SAP NetWeaver '04

Security Guide

Security Guide for SAP Mobile Infrastructure

Document Version 1.00 – April 29, 2004

SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

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 expressively 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 documentation at the following Internet address:
`service.sap.com/securityguide`

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, *F2* or *ENTER*.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help → General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Contents

Security Guide for SAP Mobile Infrastructure 5
1 Introduction 5
2 System Architecture 6
3 User Administration and Authentication 8
4 Authorizations 11
5 Network and Communications Security 12
5.1 Security of the Communications Channels 12
5.2 Network Security 13
5.3 Communication Destinations 13
6 Data Security 14
7 Appendix 15

Security Guide for SAP Mobile Infrastructure

1 Introduction

This guide does not replace the daily operations handbook that we recommend customers to create for their specific productive operations.

About this Guide

The *SAP Mobile Infrastructure* (*SAP MI*) is based on the *SAP Web Application Server* (*SAP Web AS*). You should therefore take the corresponding security information for *SAP Web AS* into consideration. This guide only describes the security information that differs from it as well as additional security information.

Related Security Guides

Application	Guide
SAP Web AS 6.40	SAP Web Application Server Security Guide

Why is Security Necessary?

A mobile device is much more vulnerable than a server. Whereas the server is in a separate room, the mobile device is used on the road. It is therefore relatively easy to access the file system of the mobile device physically. The operating systems of a number of mobile devices (especially PDAs) also provide neither sufficient protection against access nor authorization systems at file level. Its vulnerability is increased when a mobile device is used by multiple users.

The mobile device is threatened by for example the following potential dangers:

- Loss of the device
- Theft
- Unauthorized use by an unauthorized person
- Data manipulation in the file system

Target Groups

- Technical consultants
- System administrators

Important SAP Notes

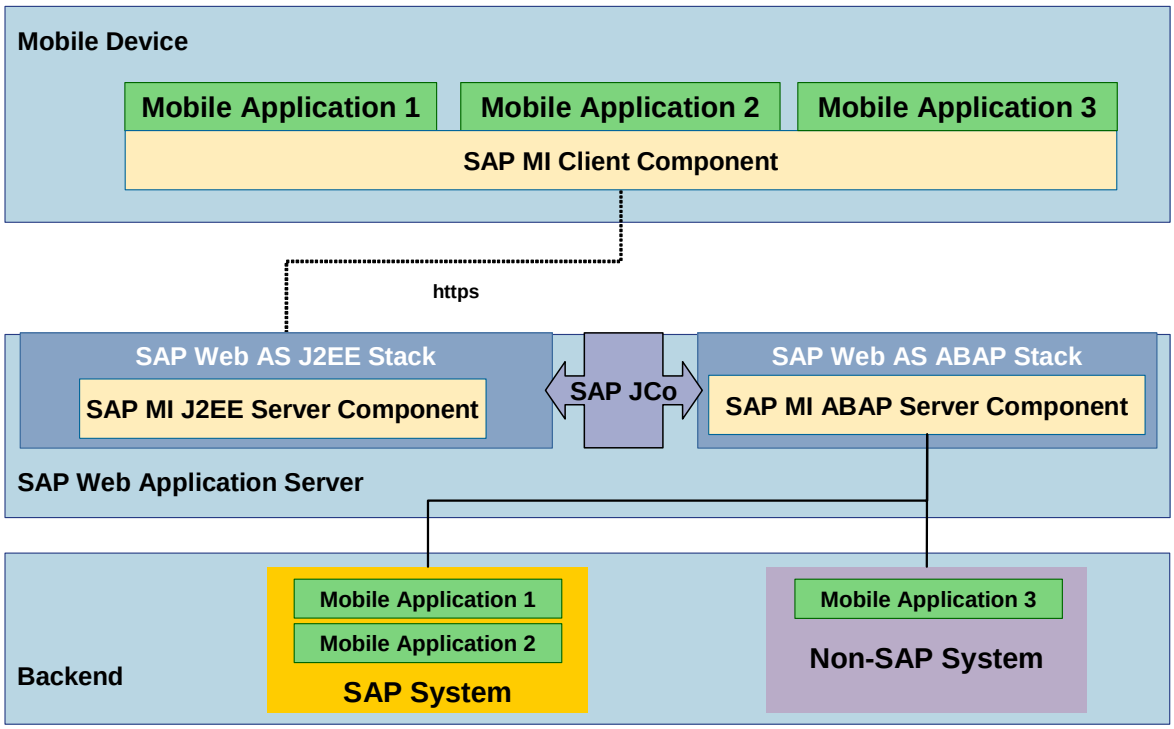
Check regularly which SAP Notes are available about the security of the application.

