Security Guide
SAP IT Infrastructure Management

Target Audience

- Technology consultants
- Security consultants
- System administrators

CUSTOMER
Document version: 1.0 – 06/11/2012

Document History

Caution

Before you start the implementation, make sure you have the latest version of this document. You can find the latest version at the following location: http://service.sap.com/instguides ▶ *SAP Components* → *SAP IT Infrastructure Management* ↵.

The following table provides an overview of the most important document changes.

Version	Date	Description
1.0	6/11/2012	New

Table of Contents

1 Introduction

 Caution

This guide does not replace the Administration or Operation Guides that are available for productive operations.

1.1 Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

1.2 Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to SAP IT Infrastructure Management. To assist you in securing SAP IT Infrastructure Management, we provide this Security Guide.

1.3 About this Document

This guide describes the important security preparations to be made before you start with the installation of SAP IT Infrastructure Management. For the operating system security, follow Microsoft's standard security guidelines.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- *Before You Start*
  This section contains information about why security is necessary, how to use this document, and references to other Security Guides that are the basis for this Security Guide.
- *Technical System Landscape*
  This section provides an overview of the technical components and communication paths that are used by SAP IT Infrastructure Management.
- *User Administration and Authentication*
  This section provides an overview of the following user administration and authentication aspects:
  - Creation of users and profiles and standard user passwords
  - Emergency user concept, which is a way to get emergency access to the software if logon to the software is not possible any longer
- *User Management*
  This section provides an overview of the user types that are required in SAP IT Infrastructure Management and standard users that are delivered with SAP IT Infrastructure Management
- *Integration into Single Sign-On Environments*
  This section provides an overview of the aspects to consider for integration into Single Sign-On environments.
- *Authorizations*
  This section provides an overview of the authorization concept that applies to SAP IT Infrastructure Management.
- *Session Security Protection*
  This section provides information about enabling Secure Session Management, which prevents JavaScript or plug-ins from accessing the SAP logon ticket or security session cookie(s).
- *Network and Communication Security*
  This section provides an overview of the communication paths used by SAP IT Infrastructure Management and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.
- *Communication Channel Security*
  This section provides an overview of the communication channels that are used for the communication between the components in the technical system landscape.
- *Network Security*
  This section provides an overview of the network configuration, including ports.
- *Communication Destinations*
  This section provides an overview of the Web services that SAP IT Infrastructure Management uses.
- *Data Storage Security*
  This section provides an overview of any critical data that is used by SAP IT Infrastructure Management and the security mechanisms that apply.
- *Security for Additional Applications*

This section provides security information that applies to third-party or additional applications that are used with SAP IT Infrastructure Management.

- *Other Security-Relevant Information*

  This section contains information about:

  - Java Script
  - XAML
  - ActiveX

- *Security-Relevant Logging and Tracing*

  This section provides an overview of the trace and log files that contain security-relevant information. These files allow you to reproduce activities in case of security breaches.

- *Services for Security Lifecycle Management*

  This section provides an overview of services provided by Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.

- *Appendix*

  This section provides references to further information.

This page is left blank for documents that are printed on both sides.

2 Before You Start

2.1 Fundamental Security Guides

Business solutions typically deal with data that is critical and important for the success of a company. This importance is typically addressed by a security concept that defines how to protect IT systems and data against illegal access, damage or modifications and espionage. Since security is especially important for SAP systems, it is to be extended also to the surrounding infrastructure of the business-relevant systems.
Security is not a simple one-dimensional issue but is related to many different areas. An efficient security concept therefore describes threads and concepts to minimize risks. In many senses, such concepts are individual for each company as some risks may be obvious in one company but do not exist in another. The following table describes a number of typical threads and the measures against them:

Threat	Measure
Illegal access, modification of data	User authentication and authorization concept, identity management
Malware, virus, trojan	Virus scan and security patch management
Intrusion, denial-of-service, and so on	Firewalls, network security, IT architecture
Espionage	User authorization, transport layer security, use of IPsec
General security vulnerabilities	Hardening of the Windows operating system
Mobile computers (which are used outside and inside a company network)	Network access protection

2.2 Important SAP Notes

The most important SAP Notes that apply to the security of SAP IT Infrastructure Management are shown in the table below.

Title	SAP Note	Comment
Install SAP IT Infrastructure Management	1652552	Install SAP IT Infrastructure Management

For a list of additional security-relevant SAP Hot News and SAP Notes, see also SAP Service Marketplace at http://service.sap.com/securitynotes.

