How to configure Single Sign-On support of SAP Mobile Infrastructure

Version 1.01 – February, 2008

Applicable Releases:
SAP NetWeaver 2004
SAP Mobile Infrastructure 2.5 SPS16 (or higher)
1 Business Scenario

Single Sign-On (SSO) is a mechanism that eliminates the need for users to enter passwords for every system that they log on to. The Single Sign-On allows users to authenticate themselves once, and then log on to all of those systems that operate in the Single Sign-On environment without further intervention.

In general, the alignment of different user ID/password based systems into a SSO environment simplifies the maintenance of authentication policies and its technical components. Accordingly, there is a business case that reveals the demand of improved usability and simpler maintainability related to password handling issues with respect to SAP Mobile Infrastructure.

Improved usability focuses directly to the end-users in the most common single user scenario 1 who are not forced anymore to handle with specific Mobile Infrastructure related user IDs and (logon/synchronization) passwords for authentication purposes at SAP Mobile Infrastructure client component and at SAP Mobile Infrastructure server component (during synchronizations). The original demand for SSO support with SAP Mobile Infrastructure fits exactly in this context: A company is using a SAP Enterprise Portal. The employees logon to the Portal with user ID/password. The company now decides to go mobile. Some employees are additionally confronted with SAP Mobile Infrastructure. However, this people should not be confronted with a second user ID/password combination particularly for their mobile business. Rather SSO integration is requested so that the employees can use their Portal logon for authentication purposes in the mobile scenario.

Besides this main business scenario there are also other scenarios feasible that are focusing additionally on the integration of the SAP Mobile Infrastructure user interfaces into SAP Enterprise Portal. The assumption here is that there is a permanent online connection to the portal server available, but not to the application backend system.

The following sections introduce the technical requirements and details and guide how to implement SAP Mobile Infrastructure in Single Sign-On environments in the view of specific example scenarios.

---

1 Single user scenario means that the SAP Mobile Infrastructure client component allows the registration (= creation) of at most one user.
2 Introduction

SAP Mobile Infrastructure supports a SAP Logon Ticket based approach to integrate mobile scenarios into Single Sign-On environments. Figure 1 shows the involved technical components\(^2\) of the environment:

- SAP Enterprise Portal as authentication component that issues SAP logon tickets for the mobile device
- SAP MI client component running on the mobile device
- SAP MI server component (= middleware) as integral part of the Web AS

---

**Single Sign-On @ SAP Mobile Infrastructure**

![Diagram of components](https://example.com/diagram.png)

*Figure 1 – Components of SAP Mobile Infrastructure Single Sign-On environment*

The Web AS the SAP Mobile Infrastructure server component is part of has to be configured to trust SAP logon tickets that are issued by the predetermined ticket issuing system. This How-to Guide focuses on a SAP Enterprise Portal as such a ticket issuing system\(^3\). Once the trusted systems relationship is established SSO works in the following way:

\(^2\) Note: The application backend system is not involved.

\(^3\) Technically, from the SAP Mobile Infrastructure point of view, any system that can issue SAP logon tickets could be used. However, all described integration steps in this document are related to SAP Enterprise Portal.
The user logs on at the Enterprise Portal server in order to get a SAP logon ticket for further actions on the mobile device\(^4\). The selected authentication scheme of the Enterprise Portal server determines the concrete steps to be performed, e.g. user ID/password entry (basic authentication) or X.509 certificates submission (client certificate based authentication). More details about these authentication options are given later in this section. After the authentication at the Enterprise Portal is successfully completed, a SAP logon ticket is issued for the corresponding user and sent back to the MI client packaged in a cookie. The MI client retrieves the ticket by reading out the cookie’s contents. The MI client can now pass the ticket to the MI server for authentication during synchronization. The evaluation of the ticket occurs only on the MI server. That’s why the Single Sign-On functionality is pure online functionality. It is only available and applicable if the SAP MI client component is online, i.e. physically connected with the SAP Enterprise Portal and SAP MI server component (Web AS).