Important SAP Notes

SAP Note Number	Title
602993	Root Certificates in the Truststore of the SAP MI Client Component

2 System Architecture

The following graphic shows the system architecture of the *SAP MI*:



The *SAP MI* contains the following technical components:

SAP MI Client Component

The SAP MI Client Component provides a mobile application with the following services:

- UI programming models

  The standard programming model for mobile applications is *Java Server Pages (JSP)*. Alternatively, you can also use the Abstract Window Toolkit (AWT) as a pure Java programming model. The SAP ME 1.0 programming model *microITS* is still supported.

- Framework services

  The framework services are provided to the mobile applications as Java APIs. The most important APIs are used for

  - Data synchronization
  - Data persistence
  - Reading and writing replicated data
  - Logging and tracing
  - Configuration of applications and framework

SAP MI Server Component

The SAP MI Server Component contains the following components:

- **SAP MI J2EE Server Component**

  The SAP MI J2EE Server Component is an integral component of the Java stack of the SAP Web AS and has the following tasks:

  - Pass the data containers from the SAP MI Client Component to the SAP MI ABAP Server Component
  - Provide an administration user interface for administration of mobile devices and components

- **SAP MI ABAP Server Component**

  The SAP MI ABAP Server Component is an integral component of the ABAP stack of the *SAP Web AS*.

  The SAP MI ABAP Server Component is responsible for:

  - Queuing and acknowledgement of synchronized data containers
  - Calling the application logic

  The application logic can be called synchronously or asynchronously, depending on the application.

  - Data replication

  Data replication defines data packages for individual mobile devices (data allocation), computes the data to be newly replicated on the device (delta comparison), finds and solves conflicts between the mobile device and the server application (conflict management) and provides a number of monitoring tools.

  - Deployment of the mobile applications to the mobile devices

  Mobile applications are automatically deployed to a mobile device when the mobile device is synchronized. This process is controlled centrally by the SAP MI Web Console. It permits the system administrator to assign application versions based on users or roles and thus gives an overview of the mobile devices, error logs and so on, in the field.

- **SAP Mobile Development Kit (SAP MDK)**

  The SAP Mobile Development Kit (MDK) offers the developer useful documentation and tools for developing mobile applications based on *SAP MI*. The MDK is part of the *SAP NetWeaver Developer Studio*.

Backend

The backend of a mobile application consists of customizing and repository objects. Both types of objects are transported using the standard mechanisms of the SAP Change & Transport System.

3 User Administration and Authentication

The SAP MI Server Component uses the SAP user administration of the *SAP Web Application Server*. *SAP Mobile Infrastructure*, however, does not support single sign-on.

The SAP MI Client Component uses its own user administration. User administration is primarily used to administer the user and local password. The local password is used for local user authentication. It is stored in coded form on the mobile device, and not in plain text. A second password, called the synchronization password, is used for synchronization with the SAP MI Server Component. The technical difference between the local password and the synchronization password allows you to scale security, see the section on *Passwords*.