2.3 Additional Information

For more information about specific topics, see the quick links shown in the table below.

Content	Quick link on SAP Service Marketplace or SDN
Security	http://sdn.sap.com/irj/sdn/security
Security Guides	http://service.sap.com/securityguide
Related SAP Notes	http://service.sap.com/notes http://service.sap.com/securitynotes
Released platforms	http://service.sap.com/pam
Network security	http://service.sap.com/securityguide
SAP Solution Manager	http://service.sap.com/solutionmanager
SAP NetWeaver	http://sdn.sap.com/irj/sdn/netweaver

3 Technical System Landscape

The server and client components of SAP IT Infrastructure Management can be installed on the same local system.

 Note

Note that only the database can be installed on a different system. For more information about installing the SAP IT Infrastructure database, see the Configuration Guide and the Installation Guide on SAP Service Marketplace at http://service.sap.com/instguides.

For more information about the technical system landscape, see the resources listed in the table below.

Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Technical description for SAP Infrastructure Management and the underlying components such as SAP NetWeaver	Master Guide	http://service.sap.com/instguides
High availability	High Availability for SAP Solutions	http://sdn.sap.com/irj/sdn/ha
Technical landscape design		http://sdn.sap.com/irj/sdn/landscapedesign
Security		http://sdn.sap.com/irj/sdn/security

To open the WPF (Windows Presentation Foundation) GUI from a browser, use following URL: **http://<servername>/controlcenter**.

This page is left blank for documents that are printed on both sides.

4 User Administration and Authentication

Each user is provided with their own logon data and with individual access rights to the system.

4.1 Creating User Groups

You use user groups to grant access rights to a defined group of users.
Administrators create user groups without any restrictions, add new groups, modify and delete existing groups.

Procedure

1. To create a user group, choose ▶ *Config* → *User group* ↵.
   The system creates the following user groups by default during installation:
   - NetworkManager Group I
   - NetworkManager Group II
   - NetworkManager Group III
2. Choose *Add* to create a new user group and enter the following information:
   - *Name*: name of the group
   - *Description*: description of the group
   - *Accessible Node Groups*: You can add as many groups that a user has access to.

4.2 Creating User Profile

User profiles define functional access rights for a simple assignment to users.

Procedure

1. To create a new user profile, choose ▶ *Config* → *User* ↵.
   The system displays the following tabs:
   - *Current User* displays the user attributes of the user currently logged on.
   - *User Admin* allows you to add, edit, and modify users.
2. On the *User Admin* tab, choose *Add*.
3. Enter the following information:
   - *Name*: logon name of the user
   - *User Type*:

- *Concurrent*: license version where one or more registered user can simultaneously log on.
- *Named*: license version, assigned to a specific user. With this license, a user cannot log on to the Microsoft Windows interface.

- *Group Membership*: You can assign the user to one ore more user groups.
- *User Level*: All users are assigned to a minimum of one of the three categories *Administrator*, *User* or *Operator*. The *Operator* category has the fewest privileges.
  For more information, see *Overview of User Management Rights* [page 21].
- *Default Profile*: The profile that is loaded automatically when you log on.
- *Password/ Confirm*: Logon password of the user. You have to enter the password twice. To save the password, choose *Set Password*.

4.3 Creating Support User

You can give access to an external support employee with the role *Read/View Only*.

Procedure

1. Create a new user on your Microsoft operating system.
   For more information, see Microsoft Help.
2. Assign a user group that has the following permissions:
   - *Read and execute*
   - *List folder contents*
   - *Read*
3. Create the same user with user level *operator* in SAP IT Infrastructure Management. For more information, see *Creating User Profile* [page 13].

4.4 Providing Emergency Access

If logging on to the software is impossible, a security user concept is provided to access the software. The administrator resets the user settings by reinstalling the default users and rights, which are part of the basic installation.

Procedure

1. Start the *Process Administrator*.
2. Start the *Database Administrator*.
3. Choose the *Maintenance* tab and choose *Reinstall/Update*.
4. To shut down the program modules, choose *Yes*.
5. In the *Database Update* dialog, choose *Reinstall Data* and then *Network Manager User*.
   Do not change any other option.

