IBM

IBM Tivoli License Compliance Manager

Version 2.2 Fix Pack 1

Common Criteria Secure Implementation and Configuration Guide

Note:

Before using this information and the product it supports, read the information in Notices on page 48.

First Edition (September 2006)

This edition applies to IBM Tivoli License Compliance Manager Version 2.2 Fix Pack 1 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

1 About this guide

This document explains how to install, configure, maintain, and use the evaluated configuration of the IBM® Tivoli® License Compliance Manager Version 2.2 Fix Pack 1 under the Common Criteria.

The Common Criteria (CC) is an internationally recognized ISO standard (ISO 15408) for the security evaluation of IT products. A CC evaluation certifies, with a sufficient level of assurance, that a product and its environment have implemented the necessary security requirements to address given threats, based on certain assumptions and organizational policies.

IBM Tivoli License Compliance Manager 2.2 FP1 has been evaluated under the CC at evaluation assurance level 2 (EAL2), augmented with Flaw Remediation (ALC_FLR.1).

This guide also includes an appendix with clarifications that apply to the books of the Tivoli License Manager 2.2 product library.

It is strongly recommended that administrators read this guide before any other documentation, and follow the instructions included here. Information contained in this guide supersedes the rest of the product documentation, and following the instructions provided ensures that IBM Tivoli License Compliance Manager 2.2 FP1 is set up and operated according to the security requirements imposed for the evaluated configuration.

1.1 Evaluated configuration

An **evaluated configuration** is a system that complies with the defined security requirements of the product and its environment.

If a system is evaluated according to the CC, the CC evaluation is valid only for a specific system configuration of hardware and software. Changing any of the relevant security configurations might result in a non-evaluated system. This does not necessarily mean that the security of the system will be reduced, but only indicates that the system is no longer in a certified configuration. This guide explains the constraints of a system that must meet the requirements of a CC evaluation.

1.2 Who should read this guide

This guide is primarily for administrators who plan to install, configure, and maintain the evaluated configuration of IBM Tivoli License Compliance Manager 2.2 FP1, but it is also intended for users who operate the product with a specific role within the organization (Procurement Manager, Software Resource Manager, etc.)

Knowledge of the Common Criteria is not required for readers of this document.

1.3 Product name

The name of the product was recently changed from IBM Tivoli License Manager to IBM Tivoli License Compliance Manager. Because the name change occurred very close to the GA release of the product, the product documentation refers to the product by the earlier name. The FixPack 1 README and this guide refer to the product by its new name.

1.4 What this guide contains

This guide contains the following sections:

- Chapter 2, “Product Overview”
  Provides an overview of the product security from the point of view of the Common Criteria evaluation.
- Chapter 3, “Installation and Configuration”
  Provides the preconditions and instructions for installing and configuring the product under the requirements of the Common Criteria evaluation.

- Chapter 4, “System Operation”
  Provides the instructions for deploying agents and maintaining the evaluated configuration under the requirements of the Common Criteria evaluation.
- Appendix A, “Input parameters in Web User Interface”
  Provides additional information about the input fields in the Administration Web User Interface: field type, maximum length and additional validation rules.
- Appendix B, “Documentation Clarifications”
  Provides additional information that applies to the books of the Tivoli License Manager 2.2 product library.

1.5 Publications

This section lists publications in the Tivoli License Compliance Manager library. It also provides pointers to publications for pre-requisite software products (IBM DB2 Universal Database™ and IBM WebSphere® Application Server), and describes how to access Tivoli publications online and how to order Tivoli publications.

1.5.1 IBM Tivoli License Compliance Manager 2.2 FP1 library

The following documents are available in the IBM Tivoli License Compliance Manager library. The library is available on the Tivoli License Compliance Manager Documentation CD as well as online, as described in “Accessing publications online” on page 7.

- IBM Tivoli License Manager: Overview, SC32-1503-00

  Provides general information about Tivoli License Manager 2.2.

- IBM Tivoli License Manager: Release Notes, SC32-1429-02

  Provides a summary of changes made in the release, lists the supported platforms for each component, documents known errors and workarounds, and includes the latest information about the product that could not be included in the main documentation.

- IBM Tivoli License Manager, Version 2.2: Planning, Installation, and Configuration, SC32-1431-02

  Provides information about planning, installing, and configuring Tivoli License Manager 2.2.

- IBM Tivoli License Manager, Version 2.2: Administration, SC32-1430-02

  Provides information about how to use Tivoli License Manager 2.2 to set up a monitoring infrastructure, define licensing conditions, and produce reports.

- IBM Tivoli License Manager, Version 2.2: Commands, SC32-1501-00

  Provides descriptions of all Tivoli License Manager 2.2 commands.

- IBM Tivoli License Manager, Version 2.2: Security Management, SC32-1502-00

  Provides information about the security features of Tivoli License Manager 2.2.

- IBM Tivoli License Manager, Version 2.2: Catalog Management, SC32-1434-01

  Describes how to use the Catalog Manager to maintain an up-to-date catalog of software products and the signatures that are used to detect their presence and use on monitored computers.

- IBM Tivoli License Manager, Version 2.2: Problem Determination, SC32-9102-01

  Provides Tivoli License Manager 2.2 diagnostic information, including messages, traces and event logs, and information about tools and techniques for diagnosing problems.

- IBM Tivoli License Manager, Version 2.2: Data Dictionary, SC32-1432-02

  Provides descriptions of the database tables and indexes maintained in the Tivoli License Manager 2.2 administration and runtime server databases.

- Readme File for Fix Pack 2.2.0-TIV-TLCM-FP0001

  Provides instructions to apply the fix pack 1 and upgrade TLCM 2.2 to version 2.2.0-FP0001, the evaluated ITLCM.

1.5.2 Related publications

IBM DB2 Universal Database (UDB) and IBM WebSphere Application Server are needed in order to use IBM Tivoli License Compliance Manager. Here are pointers to online versions of the product documentation for each product. In addition, product documentation might be installed locally when you install the products.

- IBM WebSphere Application Server library

  http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp

- IBM DB2 UDB library

  http://www-3.ibm.com/software/data/db2/library/

1.5.3 Accessing terminology online

The Tivoli Software Glossary includes definitions for many of the technical terms related to Tivoli software. The Tivoli Software Glossary is available at the following Tivoli software library Web site:

http://publib.boulder.ibm.com/tividd/glossary/tivoliglossarymst.htm

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/ibm/terminology

1.5.4 Accessing publications online

The Tivoli License Manager documentation CD contains an information center that includes the publications of the product library, other than the IBM Tivoli License Manager: Release Notes. The format of the publications is PDF and HTML, and they are available in all supported languages. See the readme.txt file to access the information center using a Web browser. The file is in the root directory on the documentation CD.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli software information center Web site. Access the Tivoli software information center by first going to the Tivoli software library at the following Web address:

http://www.ibm.com/software/tivoli/library/

Click Tivoli product manuals. In the Tivoli Technical Product Documents Alphabetical Listing window, click IBM Tivoli License Manager to access the product library at the Tivoli software information center.

Note: If you print PDF documents on other than letter-sized paper, set the option in the File -> Print window that allows Adobe Reader to print letter-sized pages on your local paper.

1.5.5 Ordering publications

You can order many Tivoli publications online at the following Web site:

http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications.

1.6 Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully.

This product is operated using a Web browser, which has certain built-in accessibility features, and has been provided with specific shortcut keys for navigating the Web interface, starting tasks, and performing toolbar actions.

1.7 Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site:

http://www.ibm.com/software/tivoli/education

1.8 Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

- Searching knowledge bases: You can search across a large collection of known problems and workarounds, Technotes, and other information.
- Obtaining fixes: You can locate the latest fixes that are already available for your product.
- Contacting IBM Software Support: If you still cannot solve your problem, and you need to work with someone from IBM, you can use a variety of ways to contact IBM Software Support.

1.9 Conventions used in this book

This book uses several conventions for special terms and actions, and operating system-dependent paths.

1.9.1 Typeface conventions

This guide uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as Tip and Operating system considerations)
- Column headings in a table
- Keywords and parameters in text

Italic

- Citations (titles of books, diskettes, and CDs)
- Words defined in text
- Emphasis of words (words as words)
- New terms in text
- Variables and values you must provide

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

<*text*> Indicates a variable in a path name. For example, in the path <INSTALL_DIR>\admin\conf, INSTALL_DIR depends on the location where you have installed a Tivoli License Manager component, while \admin\conf is constant.

1.9.2 Operating system-dependent notation

This book uses the Windows® convention for environment variables and directory notation. When using the UNIX®, Linux™, and OS/400® command line you should do the following:

Environment variables

First verify the correct value for the UNIX, Linux, or OS/400 variable name, as many variables in different platforms that perform the same task have different names (for example, %TEMP% in Windows is equivalent to $tmp in UNIX and Linux). Then replace %Windows_variable% with $UNIX_variable

File and directory paths

Replace each backslash (\ ) with a forward slash (/).

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

2 Product Overview

2.1 Common Criteria Evaluated Configuration

The following sections describe the platforms on which IBM Tivoli License Compliance Manager 2.2 FP1 was evaluated under the Common Criteria, and the required software for the IT environment.

Throughout the rest of this guide, the following terms are used to address different parts of the evaluated configuration:

- **Evaluated product**: The IBM Tivoli License Compliance Manager 2.2 FP1 itself, which must be installed, configured, and operated following the instructions provided in this guide.
- **Evaluated product environment**: the IT environment that supports IBM Tivoli License Compliance Manager 2.2 FP1, which must be configured and operated following the instructions provided in this guide.

As explained in the introduction, the term “Evaluated Configuration” refers to the product and its environment, which must be installed, configured and operated following the instructions provided in this guide. Therefore, the Evaluated Configuration is comprised of both the evaluated product and the evaluated product environment.