You can change the passwords on the client side at any time. The data, however, can only be synchronized successfully if there are equivalent values for the user ID and the synchronization password for the SAP MI Client Component on the SAP MI Server Component. Since changing the synchronization password in the SAP MI Client Component does not automatically change it in the SAP MI Server Component, you must manually adjust these two passwords.

You can replicate user data as follows:

- With Report *WAF_DEPLOYMENT_FROM_ROLES* (Activation with User Group *MESYNC*)

  Use this report to keep the user data in the SAP MI Server Component synchronous with that of the backend system.

- Manually

  On the mobile device, the end user must manually keep the user data synchronous with that on the server. The user of the SAP MI Client Component must be the same as that of the SAP MI Server Component.

- With central SAP user administration

  If you are using central user administration, you can use it to keep the user data in the SAP MI Server Component synchronous with that in the backend systems.

Tools for User Administration

- User maintenance (Transaction *SU01*)
- User maintenance mass changes (Transaction *SU10*)
- Profile generator (Transaction *PFCG*), see Profile Generator [SAP Library]
- User groups (Transaction *SUGR*)
- Central SAP user administration
- Report *WAF_DEPLOYMENT_FROM_ROLES*

User

There are the following types of users:

- Technical users
  - Batch users for replication
  - Batch users for role comparison
  - RFC users for connections to the backend systems (if you do not want to use the current logon user to connect to the backend system, see Communications Destinations [Page 13].
- Individual users (for logging onto the backend systems and for using the synchronization function)
  - Users in the backend systems
  - Users with synchronization authorization for each mobile end user in the SAP MI Server Component
  - Users on the mobile device corresponding to those on the server
  - Administrators for the SAP Mobile Infrastructure Web Console
  - Administrators for the Computing Center Management System (CCMS)

No users are delivered with the software.

System	User	Delivered?	Type	Default Password	Detailed Description
SAP MI Client Component	End user	No	Dialog	No	Installed by end users themselves
SAP MI Server Component	End user	No	Dialog	INIT if created with copy function	Installed by administrator of SAP MI Web Console
SAP MI Server Component	Administrators for the SAP MI Web Console	No	Dialog	No	Installed by superior user administrator
SAP MI Server Component	Administrator for CCMS	No	Dialog	No	Installed by superior user administrator
SAP MI Server Component	Administrator for Smart Synchronization	No	Dialog	No	Installed by superior user administrator
SAP MI Server Component	Batch user for batch tasks	No	System or dialog	No	Installed by superior user administrator
Backend	End user	No	Dialog	No	Installed by administrator of backend system

Passwords

When the administrator creates individual users for the SAP MI Server Component, the system generates a password for the initial logon. The end user then has to log onto the server once directly and change the password, see Changing the Initial Password [SAP Library].

The SAP MI Client Component supports the technical difference between the synchronization password and the local password. The local password is used for authentication on the SAP MI Client Component. The synchronization password is used for authentication on the SAP MI Server Component. The online authentication takes place at the beginning of the synchronization cycle. The user ID and the synchronization password are transferred to the server and verified there.

In configuration file *mobileengine.config* you can define how the synchronization password and the local password should be handled; see Predefining and Setting Parameters for All Users [SAP Library]. Possible values for parameter *MobileEngine.Security.SynchronizationPasswordHandlingOption* are:

- **`atSync`** – Synchronization password does not correspond to the local password and must be entered for each synchronization (default value).
- **`local`** – Synchronization password corresponds to the local password and need not be entered at synchronization.
- **`once`** – Synchronization password does not correspond to the local password and must be entered once for each logon.

The synchronization option *Timed Sync* is not possible in combination with the setting **`atSync`**. It is only possible with the setting **`once`** after the end user has entered the synchronization password once, e.g. from the user settings. With the setting **`local`**, the synchronization option *Timed Sync* can be used without restrictions.

The SAP MI Client Component does not store the synchronization password for the settings **`atSync`** and **`once`**. Instead, the user must enter it for each synchronization or once per logon, depending on the setting.