However, it has to be distinguished whether the MI client is configured for single user scenarios or shared device scenarios, because the details of the SSO integration differ in both cases. Single user scenario means that the MI client allows the registration (= creation) of at most one user. Shared device scenario means that the registrations of multiple different users are allowed. These users can subsequently, but not concurrently work with the mobile device (and in particular with the MI client).

In single user scenarios the user shall no longer be bothered to provide a Mobile Infrastructure user ID and (logon/synchronization) password for authentication purposes at MI client and at MI server (implicitly during synchronizations).

In shared device scenarios providing user ID and (logon/synchronization) password is in fact the fallback mechanism if SSO is not available / applicable for any reason.

There are several further characteristics that have to be considered beside single user/shared device scenarios: Operating platforms, authentication schemes at ticket issuing system, configurations, prerequisites and limitations. The behavior of the SAP Mobile Infrastructure client component depends on these characteristics and the concrete Single Sign-On usage may vary with respect to end-user interaction as well as the technical requirements behind.

Table 1 displays a summary of all characteristics and shows what is supported with MI AWT client and MI JSP clients. The notions of the table are explained in detail afterwards. A table cell containing “X” means that a certain characteristic is supported on all platforms of the product availability matrix. A table cell containing “(X)” means that a certain characteristic is not supported on all platforms of the product availability matrix. Finally, a table cell containing “--” means that a certain characteristic is not supported at all for a certain MI client type.

\(^4\) Depending on the concrete implementation scenarios these steps are embedded into the SAP Mobile Infrastructure user interface flow.
<table>
<thead>
<tr>
<th>Characteristics</th>
<th>AWT client</th>
<th>JSP/microITS client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Sign-On technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SAP logon tickets</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Single user scenario</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Active SAP logon ticket request</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>• Simple SAP logon ticket reception</td>
<td>--</td>
<td>X</td>
</tr>
<tr>
<td>• User ID/password fallback</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Shared device scenario&lt;sup&gt;5&lt;/sup&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Active SAP logon ticket request</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>• Simple SAP logon ticket reception</td>
<td>--</td>
<td>(X)</td>
</tr>
<tr>
<td>• User ID/password fallback</td>
<td>--</td>
<td>(X)</td>
</tr>
<tr>
<td>Authentication @ SAP Enterprise Portal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• User ID / password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Form-based authentication</td>
<td>--</td>
<td>(X)&lt;sup&gt;6&lt;/sup&gt;</td>
</tr>
<tr>
<td>• Basic authentication</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>• X.509 certificates</td>
<td>--</td>
<td>(X)&lt;sup&gt;7&lt;/sup&gt;</td>
</tr>
<tr>
<td>Platform&lt;sup&gt;8&lt;/sup&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows XP / Windows XP Tablet PC</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Edition / Windows 2000 SP03 or later</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows Mobile 2003 (SE)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Optional feature configurations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SSO (de-) activation @ runtime</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>• Logoff hook @ ticket issuing system</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>• Synchronization via application UI</td>
<td>--</td>
<td>X</td>
</tr>
<tr>
<td>• Browser close @ MI exit</td>
<td>--</td>
<td>(X)</td>
</tr>
<tr>
<td>• Suppressing the web browser control</td>
<td>--</td>
<td>(X)</td>
</tr>
<tr>
<td>Prerequisites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Trusted systems</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>• Virtual domain</td>
<td>--</td>
<td>X</td>
</tr>
<tr>
<td>• Browser settings (Proxies, Cookies)</td>
<td>--</td>
<td>X</td>
</tr>
<tr>
<td>• Configuration Parameters</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 1 – Summary of Single Sign-On details

<sup>5</sup> Not supported on Windows Mobile platforms. Users have to be created / registered at SAP Mobile Infrastructure client component before SSO can be used in shared device scenarios.

<sup>6</sup> Not supported on Windows Mobile platforms. Not supported for systems that (have to) run only in browser’s top frame like SAP Enterprise Portal.

