



License Verified: Cross-Site Enabled

Your license has been verified and successfully installed.
Your Cross-Site Management Server has been configured with the following options:

Domain:	noontide.com
Security:	Enabled, 3 clients
Availability:	Enabled, 155 clients
Deployment:	Enabled, 7 clients

After installing the license key, restart the Cross-Site server and proceed with the installation of the Cross-Site applications on the server and clients.

D

Uninstalling Cross-Site

If required, you can remove your Cross-Site installation. The general steps for uninstalling Cross-Site are as follows:

1. Stop the Cross-Site agents.
2. Backup your database if you wish to preserve the Cross-Site data. Uninstalling Cross-Site deletes the Cross-Site management repository from the database.
3. Uninstall all Cross-Site agents.
4. Uninstall the Cross-Site console from all machines on which it was installed.
5. Stop the Cross-Site server.
6. Uninstall the Cross-Site server, including any applications you may have installed.

In general, you need **root** or **Administrator** privileges to perform these procedures on AIX, Solaris, or Windows NT systems, respectively. Refer to your Cross-Site installation notes for the values specified during Cross-Site's installation. You might need them for the following procedures.

Uninstalling Cross-Site Agents

You must manually delete the agent (resource) on the Cross-Site console because removing the agent software does not remove the agent from the management repository on the Cross-Site server.

On Windows NT

Complete the following steps to stop and remove a Cross-Site for Security agent. Note that you need **Administrator** privileges to remove the agent.

1. Select **Settings –> Control Panel** from the **Start** menu on the system running the Cross-Site agent.

2. Double-click on **Services**.

3. Select the **Tivoli Cross-Site for Security** entry.

4. Click the **Stop** button.

   You can also stop the Security agent from the command line on NT systems by entering one of the following commands:

   ```
   net stop “Tivoli Cross-Site for Security - Domestic”
   ```

   ```
   net stop “Tivoli Cross-Site for Security - Export”
   ```

5. Close the **Services** dialog.

6. On the Control Panel, double-click on **Add/Remove Programs**.

7. Select **Tivoli Cross-Site for Security**.

8. Click the **Add/Remove** button.

9. Answer the prompts provided by the uninstallation program.

10. Ensure that the Cross-Site for Security directory was removed. By default, the directory is as follows:
    C:\Program Files\Tivoli\Cross-Site for Security

On AIX

Enter the following commands to stop and remove a Cross-Site for Security agent. You must be **root** to do this.

1. Enter the following command to stop a Cross-Site for Security agent:

   ```
   /etc/Tivoli/XSite/XSITids/ids stop
   ```

2. Enter the following command if you installed the domestic version of Cross-Site (see the cover of your CD-ROM to confirm which version you have):

   ```
   installp -u xsite.secagent_dom.rte
   ```

   Enter this command if you installed the export version of Cross-Site:

   ```
   installp -u xsite.secagent_exp.rte
   ```

You can also use SMIT to uninstall the agent. After uninstalling the agent, ensure that its directory was removed. By default, the Security agent is installed in **/usr/Tivoli/XSite/XSITids**.

On Solaris

Enter the following commands to stop and remove a Cross-Site for Security agent. You must be **root** to do this.

1. Enter the following command to stop a Cross-Site for Security agent:

   ```
   /etc/init.d/ids stop
   ```

2. Enter the following command to remove the agent:

   ```
   pkgrm XSITids
   ```

   The following prompts are displayed:

   a. `The following package is currently installed:`
      `XSITids Tivoli Cross-Site for Security`

```
Do you want to remove this package?
```

Enter **y** to continue.

b. `This package contains scripts which will be executed with super-user permission during the process of removing this package.`

```
Do you want to continue with the removal of this
package?
```

Enter **y** to remove the Security package.

After uninstalling the Security agent, ensure that its installation directory was removed.

Uninstalling the Console

Remove the console by completing one of the following procedures. If the console is running, close its window first.

On Windows 95, 98, and NT

Complete the following steps:

1. Select **Settings –> Control Panel** from the **Start** menu.
2. Double-click on the **Add/Remove Programs** icon.
3. Select **Tivoli Cross-Site Console**.
4. Click the **Add/Remove** button.
5. Remove the directory where the console is installed. By default, the directory is **C:\Program Files\Tivoli\Cross-Site-Console**.

On AIX

To remove the console on AIX, enter one of the following commands. You must be **root** to perform this operation.

- Enter the following command if you installed the domestic version of Cross-Site (see the cover of your CD-ROM to confirm which version you have):

  ```
  installp -u xsite.console_dom.rte
  ```

- Enter this command if you installed the export version of Cross-Site:

  ```
  installp -u xsite.console_exp.rte
  ```

You can also use SMIT to uninstall the console. After you uninstall the console, ensure that its directory was removed. By default, the console is installed in **/usr/Tivoli/XSite/XSITconsl**.

On Solaris

To remove the console on Solaris systems, complete the following steps. You must be **root** to perform this operation.

1. Enter the following on the command line of the Solaris system:

   ```
   pkgrm XSITcons
   ```

   The following prompt is displayed:

   ```
   The following package is currently installed:
   XSITcagt Tivoli Cross-site Core Agent. Basis for
   software installation and update

   Do you want to remove this package?
   ```

   Enter **y** to continue.

2. Remove the *install_dir*/**XSITcons** directory, where *install_dir* is the directory specified as the console's installation directory. (Ensure that you remove the **logs** subdirectory, as well. If not, reinstalling the console will fail.)

Uninstalling the Cross-Site Server

Complete one of the following procedures to remove the Cross-Site server:

On Windows NT

Complete the following steps to uninstall the Cross-Site management server on Windows NT:

1. Shut down the Netscape server by selecting **Start -> Programs -> Tivoli Cross-Site -> Stop Cross-Site Server**.

2. Begin the uninstall procedure. Click on **Start ->Settings-> Control Panel -> Add/Remove Programs**.

   a. Select the **Install/Uninstall** tab.

   b. Select **Tivoli Cross-Site Security Server - Domestic/Export** from the list of software that can be uninstalled.

   c. Click **Add/Remove**.

   d. Select **Tivoli Cross-Site Management Server - Domestic/Export** from the list of software that can be uninstalled.

   e. Click **Add/Remove**.