6. To overwrite the existing users, choose *Start Reinstall*.
   The existing users and rights are overwritten with the default passwords and users.
   For more information, see *Changing Standard User Passwords* [page 15].

4.5 Providing Read-Only Authorization for Administrative Tools

You can create a user with read-only authorization for relevant log entries.

Procedure

1. Create a user. For more information, see *Creating User* [page 13].
2. Add the user to the IT ISM Network Manager Group *SMC Operator Logs*.

Result

The user can now read the log file by choosing *SAP IT ISM* → *Administration* → *logs*.

4.6 Changing Standard User Passwords

After the first logon, the *superuser* must change all passwords of the automatically installed users, including their own.
The application automatically installs the following standard users:

- *superuser*
- *operator*
- *user*
- *admin*
- *administrator*

The initial password for all users is `public`. The users and their credentials are stored in the database.

Procedure

The administrator must change the initial password of the *superuser* after the installation and set up passwords for the other automatically created users as follows:

1. Log on to SAP IT Infrastructure Management with the *superuser* account and the initial password.
2. In the menu of the main window, choose *Config* → *Users...*.
   The *User Edit* dialog opens.
3. On the *Current User* tab, change the initial *superuser* password and accept the changes by choosing *Set Password*.

4. On the *User Admin* tab, change the password for each user that has been automatically created as follows:
   a) Select a user and then choose *Modify*.
   b) Enter the user account details.
   c) Enter a new password and choose *ok*.

Note

Since Microsoft Internet Information Services (IIS) and the Active Directory are used for the authentication, you cannot change passwords at the first logon, customize the minimum length of passwords, and lock users after several failed attempts to log on.
To make sure that the system works correctly, the administrator must set up the same users in SAP IT Infrastructure Management as in the operating system.

5 User Management

User management for SAP IT Infrastructure Management uses the mechanisms provided with the Microsoft Internet Information Service and additionally the Active Directory, for example, user types, and password policies.

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively must change their passwords on a regular basis, but not those users who run background processing jobs.
User types are initially classified into three user levels in SAP IT Infrastructure Management. The principal function of these user levels is to classify the users according to their privileges:

- Superuser
  Superusers have no restrictions at all.
- Normal user
  Users have limited rights.
- Operator user
  Operators, similarly to users, also have limited privileges and no write-access to the database and the nodes. Operators work within predefined settings, which they cannot modify. These restrictions are predefined and block access to specific functions of the individual program modules (for example, menus, buttons, and so on).

Standard Users

The following users are automatically created when installing SAP IT Infrastructure Management. The table below shows the standard users that are created automatically during the installation.

System	Type	Password	Description
Superuser	Superuser	public	Main user with all rights
Administrator	Superuser	public	Main user with all rights
Operator	Operator user	public	Operator user with limited rights
Admin	Superuser	public	Main user with all rights
User	Normal user	public	Normal user with limited rights

We recommend that you change the user IDs and passwords for users that are automatically created during the installation.

6 Integration into Single Sign-On Environments

User management for SAP IT Infrastructure Management uses the mechanisms provided with the Microsoft Internet Information Service and additionally the Active Directory.
To use single sign-on in the environment, you must configure the same users in the IT ISM Business Service Manager as in the Active Directory. The most widely used supported mechanisms are listed below. For a complete list, see the links provided below.

- Secure Network Communications (SNC)
  SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.
- Client certificates
  As an alternative to user authentication with a user ID and passwords, users using a Web browser as a frontend client can also use X.509 client certificates for authentication. In this case, user authentication is performed on the Web server via the Secure Sockets Layer Protocol (SSL Protocol) and no passwords have to be transmitted. User authorizations are valid in accordance with the authorization concept in the SAP system.

SAP IT Infrastructure Management supports the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver. The security recommendations and guidelines for user administration and authentication are described in the SAP NetWeaver Security Guide.
For more information about the available authentication mechanisms, see *User Authentication and Single Sign-On* in the SAP NetWeaver Library.

This page is left blank for documents that are printed on both sides.