<sup>7</sup> External PKI is required. Not supported on Windows Mobile platforms.

<sup>8</sup> See product availability matrix (PAM) of SAP Mobile Infrastructure 2.5 on SAP Service Marketplace for all details (https://service.sap.com/nw-mi → MI in Detail → Product Availability Matrix).
2.1 Single User Scenarios

In the single user scenario the end-user is not confronted with a SAP Mobile Infrastructure user ID and (logon/synchronization) password at any time. In this scenario SAP logon tickets are used for two potential actions:

- Initial user authentication
- Synchronization

Initial user authentication
An initial user authentication using the SAP logon ticket takes place if the user is not yet registered at the MI client (due to new client installation).

If there is already a user registered\(^9\), the MI client does not require any authentication steps for offline working. The authentication mechanisms of the underlying operating system on the mobile device are assumed to be sufficient (there is at most one registered user).

If the user is not yet registered and a SAP logon ticket is available then the MI client opens a connection to the MI server and submits the ticket. If the logon at MI server using the SAP logon ticket is successful (= the SAP logon ticket evaluation was successful), the user ID the SAP logon ticket belongs to is transferred back to MI client. The MI client registers the user with the received user ID.

The involved systems and their interactions (including the user) are visualized in Figure 2; it shows the straightforward success case for JSP clients on Win32 platforms\(^{10}\) in active SAP logon ticket request scenario.

---

\(^9\) In particular, the MI client does not permit the creation of more than one user in single user scenarios.

\(^{10}\) The behavior, i.e. the visualized steps, on other platforms and the behavior of other client types differ slightly in detail, but not in general. Also the concrete steps performed at synchronization are similar.
If the initial user authentication fails for any reason an appropriate message is displayed. As consequence the end-user cannot work with the MI client. In this case the reason causing the failure has to be eliminated first.

**Synchronization**

The user has to provide authentication credentials each time when synchronizing with the MI server. If available, the SAP logon ticket is used for that purpose and transferred to the MI server. If the ticket is not available for any reason the synchronization will not be started and an appropriate message is displayed.

As described above the initial user authentication and the synchronization is based on the availability of a SAP logon ticket. There are two methods supported how the MI client can get such a ticket: Simple SAP logon ticket reception and active SAP logon ticket request.

**Simple SAP Logon Ticket Reception**

The MI client has nothing to do; it simply receives the SAP logon ticket from the browser. The intention of this scenario is the integration of the SAP Mobile Infrastructure user interface into a SAP Enterprise Portal environment. The MI client UI should be started in an own (newly opened) browser window by clicking an appropriate link that is already displayed in the browser within the UI of the SAP Enterprise Portal11 (e.g. from an iView or HTML-page). As precondition the MI client’s local web server must already be running.

---

11 The SAP Enterprise Portal has to be configured to send the SAP logon ticket to the browser before the user clicks on the corresponding link to start MI client UI displaying. I.e. the authentication steps at the portal have already to be occurred.
(e.g. started as operating system service) in a mode that suppresses the opening of the MI client’s own web browser control.

**Active SAP Logon Ticket Request**
The MI client always looks for the presence of a SAP logon ticket first. If no ticket is detected the MI client automatically\(^\text{12}\) requests a ticket via a configurable URL. Ticket requests with and without user interaction are supported. A ticket request can be triggered for the initial user authentication as well as for the synchronization.

### 2.2 Shared Device Scenarios

As prerequisite for this kind of scenario (opposite to single user scenarios) the users have already to be registered at MI client (initial user authentication is not supported). In shared device scenario SAP logon tickets are used for two potential actions:

- Online user authentication
- Synchronization

The focus of this scenario is placed on integration of the SAP Mobile Infrastructure user interface into a SAP Enterprise Portal environment. Therefore only simple SAP logon ticket reception is supported as method to get a SAP logon ticket in shared device scenarios.