After the management server is removed, ensure that its installation directory was deleted. By default, the server was installed in **C:\Program Files\Tivoli\Cross-Site-Server\XSITsagt**.

On AIX

Complete the following steps to remove the Cross-Site server on AIX:

1. If the Cross-Site server is running, shut it down by stopping the web server, as follows:

   a. To stop the Netscape web server, enter the following command:

   ```
   install_dir/https-server/stop
   ```

   where *install_dir* is the directory path to the web server's installation directory. By default, the Netscape Enterprise Server is installed in **/usr/netscape/suitespot** on AIX. The *server* variable specifies the name of the web server. Wait several minutes to ensure that the web server shuts down completely.

   b. Verify that all processes related to Cross-Site were shutdown with the web server. Enter the following command:

   ```
   /bin/ps -ef | grep user
   ```

   where *user* is that of the Netscape Enterprise Server.

   c. If processes are listed that are owned by the Netscape user, enter the following command to stop each process:

   ```
   kill -9 process
   ```

   You need to ensure that the **tuner.sh**, **native_threads/jre**, and (Java) **OutOfProcEngine** processes are stopped.

2. To remove the Cross-Site for Security package, enter the following command:

   ```
   installp -u xsite.secserver.rte
   ```

   If you would like to remove other Cross-Site application packages, such as Availability or Deployment, refer to the uninstalling section in the appropriate application's installation guide.

3. To remove the Cross-Site server's package, enter one of the following commands from the command line.

   ```
   installp -u xsite.mgmtserver_dom.rte
   ```

   if you have installed the domestic version of Cross-Site, or enter

   ```
   installp -u xsite.mgmtserver_exp.rte
   ```

   if you have installed the export version of Cross-Site.

4. If WebSphere is installed for Cross-Site's use only, you need to remove its packages. To remove all installed WebSphere filesets, enter the following:

   ```
   installp -u IBMWebAS
   ```

You can also use SMIT to uninstall the management server. After the management server is removed, ensure that its installation directory was deleted. By default, the server is installed in **/usr/Tivoli/XSite/XSITsagt**.

On Solaris

Complete the following steps to remove the Cross-Site server on Solaris:

1. If the server is running, shut it down by stopping the web server, as follows:

   a. To stop the Netscape web server, enter the following command:

      ```
      install_dir/https-server/stop
      ```

      where *install_dir* is the directory path to the web server's installation directory. By default, the Netscape Enterprise Server is installed in **/opt/netscape/suitespot** on Solaris. The *server* variable specifies the name of the web server. Wait several minutes to ensure that the web server shuts down completely.

   b. Verify that all processes related to Cross-Site were shutdown with the web server. Enter the following command:

```
/usr/ucb/ps -auxlww | grep user
```

where *user* is the user used when the Netscape Enterprise Server was installed.

c. If processes are listed that are owned by the Netscape user, enter the following command to stop each process:

```
kill -9 process
```

You need to ensure that the **tuner.sh** and **native_threads/jre** processes are stopped.

2. To remove the Cross-Site for Security package, enter the following command from the command line:

```
pkgrm XSITsecs
```

The following prompt is displayed:

```
The following package is currently installed:
XSITsecs Tivoli Cross-Site Security Server

Do you want to remove this package?
```

Enter **y** to continue. The following prompt is displayed:

```
This package contains scripts which will be executed with
super-user permission during the process of removing
this package.

Do you want to continue with the removal of this package?
```

Enter **y** to remove the Security package.

3. To remove the Cross-Site server’s package, enter the following command from the command line:

```
pkgrm XSITsagt
```

The following prompt is displayed:

```
The following package is currently installed:
XSITsagt Tivoli Cross-Site Server

Do you want to remove this package?
```

Enter **y** to continue. The following prompt is displayed:

```
This package contains scripts which will be executed with
super-user permission during the process of removing
this package.

Do you want to continue with the removal of this package?
```

Enter **y** to remove the Cross-Site server's package.

4. If WebSphere is installed for Cross-Site's use only, you need to remove its packages and directory. Complete the following steps to remove WebSphere:

   a. To remove WebSphere's resource files, enter the following command:

      ```
      pkgrm SERSCSEN
      ```

      The following prompt is displayed:

      ```
      The following package is currently installed:
      SERSCSEN IBM WebSphere Application Server Resource/
      Documentation Files - English

      Do you want to remove this package?
      ```

      Enter **y** to continue.

   b. To remove the Netscape plug-in package, enter the following:

      ```
      pkgrm SENs351
      ```

      The following prompt is displayed:

```
The following package is currently installed:
SENs351 IBM WebSphere Application Server - Netscape
Version 3.5.1 Plugin

Do you want to remove this package?
```

Enter **y** to continue. The following prompt is displayed:

```
This package contains scripts which will be executed
with super-user permission during the process of
removing this package.

Do you want to continue with the removal of this
package?
```

Enter **y** to remove WebSphere’s Netscape plug-in package.

c. To remove the WebSphere Application Server package, enter the following command:

```
pkgrm IBMWebAS
```

The following prompt is displayed:

```
The following package is currently installed:
IBMWebAS IBM WebSphere Application Server

Do you want to remove this package?
```

Enter **y** to remove WebSphere.

d. To remove WebSphere’s directory, remove the **/opt/IBMWebAS** directory.

5. To remove the directories containing the Cross-Site server, remove the *base_dir*/**XSITsagt** directory, where *base_dir* is the directory specified as the Cross-Site server’s base directory.

Files and Directories Installed for the Cross-Site Server

This section lists the files and directories that are installed and created when you install and run the Cross-Site management server. The *base_dir* indicates the base directory of the management server installation.