7 Authorizations

All roles that are required are delivered with the installation of SAP IT Infrastructure Management. The following user types are delivered with the system:

- Superuser
- User
- Operator

The user types can perform the following tasks:

Task	Superuser	User	Operator
Creating and managing user accounts	x		
Managing user groups	x		
Starting SNMP set-commands	x	x	
Creating and managing profiles	x		
Saving opened profiles	x	x	
Editing opened filter configurations	x	x	
Editing profile settings	x	x	
View of system tasks and schedules	x	x	x
Editing of system tasks and schedules	x		
Creating custom tasks	x		
Editing own tasks	x	x	x
Start/stop/pause of own tasks	x	x	x
Start/stop of system tasks	x	x	
Database administration	x		
Topology views	x	x	
Configuring/starting of discovery scans	x	x	

Task	Superuser	User	Operator
View/configuration/ starting macro	x	x	
Starting license dialog	x	x	
Severity slider view	x	x	
Starting of communication server options	x	x	
View of station list in multi-user-system	x	x	
Editing/changing profile configuration	x		
Repeal of profile barriers (filter/map)	x		
Administration of authentication sets	x	x	
Administration of maintenance intervals	x	x	
Editing of alerting options	x	x	
Configuration of node groups	x	x	
Running of poll-resets for whole system	x		
Deactivating of polling for whole system	x		
Initiating of shutdown in multi-user-system	x		
Editing of node options, filter configurations and maps	x	x	
Modifying of status and event log entries	x	x	
Adding/deleting of nodes	x	x	
Change of node user group assignment	x		
Multi-site/backup server configuration	x		
Global/product-specific saving of window layout	x	x	

User Group and Authorization Concept for SAP IT Infrastructure Management

Each user is assigned to a user group. User groups are freely expandable. Assign user groups to nodes in all product deployments. Members of a group only have access to those nodes that are assigned to their group. If no assignment is made, the User and Operator do not have access to the nodes. A profile contains settings managed individually for each user to specify the following functions:

- Functions that are to be started and/or used when logging on
- Maps that are to be loaded
- Event filter configurations (and individual alerting reactions)
- Screen configurations (layout), window positions

You can also assign a profile or elements of it to multiple users. For example, you can configure that Operator users can work with the same event filters but with different maps.

Standard User Groups

The table below shows the standard user groups that can be used by SAP IT Infrastructure Management.

User group	Description
Administrator	Administrator group
Helpdesk	Default helpdesk group
Network Manager Group I	
Network Manager Group II	
Network Manager Group III	
Public News	Default news group for external news
SMC Auditor	SMC-Group
SMC Dashboard User	SMC-Group
SMC Manager	SMC-Group
SMC Network Administrator	Network administration group (Superuser)
SMC Operator	SMC-Group
SMC Operator Logs	SMC-Group
SMC Report User	SMC-Group
SMC User	SMC-Group

This page is left blank for documents that are printed on both sides.

8 Session Security Protection

To increase the security and prevent access to the SAP logon ticket and security session cookie(s), we recommend enabling secure session management. We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

To enable the session security on the AS ABAP, set the corresponding profile parameters and activate the session security for the client(s) using the transaction `SICF_SESSIONS`.
For more information, a list of the relevant profile parameters, and detailed instructions, see *Activating HTTP Security Session Management on AS ABAP* [external document] in the AS ABAP security documentation.

Session Security Protection on the AS Java

On the AS Java, set the HTTP Provider properties as described in *Session Security Protection*.

This page is left blank for documents that are printed on both sides.

9 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network must support the communication required for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and the application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, intruders cannot compromise the machines and gain access to the back-end system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit known bugs and security holes in network services on the server machines.
The network topology for SAP IT Infrastructure Management is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to SAP IT Infrastructure Management. Details that specifically apply to SAP IT Infrastructure Management are described in the following topics:

- *Communication Channel Security* [page 29]
  This topic describes the communication paths and protocols used by SAP IT Infrastructure Management.
- *Network Security* [page 31]
  This topic describes the recommended network topology for the SAP IT Infrastructure Management. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports required to operate SAP IT Infrastructure Management.
- *Communication Destinations* [page 33]
  This topic describes the information required for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the SAP NetWeaver Security Guide:

- *Network and Communication Security*
- *Security Guides for Connectivity and Interoperability Technologies*

This page is left blank for documents that are printed on both sides.