**Online user authentication**
Initial user authentication (only supported in single user scenarios) means that the user has to authenticate himself against the MI server only once (to be registered and) to be authorized to work with MI client. Online user authentication means that the user has to authenticate himself each time he wants to logon to the MI client. The SAP logon ticket is used for this purpose in the same manner as for the initial user authentication. The (non-configurable) fallback in cases where the SAP logon ticket is not available is to provide the “normal” MI logon dialog via Mobile Infrastructure user ID/password. This means the MI client has not only to be online at synchronization time, but also at logon time. Here the business cases between shared device scenarios and single user scenarios differ.

**Synchronization**
If available, the SAP logon ticket is used for the authentication during synchronization and transferred to the MI server. If the ticket is not available and the synchronization password is not available, the user is prompted for the synchronization password.

### 2.3 Authentication at SAP Enterprise Portal

The Enterprise Portal supports different authentication schemes\(^\text{13}\). The decision tree in Figure 3 shows what authentication scheme shall be selected at the SAP Enterprise Portal to get a SAP logon ticket for MI client. The selection depends on the operating platform, the MI client type (JSP/AWT), the number of MI client users on the same device, the method how to retrieve the SAP logon ticket and the availability of a public key infrastructure.

---

\(^{12}\) This is the specified behavior in single user scenarios.

On Windows Mobile platforms only Basic Authentication is supported. The same holds for MI AWT clients independent of the platform.

![Flowchart](image)

**Figure 3 – Authentication @ SAP Enterprise Portal**

Theoretically a form-based authentication is also supported with limitation for active SAP logon ticket requesting with JSP clients on Win32 platforms. The limitation: Ticket issuing systems are excluded that (have to) run only in browser’s top frame like SAP Enterprise Portal. There is a technical reason: The MI JSP client creates an HTML frameset in the browser while requesting the SAP logon ticket. The SAP Enterprise Portal collapses this frameset because it requires running in the browser’s top frame. Therefore form-based authentication is not further considered in this document.

### 2.4 Platform

Single Sign-On integration is supported on Win32 operating platforms as well as on Windows Mobile platforms. The operating platform determines the concrete integration and configuration options.
2.5 Optional Feature Configurations

- **SSO (de-) activation @ runtime**
  The recommended Mobile Infrastructure setup of integration into a Single Sign-On environment is to do it from the scratch. This includes the new or re-installation of the MI client with the corresponding configuration on the mobile devices. However, there may be situations where from the scratch setups are not possible. Therefore SAP Mobile Infrastructure supports the activation (and deactivation) of the SSO support of the MI client via appropriate configuration deployments.
  Note: There may be additional configuration steps necessary on operating system or browser level.

- **Logoff hook @ ticket issuing system**
  If the MI client actively requests a SAP logon ticket from the Enterprise Portal, there are two facts that have to be mentioned: A portal session is implicitly created if the user logs on to get the SAP logon ticket (with JSP as well as with AWT client). When is this session closed again? Further, the SAP logon ticket remains as a non-persistence cookie at the browser or web browser control (with JSP client). When is this cookie removed again? The answer to both questions gives the logoff hook.
  Logoff functionality at the Enterprise Portal can be integrated by configuring an appropriate URL. The corresponding Mobile Infrastructure property is `MobileEngine.UM.SAPLogonTicketLogoffURL`. This URL is called immediately after the SAP logon ticket is received at MI client. The effect of URL call shall be the termination of the user session at the Enterprise Portal (that cannot be controlled by the MI client) and a removal of the SAP logon ticket cookie at the browser (that is controlled by the MI client). In general, a web service could be developed and used for these actions. However, there are also other possibilities. If the logoff URL property is configured the time available to perform this logoff depends on whether the MI JSP client or the MI AWT client is used. The mentioned actions have to be performed with the MI JSP client within the timeframe configured via `MobileEngine.UM.SAPLogonTicketRequestTimeout` property. However, the MI AWT client grants again the timeframe configured via `MobileEngine.UM.SAPLogonTicketRequestTimeout` to perform the logoff.
  In any case of failures an appropriate error message is displayed and the whole ticket request fails (independent on whether the SAP logon ticket was already received).
  If no such logoff functionality shall be performed the `MobileEngine.UM.SAPLogonTicketLogoffURL` property should be omitted. In this case the Enterprise Portal user session ends if a defined timeout (Enterprise Portal configuration parameter) is reached and cookie is removed if the browser window or web browser control is closed (e.g. by shutting down the MI client).