2.1.1 Evaluated product

The runtime and administration servers have been evaluated on the following platforms:

- Windows® Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows 2000 Advanced Server
- Windows 2000 Server
- IBM AIX® 5.2 and 5.3
- HP/UX 11i
- Red Hat Enterprise Linux® 3.0 and 4.0
- SUSE LINUX® Enterprise Server 8 and 9
- Sun Solaris 9 and 10

Agents have been evaluated on the following platforms:

- Windows Server 2003 Standard Edition
- IBM AIX 5.3
- Red Hat Enterprise Linux 4.0
- Sun Solaris 9

The Agent component includes two library packages that are also used in other Tivoli products:

- Global Security Kit (GSKit), a library package that implements SSL and other cryptographic functions.
- Common Inventory Technology (CIT) , which provides software scanning capabilities on several platforms.

The following versions of GSKit and CIT are included in the evaluated product:

Operating System Family	GSKit version	CIT version
AIX	**7.0.3.15**	**2.2.1**
Linux	**7.0.3.15**	**2.2.1**
Sun Solaris	**7.0.3.18**	**2.2.1**
Windows	**7.0.3.16**	**2.2.1**

Table 1 - Component versions of the evaluated product

2.1.2 Evaluated product environment

The following products are required by the evaluated configuration:

- Universal Database Enterprise Edition, version 8.2
- IBM WebSphere Application Server version 6.0.2.5
- IBM HTTP Server, version 6.0.2
- WebSphere Application Server plug in version 6.0.2.5

These products are bundled in the evaluated product package and installed by the installation wizard. However the administrator might choose to install these products independently.

Note: for database servers running on a Sun Solaris 10, DB2 UDB version 8.2 must be installed and upgraded to Fix Pack 9 before installing the evaluated product.

In addition, the evaluated product requires installation of a web browser on the Administration server to manage some administration tasks, and on the runtime server if the pull deployment mechanism will be used to distribute the Agent software. These are the supported web browsers:

Operating System Family	Pull Deployment from Web Page	Administration Web User Interface
AIX	**Mozilla 1.4, 1.5**	**Mozilla 1.4, 1.5, 1.6, 1.7**
Linux	**Mozilla 1.0 (iSeries and pSeries)** **Mozilla 1.4, 1.5 (others)**	**Mozilla 1.4, 1.5, 1.6, 1.7**
HP/UX 11i	**Mozilla 1.4, 1.5**	**Mozilla 1.4, 1.5, 1.6, 1.7**
Sun Solaris	**Mozilla 1.4, 1.5**	**Mozilla 1.4, 1.5, 1.6, 1.7**
Windows	**MS IE 6.x or later**	**Mozilla 1.4, 1.5, 1.6, 1.7** **MS IE 6.x or later**

Table 2 - Web Browser requirements

2.2 Security Functions

The evaluation of IBM Tivoli License Compliance Manager under the Common Criteria has been focused on the following security functionality of the product:

2.2.1 Identification and authentication

2.2.1.1 Administrator authentication to the administration server

When the Super Administrator (see section 2.2.4.3) creates a new administrator (user) of the evaluated product, the administrator is assigned a user name and password. To access the administration server using the GUI (via a web browser), all administrators including the Super Administrator are required to provide their credentials (user name and password).

2.2.1.2 Agent to runtime server authentication

In the evaluated configuration, an install-time option is set to require agents to authenticate to the runtime servers using the authentication feature of SSL as provided by IBM Global Security Kit (GSKit), which is deployed with the license management agent software and is part of the evaluated product. When the SSL with client authentication security option is chosen for the agent, deployment also includes creation, distribution, and installation of an X.509v3 certificate to each agent (management of the certificate is outside the evaluated product itself). Agents then connect to a runtime server through the runtime Web server using the SSL protocol configured to use encryption and digests.

2.2.1.3 Runtime server to administration server authentication

Depending on the nature of the deployment, the evaluated product can be configured at install time to require runtime server to administration server authentication. This model might be chosen, for example, if the runtime server is deployed remotely from the administration server. If, on the other hand, the runtime server and the administration server are installed on the same machine or installed in a well-protected Data Center, the system administrator or other individual choosing security levels is likely to conclude that such authentication is not necessary. Other deployments will fall somewhere between these two extremes, and administrators will decide whether implementing secure communication is appropriate.

If runtime authentication is to be used, during installation of each runtime server, a runtime server name and a communication password are created. The password is stored encrypted in the passwd.properties file on the runtime server. During registration of the runtime server to the administration server, these credentials are written to the administration server database. Each time it needs to initiate a transaction to the administration server, the runtime server is required to provide its credentials (runtime server name and password) to the administration server. The administration server identifies and authenticates the runtime server by comparing the credentials submitted by the runtime server to the runtime server credentials stored in the administration server database.

2.2.2 Password policy enforcement

In order to resist attempts to guess a password, the evaluated product enforces a global password policy for administrator (user) and runtime server communication passwords. All administrators are required to comply with the policy regardless of their role and organization. The policy defines a minimum password length of 8 characters and password composition rules (passwords must contain a minimum of 2 non-alphabetic characters; passwords may consecutively repeat a maximum of 2 characters).

2.2.3 Session timeout

An administration server GUI session will terminate if the time interval *n* set for session inactivity timeout (the sessionTimeout parameter in the system.properties configuration file on the administration server) is exceeded. The default value is 60 minutes.

2.2.4 Security Roles and Management

2.2.4.1 Association of software usage records to organizations

An important element in limiting access by individual administrators to software usage records that are relevant to organizations in which the administrator plays a role is associating each software usage record to an organization as the data is collected and then stored in the administration server database.

The Super Administrator (see section 2.2.4.3) creates logical organizations for which software licensing needs to be managed. Both the runtime server and the agent are configured to a specific organization, so that software usage data collected and passed by those components is identified with that organization. Each runtime server is associated with an organization at the time the runtime server is registered to the administration server. Each agent is associated with an organization and a runtime server when the agent is installed.

Software usage records are then collected from agents and sent to the runtime server, and then sent on the administration server database. In the administration server database, each software usage record is associated with its configured organization.

2.2.4.2 Access control

The administration server controls access to software usage records in the administration server database based on the organizations, roles, and privacy policies associated with an administrator (note that all “users” of the evaluated product are administrators)

Each administrator’s profile contains a list of organizations that the administrator belongs to, as well as the administrator’s configured role within each organization and the administrator’s privacy policy setting within each organization.

Each administrator is only allowed to access software usage records associated with the organizations listed in his or her profile. The access rights that an administrator is granted to the software usage records depend on the roles assigned to the administrator within the organization.

The privacy policy associated with the administrator defines the level of detail about individual monitored computers in an organization that an administrator can view. If the privacy policy parameter is set to show computer information, then search criteria and report data related to individual agents and computers is displayed. If the parameter is set to not show computer information, the search criteria in reports is hidden to limit report data of defined agents and computers, and the data is queried on a division granularity basis only.

2.2.4.3 Security roles

The Super Administrator role is created at install time.

The Super Administrator can assign these roles to administrators, each of which entitles the individual assigned to the role with a specific level of access to data stored in the administration server database:

- Administrator
- Procurement Manager
- Software Resources Manager
- License Administrator
- System Resources Manager
- Procurement and Licensing Manager

2.2.5 Secure data transfer between components

2.2.5.1 Agent to runtime server communication

Communication between the agent and the runtime server uses SSL encryption and client authentication to protect the confidentiality and integrity of the data flow between them. The evaluated product uses the IBM Global Security Kit (GSKit) library for the implementation of the SSL protocol and its underlying cryptographic functions on the agent side.

2.2.5.2 Runtime server to administration server communication

For runtime server to administration server communication, administrators will decide whether to enable runtime server to administration server security based on the nature of the deployment, as previously described in section 2.2.1.3.

If secure communication is selected, encryption is provided by the SSL protocol as a function of the environment (through the JSSE library of the IBM JDK in the WebSphere Application server). In addition, mutual authentication is performed. The administration server authenticates itself to the runtime server using an SSL certificate. Authentication of the runtime server to the administration server is provided by the evaluated product using runtime server credentials (a unique name and password for each runtime server) known by both parties.

2.2.5.3 Guaranteed data delivery

The data flow between an agent and runtime server and between a runtime server and administration server also provides an extra level of data protection beyond the communications protocol. Specifically, when a server receives software usage records from a client, the server sends a message back to the client after the server saves the software usage records in its database. This message informs the client that the data has been successfully persisted at its target. The client then can delete the transmitted software usage records. For example, when an agent sends software usage records to the runtime server, the runtime server signals the agent when it has saved the software usage records in its database. The agent then is free to delete the software usage records from internal storage.

2.2.6 Management of security functions

2.2.6.1 Administration server GUI

The administration server GUI (via a web browser) provides the Super Administrator with the ability to manage the security functionality of the evaluated product. After successful identification and authentication (see section 2.2.1.1), the Super Administrator can perform the following management tasks:

- create and manage organizations
- create and manage administrators (users) including assigning roles, organizations, and privacy policies to administrators (users)
- change administrator (user) passwords and his or her own password
- change runtime server communication passwords (note that in addition, the password must be changed on the runtime server – see section 2.2.6.2)

Other administrator roles are able to perform a single security function management task through the administration server GUI:

- change their own passwords

For more information regarding security management functions, please refer to *4.1 - Administrative Functions*

on page 32.

2.2.6.2 Runtime server CLI

The runtime server provides a command line interface (CLI) to manage the following security-relevant tasks:

- changing the runtime server to administration server communication password using the **rtpasswd** command (note that in addition, the password must be changed on the administration server through the administration server GUI - see section 2.2.6.1)
- changing the runtime server to runtime server Database password using the **dbpasswd** command
- changing the password used by the runtime server to open its truststore file (key.jks) using the **sslpasswd** command.
- re-encrypting all passwords in the password.properties file on the runtime server using the **kstoreupdate** command.

The command line can only be used by Windows users with administrator rights and UNIX® user root from the UNIX Shell. Executing the **rtpasswd**, **dbpasswd**, or **sslpasswd** command requires entering the old password.

For more information regarding security management functions, please refer to *4.1 - Administrative Functions*

on page 32.

2.2.6.3 Administration server CLI

The administration server provides a command line interface (CLI) to manage the following security-relevant tasks:

- changing the administration server to administration server Database password using the **dbpasswd** command
- re-encrypting all passwords in the password.properties file on the administration server using the **kstoreupdate** command

The command line can only be used by Windows users with administrator rights and UNIX user root from the UNIX Shell. Executing the **dbpasswd** command requires entering the old password.