10 Communication Channel Security

The following communication channels are used between the components:

- Technical infrastructure
  - Control Center client to Control Center server
  - Control Center server to request server
  - Build-In ASP and ASP.NET pages used by Control Center client to DB server
  - Built-In ASP and ASP.NET pages used by Control Center client to SQL server
  - DB server to SQL server (local or remote)
- Process/data flow
  Application data is transferred to Control Center client

The following technologies are used for the communication: HTTP, HTTPS, SSL, SOAP, WCF, Net.TCP, ADO, COM
The following data requires special protection:

- Passwords
- Certificates

The table below shows the communication channels used by SAP IT Infrastructure Management, the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Control Center client to Control Center server	TCP	All application data	Passwords, certificates
Control Center server to request server	TCP	Statistical data	
ASP pages to SQL server/DB server	ADO/TCP	All application data	

DIAG and RFC connections can be protected by using Secure Network Communications (SNC). HTTP connections are protected by using the Secure Sockets Layer (SSL) protocol. SOAP connections are protected with Web services security.

Recommendation

We strongly recommend that you use secure protocols (SSL, SNC) whenever possible.

For more information, see *Transport Layer Security* and *Web Services Security* in the SAP NetWeaver Security Guide.

11 Network Security

You can operate the different components of the application in different network segments. The Control Center client can be used anywhere on a system with an internet browser. To work properly in the customer network, you have to set the default TCP/UPD port 81. Port 81 is the basic TCP/UPD port, which comes with the installation if the administrator has not changed it during the installation process. This is also the port through which the communication takes place. For HTTP/HTTPS connections, the standard ports 80 (HTTP) and port 443 (HTTPS) have to be configured and have to be able to access SAP IT Infrastructure Management. For more information, see *Using Firewall Systems for Access Control* in the SAP NetWeaver Security Guide. You have to set up the application is to be set up in the standard LAN segment For more information, see *Using Multiple Network Zones* in the SAP NetWeaver Security Guide.

Ports

SAP IT Infrastructure Management uses the ports from the AS ABAP or AS Java and the default TCP/UDP port 81, HTTP port 80, and HTTPS 443. For more information, see the topics for *AS ABAP Ports* and *AS Java Ports* in the corresponding SAP NetWeaver Security Guides. For further components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see also the document *TCP/IP Ports Used by SAP Applications* located on the SAP Developer Network at `http://sdn.sap.com/irj/sdn/security` under *Infrastructure Security* → *Network and Communications Security*.

This page is left blank for documents that are printed on both sides.

12 Communication Destinations

SAP IT Infrastructure Management uses the following Web services hosted by the Microsoft Internet Information Server:

- SAP Mapping Web service
  This Web service provides mapping information regarding technical systems and their hosts
- SAP DPC Web service
  IT ISM sends event data to this Web service.
- SAP Alerting-Error Web service
  IT ISM sends information about errors regarding altering to this Web service.
- IT ISM Notification Web service
  This Web service is called when changes happen in the Configuration Management Database (CMDB). It enables notification about CMDB changes on SAP side.
- IT ISM Main Web service
  This Web service is called during the SAP Solution Manager setup for initialization (address exchange, and so on).
- IT ISM Data Access Web service
  This Web service provides an interface for the retrieval of CMDB data.
- IT ISM Configuration Web service
  This Web service accepts configuration information from alerting.

To communicate between the destinations in SAP IT Infrastructure Management, a user with administrator rights has to be configured.

This page is left blank for documents that are printed on both sides.

13 Data Storage Security

13.1 Data Storage

The system data is stored in the Configuration Management Database (CMDB). A user account with local administrator rights on the terminal server is required to log on to the terminal server using logical path and filenames to provide access to the file system. SAP IT Infrastructure Management saves data in the CMDB. It is therefore required to provide access to the corresponding databases in the system.

13.2 Data Protection

By default, all sensible data (passwords) is stored in the database with a 64-bit encryption. Sensible data is automatically encrypted. Log files with personal data are stored in the database. For more information, see *Security-Relevant Logging and Tracing* [page 41] in this Security Guide. In many cases, it is legally required. It typically applies to the deletion of the data in the application storage and to archives. To delete data in the application storage and archives, you must have administration rights for the Configuration Management Database (CMDB).

1. Start the SQL Database Administrator Console.
2. Open the database (standard name) *Main*.
3. To delete the log files, you must perform the following SQL statement in the SQL Database Administration Console: `TRUNCATE TABLE ERMsyslog`


Caution

If you perform the SQL statement, all data included in the table is deleted. This step is irreversible.