On Windows NT

The following files and directories are installed with the management and security servers:

base_dir \Backup*

base_dir \downloads*

base_dir \XSITsagt*

base_dir \XSITsecs*

The following files are installed with the Cross-Site for Security component of the management server:

base_dir \XSITsagt\bin\parse-ids.exe

base_dir \XSITsagt\bin\xs_createpol

base_dir \XSITsagt\bin\xs_updatepol

base_dir \XSITsagt\lib\secservice.jar

On AIX

The following files and directories are installed with the management server:

/usr/Tivoli/XSite/XSITsagt/*

/usr/Tivoli/XSite/XSITsagt/lib/*

/usr/Tivoli/XSite/XSITsagt/bin/*

/usr/Tivoli/XSite/XSITsagt/downloads/*

The following files are installed with the Cross-Site for Security component of the management server:

/usr/Tivoli/XSite/XSITsagt/bin/parse-ids

/usr/Tivoli/XSite/XSITsagt/bin/xs_createpol

/usr/Tivoli/XSite/XSITsagt/bin/xs_updatepol

/usr/Tivoli/XSite/XSITsagt/lib/secservice.jar

The installation of the Security component modifies the following files:

WebAS_base_dir/properties/bootstrap.properties

NSHOME/https-*server*/start

On Solaris

The following files and directories are installed with the management server:

base_dir /XSITsagt/*

base_dir /XSITsagt/lib/*

base_dir /XSITsagt/bin/*

base_dir /downloads/*

/opt/IBMWebAS/*

The following files are installed with the Cross-Site for Security component of the management server:

base_dir /XSITsagt/bin/parse-ids

base_dir /XSITsagt/bin/xs_createpol

base_dir /XSITsagt/bin/xs_updatepol

base_dir /XSITsagt/lib/secservice.jar

The installation of the Security component modifies the following files:

/opt/IBMWebAS/properties/bootstrap.properties

NSHOME/https-*server*/start

Files and Directories Installed for the Console

This section lists the files and directories that are installed and created when you install and run the Cross-Site console. The *base_dir* indicates the base directory of the installation. By default, the console is installed in the **C:\Program Files\Tivoli\Cross-Site-Console** folder on Windows, in **/usr/Tivoli/XSite/XSITconsl** on AIX, and in the **/opt/Tivoli/XSITcon** directory on Solaris.

On Windows 95, 98, and NT

These files and directories are installed with the Cross-Site console:

base_dir *

base_dir \bin*

base_dir \lib*

base_dir \OEM*

base_dir \.staging*

base_dir \configuration*

base_dir \logs*

These files and directories are created in the current working directory when you run the console:

base_dir \debug_console.cmd

base_dir \debug_stdout.log

base_dir \debug_stderr.log

base_dir \install.log

base_dir \Unwise.exe

base_dir \update.log

base_dir \configuration\console_curr.properties

base_dir \configuration\console_old.properties

On AIX

These files and directories are installed with the Cross-Site console:

/usr/Tivoli/XSite/XSITconsl/*

/usr/Tivoli/XSite/XSITconsl/bin/*

/usr/Tivoli/XSite/XSITconsl/lib/*

/usr/Tivoli/XSite/XSITconsl/logs/*

These files and directories are created in the current working directory when you run the console:

usr/Tivoli/XSite/XSITconsl/logs/Cross-Site_stdout.log

usr/Tivoli/XSite/XSITconsl/logs/Cross-Site_stderr.log

usr/Tivoli/XSite/XSITconsl/lib/console_curr.properties

usr/Tivoli/XSite/XSITconsl/lib/console_old.properties

On Solaris

These files and directories are installed with the Cross-Site console:

base_dir /XSITcons/*

base_dir /XSITcons/bin/*

base_dir /XSITcons/lib/*

base_dir /XSITcons/logs/*

These files and directories are created in the current working directory when you run the console:

base_dir /XSITcons/logs/Cross-Site_stdout.log

base_dir /XSITcons/logs/Cross-Site_stderr.log

base_dir /XSITcons/bin/console_curr.properties

base_dir /XSITcons/bin/console_old.properties

Files and Directories Installed for the Security Agent

This section lists the files and directories that are installed and created when you install and run the Cross-Site for Security agent. The *base_dir* indicates the base directory of the Security agent's installation. By default, the agent is installed in the **C:\Program Files\Tivoli\Cross-Site for Security** folder on Windows NT, in **/usr/Tivoli/XSite/XSITids** on AIX, and in the **/opt/XSITids** directory on Solaris.

On Windows NT

These files and directories are installed with the Security agent:

base_dir *

base_dir \bin*

base_dir \lib*

The following files are created when the agent starts.

base_dir \ids.cfg

base_dir \ids.msg

base_dir \ids.rules

The following directories are created when the agent starts. These directories reflect the files published on the Security agent channel, on the management server.

base_dir \.staging*

On AIX

These files and directories are installed with the Security agent:

/usr/Tivoli/XSite/XSITids/ids/*

/usr/Tivoli/XSite/XSITids/idsconfig

/etc/Tivoli/XSite/XSITids/ids

The following files are created when the agent starts:

/usr/Tivoli/XSite/XSITids/ids/ids.cfg

/usr/Tivoli/XSite/XSITids/ids/ids.pass

/usr/Tivoli/XSite/XSITids/ids/ids.msg

/usr/Tivoli/XSite/XSITids/ids/ids.rules

/etc/Tivoli/XSite/XSITids/ids.pass

The following directory is created when the agent starts. This directory reflects the files published on the Security agent channel, on the management server.