For more information regarding security management functions, please refer to *4.1 - Administrative Functions*

on page 32.

2.3 Assumptions

The security functions of IBM Tivoli License Compliance Manager 2.2 FP1 are based on the assumptions described in the following sections. The evaluated configuration must fulfill these assumptions.

2.3.1.1 Intended usage of the evaluated product

- The evaluated product is configured and operated in accordance with the information provided in this guidance and the corresponding product documentation.
- The evaluated product environment is configured and managed in accordance with the information provided in this guidance and the corresponding product documentation.
- Identification and authentication between some components of the evaluated product (agent <-> runtime server, runtime <- administration server) are implemented through the use of X.509v3 certificates. In order to ensure confidentiality and integrity, these certificates must be generated and managed in a secure way. Furthermore, a PKI infrastructure would be necessary to support the generation of certificates. Refer to “PKI Infrastructure” in this guide for more information.
- Depending on the topology of the evaluated configuration, the runtime servers and the administration server can be in different networks, within the same secure network, or in the same machine (in the case of a single runtime server and an administration server

hosted by the same machine). Administrators ensure, through appropriate security measures, the integrity and confidentiality of the data transferred between the runtime servers and the administration server. The product provides SSL encryption of this communication path choosing the appropriate security level; administrators might legitimately conclude that selecting this option is necessary.

2.3.2 Environment of use of the evaluated product

2.3.2.1 Physical aspects

- All machines housing components of the evaluated product and components in the evaluated product environment on which the evaluated product relies are protected against unauthorized physical access and modification. This includes all the machines housing the following components:
  - the administration server and the administration web server
  - the administration database server
  - the runtime server and the runtime web server
  - the runtime database server
  - the agent
  - the catalog manager
  - the web browser from which the administrator connects to the administration server

Note: depending on the topology chosen for the deployment of the evaluated configuration, some or all the servers might be hosted by the same machine.

- The machine hosting the administration server must provide a reliable time function to support the inactivity timeout security function. This means that the system time must be verified periodically or updated from a reliable time source.

2.3.2.2 Personnel aspects

- One or more administrators might be assigned to manage the different components of the evaluated product. These administrators are competent and trustworthy to perform their tasks; and the organizational procedures and policies are sufficient to ensure that they are held accountable for their security-relevant actions.
- One or more administrators might be assigned to manage the different components of the evaluated product environment. These administrators are competent and trustworthy to perform their tasks.
  - Database management for the administration and/or runtime database servers.
  - Web server and WebSphere management for the administration and/or runtime servers.
  - Operating System management for the computers that host the administration server, runtime servers and agents.
  - Public Key Infrastructure management.
- Non-administrator users are part of a well-managed and cooperative user community. Although the product does not provide functionality to these users, they have access to the agents for daily tasks and may have access to servers for non-administrative tasks or other tasks hosted by the same server.
- Administration personnel in charge of the installation, configuration and operation of the evaluated configuration must have the following skills and knowledge:
  - Organizational policies
  - Basic knowledge of the operating systems in which IBM Tivoli License Compliance Manager components will run
  - Installation, configuration, and maintenance of DB2 UDB
  - Installation, configuration, and maintenance WebSphere Application server and IBM HTTP server.

- Configuration of SSH communication (if this agent deployment mechanism is used)
- Windows Logon scripting (if this agent deployment mechanism is used)
- Installation, configuration, and maintenance of a PKI Infrastructure

2.4 Security requirements for the environment

The evaluated product environment must comply with the following requirements:

2.4.1 Secure Network

In the evaluated configuration, confidentiality and integrity of the communication between the different components must be ensured.

IBM Tivoli License Compliance Manager provides appropriate security levels for ensuring the confidentiality and integrity of two communication paths:

- Communication between agents and runtime servers
- Communication between the runtime servers and the administration server

Secure communication between agents and runtime servers is mandatory for the evaluated configuration. Communication between the runtime servers and the administration server can be protected by other means. If the maximum security level is not used for this purpose, both the runtime servers and the administration server must be in a secure network. This does not apply in a scenario where there is only one runtime server on the same machine that hosts the administration server.

The administration and runtime servers also communicate with an associated database, which can be hosted by the same computer or a different one. As communication with the database is not protected by ITLCM, communication between them must be protected in a secure network when the application and database servers reside in different computers.

2.4.2 PKI Infrastructure

A PKI infrastructure supporting X.509v3 certificates must be provided in order to implement the following security functions through the SSL protocol:

- Identification and authentication of the agents against the appropriate runtime server, if the Maximum security level is chosen.
- Identification and authentication of the runtime server towards its agents.
- Identification and authentication of the administration server to the runtime servers.

The PKI infrastructure may be provided by a publicly known Certification Authority, an existent CA within the organization, or a specific deployment for the evaluated configuration.

The evaluated product environment provides 1024 key-length certificate requests in PCKS#7 format for the agents. For the rest of the certificates a key length of 1024 or greater is recommended.

It is up to the administrators to decide what kind of PKI infrastructure will best serve the needs of the organization. When making that decision, please consider:

- The CA root chain must be deployed to all agents, runtime and administration servers.
- One certificate must be generated for each agent.
- One certificate must be generated for each runtime server.
- One certificate must be generated for the administration server.
- Renewal of certificates may be necessary.

Although IBM Tivoli License Compliance Manager provides one already generated self-signed certificate both for admin and runtime, this feature is not allowed in the evaluated configuration.

2.4.3 WebSphere Secure Cell

The administration and runtime servers are applications running under a WebSphere Application Server cell. Global security must be enabled for application servers running within a cell so that authentication is requested before an application server can be stopped or uninstalled.

Note: As this requirement would also require authentication to access to the secure cell when installing the evaluated product, this feature is set as a post-installation step.

2.5 Limitations for the evaluated configuration

2.5.1 Language support

Although IBM Tivoli License Compliance Manager supports several languages, only the English language version evaluated configuration was tested. This applies also to the language chosen for the installation wizard.

2.5.2 LDAP authentication

The evaluated configuration was only tested with database authentication. Therefore, LDAP authentication is not allowed.

2.5.3 Self-signed certificates

The evaluated product does not allow the use of self-signed certificates. Only certificates issued by a Certificate Authority are allowed.

2.5.4 Agent update feature

The evaluated product does not allow the automatic update feature for agents. This feature must remain disabled (**updateAgentEnabled** =NO).

2.5.5 Co-existence with ITLM 2.1 and 2.2

The evaluated configuration does not support the co-existence of previous versions of ITLCM. Previous versions of the product must be uninstalled before installing and configuring the evaluated configuration of ITLCM.

2.5.6 Agent deployment with Tivoli Configuration Manager

The evaluated configuration does not support agent deployment using Tivoli Configuration Manager. This mechanism requires the pre-installation of the CIT component on each agent before deployment; this would cause the CIT shipped with the evaluated product not to be installed, therefore the evaluated product would be partially installed with a component not evaluated.

2.5.7 Co-existence with other Tivoli products

As explained earlier in this guide, the evaluated ITCLM includes the CIT and GSKit components, which are also used by other Tivoli products. If you are planning to install other Tivoli products on the same machine on which the agent is installed, be aware that:

- Only one instance of the component (CIT or GSKit) can reside on the machine.
- In order to keep IBM Tivoli License Compliance Manager under the evaluated configuration, none of the components of the product can be replaced, even if this implies an upgrade and the component is forward- compatible.
- Tivoli installation wizards automatically replace any common component whose version is older than the one included in the product to install.

Therefore, the following limitations apply if the evaluated product agent and another Tivoli product that uses the CIT or GSKit components are installed on the same machine:

- If the CIT and GSKit versions of the other Tivoli product are the same as the version provided by ITLCM, the evaluated product must be installed first.
- If the CIT and GSKit versions of the Tivoli product are lower than the version provided by ITLCM, the evaluated product must be installed after the other Tivoli product. The other Tivoli product should work, because versions are forward-compatible.
- If the version of any of the components of the other Tivoli product is higher than the version provided by ITLCM, coexistence is not possible (if the evaluated product is installed before the other Tivoli product, the components would be overwritten during installation of the other Tivoli product; if the evaluated product is installed after the other Tivoli product, installation of IBM Tivoli License Compliance Manager would not replace the installed higher version).

2.6 Known Issues

2.6.1 Administration server login under Solaris or HP-UX

When the administration server is installed on **Websphere 6.0.2.5** and the **Solaris** or **HP-UX** operating systems the secure login fails (even if the SSL is well configured on HTTP Server and on Websphere Application Server). If you try to connect to the administration server login page through SSL, an error message (**CODIF1509E**) is displayed.

There is a workaround for this defect that is part of the post-installation steps. See *3.3.4 - Applying workarounds for known issues* on page 28 for more information.

3 Installation and Configuration

This section constitutes a roadmap for installing and configuring the evaluated configuration of ITLCM. Generally, this information points to the appropriate information included in the *Planning, Installation and Configuration Guide for ITLM version 2.2* and provides additional information for specific security requirements for the evaluated configuration. If there is any discrepancy between the two sources, this CC security guide takes precedence, as it addresses the requirements for the evaluated configuration of ITLCM.

Installation and configuration activities occur not only at the beginning, but also while the system is in operation. The following are the typical scenarios in which installation and configuration activities occur:

- The initial installation and configuration of the administration server
- The initial installation and configuration of runtime servers
- The deployment of agents on the machines to be managed
- Additional installation and configuration of runtime servers, either to support a new organization or redistribute workload.

This chapter covers the first two scenarios; the deployment of agents and the additional installation and configuration of runtime servers are covered in chapter 5, System Operation.

3.1 Pre-Installation steps

Before you start the installation, do the following steps:

- Plan the distribution and allocation of the different servers and agents.
- Verify that the package you have corresponds to the evaluated product.
- Verify that the evaluated product environment meets all the security requirements defined in this guide.
- Collect all the information that the installation wizards will request.

3.1.1 Planning the evaluated product topology

The IBM Tivoli License Compliance Manager architecture allows the allocation of the administration, runtime and database servers in one or several computers; the administrator chooses the most appropriate topology to meet the needs of the organization.