To work with SAP IT Infrastructure Management, the application requires a current web browser used as a user interface. For more information about the system requirements and the supported browser versions, see the Master Guide for SAP IT Infrastructure Management on SAP Service Marketplace at `http://service.sap.com/instguides`.
The system temporarily saves session variables of ASP and ASP.net within the application. The cookies are automatically deleted after closing the session. SAP IT Infrastructure Management sets and saves no other cookies. Since the Windows authentication is used, no other special protection is required for the data (for example, persistent authentication data).

This page is left blank for documents that are printed on both sides.

14 Security for Additional Applications

SAP IT Infrastructure Management uses the following third-party applications:

- Microsoft Internet Information Server (IIS)
  The Microsoft Windows Internet Information Server (IIS) supports Secure Sockets Layer (SSL) communications.
  The Web sites of SAP IT Infrastructure Management must use secure SSL connections if you access the Web sites over the Internet. Even if you use SAP IT Infrastructure Management in the Intranet, you should use secure SSL connections. Without SSL connections, passwords and communication can be retrieved from any simple spyware. However, before the web server can support SSL sessions, a web site certificate is to be installed. For more information about how to install the certificate on your version of IIS, see the Microsoft support sites. For more information about installing and configuring the Internet information server, see the Installation Guide for SAP IT Infrastructure Management on SAP Service Marketplace at http://service.sap.com/instguides.
- SQL Service Authentication
  We highly recommend that you do not run the Microsoft SQL Server and the Microsoft Reporting Services under the local system account. Use instead a computer/domain user account. If authorizations have not already been made during the installation, it can be done with the SQL Server Configuration Manager in the configuration tools submenu of the SQL Server start menu. Set at least the following services for a local or domain user account:
  - SQL Server Full Text Search
  - SQL Server (Microsoft SQL Server)
  - SQL Server Reporting Services
  - SQL Server Agent

  > Note
  > You must start the SQL Server agent service so that e-mails can be sent to those recipients required to receive scheduled reports. Therefore set the status mode for this service to *automatic*.

  For more information about installing and configuring the Microsoft SQL Server, see the see the Installation Guide for SAP IT Infrastructure Management on SAP Service Marketplace at http://service.sap.com/instguides.
- Open SSL
  Open SSL is a library that provides cryptographic functionality to applications such as secure web servers.

 Note

If you have high security requirements, you have to operate the system by using these third-party products.

15 Other Security-Relevant Information

The following security-relevant features have to be enabled to work correctly with SAP IT Infrastructure Management. If your security policy does not allow the use of these features, active code, or functions, SAP IT Infrastructure Management does not work correctly:

- JavaScript has to be enabled. Otherwise, the application does not work correctly.
- XAML has to be enabled. Otherwise, the WPF surface does not work correctly.
- ActiveX has to be enabled. Otherwise, you cannot access the SAP Library.

This page is left blank for documents that are printed on both sides.

16 Security-Relevant Logging and Tracing

You can use the following options to find security-relevant logging events in SAP IT Infrastructure Management:

- Logging events of the Infrastructure Manager
  You can find logging events under *view* → *current log*.
  The system writes the following events:
  - User <user name> logged in
  - User <user name> logged off
- WPF (Windows Presentation Foundation) GUI
  You can find logging events under *Administration* → *Log*.
  The system writes the following events:
  - User <user name> has successfully logged into <server name>
  - User <user name> has successfully logged out from <server name>
  - User <user name> has been rejected by <server name>
  - User <user name> with logon <user name> and description <description> has been inserted by user <user name>
  - User <user name> with logon <user name> and description <description> has been updated by user <user name>
  - User <user name> with logon <user name> and description <description> has been deleted by user <user name>
  - User <user name> with ID <user name> and description <description> has been assigned to support employee group <group> with ID <ID> by user <user name>
  - User <user name> with ID <user name> and description <description> has not been assigned from support employee group <group> with ID <ID> by user <user name>
  - Group <group> with ID <ID> and description <description> has been added by user <user name>
  - Group <group> with ID <ID> and description <description> has been updated by user <user name>
  - Group <group> with ID <ID> and description <description> has been deleted by user <user name>
  - Support employee group <group> with ID <ID> has been assigned to user <user name> with ID <ID> and description <description> by user <user name>
  - Support employee group <group> with ID <ID> has not been assigned from user <user name> with ID <ID> and description <description> by user <user name>