/usr/Tivoli/XSite/XSITids/ids/.staging/*

On Solaris

These files and directories are installed with the Security agent:

base_dir/XSITids/*

base_dir/XSITids/xsite/*

/etc/init.d/ids

/etc/rc2.d/K95ids

/etc/rc2.d/S95ids

The following files are created when the agent starts:

base_dir/XSITids/ids.cfg

base_dir/XSITids/ids.msg

base_dir/XSITids/ids.rules

The following directories are created when the agent starts. This directory reflects the files published on the Security agent channel, on the management server.

base_dir/XSITids/.staging/*

E

Glossary

If you cannot find a term in this glossary, refer to the IBM Dictionary of Computing, which is located at the following URL:

http://www.networking.ibm.com/nsg/nsgmain.htm

It defines technical terms used in the documentation for many IBM products. It also includes IBM product terminology as well as selected terms and definitions from various industry sources.

A

access control
In computer security, the process of ensuring that the resources of a computer system can only be accessed by authorized users in authorized ways. In Cross-Site, access control restricts access to services and channels on a Cross-Site management server.

access control list (ACL)
A list associated with an object that identifies all the subjects that can access the object and their access rights; for example, a list associated with a file that identifies users

who can access the file and identifies their access rights to that file. In Cross-Site, there are also ACL entries. These are the individual Cross-Site methods to which roles are assigned.

admin role See *role*.

administrator
A system or web administrator who is authorized to perform management tasks on the Cross-Site console. See also *end user* and *user resource*.

agent resource
A Cross-Site resource that represents the client on which a Cross-Site agent has been installed. When a Cross-Site agent is installed, it registers itself with its Cross-Site management server. A representation of the agent is then created in the management server's repository; this is the agent resource.

agent role See *role*.

alert A message generated when a Cross-Site for Security agent detects an intrusion attempt. An alert contains information about the incident and the severity of the intrusion.

any role See *role*.

application channel
See *channel*.

attack Any attempt by an unauthorized person to compromise the functionality of a networked system. See also *intrusion attempt.*

authentication
Verification of the identity of a user or the user's eligibility to access an object.

authorization

The process of granting a user either complete or restricted access to an object, resource, or function.

availability role

See *role*.

B

BAROC file (.baroc file)

In the event server of the Tivoli Enterprise Console, the internal representation of the defined event classes. Cross-Site provides a BAROC file for event integration with the TEC.

C

CA See *certificate authority*.

Castanet A suite of Java-based applications provided by Marimba Inc. that automatically distribute and maintain software applications and content within a company or across the Internet. Cross-Site uses the Castanet technology to implement it’s Cross-Site for Deployment and auto-update features.

certificate A digital document obtained from a registered certification authority (CA) that contains the identity and public key for a user or system component. In Cross-Site, certificates are used for authenticating and signing channels (using signing certificates), and for securing the Cross-Site management server (using root certificates). See also *foreign certificate*.

certificate authority (CA)

An organization that issues and signs certificates. A CA authenticates the certificate owner’s identity, the services that the owner is authorized to use, issues new certificates, renews existing certificates, and revokes certificates belonging to users who are no longer authorized to use them.

certification authority
See *certification authority*.

channel A container that resides on the Cross-Site server and provides restricted access to applications and information. A channel's content, which is one or more content bundles, can be downloaded, installed, and executed by agents. Cross-Site provides two types of channels:

data channel, which enables you to bundle any information with a channel that an end user can then download and copy to their local machine.

application channel, which enables you to bundle Java applications, applets, Windows applications, Visual Basic applications, or any native applications with a channel. The channel then runs on the end users machine, thereby running the contained application. This type of channel is supported through Tivoli Services only.

collaborative management
A cooperative relationship between Internet commerce partners and Internet service providers (ISPs) to ensure the successful completion of business transactions.

collection A Cross-Site resource that groups other resources, thus providing users with a single view of related resources. The Cross-Site console uses folders to represent collections in trees.

console See *Cross-Site console*.

content bundle
A grouping of application or data files that define the content associated with a Deployment channel.

coordinated universal time (UTC)

The time scale, based on the Systeme International (SI) second, as defined and recommended by the Comite Consultatif International de la Radio (CCIR) and maintained (using an atomic clock) by the Bureau International des Poids et Mesures (BIPM). The Systeme International is based on three fundamental units of measure (the meter, the kilogram, and the second) and is sometimes called the “MKS system” because of these units. For most practical purposes, UTC is equivalent to the mean solar time at the prime meridian (0 degrees longitude) of Greenwich, England, which is known as Greenwich mean time.

core services

Services provided by the Cross-Site management server that support all Cross-Site applications. These services include the event service, task manager, policy manager, data manager, channel manager, framework security, and auto-updating.

Cross-Site agent

The client software that can include the Cross-Site for Availability, Cross-Site for Deployment, and Cross-Site for Security components.

Cross-Site console

Cross-Site’s desktop. The console is the user interface where basic operations to manage the Cross-Site environment are performed. The console displays and organizes the resources, policies, tasks, events, and reports of the different Cross-Site applications.

Cross-Site for Availability

A policy-based application that gathers Internet and intranet information. Availability agents monitor and collect data about the performance of actual Internet and TCP/IP transactions from client machines. Availability also scans web sites to determine the integrity of each page.

Cross-Site for Deployment

A policy-based Cross-Site application that enables companies to securely distribute applications to end users over an intranet or the Internet. Cross-Site for Deployment leverages Marimba's Castanet technology to provide its distribution and update capabilities.

Cross-Site for Security

A policy-based intrusion detection system that relies on the Security agent to monitor networks to detect external and internal attacks.

Cross-Site management repository

A collection of tables and data that support Cross-Site functions in a relational database management system (RDBMS). The management repository is created in your RDBMS during Cross-Site installation.

Cross-Site management server

In the Cross-Site environment, the server hosts all of the resources and provides services to all of the Cross-Site applications. The Cross-Site management server works in conjunction with the web server, database server, and IBM WebSphere Application Server to provide services to the Cross-Site applications and console. Also known as the management server or Cross-Site server.