Chapter 1 of the *Planning, Installation and Configuration Guide*, *Planning a Tivoli License Manager Implementation* on page 1 gives an overview of the things to be considered before installing and configuring ITCLM. Please read it considering the following factors that are applicable to the evaluated configuration:

Planning a monitoring structure (page 1)

- When you define the computers that are to be monitored, remember that only the platforms evaluated for agents can be considered. Please refer to *2.1.1 - Evaluated product* on page 10 for a list of the supported platforms in the evaluated product
- Communication between the agents and the runtime servers must be always encrypted in the evaluated configuration (security level: Maximum).
- Table 1 shows a scenario in which all agents use unsecured communication. In the evaluated configuration, all agents and runtimes must have enabled the maximum security level.

Installation and setup overview

As this guide provides the steps that must be followed to install and setup the evaluated configuration, use this section only to have a general idea of the tasks to be performed.

Planning to upgrade from version 2.1 (page 5)

Version 2.1 is not allowed in the evaluated configuration. Computers with previous versions of the product must be reinstalled.

Supported platforms for agents (page 10 to 12)

IBM Tivoli License Compliance Manager has been evaluated for a subset of the platforms supported by the agent. Please refer to *2.1.1 - Evaluated product* on page 10 for a list of the supported platforms in the evaluated product, and use Table 4 to verify that the operating system is updated with the appropriate level, service pack or compatibility pack.

Supported partition technologies (page 12)

IBM Tivoli License Compliance Manager has been evaluated for a subset of the platforms supported by the agent. Please refer to *2.1.1 - Evaluated product* on page 10 for a list of the supported platforms in the evaluated product, and use Table 5 to verify that the operating system runs in a supported partition technology.

Prerequisites - Administration and runtime servers (page 14)

- WebSphere Application server version 5.1.1.8 is not supported in the evaluated configuration.

3.1.2 Verifying the evaluated product

Please verify that the product you have received corresponds to the evaluated product, and verify the integrity of the CDs.

The evaluated product is shipped through the following mechanisms:

- Physical media: CDs or DVDs
- Electronic download, via Passport Advantage Online

If you have purchased the evaluated product on CDs:

- Verify that the package has the following CDs and labels:
    - Tivoli License Compliance Manager
Servers for AIX, Windows, HP and Solaris plus Agent on i5/OS
Version 2.2.0
    - Tivoli License Compliance Manager
Servers for Linux Intel
Version 2.2.0
    - Tivoli License Compliance Manager
Servers for Linux 390S
Version 2.2.0
    - Tivoli License Compliance Manager
Servers for Linux PPC
Version 2.2.0
    - Tivoli License Compliance Manager
Agent and CIT enabler Windows, AIX, HP, Solaris and Linux Intel
Version 2.2.0
    - Tivoli License Compliance Manager
Agent for Linux 390
Version 2.2.0
    - Tivoli License Compliance Manager
Agent for Linux PPC
Version 2.2.0
    - Tivoli License Compliance Manager
RSH/SSH Agent Deployment for AIX, Windows, HP, Solaris, Linux Intel
Version 2.2.0
    - Tivoli License Compliance Manager
RSH/SSH Agent Deployment for Linux 390 and PPC
Version 2.2.0

    - Tivoli License Compliance Manager
      RSH/SSH Agent Deployment for AIX, Windows, HP, Solaris, Linux Intel
      Version 2.2.0
    - Tivoli License Compliance Manager
      Agent Software Package Block
      Version 2.2.0
    - Tivoli License Compliance Manager
      Publications CD
      Version 2.2.0
    - Tivoli License Compliance Manager
      Catalog manager
      Version 2.2.0
- Verify that the packaging containing the CDs has not been opened, and the protection seal is intact.

If you have purchased the evaluated product on DVDs:

- Verify that the package has the following DVDs and labels:
    - Tivoli License Compliance Manager
      Servers and Agent DVD
      Version 2.2.0
    - Tivoli License Compliance Manager
      Catalog Manager DVD
      Version 2.2.0
    - Tivoli License Compliance Manager
      Documentation DVD
      Version 2.2.0
- Verify that the packaging containing the DVDs has not been opened, and the protection seal is intact.

If you have downloaded the product through the Passport Advantage Online:

- Verify that you have downloaded all or some of the following eAssemblies:
    - IBM Tivoli License Compliance Manager 2.2.0 Catalog Manager eAssembly, Multiplatform, Multilingual (CR3JBML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager 2.2.0 Documentation eAssembly, Multiplatform, Multilingual (CR3JEML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager 2.2.0 RSH/SSH Agent Deployment eAssembly, Multiplatform, Multilingual (CR3JCML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager 2.2.0 Servers eAssembly, Multiplatform, Multilingual (CR3J2ML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager 2.2.0 for Agent Manual Deployment eAssembly, Multiplatform, Multilingual (CR3JAML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager 2.2.0 for Agent Software Package Blocks eAssembly, Multiplatform, Multilingual (CR3JDML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager for IBM Software 2.2.0 Agent Manual Deployment eAssembly, Multiplatform, Multilingual (CR3JNML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager for IBM Software 2.2.0 Documentation eAssembly, Multiplatform, Multilingual (CR3JRML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager for IBM Software 2.2.0 RSH/SSH Agent Deployment eAssembly, Multiplatform, Multilingual (CR3JPML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager for IBM Software 2.2.0 Servers eAssembly, Multiplatform, Multilingual (CR3JKML) 24-Feb-2006
    - IBM Tivoli License Compliance Manager for IBM Software 2.2.0 for Agent Software Package Blocks eAssembly (CR3JQML) 24-Feb-2006

IBM Tivoli License Compliance Manager 2.2, Fix Pack 1 will also be necessary to install the evaluated product. This Fix Pack can be ordered from the support web site (PTF number **U808555**).

- Verify that the package contains 13 CDs with the following label: **IBM TLCM, Version 2.2 Fixpack 1**
- Verify that the packaging has not been opened, and the protection seal is intact.

Note: Fix Pack 1 cannot be obtained through Electronic Downloads.

3.1.3 Verifying the requirements for the evaluated product environment

If you are planning to install a database server in Solaris 10 platforms, DB2 UDB must be installed before the evaluated product is installed, and requires the installation of fix pack 9.

3.1.4 Collecting information for the wizard

During the installation process, the wizard will ask for different parameters, most of them are security relevant and must be input consistently in the different wizards so identification and authentication between the different components of the evaluated product are successful. The following table enumerates the parameters needed during the installation:

Installation Mode Parameters	Full	Custom				Prerequisites			
		Admin Server		Runtime Server		DB2 UDB		WebSphere Application Server	
		SRV	DB	SRV	DB	Yes	No	Yes	No
DB2 UDB administration user and password			✓		✓	✓			
tlmsrv user password	✓	✓	✓	✓	✓	✓	✓		
Windows administration user and password								✓	✓
Database Host Name		✓		✓					
Runtime Server Name				✓					
Organization Name	✓			✓					
Administration Server Host Name/Address				✓					
Runtime Server communication password	✓			✓					

Table 3 - Information required during installation

3.2 Installation steps

The evaluated product consists of two sub packages, which must be installed in the following order:

- IBM Tivoli License Compliance Manager 2.2
- IBM Tivoli License Compliance Manager 2.2 Fix Pack 1

The IBM Tivoli License Compliance Manager 2.2 installation wizard allows the following alternatives:

- Full Installation, where all components are installed on the same computer.
- Custom Installation, which allows the administrator to select the desired components, as follows:
  - Administration server
  - Administration server Database
  - Runtime server
  - Runtime server Database

Additionally, the wizard can install a bundled version of the following products, or the administrator may choose to locate them if one or both products are already installed:

- DB2 UDB Enterprise Edition, Version 8.2, if the administration or runtime Database is selected.
- IBM WebSphere Application Server Version 6.0, if the administration or runtime server is selected.

If DB2 UDB, IBM WebSphere Application Server, or both, are installed separately, the product versions defined in section 2.1.2 must match the installed versions.

Deployment of agents can be performed only after the administration and runtime servers have been completely installed.

Chapter 2 of the *Planning, Installation and Configuration Guide*, *Installing Tivoli License Manager servers and databases*, provides detailed instructions for the following two possible scenarios:

- Administration server database and administration server in different computers; runtime server and its database in a third computer (Custom Installation)
- Administration server and its database, and runtime server and its database in a single computer (Full Installation)

Read the following sections of the Planning, Installation, and Configuration Guide before you start the installation:

- Before you start, page 25
- Using the installation and upgrade wizard, page 27

In the following sections, we provide additional information based on these scenarios.

Note: In scenarios where the components are installed in the same computer, the wizard requires the same information only once. When components are installed in different computers, it is important that you enter the same values to avoid problems during start up.

The evaluated product also provides logging of the installation process, which can be useful to determine whether the installation was successful or to troubleshoot it if any problem arises. Please refer to *Chapter 3 – Installation Logging*, on page 7 of *IBM Tivoli License Manager 2.2: Problem Determination Guide*, for a detail explanation of this topic.

3.2.1 Full installation

1. Follow the installation steps 1 through 12 included in “Scenario 2: Installing all elements on a single computer” on page 46, considering also the following:
    - In step 2 (page 47), when the wizard request to enter the language version, select “English”.
    - In step 4 (page 48), you can either let the wizard install the bundled version of DB2 UDB or locate the directory where it is already installed.
    - In step 6 (page 49), you can either let the wizard install the bundled version of WebSphere Application Server or locate the directory where it is already installed.
    - In step 7 (page 49):
        - Select the “Specify security settings” check box.
        - Specify the organization name that will uniquely identify the organization to which the runtime server belongs.
        - Provide a password for the tlmsrv user.
        - In step 8 (page 50):
        - If you have decided to establish encrypted communication between the runtime and administration server, select the “Enable runtime to administration server security” option and provide the runtime server password and the admin ssl port number. Note that in this case two different SSL ports must be configured with their own keystore: one for the admin and one for the runtime.
        - Select Maximum (SSL with server and client authentication) for the security level between agents and the runtime server.
        - Leave the default port number (443) or specify a new value (you must configure the HTTP server to listen to this new port number)
2. Apply the refresh and fix pack to bring the version of WebSphere Application server to 6.0.2.5, and IBM HTTP server to version 6.0.2.
3. Apply the ITLM 2.2 Fix Pack 1, following the instructions provided in the document “*Readme File for Fix Pack 2.2.0-TIV-TLCM-FP0001”*, included in the evaluated product package.