- Privilege <privilege> with ID <ID> and activity <activity> has been assigned to support employee group <group> with ID <ID> by user <user name>
- Privilege <privilege> with ID <ID> and activity <activity> has not been assigned from support employee group <group> with ID <ID> by user <user name>
- Support employee group <group> with ID <ID> has been assigned to privilege <privilege> with ID <ID> and activity <activity> by user <user name>
- Support employee group <group> with ID <ID> has not been assigned from privilege <privilege> with ID <ID> and activity <activity> by user <user name>
- Node <node> with ID <ID> has been assigned to support employee group <group> with ID <ID> by user <user name>
- Node <node> with ID <ID> has not been unassigned from support employee group <group> with ID <ID> by user <user name>
- Node <node> with ID <ID> has not been assigned to support employee group <group> with ID <ID> by user <user name>
- Node <node> with ID <ID> has not been assigned from support employee group <group> with ID <ID> by user <user name>

17 Services for Security Lifecycle Management

Active Global Support provides the following services to assist you in maintaining security in your SAP systems on an ongoing basis.

17.1 Security Chapter in the EarlyWatch Alert (EWA) Report

This service regularly monitors the Security chapter in the EarlyWatch Alert report of your system. It lets you know:

- Whether SAP Security Notes have been identified as missing on your system
  In this case, analyze and implement the identified SAP Notes, if possible. If you cannot implement the SAP Notes, the report should be able to help you decide on how to handle the individual cases.
- Whether an accumulation of critical basis authorizations has been identified
  In this case, verify whether the accumulation of critical basis authorizations is all right for your system. If not, correct the situation. If you consider the situation as all right, you should still check for any significant changes compared to former EWA reports.
- Whether standard users with default passwords have been identified on your system
  In this case, change the corresponding passwords to non-default values.

17.2 Security Optimization Service (SOS)

The Security Optimization Service is used for a more thorough security analysis of your system including:

- Critical authorizations in detail
- Security-relevant configuration parameters
- Critical users
- Missing security patches

This service is available as a self-service within SAP Solution Manager, as a remote service, or as an on-site service. We recommend that you use it regularly (for example once a year) and in particular after significant system changes or in preparation for a system audit.

17.3 Security Configuration Validation

The Security Configuration Validation can be used to continuously monitor a system landscape for compliance with predefined settings, for example, from your company-specific SAP Security Policy. This primarily covers configuration parameters, but it also covers critical security properties like the existence of a non-trivial Gateway configuration or making sure standard users do not have default passwords.

17.4 Security in the RunSAP Methodology / Secure Operations Standard

With the E2E Solution Operations Standard Security service, a best practice recommendation is available on how to operate SAP systems and landscapes in a secure manner. It guides you through the most important security operation areas and links to detailed security information from SAP's knowledge base wherever appropriate.

17.5 More Information

For more information about these services, see:

- EarlyWatch Alert: http://service.sap.com/ewa
- Security Optimization Service / Security Notes Report: http://service.sap.com/sos
- Comprehensive list of Security Notes: http://service.sap.com/securitynotes
- Configuration Validation: http://service.sap.com/changecontrol
- RunSAP Roadmap, including the Security and the Secure Operations Standard: http://service.sap.com/runsap (see the RunSAP chapters 2.6.3, 3.6.3 and 5.6.3)

18 Appendix

For more information, see SAP Marketplace at http://service.sap.com/instguides *SAP ComponentsSAP IT Infrastructure Management*. You can find the following guides:

- Configuration Guide
- Installation Guide
- Master Guide
- Operations Guide

For the application help, see SAP Library at http://help.sap.com → *Application Lifecycle Mgmt* → *SAP IT Infrastructure Management*.

This page is left blank for documents that are printed on both sides.

A Reference

A.1 The Main SAP Documentation Types

The following is an overview of the **most important** documentation types that you need in the various phases in the life cycle of SAP software.

Cross-Phase Documentation

SAPterm is SAP's terminology database. It contains SAP-specific vocabulary in over 30 languages, as well as many glossary entries in English and German.

- Target group:
  - Relevant for all target groups
- Current version:
  - On SAP Help Portal at http://help.sap.com → *Glossary*
  - In the SAP system in transaction STERM

SAP Library is a collection of documentation for SAP software covering functions and processes.

- Target group:
  - Consultants
  - System administrators
  - Project teams for implementations or upgrades
- Current version:
  - On SAP Help Portal at http://help.sap.com (also available as documentation DVD)

The **security guide** describes the settings for a medium security level and offers suggestions for raising security levels. A collective security guide is available for SAP NetWeaver. This document contains general guidelines and suggestions. SAP applications have a security guide of their own.