D

database A collection of interrelated data organized according to a database schema to serve one or more applications.

data channel

See *channel*.

default policy

A set of resource property values that are assigned to a resource when the resource is created. When you create a

Cross-Site resource, it is assigned the default policy for its type. See also *policy types*.

demilitarized zone (DMZ)
The area between two firewalls that insulates your internal network from the Internet.

deployment role
See *role*.

DHCP See *Dynamic Host Configuration Protocol*.

digital certificate
See *certificate*.

digital signature
Data that is appended to or cryptographically transformed by a digital certificate. This data, or digital signature, enables the recipient of the data to verify the source and integrity of the data and to recognize potential forgery. In Cross-Site, some channels must be signed with a digital signature from a trusted certification authority.

DMZ See *demilitarized zone*.

DNS See *Domain Name System*.

domain In general, the part of a computer network in which the data processing resources are under common control. In Cross-Site, all elements of Cross-Site that enable the core services and applications to provide function and are managed by a Cross-Site management server. This can also be referred to as an administrative domain. See also *foreign domain*.

domain name
On the Web, a domain name is the part of the URL that tells a server using Domain Name System (DNS) where to forward a request for a web page. A domain name consists of a sequence of sub-domain names separated by a

delineator character. For example, if the fully qualified domain name (FQDN) of a host system is ralvm7.vnet.ibm.com, each of the following is a domain name: ralvm7.vnet.ibm.com, vnet.ibm.com, and ibm.com.

Domain Name System (DNS)
The way that Internet domain names are located and translated into Internet protocol (IP) addresses. Because maintaining a central list of domain-name or IP-address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority.

Dynamic Host Configuration Protocol (DHCP)
A protocol defined by the Internet Engineering Task Force (IETF) that is used for dynamically assigning IP addresses to computers in a network.

E

encryption A method of encoding messages to provide privacy for communications as they move over intranets or the Internet. Some methods of encrypting, such as 128-bit encryption, are so difficult to break that US export laws permit them to be used only within the United States. The Cross-Site suite is available in two levels of encryption: 56-bit encryption, for non-financial institutes outside of the US and Canada, and 128-bit encryption, for all other customers.

end user Any computer user who relies on or requires the services of the Cross-Site agent. In particular, an end user interacts with the agent on a client machine and does not have access to the Cross-Site console or administrative functions. See also *administrator* and *user resource*.

ethernet A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. See also *token ring*.

event In Cross-Site, an alert, error, or status message generated by Cross-Site server and application operations and displayed on the console. An event informs you when a service or application is functioning and notifies you when policy has been violated.

event adapter

In a Tivoli environment, software that converts events into a format that the Tivoli Enterprise Console can use and forwards the events to the event server.

environment variable

An open-ended set of names, each of which identifies a null-terminated string that represents its value. The following are common environment variables that may be handy during the installation and use of Cross-Site.

JAVA_HOME, which represents the root location of a Java installation

ORACLE_HOME, which represents the root location of an Oracle installation

ORACLE_SID, which represents the name of the Oracle database; SID stands for system identifier

NSHOME, which represents the full path to Netscape’s home directory

explorer A panel on the Cross-Site console that enables you to review and set properties for resources, policy, tasks, and events in a view. Explorers separate the elements that are managed. For example, if you are working in the Admin view, the Roles, Certificates, and Permissions explorers are displayed.

Glossary

extranet A private, virtual network that uses access control and security features to restrict the usage of one or more intranets attached to the Internet to selected subscribers (such as personnel from a sponsoring company and its business partners). See also *intranet*.

F

firewall A gateway device that protects and controls the connection of one network to other networks. The firewall (a) prevents unwanted or unauthorized communication traffic from entering the protected network and (b) allows only selected communication traffic to leave the protected network.

flooding In computer security, “classic” Denial of Service (DOS) attacks that do not directly harm the target system but make it difficult for other systems to use the target system. Flooding is used by hackers to determine where the holes on a network exist. This is done by scanning a network for the systems (IP addresses) and ports that respond to connection requests.

foreign certificate

A certificate that is generated by a certificate authority that Cross-Site does not support or recognize, such as one generated by your company.

foreign certificate authority (CA)

A certificate authority that Cross-Site does not support or recognize.

foreign domain

A domain associated with a Cross-Site management server other than the local management server. (Each management server represents a domain.)

framework services

See *core services*.

fully qualified domain name

In the Internet suite of protocols, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is ralvm7.vnet.ibm.com.

G

Greenwich mean time (GMT)

The mean solar time at the prime meridian (0 degrees longitude) of Greenwich, England. Greenwich mean time is sometimes called Z time or Zulu time. Although Greenwich mean time and coordinated universal time are sometimes used interchangeably, they are not synonyms. Greenwich mean time is an approximate time. Because the second is no longer defined in terms of astronomical phenomena, the preferred name for this time scale is coordinated universal time (UTC).

H

heartbeat A signal that the Cross-Site for Security agent sends to the Cross-Site management server to convey that it is still active.

host name See *fully qualified domain name*.

HTML See *Hypertext Markup Language*.

HTTP See *Hypertext Transfer Protocol*.

HTTPS See *Hypertext Transfer Protocol Secure*.

HTTP proxy server

An HTTP server that receives requests intended for another server and that acts on the client's behalf (as the client's proxy) to obtain the requested service.

Hypertext Markup Language (HTML)
A markup language that is specified by an SGML document type definition (DTD) and is understood by all web servers.

Hypertext Transfer Protocol (HTTP)
The protocol that is used to transfer and display hypertext documents. HTTP is the standard web browser protocol.

Hypertext Transfer Protocol Secure (HTTPS)
The standard secure web protocol. This protocol uses Secure Sockets Layer (SSL) encryption.

I

IBM WebSphere Application Server (IBMWebAS or WebSphere)
IBM's Java servlet-based application environment for building, displaying, and managing web applications. In Cross-Site, WebSphere is installed behind the web server.

incident A signature detected by the Cross-Site for Security agent that indicates questionable network activity.

install role See *role*.