3.2.2 Administration server

1. Follow the installation steps 1 through 16 included in “Installing the administration server and prerequisite software” on page 34, considering also the following:
    - In step 3 (page 29), when the wizard request to enter the language version, select “English”.
    - In step 7 (page 31), you can either let the wizard install the bundled version of DB2 UDB or locate the directory where it is already installed.
    - In step 9 (page 33), provide a password for the tlmsrv user.
2. Apply the refresh and fix pack to bring the version of WebSphere Application Server to 6.0.2.5, and IBM HTTP server to version 6.0.2.
3. Apply the ITLM 2.2 Fix Pack 1, following the instructions provided in the document “*Readme File for Fix Pack 2.2.0-TIV-TLCM-FP0001”*, included in the evaluated product package.

3.2.3 Administration database server

1. Follow the installation steps 1 through 13 included in “Installing the administration server database and prerequisite software” on page 29, considering also the following:
    - In step 3 (page 35), when the wizard request to enter the language version, select “English”.
    - In step 6 (page 36), select the “Administration server” check box and optionally the “Administration server database” check box, in case you want to install the server database in the same machine. In case you have chosen the installation of the administration server database in the same machine, the wizard will prompt for entering additional information before step 7. Please refer to the administration server database for these specific steps.
    - In step 7 (page 37), you can either let the wizard install the bundled version of WebSphere Application Server or locate the directory where it is already installed. Please consider that in both cases the WebSphere Application Server version must be upgraded to the version supported by the evaluated configuration.
    - In step 11 (page 38):
        - Select the “Specify security settings” check box.
        - Provide a password for the tlmsrv user.
    - Step 12 (page 39) will not be prompted if you have chosen the installation of the administration server database in the same machine.
2. Apply the ITLM 2.2 Fix Pack 1, following the instructions provided in the document “*Readme File for Fix Pack 2.2.0-TIV-TLCM-FP0001”*, included in the evaluated product package.

3.2.4 Runtime server

1. Follow the installation steps 1 through 14 included in “Installing a runtime server and its database” on page 41, considering also the following:
    - In step 2 (page 41), when the wizard request to enter the language version, select “English”.
    - In step 5 (page 42), select the “Runtime server” check box and optionally the “Runtime server database” check box, in case you want to install the server database in the same machine. In case you do not select the option, the wizard skips step 6.
    - In step 6 (page 43), you can either let the wizard install the bundled version of DB2 UDB or locate the directory where it is already installed.
    - In step 8 (page 44):
        - Provide a password for the tlmsrv user.
        - Select the “Specify security settings” check box.
    - In step 10 (page 45):

    - If you have decided to establish an encrypted communication between the runtime and administration server, select the “Enable runtime to administration server security” option and provide the runtime server password.
    - Leave the default port number (443) or specify a new value (you must configure the HTTP server to listen to this new port number)
    - Select Maximum (SSL with server and client authentication) for the security level between agents and the runtime server.

2. Apply the refresh and fix pack to bring the version of WebSphere Application server to 6.0.2.5, and IBM HTTP server to version 6.0.2.
3. Apply the ITLM 2.2 Fix Pack 1, following the instructions provided in the document “*Readme File for Fix Pack 2.2.0-TIV-TLCM-FP0001”*, included in the evaluated product package.

3.2.5 Runtime database server

1. Follow the installation steps 1 through 14 included in “Installing a runtime server and its database” on page 41, considering also the following:
    - In step 2 (page 41), when the wizard request to enter the language version, select “English”.
    - In step 5 (page 42), select only the “Runtime server database” check box.
    - In step 6 (page 43), you can either let the wizard install the bundled version of DB2 UDB or locate the directory where it is already installed. Please consider that in the latter case the DB2 UDB version must coincide with the version supported by the evaluated configuration.
    - The wizard will skip step 7.
    - In step 8 (page 44), the wizard will only prompt for the password for the tlmsrv user.
    - The wizard will skip steps 9 and 10.

2. Apply the ITLM 2.2 Fix Pack 1, following the instructions provided in the document “*Readme File for Fix Pack 2.2.0-TIV-TLCM-FP0001”*, included in the evaluated product package.

3.3 Post-Installation steps

3.3.1 Verifying the evaluated product

3.3.1.1 Verify product version

Verify the version of the evaluated product at each of the computers where the administration and runtime servers have been installed. For this purpose, search for the product.xml file under the installation directory and verify it includes the correct timestamp and Fix Pack version (in bold):

```
<?xml version="1.0" ?>
<TLM>
<Product>
<Name>IBM Tivoli License Compliance Manager</Name>
<Version>2.2.0.1</Version>
<InstallDir>C:\TLM</InstallDir>
<BackupDir>C:\TLM_22_backup</BackupDir>
</Product>
<Components>
<Component>
<Name>admDb</Name>
<FixPack timestamp="2006.06.21 10:57:36">2.2.0-TIV-TLCM-FP0001</FixPack>
</Component>
<Component>
<Name>admEar</Name>
<FixPack timestamp="2006.06.21 10:57:36">2.2.0-TIV-TLCM-FP0001</FixPack>
</Component>
<Component>
<Name>rtmDb</Name>
<FixPack timestamp="2006.06.21 10:57:36">2.2.0-TIV-TLCM-FP0001</FixPack>
</Component>
```

```
<Component>
<Name>rtmEar</Name>
<FixPack timestamp="2006.06.21 10:57:36">2.2.0-TIV-TLCM-FP0001</FixPack>
</Component>
<Component>
<Name>rtmEarAgent</Name>
<FixPack timestamp="2006.06.21 10:57:36">2.2.0-TIV-TLCM-FP0001</FixPack>
</Component>
<Component>
<Name>rtmEarWasAgent</Name>
<FixPack timestamp="2006.06.21 10:57:36">2.2.0-TIV-TLCM-FP0001</FixPack>
</Component>
</Components>
</TLM>
```

Table 4 – IBM Tivoli License Compliance Manager Version label in product.xml file

3.3.2 Installing the Catalog Manager

Follow instructions in Chapter 5 of the *Planning, Installation and Configuration Guide*, to install the Catalog Manager. The Catalog Manager is not part of the evaluated product, and its installation is optional.

3.3.3 Configuring the evaluated product

Chapter 3 of the *Planning, Installation and Configuration Guide, Configuring and setting up Tivoli License Manager*, describes post-installation tasks to configure, set up, and tune Tivoli License Manager. Follow the instructions in the different sections.

The default value for the session timeout of the Web Administration User Interface is 60 minutes. If you want to change to a lower value, edit the system.properties file and assign to the **sessionTimeout** parameter the timeout in minutes.

3.3.4 Applying workarounds for known issues

In case the administration server was installed in a **Solaris** or **HP-UX** operating system, please follow the steps below to make the administration server login work in the evaluated configuration:

1. Start **server1** on Websphere at the administration server
2. Connect to the Websphere administration console (http://<administration server>:9060/ibm/console) and log in.
3. On the left, expand **Servers**, and click on **Application Servers**.
4. In the servers list, click on **IBM_TLM_Administration_Server**
5. Under **Server Infrastructure**, expand Java and Process Management and click on Process Definition
6. Under **Additional Properties** click on **Java Virtual Machine**
7. Under **Additional Properties** click on **Custom Properties**.
8. Add a new property with the following name and value:
   - Name: java.protocol.handler.pkgs
   - Value: com.ibm.net.ssl.internal.www.protocol
9. Save the configuration
10. Restart the Administration Server.

3.3.5 Protecting the evaluated product environment

3.3.5.1 Obtaining SSL certificates

The following X509v3 certificates must be obtained in order to provide identification and authentication, and allow SSL communication:

- One certificate for the administration server, to provide server authentication in the SSL protocol between Web browsers and the administration Web User Interface, and optionally between the runtime servers and the administration server, if the maximum security level has been chosen.

- One certificate for each runtime server, to provide server authentication in the SSL protocol between agents and their assigned runtime server.

3.3.5.2 Enabling secure communications

The administration User Interface requires SSL to protect the communications between the web browser and the administration server. Follow the instructions included in *Web browser to administration server communication*, on page 31 of *IBM Tivoli License Manager 2.2: Security*.

If you have decided to enable the maximum security level between the runtime servers and the administration server (SSL encryption), follow the instructions included in *Defining runtime to administration server communication*, on page 9 of *IBM Tivoli License Manager 2.2: Security*. If you have decided to establish the minimum security level, remember that you must ensure that communication is secure by other means provided by the evaluated product environment.

The evaluated configuration requires the maximum security level between agents and runtime servers, that is, communication under HTTPS with client and server authentication. Follow the instructions included in *Defining agent to runtime server communication*, on page 17 of *IBM Tivoli License Manager 2.2: Security*.

Pull deployment of an agent from the runtime server must be performed also using secure communications. For this purpose, ensure that the following path can be only accessed through HTTPS:

```
https://<runtime_server_name>/slmruntime/deploy
```

3.3.5.3 Changing default values for credentials and enforcing password policy

The IBM Tivoli License Compliance Manager 2.2 installation wizard sets default values for several credentials that allow access to sensitive information. Besides, the wizard does not enforce the password policy defined for the evaluated product; the password policy enables once the FixPack1 is installed. For both reasons**, you are required to change the passwords** described in the following table**:**

Subject	Default value	Where	Command / Mechanism to change the Password
tlmroot user	system	administration server	User Account Change Password from the administration Web User Interface
tlmsrv user	value entered in the wizard	Administration server Runtime server OS account where the db is hosted.	**dbpasswd** command from the administration server or runtime server CLI Change password command in the OS where the db is hosted.
runtime server name	value entered in the wizard	Runtime server Administration server	**rtpasswd** command from the runtime server CLI Server Change Password from the Administration Web User Interface
keystore database	slmtest	Administration server Runtime server	**IKEYMAN** or gsk7ikm command, which is bundled with the IBM HTTP server.
trust store	slmtest	Runtime server	**sslpasswd** command from the runtime server

database (key.jks)			CLI **IKEYMAN** or gsk7ikm application, which are bundled with the IBM HTTP server.