- Target group:
  - System administrators
  - Technology consultants
  - Solution consultants
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/securityguide

Implementation

The **master guide** is the starting point for implementing an SAP solution. It lists the required installable units for each business or IT scenario. It provides scenario-specific descriptions of

preparation, execution, and follow-up of an implementation. It also provides references to other documents, such as installation guides, the technical infrastructure guide and SAP Notes.

- Target group:
  - Technology consultants
  - Project teams for implementations
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

The **installation guide** describes the technical implementation of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
  - Technology consultants
  - Project teams for implementations
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

Configuration Documentation in SAP Solution Manager – SAP Solution Manager is a life-cycle platform. One of its main functions is the configuration of business scenarios, business processes, and implementable steps. It contains Customizing activities, transactions, and so on, as well as documentation.

- Target group:
  - Technology consultants
  - Solution consultants
  - Project teams for implementations
- Current version:
  - In SAP Solution Manager

The **Implementation Guide (IMG)** is a tool for configuring (Customizing) a single SAP system. The Customizing activities and their documentation are structured from a functional perspective. (In order to configure a whole system landscape from a process-oriented perspective, SAP Solution Manager, which refers to the relevant Customizing activities in the individual SAP systems, is used.)

- Target group:
  - Solution consultants
  - Project teams for implementations or upgrades
- Current version:
  - In the SAP menu of the SAP system under ▶ *Tools* → *Customizing* → *IMG* ↵

Production Operation

The **technical operations manual** is the starting point for operating a system that runs on SAP NetWeaver, and precedes the application operations guides of SAP Business Suite. The manual refers

users to the tools and documentation that are needed to carry out various tasks, such as monitoring, backup/restore, master data maintenance, transports, and tests.

- Target group:
  - System administrators
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

The **application operations guide** is used for operating an SAP application once all tasks in the technical operations manual have been completed. It refers users to the tools and documentation that are needed to carry out the various operations-related tasks.

- Target group:
  - System administrators
  - Technology consultants
  - Solution consultants
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

Upgrade

The **upgrade master guide** is the starting point for upgrading the business scenarios and processes of an SAP solution. It provides scenario-specific descriptions of preparation, execution, and follow-up of an upgrade. It also refers to other documents, such as upgrade guides and SAP Notes.

- Target group:
  - Technology consultants
  - Project teams for upgrades
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

The **upgrade guide** describes the technical upgrade of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
  - Technology consultants
  - Project teams for upgrades
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

Release notes are documents that contain short descriptions of new features in a particular release or changes to existing features since the previous release. Release notes about ABAP developments are the technical prerequisite for generating delta and upgrade Customizing in the Implementation Guide (IMG).

- Target group:

- Consultants
- Project teams for upgrades

- Current version:
  - On SAP Service Marketplace at http://service.sap.com/releasenotes
  - In the SAP menu of the SAP system under *Help* → *Release Notes* (only ABAP developments)

Typographic Conventions

Example	Description
<Example>	Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, “Enter your **<User Name>**”.
Example → *Example*	Arrows separating the parts of a navigation path, for example, menu options
Example	Emphasized words or expressions
Example	Words or characters that you enter in the system exactly as they appear in the documentation
http://www.sap.com	Textual cross-references to an internet address
/example	Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web
123456	Hyperlink to an SAP Note, for example, SAP Note 123456
Example	■ Words or characters quoted from the screen. These include field labels, screen titles, pushbutton labels, menu names, and menu options. ■ Cross-references to other documentation or published works
Example	■ Output on the screen following a user action, for example, messages ■ Source code or syntax quoted directly from a program ■ File and directory names and their paths, names of variables and parameters, and names of installation, upgrade, and database tools
EXAMPLE	Technical names of system objects. These include report names, program names, transaction codes, database table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE
EXAMPLE	Keys on the keyboard

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 34
F +49/18 05/34 34 20
www.sap.com

This document was created using stylesheet 2007-12-10 (V7.2) / XSL-FO: V5.1 Gamma and XSLT processor SAXON 6.5.2 from Michael Kay (http://saxon.sf.net/), XSLT version 1.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.
Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace

You can find this document at the following address: http://service.sap.com/instguides

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 34
F +49/18 05/34 34 20
www.sap.com