The end user must manually synchronize the user ID and synchronization password on the mobile device with the settings used on the server. If multiple users are using the same mobile device, they all need their own user IDs and must keep the ID and synchronization password synchronous with the settings used on the server.

The synchronization password should:

- Have at least three and at most eight characters
- Not use any simple short words
- Use special characters or numbers

The SAP MI Client Component distinguishes between uppercase and lowercase.

The local password should satisfy the same criteria as the synchronization password. There are no restrictions for the minimum and maximum lengths of the **`atSync`** and **`once`** settings.

For general information about passwords, see Security Measures Related to Password Rules [SAP Web AS Security Guide].

4 Authorizations

With Release *SAP MI* 2.5, access to data and applications on the SAP MI Client Component are controlled by user-specific data filtering based on the SAP authorization concept. To set up user-specific data filtering, use the profile generator. For more information see Defining User-Specific Data Filtering [SAP Library].

No roles are shipped with the application. You must create the following roles in the SAP MI Server Component:

- Role for end users of the mobile application

  Technical role for all end users with which synchronization authorization is assigned for the SAP MI Server Component.

  With Release *SAP MI* 2.5 this role is also used to control user-specific data filtering.
- Role for administrators of the SAP MI Web Console
- Role for administrators of Computing Center Management

Once you have created the roles, you can edit them and assign them the following authorization objects:

- **S_ME_SYNC** (authorization to perform synchronization)
- **S_RFC** (RFC authorizations for all function groups contained in Table *BWAFMAPP*)
- For the administrator of the SAP MI Web Console **S_TCODE** (authorization to use the SAP MI Web Console), see Authorizations for the SAP MI Web Console [SAP Library].

Further authorizations could be necessary for the applications. For more information, see the documentation for the applications.

For more information see Role Editing for Mobile Applications [SAP Library].

5 Network and Communications Security

5.1 Security of the Communications Channels

The following communications channels are used in the system landscape of the *SAP Mobile Infrastructure*:

- From the SAP MI Client Component to the SAP MI J2EE Server Component and vice versa (A)
- From the SAP MI J2EE Server Component to the SAP MI ABAP Server Component and vice versa (B)
- From the SAP MI ABAP Server Component to the backend system and vice versa (C)

These technologies are used for communications:

- For (A): Hypertext Transfer Protocol (HTTP), Secure Sockets Layer (SSL) or Secure Hypertext Transmission Protocol (HTTPS)

  You must explicitly configure the use of HTTPS for both the SAP MI Client Component and the SAP MI J2EE Server Component. You can download the corresponding cryptographic libraries, which are subject to export restrictions, from the *SAP Service Marketplace*.
- For (B): SAP Java Connector (SAP JCo)
- For (C): Remote Function Call (RFC)

The following data is exchanged between the components:

- Application data (A,B,C)
- Control data of the *SAP Mobile Infrastructure* (A,B)

This data requires special protection:

- The synchronization password is copied from the mobile device to the SAP MI J2EE Server Component with each http request. We therefore urgently recommend that you use SSL or HTTPS.

  If JSP applications are running on the SAP MI Client Component, the SAP MI Client Component will contain a Web server with a configurable log function. `INFORMATION` or `DEBUG` may *not* be set as verbosity level for the Jasper log function, as otherwise the user password might be logged on the client side. The default setting is `FATAL`. You can check the configuration in file `<Installation directory of the SAP MI client component>\conf\server.xml` and adjust it if necessary.
- (B): The synchronization password is copied from the SAP MI J2EE Server Component to the SAP MI ABAP Server Component with SAP JCo. Secure Network Communications (SNC) should be used here.