Table 5 - Default values for passwords

3.3.5.4 Enabling Global Security on Websphere Application Server

The administration and runtime servers must run on a Websphere secure cell. Please refer to the following sources to enable Global Security on the Websphere Application Server:

- *Global security settings and Tivoli License Manager servers*, on page 35 of *IBM Tivoli License Manager 2.2: Security*.
- *Global Security*, on the Websphere Information Center, at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.base.doc/info/aes/ae/csec_global.html
- *Enabling security for all application servers*, on the Websphere Information Center, at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tsec_csec.html

Note: Java 2 Security is not required.

3.3.5.5 Verify user password policy

Installation of Fix Pack 1 updates the user password policy corresponding to the evaluated product. Please verify that it has been updated with the values provided in the table below, looking at the **system.properties** file located under <Install_DIR>\admin\SLM_Admin_Application.ear\slm_admin.war\WEB-INF\conf,

```
# Minimum length of a user or runtime server password
# Type: integer, Range: [8-12]
minimumPasswordLength=8

# Max number of times that a given char can be repeated consecutively in the
password
# Type: integer, Range: [2-5]
maxNumberCharsRepeated=2

# Minimum number of non alphabetical characters required in the password
# Type: integer, Range: [2-10]
minimumNumberNonAlphaChars=2
```

Table 6 - Password policy parameters in system.properties file

3.3.5.6 Verify secure communication

Please verify that the property settings below match the ones included in the administration server **system.properties** file located under <Install_DIR>\admin\SLM_Admin_Application.ear\slm_admin.war\WEB-INF\conf,

```
runtimeToAdminSecurityLevel=(min or max, see note)
```

Please verify that the property settings below match the ones included in the **system.properties** file of all runtime servers, located under <Install_DIR>\runtime\SLM_Admin_Application.ear\slm_runtime.war\WEB-INF\conf,

```
runtimeToAdminSecurityLevel=(min or max, see note)
agentToRuntimeSecurityLevel=2
```

Note: The value of the **`runtimeToAdminSecurityLevel`** property must be the same in all servers. **max** should be used in case the communication between the administration server and the runtime servers must be protected by the evaluated product through SSL; in case the communication is protected by other means, **min** can be chosen.

4 System operation

4.1 Administrative Functions

4.1.1 Administration Web User Interface

This section describes the management functions that the administrator should take into account for the secure operation of the evaluated product.

In order to access to these administrative functions, the administrator must logon to the web user interface with her/his user id and password and select an organization to work with. The administrative functions that an administrator may execute depend on the assigned role for each organization. The user **tlmroot** is a special user with full privileges, whose password is set up during installation.

Please refer to *Accessing the administration server* on page 18 of *IBM Tivoli License Manager 2.2: Administration* for a description of the Login, Logoff and Organization Selection functions.

For details regarding the input data for each of the security functions in the administration Web User Interface, please refer to *5- Appendix A – Input parameters in Web User Interface* on page 39 of this guidance.

For error and warning messages of the administration Web User Interface, please refer to *Administration and runtime server errors* on page 111 and *Administration and runtime server warnings* on page 122 of *IBM Tivoli License Manager 2.2: Problem Determination Guide.*

4.1.1.1 Create an Organization

This security management function adds a new organization to the admin server database. Please refer to *Creating organizations* on page 29 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.2 Update an Organization

This security management function changes an existent organization. Please refer to *Updating organizations details* on page 30 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.3 Delete an Organization

This security management function deletes an existent organization and the entire infrastructure related with it. Please refer to *Deleting an organization* on page 31 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.4 Create an Account

This security management function creates a user account. Please refer to *Adding administrator accounts* on page 31 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.5 Update an Account

This security management function updates a user account. Please refer to *Updating administrator accounts details* on page 32 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.6 Delete an Account

This security management function deletes a user account. Please refer to *Deleting accounts* on page 34 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.7 Define a Profile

This security management function creates roles and private policy for user accounts in organizations. Please refer to *Defining user profiles* on page 34 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.8 Change a Profile

This security management function changes roles and private policy for user accounts in organizations. Please refer to *Defining user profiles* on page 34 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.9 Remove a Profile

This security management function deletes roles and private policy for user accounts in organizations. Please refer to *Defining user profiles* on page 34 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.10 Change your own password

This security management function changes the password of the current user. Please refer to *Updating administration account details* on page 32 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.11 Change the password of another user

This security management function changes the password of a different user. Please refer to *Updating administration account details* on page 32 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.1.12 Register a Runtime Server

This security management function registers a new runtime server in the organization infrastructure. Please refer to *Registering a runtime server* on page 38 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

Please remember that the credentials assigned to the runtime server (runtime server name and password) must match the ones contained in the runtime server when it was installed and configured.

4.1.1.13 Change a runtime server

This security management function updates an existing runtime server. Please refer to *Reviewing and changing runtime servers* on page 40 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

Please remember that the credentials assigned to the runtime server (runtime server name and password) must match the ones contained in the runtime server.

4.1.1.14 Change the runtime server password

This security management function changes the password of a runtime server at the administration server's side. Please refer to *Reviewing and changing runtime servers* on page 40 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

Please remember that the new password must match the one contained in the runtime server. Please refer to xx for changing the password at the runtime server.

4.1.1.15 Delete a runtime server

This security management function deletes a runtime server in the administration server's database. Please refer to *Reviewing and changing runtime servers* on page 40 of *IBM Tivoli License Manager 2.2: Administration* for a description of the user interface.

4.1.2 Administration server command line interface

For error messages of the administration command line interface, please refer to *Server command-line messages* on page 31 of *IBM Tivoli License Manager 2.2: Problem Determination Guide.*

4.1.2.1 Change the db password (dbpasswd command)

This security management function changes the password for the DB2 database associated with the administration server.

Please refer to the **dbpasswd** command on page 28 of *IBM Tivoli License Manager 2.2: Commands* for a description of the user interface.

4.1.2.2 Reencrypt passwords (kstoreupdate command)

This security management function generates a new set of keys and re-encrypts all passwords stored in the configuration (keys.jks file).

Please refer to the **kstoreupdate** command on page 43 of *IBM Tivoli License Manager 2.2: Commands* for a description of the user interface.

4.1.3 Runtime server command line interface

For error messages of the administration command line interface, please refer to *Server command-line messages* on page 31 of *IBM Tivoli License Manager 2.2: Problem Determination Guide.*

4.1.3.1 Change the db password (dbpasswd command)

This security management function changes the password for the DB2 database associated with the server.

Please refer to the **dbpasswd** command on page 28 of *IBM Tivoli License Manager 2.2: Commands* for a description of the user interface.

4.1.3.2 Reencrypt passwords (kstoreupdate command)

This security management function generates a new set of keys and re-encrypts all passwords stored in the configuration.

Please refer to the **kstoreupdate** command on page 43 of *IBM Tivoli License Manager 2.2: Commands* for a description of the user interface.

4.1.3.3 Change runtime server password (rtpasswd command)

This security management function changes the communication password for the runtime server at the runtime server end.

Please refer to the **rtpasswd** command on page 52 of *IBM Tivoli License Manager 2.2: Commands* for a description of the user interface.

Please remember that the new password must match the one entered when the runtime server was added through the web user interface.

4.1.3.4 Change trust store file password (sslpasswd command)

This security management function changes the password used by the runtime server to open its trust store file (key.jks).

Please refer to the **sslpasswd** command on page 56 of *IBM Tivoli License Manager 2.2: Commands* for a description of the user interface.

4.2 Agent Deployment

Agent deployment in the evaluated configuration consists of the following steps:

1. Generate agent certificates for each target computer.

2. Install the agent software on each target computer.
3. Import the agent certificate on each target computer.
4. Verify the correct deployment of the agent

The following sections describe each of these steps.

4.2.1 Generating the Agent Certificate

Follow the instructions provided in the *Security Management* guide, *Preparing agent certificates for client authentication* section on page 22 and 23.

4.2.2 Installing the Agent

In the evaluated configuration, the administrator can deploy agents using the following deployment mechanisms:

- Pull deployment from a Web page
- Individual local installation using a wizard
- Remote bulk distribution using SSH or RSH for UNIX nodes
- Using Windows Logon scripts

Follow the instructions provided in Chapter 4 of the *Planning, Installation and Configuration* guide, *Deploying and upgrading agents* chapter, considering the security factors provided in the following sections.

4.2.2.1 Pull deployment from a Web page

Follow the instructions provided in *Pull deployment from a Web Page*, on page 71. Use SSL communication to deploy agents from a runtime server using the following address:

```
https://<runtime_server_name>/slmruntime/deploy
```

4.2.2.2 Individual local installation using a wizard

Follow the instructions provided in *Individual local installation using a wizard*, on page 73:

- In step 2, select English as the wizard language.
- In step 3, select Custom installation.
- In step 4, select Security level = Maximum and Runtime server port = 443

4.2.2.3 Remote bulk distribution using SSH or RSH for UNIX nodes

Follow the instructions provided in *Remote bulk distribution using SSH or RSH for UNIX nodes*, on page 78:

- Deployment must be performed using SSH.
- Prepare to use the tool as described in page 79.
- When using the tool, as described in page 80, specify Startup mode = Maximum

4.2.2.4 Using Windows Logon scripts

Follow the instructions provided in *Deployment using Windows logon scripts* on page 82.

4.2.3 Importing the Agent Certificate

Follow the instructions provided in the *Security Management* guide, *Deploying agents and certificates* section on pages 24 and 25.

4.2.4 Verifying the Agent installation

Verify that the agent installed in the computer corresponds to the evaluated product.