Internet service provider (ISP)
An organization that provides access to the Internet.

intranet A private network that integrates Internet standards and applications (such as web browsers) with an organization's existing computer networking infrastructure. See also *extranet*.

intrusion attempt
An attempt by an unauthorized person to access or destroy a network resource.

Internet protocol (IP) address

The unique 32-bit address that specifies the location of each device or workstation on the Internet. For example, 9.67.97.103 is an IP address.

ISP See *Internet service provider*.

J

Java Database Connectivity (JDBC)

An application programming interface (API) that has the same characteristics as Open Database Connectivity (ODBC) but is specifically designed for use by Java database applications. Also, for databases that do not have a JDBC driver, JDBC includes a JDBC to ODBC bridge, which is a mechanism for converting JDBC to ODBC; it presents the JDBC API to Java database applications and converts this to ODBC. JDBC was developed by Sun Microsystems, Inc. and various partners and vendors.

Java Development Kit (JDK)

A software package that can be used to write compile, debug, and run Java applets and applications.

Java Runtime Environment (JRE)

A subset of the Java Development Kit (JDK) that contains the core executables and files that constitute the standard Java platform. The JRE includes the Java Virtual Machine (JVM), core classes, and supporting files.

Java servlet The server-side analog of a Java applet. Servlets are dynamically loaded in response to HTTP requests. Their effects might range from simple HTML generation to complex DBMS queries. In Cross-Site, all management server facilities are implemented through Java servlets.

Java Virtual Machine (JVM)

A software implementation of a central processing unit (CPU) that runs compiled Java code (applets and applications).

JAVA_HOME

An environment variable that represents the root location of a Java installation.

JDBC See *Java Database Connectivity*.

JDK See *Java Development Kit*.

JRE See *Java Runtime Environment*.

JVM See *Java Virtual Machine*.

K

KeyRing A special control file that governs access to secure web servers and Cross-Site management servers. The KeyRing contains the public keys, private keys, trusted roots, certificates, names of sites, and CAs that are trusted and, therefore, authorized for access.

Key File Password

The password for the web server's key file that secures a server. This password is chosen when a certificate is purchased from a CA and is needed when you start the (secure) web server.

key ring See *KeyRing*.

M

management repository

See *Cross-Site management repository*.

management server
See *Cross-Site management server*.

mgmtserver role
See *role*.

N

NetView See *Tivoli NetView*.

Network File System (NFS)
A protocol developed by Sun Microsystems Incorporated, that allows any host in a network to mount another host's file directories. Once mounted, the file directory appears to reside on the local host.

NSHOME An environment variable that represents the full path to Netscape's home directory.

O

Open Systems Interconnection (OSI)
A standard architecture or model for how messages should be transmitted between any two points in a telecommunication network. The reference model defines seven layers of functions that take place at communication endpoints. This standard is a guide for product developers that ensures that their products will consistently work with other products.

ORACLE_HOME
An environment variable that represents the root location of an Oracle installation.

ORACLE_SID
An environment variable that represents the name of the Oracle database; SID stands for system identifier.

P

PDF See *portable document format*.

performance monitoring
The Cross-Site for Availability function that monitors TCP/IP services on a client system and logs data to a local file. Availability agents upload this data to the Cross-Site management server.

policy A set of rules applied to Cross-Site resources that control the behavior of those resources.

policy types The predefined set of policies from which you can create policy for a Cross-Site resource. Policy can be created in Cross-Site using the following pre-defined policy types:

Intrusion Detection policy is a Cross-Site for Security policy that assigns Security-related rules to an agent resource to define security and intrusion detection behavior.

Availability Agent policy is a Cross-Site for Availability policy that assigns monitoring rules to an agent.

Site Scan policy is a Cross-Site for Availability policy that controls the behavior of the scan that collects information about a particular web site.

Channel policy is a Cross-Site for Deployment policy that controls how often each agent checks the channel for updates; the interval between each check for channel updates; and the time period during which checks for channel updates should occur.

Portable Document Format (PDF)
A standard specified by Adobe Systems, Incorporated, for the electronic distribution of documents. PDF files are compact; can be distributed globally via e-mail, the Web, intranets, or CD-ROM; and can be viewed with the Acrobat

Reader, which is software from Adobe Systems that can be downloaded at no cost from the Adobe Systems home page, which is located at the following URL:

http://www.adobe.com

PostScript (PS)
A standard specified by Adobe Systems, Incorporated, that defines how text and graphics are presented on printers and display devices.

proxy server
A server that receives requests intended for another server and acts on the client's behalf to access the requested server. A proxy server is often used when a client and the server are incompatible for direct connection. For example, when the client is unable to meet the security authentication requirements of a server but should be permitted some service, a proxy with the appropriate access is used. See also *HTTP proxy server* and *SOCKS server*.

principal A Cross-Site entity to which security roles can be assigned in order to grant permissions.

PS See *PostScript*.

publish The process of making a channel available on a Cross-Site server, enabling the channel to be downloaded by subscribed agents.

R

RDBMS See relational database management system.

realm A name used by a browser in correlation with a URL to save the password information you enter so that it can authenticate automatically on the next challenge.

relational database management system (RDBMS)

A collection of hardware and software that organizes and provides access to a relational database.

remote procedure call (RPC)

1) A facility that a client uses to request the execution of a procedure call from a server. This facility includes a library of procedures and an external data representation.
(2) A client request to a service provider located in another node.

resource In Cross-Site, any entity that can have policy applied to it and, therefore, can be managed. A resource is represented in the management repository by a database object and, on the Cross-Site console, by an icon in the explorer's tree. Resources include agents, sites, channels, collection, and users.

role A set of actions and responsibilities associated with a particular activity. In Cross-Site, roles are used to grant privileges to principals and control access to services and Deployment channels. The following roles are provided by Cross-Site:

admin, which is for administrators who need full access to all services and channels. Assign this role to a person who is responsible for making organizational and content changes to the management server. This role is equivalent to root on UNIX, or Administrator on NT. agent, which is assigned only to Cross-Site agents for Cross-Site operations.

any, which is only used in ACL entries. It provides read-only access to non-critical information for any authenticated principal.

availability, which is for end users of Cross-Site agents who must install and use the agent component of the Cross-Site for Availability application.

deployment, which is for end users of Cross-Site agents who must install and use the agent component of Cross-Site for Deployment.

install, which is for users who are responsible for installing Cross-Site for Security agents.

mgmtserver, which is automatically assigned to Cross-Site servers only; this role is for inter-domain operations. This role is not for users.

securityAgent, which is automatically assigned to all Cross-Site for Security agents. This role is not for users.

user, which is for end users who run agents an need read-only access to information an executable files on the Cross-Site server. This role should be assigned to end users who do not administer the product.