- **Synchronization via application UI**
  The MI JSP client supports active SAP logon ticket requesting not only if the synchronization is triggered via the MI client UI, but also if the synchronization is triggered via a JSP application own UI. The configuration property is the following one: `MobileEngine.UI.SAPLogonTicketApplicationSync`. The MI AWT client does...

14 It is not necessary that the cookie remains at the browser, because the MI client takes care on it.
not support this configuration option. However, the following requirements must be fulfilled for MI JSP clients:

- The following MI client configuration must be set:
  \[ \text{MobileEngine.UI.SAPLogonTicketApplicationSync} = \text{true} \]

- A synchronization has to be indicated by the presence of one of those name/value pairs in the query string of the request (sent to the local server of the MI client): \~\text{event}=\text{sync}* or \text{event}=\text{sync}* (The value sync* means prefix: sync, suffix is arbitrarily). Application developers have to take care on this.

- JSP applications that contain frames are responsible to restore the complete UI screens (e.g. all framesets) after active ticket requesting is finished at synchronization. Active ticket requesting will collapse any application frameset. Application developers have to take care on this.

- Active ticket requesting does not support references (anchors) in the synchronization URL. Example: \text{http://localhost:4444/application?\~\text{event}=\text{syncData}\#step1} is not supported (#step1 should be omitted). Application developers have to take care on this.

2.6 Prerequisites

- Trusted Systems
  Enablement of Single Sign-On between SAP Enterprise Portal and SAP Web AS is the general prerequisite of the SAP Mobile Infrastructure Single Sign-On integration. This holds for the MI AWT client as well as for the MI JSP client (see Figure 1).

- Virtual Domain
  Technically, a SAP logon ticket is sent as non-persistent cookie from the SAP Enterprise Portal to the end-user’s browser as response of an appropriate HTTP request. This cookie remains at the browser until an appropriate logoff-functionality is triggered for the SAP Enterprise Portal or all browser windows are closed.
However, a SAP logon ticket kept by the browser is not sufficient. It has to be transferred to the local web server (= Tomcat) of the MI JSP client. Due to general cookie specification this transfer is technically only possible if Tomcat runs (at least virtually) in the same domain or sub-domain of the SAP Enterprise Portal. The configuration of the mobile device and the MI client has to ensure this via the `MobileEngine.Runtime.Host` property (a full qualified domain name must be set as value). Figure 4 shows the involved components and the HTTP(S) boundaries.

Example:
- Full qualified domain name of SAP Enterprise Portal server: `pwdf1234.wdf.sap.corp`
- Potential `MobileEngine.Runtime.Host` configuration options:
  - `localhost.wdf.sap.corp`
  - `localhost.sap.corp`
  - `localhost.igb.sap.corp`
The option that is finally selected for a specific mobile device depends on the company’s network topology and the domain relaxing property of the SAP Enterprise Portal (ume.logon.security.relax_domain.level)\(^\text{15}\).

Furthermore, it has to be ensured that the selected property value \(\text{MobileEngine.Runtime.Host}\) is \textit{resolvable}\(^\text{1}\) to 127.0.0.1 to technically send the cookie containing the SAP logon ticket to local web server of the MI JSP client. For instance, this could be done by adjusting the \textit{hosts}-file (e.g. \texttt{<Win32 system dir>\drivers\etc\hosts}) or configuring an appropriate entry of the company’s DNS server.