5.2 Network Security

The *SAP Mobile Infrastructure* uses the Hypertext Transfer Protocol (HTTP) or Secure Hypertext Transmission Protocol (HTTPS) for communications between the mobile device and the server. Secure Sockets Layer (SSL) should be used for data transfer, see Secure Sockets Layer (SSL)-Setting Support [SAP Library].

The components only transfer data if the user of the device was identified by the SAP MI Server Component, that is if there is a valid user on the server. The user must also be authorized to synchronize data (*S_ME_SYNC*).

The *SAP Mobile Infrastructure* only transfers data using certain channels (wrapper functions, SyncBOs, synchronization between SAP MI Client Component and SAP MI Server Component) and does not have access to other data in the network.

For more information about network security, see the documentation about the *SAP Web AS 6.40* under SAP Web Application Server Security Guide [SAP NetWeaver Security Guide].

5.3 Communication Destinations

You must define the following communication destinations:

- URL for the synchronization in which the user logs on with the mobile device.
- URL for the installation of the SAP MI Client Component on the mobile device.
- RFC destinations for the connection to the backend systems.

RFC Destinations

Try to define the RFC destinations so that the same user as in the logon to the server is used.

However, this means that the backend system is only fully utilized for synchronous synchronization. For asynchronous synchronization, the system uses a batch user to log onto the backend system. The batch user needs authorization for all mobile applications in the backend system and for all wrapper functions and BAPI wrappers.

The wrapper functions for generic synchronization pass the data on to function modules in the backend system. The user information is lost if this call was asynchronous. You can increase the authorization protection by modifying the wrapper functions. The modification is based on the fact that information about the synchronizing user still exists in the wrapper information and cannot be changed by manipulations at the client. Using this information, you can simulate an additional authorization check and make the call of the backend function module dependent on it. There is usually a suggestion for the source code in the comments.

The communications user for the RFC connection used for the system logon needs at least authorization for the wrapper functions and BAPI wrappers.

6 Data Security

Data is stored on both the SAP MI Client Component and on the SAP MI ABAP Server Component. Data is stored on the server side in the *SAP Web AS*.

The SAP MI Client Component does not protect the stored data actively. Since the mobile device can be easily stolen or lost, you should place great emphasis on data security. The following measures increase the data security on your mobile device:

- On Win32 platforms, use encryption software to encrypt the entire directory structure in which the data for the SAP MI Client Component is stored, thus protecting it from unauthorized access. You must decrypt the data again before working with the *SAP MI*.

  Mobile devices such as PDAs currently do not strictly distinguish between main storage and file systems. Code fragments could therefore remain in main storage, endangering the entire encryption. In this case the use of encryption software therefore does not offer the same security as on Win32 platforms.
- Use antivirus software and update the virus databases at regular intervals.
- Only install software which you can trust. External software that you do not trust could manipulate the application data of the *SAP MI* without your noticing it.
- If available, use the password or PIN protection for operating systems.
- If you lose the device, have the administrator of the *SAP MI* immediately lock the user in the SAP MI Server Component to prevent unauthorized access to the system and then change the user's password.

A mobile device can be used be one or more users.

- If the device is used by one user, this user is responsible for the device and must make sure that nobody accesses the device without authorization.
- If more than one user is using the device, these users must share one another's trust. It is not possible to protect the data of one user from access by another user.

If the applications on the mobile device require data protection or non-repudiation (e. g. for time recording), the device should only be used by *one* user.

7 Appendix

Related Security Guides

For more information about the security of SAP applications, see the *SAP Service Marketplace* at `service.sap.com/security`. Security guides are available at `service.sap.com/securityguide`.

Related Information

For more information about topics related to security, see the links shown in the table below.

Links to Related Information

Content	**Quick Link on the *SAP Service Marketplace* (`service.sap.com`)**
Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides	`instguides` `ibc`
Related SAP Notes	`notes`
Released Platforms	`platforms`
Network Security	`network` `securityguide`
Technical Infrastructure	`ti`
SAP Solution Manager	`solutionmanager`