RPC See *remote procedure call*.

S

Secure Sockets Layer (SSL)
A secure protocol that allows data to be encrypted and enables clients to authenticate a server in client-server communication.

securityAgent role
See *role*.

Security agent
See *Cross-Site agent*.

SENs351 A Netscape 3.5.1 plug-in for WebSphere.

SERSCSEN The WebSphere Application Server resource files, which enable you to administer WebSphere, if necessary.

servlet See *Java servlet*.

signature In Cross-Site for Security, a sequence of IP packets that characterizes a security threat.

signing certificate
See *certificate.*

signing password
In general, the password required to use a digital certificate. In Cross-Site, the password that must be entered by the publisher of the channel to sign a channel with the particular signing certificate.

Simple Mail Transfer Protocol (SMTP)
In the Internet suite of protocols, an application protocol for transferring mail among users in the Internet environment. SMTP specifies the mail exchange sequences and message format. It assumes that the Transmission Control Protocol (TCP) is the underlying protocol.

Simple Network Management Protocol (SNMP)
In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

site resource
A Cross-Site resource that represents a web site that you wish to monitor. You create a site resource to designate it as the target of an Availability task, or site scan.

site scan An Availability task that is used to "crawl" web sites, scanning them for availability information such as the presence of broken links.

SMIT See *System Management Interface Tool.*

SMTP See *Simple Mail Transfer Protocol*.

SNMP See *Simple Network Management Protocol*.

SOCKS server

A circuit-level gateway that provides a secure one-way connection through a firewall to server applications in network that is not secure.

SSL See *Secure Sockets Layer.*

subscribe An action that enables an interested end user to use his or her Deployment agent to download, install, launch and view a channel’s files onto your local drive.

System Management Interface Tool (SMIT)

An interface tool of the AIX operating system for installing, maintaining, configuring, and diagnosing tasks.

T

tablespace In relational database management systems, an abstraction of a collection of containers in which database objects are stored.

task An action that can be performed on one or more resources in a Cross-Site domain. A task defines the application or class to be invoked when the task is executed. It also defines the schedule under which the task will execute.

TCP/IP See *Transmission Control Protocol/Internet Protocol*.

TEC See *Tivoli Enterprise Console*.

timeout A time interval allotted for certain operations to complete; for example, the period of time allotted for a response before a system operation is interrupted and must be restarted.

time stamp The value on an object that is an indication of the system time at some critical point in the history of the object.

Tivoli Enterprise Console (TEC)

A Tivoli Enterprise product that collects, processes, and automatically initiates corrective actions for system, application, network, and database events; it is the central control point for events from all sources. The Tivoli Enterprise Console provides a centralized, global view of the network computing environment; it uses distributed event monitors to collect information, a central event server to process information, and distributed event consoles to present information to system administrators.

Tivoli NetView

A Tivoli Enterprise product that enables distributed network management across multiple operating systems and protocols.

Tivoli Software Distribution

A Tivoli Enterprise product that automates software distribution to clients and servers in a network computing environment. An organization can use this product to install and update applications and software in a coordinated, consistent manner across a network. Tivoli Software Distribution creates file packages and distributes them to predefined subscribers.

token ring (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations.
(2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another.
See also *ethernet*.

Transmission Control Protocol/Internet Protocol (TCP/IP)

(1) The Transmission Control Protocol and the Internet Protocol, which together provide reliable end-to-end connections between applications over interconnected networks of different types.
(2) The suite of transport and application protocols that run over the Internet Protocol.

trusted root In the Secure Sockets Layer (SSL), the public key and associated distinguished name of a certificate authority (CA).

U

user resource

A Cross-Site principal that provides unique access to different types of Cross-Site administrators and end users. You, acting as a Cross-Site administrator, create a user resource that the agent’s installation program can use to access the Cross-Site server.

user role See *role*.

UTC See *coordinated universal time*.

V

view On the Cross-Site console, a collection of panels that enables you to view and manipulate Cross-Site objects. Cross-Site offers six views: Global, Availability, Security, Deployment, Admin, and Help. The views that are available to you depend on the particular applications that you have installed.

W

WebSphere See *IBM WebSphere Application Server*.

X

XSITavls The package name for the Cross-Site for Availability component of the management server.

XSITsagt The Cross-Site package name for the management server.

XSITsdep The package name for the Cross-Site for Deployment component of the management server.

XSITsecs The package name for the Cross-Site for Security component of the management server.