Log on with an administrator account in the computer where the agent was installed, go to the IBM Tivoli License Compliance Manager installation directory and run the following command from the OS command line:

```
./tlmagent –v
```

Verify that the command provides the following information:

```
Tivoli License Mgr Agent version 2.2.0.10 - Build Jun 20 2006

Tivoli License Manager Version 2.2 (C) Copyright IBM Corp., 2002-2006. All
rights reserved.

(follows copyright information)

CODAG010I The command has been successfully completed.
```

Perform a first plug-in to verify the communication between the agent and the runtime server:

```
./tlmagent –p
```

Verify that the command echoes the following information:

```
CODAG010I The command has been successfully completed.
```

4.3 Recommendations for a Secure Operation

4.3.1 Web User Interface Session ID

After the user has logged in, the Web User Interface creates a Session ID in order to keep track of the user session and avoid user impersonation by an attacker. Please follow the rules below:

- Keep always the browser in kiosk mode.

  The application forces the web browser to hide the navigation toolbar and the status bar in order to make the Session ID not visible. However, you can turn the browser back to its original state easily; or in some occasions, the hiding may not work properly in your browser. Please keep always the browser in a state that the session ID is not visible, an attacker might guess your session id and clone your session in another machine.

- Do not clone the session yourself

  If you are able to copy a URL in another browser instance, either in the same machine or in a different one, you will probably be able to use both instances at the same time with the same session ID. Please avoid this cloning mechanism, as the application may not function properly.

- Once you have finished working with the Web User Interface, please logoff using the button located at the left bottom of the windows panel before closing the browser. In this way, the session id is destroyed. You can close the web browser without logging off; but the session remains effective until the administration server detects timeout has been reached.

4.3.2 Trace and Logging

The evaluated product provides tracing and logging capabilities for the administration and runtime servers, catalog manager, and command-line interface. A minimum level of tracing is enabled by default and cannot be disabled to ensure that some trace information is always available when a problem occurs. Even at a high level of detail, information provided does not sensitive information.

Please refer to chapters 4 through 7 of *IBM Tivoli License Manager 2.2: Problem Determination Guide*, for a detail explanation of these capabilities.

4.3.3 Use of additional commands

The evaluated product provides several commands for maintenance and bulk data import and export. Although these commands are not directly involved in the security of the product, they access sensitive information and in consequence they must be handled with extreme care.

4.3.3.1 PKI support

During the agent certificate generation process, the following commands are used to generate or convert information needed either for the evaluated product or the PKI system:

exportagentid: exports a list of agent IDs from an existent infrastructure.

generateAgentId: generates the agent ID and creates a Certificate Signing Request (CSR) and the associated private key for each agent ID found.

convertcertificate: converts certificate files from PKCS12 format to a format supported by the security software used by the agent.

Please follow the rules below to ensure integrity and confidentiality:

- Keep the information generated by the commands in a protected directory or media.
- Transfer the output information generated by the commands and the input information needed by the commands through a secure channel.

For more information about this commands, please refer to *IBM Tivoli License Manager 2.2: Commands.*

4.3.3.2 Backup and restore of configuration files

Configuration files of administration or runtime servers can be backed up and restored using the **backupconf** and **restoreconf** commands.

These commands use a specific directory for safeguarding data, which is located within the evaluated product environment. If you decide to copy these files to a different media, please follow the rules below to ensure integrity and confidentiality:

- Keep the media in a safe and protected place.
- Transfer the information to the new media through a secure channel.

For more information about this commands, please refer to *IBM Tivoli License Manager 2.2: Commands.*

4.3.3.3 Data Import and Export

Information about the existent infrastructure can be exported and imported with the **dataexp** and **dataimp** commands, respectively. Files can be generated in cvs or xml format, and the output and input directories must be specified.

In terms of the evaluated configuration and its security, information regarding administrators is considered sensitive. The **dataimp** command can be used to perform a bulk import of administrators; likewise, the **dataexp** command can export information about administrators to a text file.

Please follow the rules below to ensure integrity and confidentiality:

- Keep the export files in a protected directory or media.
- Transfer the export files through a secure channel.

Please note that the administrator password is not part of the export file. The **dataexp** command does not generate this information, and the **dataimp** command sets each administrator password to a blank value. The administrator account is inactive until the Super Administrator sets a password through the administration web user interface.

For more information about this commands, please refer to *IBM Tivoli License Manager 2.2: Commands.*

5 Appendix A – Input parameters in Web User Interface

The following table enumerates all the functions of the web user interface that implies a direct security function implemented in the evaluated product. For each of the functions, all needed input parameters are described, including the type of control in the web user interface, the maximum length in chars and any additional validation rule imposed.

Function	Input parameters	Type	Max Len	Validation Rule
Login	User name	Text	60	
	Password	Text	20	
Logoff				
Organization Selection	Name	Radio button		
Create an Organization	Name	Text	40	
	Organization code	Text	21	
	Country	Dropdown		
Update an Organization	Organization code	Text	21	
	Country	Dropdown		
Delete an Organization	Name	Link		
Create an Account	Last name	Text	40	
	First name	Text	40	
	Middle name	Text	20	
	User name	Text	60	
	Password	Text	20	
	Confirm password	Text	20	
	e-mail address	Text	40	Comply with RFC822 norm.
	Phone number	Text	80	
Update an Account	Last name	Text	40	
	First name	Text	40	
	Middle name	Text	20	
	User name	Text	60	
	e-mail address	Text	40	Comply with RFC822 norm.
	Phone number	Text	80	
Delete an Account	User name	Radio Button		
Change Own Password	Old password	Text	20	
	New password	Text	20	Comply with password policy.
	Confirm password	Text	20	Match New Password
Change Password	New password	Text	20	Comply with password policy.

	Confirm password	Text	20	Match New Password
Define Profile	Organization Name	Check box		
	Role	Radio button		
	Show computer information for software installs	Check box		
Change Profile	Organization Name	Check box		
	Role	Radio button		
	Show computer information for software installs	Check box		
Remove Profile	Organization Name	Check box		
Create a Server	Name	Text	60	
	Address	Text	60	
	Port number	Numeric	5	
	SSL port number	Numeric	5	
	Location	Text	40	
	Password	Text	20	Comply with password policy.
	Confirm password	Text	20	Match Password
Update a Server	Name	Text	60	
	Address	Text	60	
	Port number	Numeric	5	
	SSL port number	Numeric	5	
	Location	Text	40	
Change Server Password	New password	Text	20	Comply with password policy.
	Confirm password	Text	20	Match New Password
Delete a Server	Server name	Radio button		

Table 7 - Web User Interface input parameters

6 Appendix B – Documentation Clarifications

This appendix clarifies information in the product documentation provided for IBM Tivoli License Compliance Manager 2.2.

Each section of the appendix corresponds to a different document. Section name, page number and optionally paragraph and bullet number are cited as a reference.

6.1 ITLM Version 2.2 - Planning Installation and Configuration

- Planning monitoring structure, page 1: Which computers are to be monitored?

You cannot consider computers whose hardware and operating system are not part of the evaluated configuration. Please refer to “Supported Operating Systems” in page xx for a list of allowed hardware and operating systems.

- Planning monitoring structure, page 2: Runtime servers

Implementation of SSL between the runtime server and the agents is a security requirement in the evaluated product environment.

- *Planning monitoring structure*, pages 3 and 4: Tables 1 and 2

  The test environment described in these tables is not the environment in which the evaluated configuration was tested: communications between agents and the runtime server must be always set to the Maximum security level.

- *Installation and setup overview*, pages 4 and 5

  The evaluated configuration has prerequisites and steps to be performed before, during, and after the installation of the product. Please follow the instructions provided in *3 - Installation and Configuration* on page 20 of this guide.

- *Planning to upgrade from version 2.1*, page 5

  ITLM Version 2.1 is not allowed in the evaluated configuration, either in runtime servers or agents. Computers with this version of the product must be reinstalled.

- *Supported platforms*, pages 8 through 13

  The evaluated configuration has been tested on a subset of the platforms supported by the product. Please refer to *2.1.2 -Evaluated product environment* on page 11 of this guide.

- *Prerequisites*, pages 14 through 21.

  The evaluated configuration has been tested on a subset of the platforms supported by the product. Please refer to 2.1.2 - Evaluated product on page 11 of this guide.

- *Check the prerequisites for installing DB2 and WebSphere Application Server*, page 26.

  On some UNIX platforms, specifically AIX, HP and Solaris, DB2 and/or WebSphere Application Server could require changing some system parameters to get the products successfully installed. Please refer to WebSphere Application Server and DB2 documentation for more details.

- *Scenario 1: Installing Tivoli License Manager on several computers*, page 28.

  First sentence of the section should be: “This scenario describes a typical implementation of ITLM in which the different servers and database elements are distributed between several computers”.

- *Step 8*, page 32.

  For Windows platforms, the following parameters must be provided:

  - IBM DB2 path
  - Port
  - DB2 administrator user and password

For UNIX platforms, the following parameters must be provided:

  - IBM DB2 instance owner's path
  - Port
  - DB2 instance owner and password

- *Installing the administrator server and prerequisite software*, page 35, step 3.

  Please select **English** as the language version of the wizard.

- *Step 6*, window panel, pages 43 and 46.

  The window panels are outdated. Prerequisite for IBM WebSphere Application Server is 6.0.2.5 or later. For the evaluated configuration, only 6.0.2.5 is allowed.

- *Moving a database*, page 51.

  The database contains sensitive information. The backup of the database must be safeguarded in a secure place.

  Drop the database in the old computer once you have restored it onto the new database.

- *Configure the event notification settings for a server*, page 61.

  Mail recipients must be specified for both the runtime and administration servers.

  E-mails are lost if the SMTP is unreachable.

  For a complete list of notification messages, refer to *Events and notifications on the administration server*, page 39, of the *ITLM Version 2.2 Problem Determination* guide.

- *Chapter 4. Pull deployment from a Web page*, page 71

  Always connect to the runtime server using SSL communications:

      https://<runtime_server_address>/slmruntime/deploy

  The field **Server name** that appears in the Web page form has no effect; pull deployment can be performed only from the runtime server the agent would plug in.

- *Chapter 4. Individual local installation using a wizard*, page 73.

  In step 2, specify **English** as the language to use for the wizard.