Index

A

admin user 70
agents
- installing on AIX 144
- installing on NT 138
- installing on Solaris 149
- stopping on AIX 237
- stopping on NT 236
- stopping on Solaris 237
- uninstalling on AIX 237
- uninstalling on NT 236
- uninstalling on Solaris 237
- verifying installation 154

C

certificate authority (CA), description of 173
certificates 173
- certificate authority (CA) 173
- channel signing, description of 178
- exporting to a PKCS#12 file 213
- generating a CSR 188
- generating an in-house server certificate 194
- generating an in-house signing certificates 215
- how Cross-Site uses certificates 179
- importing roots for signing certificates 217
- importing signing certificates 220
- obtaining for securing the server 179

certificates (cont.)
- obtaining for signing channels 203
- overview 173
- purchasing a server certificate 190
- purchasing signing certificates 209
- root, description of 177
- server, description of 177
- supported server certificates 182
- supported signing certificates 206
- types 176

channel signing certificate, description of 178
console
- files and directories installed on AIX 249
- files and directories installed on Solaris 249
- files and directories installed on Windows 248
- importing root certificates 217
- importing signing certificates 220
- installing on AIX 117
- installing on Solaris 122
- installing on Windows 111
- prerequisites for installing 107
- proxy settings 116
- running on AIX 121
- running on Solaris 126
- running on Windows 115
- uninstalling on AIX 239
- uninstalling on Solaris 239
- uninstalling on Windows 238

creating users for agent installation 134
Cross-Site core services
- *See* core services

Cross-Site for Security
- *See* Security

Cross-Site management repository
  See management repository
Cross-Site management server
  See Cross-Site server
Cross-Site server
  files and directories installed on AIX 246
  files and directories installed on NT 246
  files and directories installed on Solaris 247
  installing on AIX 59
  installing on NT 48
  installing on Solaris 83
  pinging 55
  prerequisites 7
  restarting on AIX 77
  restarting on NT 54
  restarting on Solaris 102
  stopping on AIX 241
  stopping on NT 240
  stopping on Solaris 242
  uninstalling on AIX 241
  uninstalling on NT 240
  uninstalling on Solaris 242
  users created during installation 70

D

database
  configuring before Cross-Site server installation 15
  installation recommendations 15
  verifying the Cross-Site tables 57
directories
  created for console on AIX 249
  created for console on Solaris 249
  created for console on Windows 248
directories (cont.)
  created for Cross-Site server on AIX 246
  created for Cross-Site server on NT 246
  created for Cross-Site server on Solaris 247
  created for Security agent on AIX 251
  created for Security agent on NT 250
  created for Security agent on Solaris 251

E

exporting certificates 213

G

generating
  certificate signing request (CSR) 188
  in-house server certificate 194
  in-house signing certificate 215
  key-pair file 184
getting started 157

H

HTTPS, enabling on the web server 196

I

IBM WebAS
  See WebSphere

IBM WebSphere Application Server
  See WebSphere
importing
  root certificates 199, 217
  signing certificates 220
installation
  console on AIX 117
  console on Solaris 122
  console on Windows 111
  Cross-Site server on AIX 59
  Cross-Site server on NT 48
  Cross-Site server on Solaris 83
  files and directories of Security agent on AIX 251
  files and directories of Security agent on NT 250
  files and directories of Security agent on Solaris 251
  getting started after 157
  Security agent on AIX 144
  Security agent on NT 138
  Security agent on Solaris 149
  Security on AIX server 64
  Security on NT server 53
  Security on Solaris server 100
  server certificate 196
  users created 70

K

Key File Password
  generating 187
  value of 69
key-pair file 184
key-pair password 187
KeyRing.class file 199
keys, description of 174

L

license key
  installing 52
  modifying and reinstalling 225
License manager 52
logging in to Cross-Site
  using AIX console 121
  using NT console 115
  using Solaris console 126

M

management repository
  table space prerequisites 15
  verifying installation 57

N

NES requirements 25

P

pinging the Cross-Site server 55
PKCS#12 file format 213
pre-installation steps 7
prerequisites
  Cross-Site server 7
  database configuration 15
  database size estimates 15
  installing the console 107
  installing the Security agent 129
  management repository table space 15
  web server 25
private key 174
proxy server, specifying during login 116
public key 174

purchasing
- server certificate 190
- signing certificates 209

R

restarting the Cross-Site server on AIX 77
restarting the Cross-Site server on NT 54
restarting the Cross-Site server on Solaris 102
running the console on AIX 121
running the console on Solaris 126
running the console on Windows 115

S

Secure Sockets Layer
- *See* SSL

Security
- agent prerequisites 129
- installing on AIX server 64
- installing on NT server 53
- installing on Solaris server 100
- installing the agent on AIX 144
- installing the agent on NT 138
- installing the agent on Solaris 149
- server prerequisites 7
- stopping agents on AIX 237
- stopping agents on NT 236
- stopping agents on Solaris 237
- uninstalling the agent on AIX 241
- uninstalling the agent on NT 240
- uninstalling the agent on Solaris 242
- uninstalling the console on AIX 239

Security (cont.)
- uninstalling the console on Solaris 239
- uninstalling the console on Windows 238
- uninstalling the server on AIX 237
- uninstalling the server on NT 236
- uninstalling the server on Solaris 237

Security agent
- installation files and directories on AIX 251
- installation files and directories on NT 250
- installation files and directories on Solaris 251
- installing on AIX machine 144
- installing on NT machine 138
- installing on Solaris machine 149
- prerequisites for installing 129
- stopping on AIX 237
- stopping on NT 236
- stopping on Solaris 237
- uninstalling on AIX 237
- uninstalling on NT 236
- uninstalling on Solaris 237

server certificate, description of 177
signing certificate
- *See* certificates

SSL, enabling on the web server 196
starting the console on AIX 121
starting the console on Solaris 126
starting the console on Windows 115
stopping
- Cross-Site server on AIX 241
- Cross-Site server on NT 240
- Cross-Site server on Solaris 242
- Security agents on AIX 237
- Security agents on NT 236
- Security agents on Solaris 237

U

uninstalling
- consoles on AIX 239
- consoles on Solaris 239
- consoles on Windows 238
- Cross-Site servers on AIX 241
- Cross-Site servers on NT 240
- Cross-Site servers on Solaris 242
- Security agents on AIX 237
- Security agents on NT 236
- Security agents on Solaris 237

users
- admin 70
- changing password of 157
- creating 134
- install 70

V

verifying
- agent installation 154
- database tables 57

W

web server requirements 25

X

xs_editkeyring command 199