- *Chapter 4. Individual local installation using a wizard*, page 74

  Select always **Custom** installation type, as security parameters must be configured to ensure secure communication.

- *Chapter 4. Individual local installation using a wizard*, page 75

  Specify the following values for the agent parameters:

  - Security level: **Maximum**
  - Runtime server port / SSL port: **443** or the one defined in case the runtime and administration servers run in the same machine.

- *Remote bulk distribution using IBM Tivoli Configuration Manager*, page 76.

  This agent deployment mechanism is not allowed in the evaluated configuration.

- *Preparing to use the tool*, page 79

  The fourth paragraph should say "To install the tool and enable the Windows computer as an SSH client, do the following"

  In step 1, copy the agent deployment tool files to a directory with restricted access.

- *Using the tool*, page 80

  In step 1, select **English** as the language version of the wizard.

- *Using the tool*, page 81, step 5.

Specify **Maximum** for Startup mode.

- *Deployment using Windows logon scripts, Prerequisites and preparation*, page 83.

  Only administrators must logon in the computers to in order to deploy the agents, end users should not have administrator's rights.

- *Deployment of i5/OS (OS/400) agents*, page 85

  This method is not allowed as the platform is not supported in the evaluated configuration.

- *Updating agents*, page 91

  If an agent is upgraded with a newer version of the product or any prerequisite component, the agent does not meet the evaluated configuration anymore. Therefore, the only operation that keeps the evaluated configuration is the redeployment of agents only to transfer an agent to a different runtime server or division.

- *Agent self-update,* page 91

  This operation is not allowed in the evaluated configuration. The **updateAgentEnabled** parameter in the agent settings section of the runtime server **system.properties** file must be ALWAYS set to **No**.

- Appendix A. Configuration settings, page 107

  The following parameters in the administration server's **system.properties** file may have only the following values in the evaluated configuration:

  - **sessionTimeout** <= 60 (minutes)
  - **minimumPasswordLength** = 8 (characters)
  - **runtimeToAdminSecurityLevel** = **max**, if secure communication through SSL has been defined between the runtime and administration servers. If secure communication has been defined by other means (e.g. a secure network), **min** is accepted.

  IBM Tivoli License Compliance Manager 2.2 FP1 has added the following parameters:

  - **maxNumberCharsRepeated** = 2 (characters)
  - **minimumNumberNonAlphaChars = 2** (characters)

  The following parameters in the runtime server's **system.properties** file may have only the following values in the evaluated configuration:

  - **agentToRuntimeSecurityLevel**: 2
  - **minimumPasswordLength**: 8 characters

- Appendix B. Installation parameter files (silent mode)

  If you choose to perform silent installations, protect the following information from disclosure:

  - tmlsrv user password (table 22)
  - DB2 UDB administrator user ID (table 23)
  - DB2 UDB administrator password (table 23)
  - Administrator user ID (WebSphere Application Server prerequisite for Windows only) (table 26)
  - Administrator password (WebSphere Application Server prerequisite for Windows only) (table 26)
  - Runtime server's communication password (Table 28)

  Uninstallation parameter files must be protected, as it contains sensitive information:

  - WebSphere Application Server user ID (server running under secure cell) (table 29)
  - WebSphere Application Server password (server running under secure cell) (table 29)

- Appendix B. Agent Installation response file and Windows logon script configuration file, page 134.

  If you choose to perform silent installation of agents, indicate the following parameter values:

  - **setLang.languageCode**=”**2924**” (English**)**
  - **agentConfig.startupMode**=”**Max**”
  - **sslCert.searchCertDir**=**true**
  - **sslCert.certFilePath**= (SSL certificate pathname)

- Appendix D. UNIX agent deployment wizard import file formats (page 145)

  If you choose to perform silent installations, protect the following information from disclosure:

  - <Password> tag content

6.2 ITLM Version 2.2 - Administration

- *The work area,* page 13

  When you type information for a search (for example, a product name or a license name) you can type part of the information preceded, followed, or enclosed by wildcard characters (**%**). The information you type is not sensitive.

- *Browser level and settings*, page 17.

  It is said that a web browser enters in kiosk mode when its toolbar and status bar are no longer visible. Once the administrator has logged in, the web application instructs the web browser to enter in kiosk mode. This is in order to hide the user session id, which is part of the URL during the whole session. Therefore, users logged into the web user interface should not leave kiosk mode.

  Please do not use browser features to save login information, either user name or password.

- *Browser level and settings*, page 17.

  In Windows platforms, you must have MS Internet Explorer 6.x or later to run the administration web user interface.

- *Accessing the administration server*, page 18.

  The first time the super administrator enters to the web user interface an organization may appear at the welcome page. This occurs if the installation of the administration server and the runtime server was performed in the same computer. Otherwise, the super administrator will be taken directly to the Manage Organizations task and will have to create a new organization.

  In case you want to change the organization which you are working on, you don’t need to logoff and logon again. You can click on the home page icon, and the application will return to the Welcome page where you can select a new organization.

- *Adding administrator accounts*, page 31.

  The password assigned to the new administrator account must comply with the password policy as stated in *2.2.2 - Password policy enforcement* on page 12.

- *Updating administration account details*, step 6 on page 34.

  The window panel in the documentation corresponds to the scenario in which the Super Administrator changes an administrator’s password. If an administrator wants to change his/her own password, he/she must enter the current password.

- *Defining user profiles*, step 5, page 36.

  The concept of privacy policy is described in more detail at the information panel of the Web User Interface, as follows:

“The IBM Tivoli License Manager agent gathers information about the software installed on a computer and its use.

You must define appropriate privacy policies for the administrators who are authorized to work with each organization. The privacy policy of an administrator is part of the profile that is defined for each administrator who is authorized to use the Web interfaces.

The default profile implements a privacy policy that allows the computer information for installed software to be reported.

Privacy policies for each administrator can be customized to disable reporting of these details. If you disable the reporting of computer information, the installed software and software use reports relate the product information to the agent that has provided the information. To avoid this level of disclosure, you can uninstall the agent. If you want to uninstall the agent at a later date, you can return to this form for instructions on how to uninstall the agent, or refer to the Tivoli License Manager Planning, Installation and Configuration book.”

- *Registering a runtime server*, page 40.

  The password assigned to the runtime server must match the password assigned during the runtime server installation and must comply with the password policy as stated in *2.2.2 - Password policy enforcement* on page 12.

- *Deleting a server*, page 42.

  If you delete a runtime server permanently, you must redeploy the agents on all the computers belonging to that runtime server and assign them to an existent runtime server.

- *Reviewing and changing divisions*, page 44.

  If you delete a division permanently, you must redeploy the agents on all the computers belonging to that division and assign them to an existent division.

- *Managing Agents*, page 45.

  This function should not be used before redeploying an agent. It is not necessary to delete the agent and add it after redeployment.

  Use the delete agent function when a node is no loner being monitored. The agent must be uninstalled from the node before the agent is deleted from the database.

- *Chapter 12. IBM end-to-end processing*, page 133.

  The IBM web site provides secure communication through SSL.

6.3 *ITLM Version 2.2 – Security Management*

- Chapter 1. Overview. Interaction using the DB2 UDB protocol, page 2.

  The connection between the runtime or administration server with its corresponding database server must be within a secure network.

- Secure communications, page 3.

  Security Level for Agent to runtime server communication must be always set to Maximum, that is, mutual authentication under SSL.

  Web browser to administration server communications must be always under SSL.

- Authentication, page 4.

  Only certificates signed by a certificate authority can be used in the evaluated configuration. Self-signed certificates are not allowed.

- Upgrading and backward compatibility, page 5.

  Upgrade from Version 2.1 or 2.2 is not allowed in the evaluated configuration.

- Web UI access authorization, page 7.

LDAP is not allowed as an identification and authentication mechanism in the evaluated configuration.

- Chapter 3. Defining agent to runtime server communication, page 17.

  Only communication using the HTTPS protocol with server and client authentication (MAX) is allowed.

- Deployment of agents with maximum security level, page 25.

  The correct paragraph under this section title is: “Agents deployed from runtime servers that use this level of security are not able to contact the runtime server *unless* a personal certificate to be used for client authentication is available in the agent keystore database”

- *Step 7*, page 29.

  The correct paragraph in this step is: “On each computer where an *agent* that is to be upgraded is installed, import the certificate.”

- *Step 11*, page 30.

  The correct paragraph in this step is: “Restart the runtime server”

- Chapter 6. Authentication of user credentials, page 39.

  The LDAP authentication method is not allowed in an evaluated configuration.

- Maintain password security, Notes 3, page 43.

  The password policy stated in the Commands guide is the correct one, which is:

  > *The password has a maximum length of 20 characters and can contain only the following characters: A–Z, a–z, 0–9, +, –, *, |, =*

  For the runtime server communication password, the policy described in *2.2.2 - Password policy enforcement* on page 12 of this guidance also applies.

6.4 ITLM Version 2.2 - Commands

- **dataimp** command, page 25

  If you import administrators with this command, the database is updated in the following way:

  - An existent user is updated with the information provided; the user password remains the same (as it is not part of the import file).
  - A new user is added, the password is not set and the user remains inactive until the administrator sets the password through the Web Administration User Interface.
  - An existent user not included in the import file remains in the database (it is not deleted, the command only adds or updates information).

- **rtpasswd** command, page 52

  The password must also comply with the policy for runtime servers, enforced by the Web Administration User Interface. See *2.2.2 - Password policy enforcement.*

6.5 ITLM Version 2.2 – Data Dictionary

- *ADMINISTRATOR* table, page 9.

  The PASSWORD field contains a hashed value of the administrator password, not the encrypted password.

- *SERVER* table, page 70.

  The PASSWORD field contains a hashed value of the runtime server password, not the encrypted password.

- *SERVER_DELETED* table, page 70.

The PASSWORD field contains a hashed value of the deleted server password, not the encrypted password.

7 Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described 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:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee. The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental. This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not appear.

Trademarks

IBM, the IBM logo, Tivoli, the Tivoli logo, AIX, DB2, DB2 Universal Database, Tivoli, Tivoli Enterprise, WebSphere and Redbooks™ are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft, Windows and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.