- **Browser settings (Proxies, Cookies)**
  Integrating a MI JSP client into a Single Sign-On environment also often requires an investigation of the browser settings (i.e. Internet Options of the Microsoft Internet Explorer). The privacy settings influence the cookie handling. The local area network settings may influence the resolution of the property \(\text{MobileEngine.Runtime.Host}\), because this is potentially depending on certain (automatic) proxy scripts that are company-wide valid.

\[\text{15} \text{ Note: Changing the domain relaxing property may affect the company’s security policy.}\]
• **Configuration Parameters**
  The following properties are available to configure (*MobileEngine.config* file) the MI client with respect to a specific SSO integration\(^{16}\) scenario.
  - **Common connection properties**\(^{17}\):
    - `MobileEngine.Sync.Gateway.Host`
    - `MobileEngine.Sync.Gateway.Port`
    - `MobileEngine.Sync.Gateway.System`
    - `MobileEngine.Sync.Client`
    - `MobileEngine.Sync.Language`
  - **ABAP synchronization service specific properties**:
    - `MobileEngine.Sync.Gateway.Service`
    - `MI.Sync.ProtocolVersion`
  - **User Management properties**:
    - `MobileEngine.UM.SingleUserMode`
  - **Common\(^{18}\) SAP logon ticket support properties**:
    - `MobileEngine.UM.SAPLogonTicketSupport`
    - `MobileEngine.UM.SAPLogonTicketRequestURL`
    - `MobileEngine.UM.SAPLogonTicketRequestTimeout`
    - `MobileEngine.UM.SAPLogonTicketLogoutURL`
  - **MI JSP client specific SAP logon ticket support properties**:
    - `MobileEngine.Runtime.Host`
    - `MobileEngine.UM.SAPLogonTicketBackgroundRequest`
    - `MobileEngine.UM.SAPLogonTicketWaitingRefresh`
    - `MobileEngine.UI.CloseBrowserWindowSupport`
    - `MobileEngine.UI.SAPLogonTicketApplicationSync`
  - **MI AWT client specific SAP logon ticket support properties**:
    - `MobileEngine.UM.ExternalAuthUserParameter`
    - `MobileEngine.UM.ExternalAuthPasswordParameter`
    - `MobileEngine.UM.ExternalAuthAdditionalParameters`

See SAP Mobile Infrastructure Installation Guide or online help (http://help.sap.com/saphelp_nw04/helpdata/en/a8/64b54cf975904da6f0ef47298cf433/frameset.htm → SAP MI for Administrators → Administration using the MI Web Console → Configuration of Mobile Devices → Parameters in MobileEngine.config) for detailed explanations of the different parameters listed above.

---

\(^{16}\) Note: It depends on the scenario which properties are concretely required.

\(^{17}\) These properties are used for MI Sync Servlet as well as for MI ABAP Sync Service.

\(^{18}\) These properties are used for MI JSP clients as well as for MI AWT clients.
3 The Step By Step Solution

In this chapter the enablement of Single Sign-On @ SAP Enterprise Portal and Web AS is referred; followed by selected scenario descriptions. These scenarios should be regarded as examples. In real implementation projects adjustments of the described steps may be necessary to meet the customer’s network topology and other specific requirements. However, even in such a case the steps described in this section can and should be used as guidelines.

Scenario 1

In this scenario the following shall be realized:

- MI JSP client on a mobile device based on Windows XP (e.g. Laptop)
- Single user scenario with active SAP logon ticket request
- Basic Authentication shall be performed to get the SAP logon ticket from SAP Enterprise Portal
- Preconfiguration of the MI JSP client for initial rollout
- Usage of logoff-hook
- The ABAP Synchronization Service shall be used instead of the MI Sync Servlet.

Further basic conditions:

- If connected the mobile device is registered in the network domain wdf.sap.corp
- Default domain relaxation property shall be used
- The connection between the SAP MI client and SAP MI server is SSL secured as well as the connection between the SAP MI client and the SAP Enterprise Portal. Generally, this is recommended, but the decision in has finally be argued in the customer’s implementation project.

Scenario 2

In this scenario the following shall be realized:

- MI AWT client on a mobile device based on Windows Mobile 2003 SE
- Single user scenario with active SAP logon ticket request
- Basic Authentication shall be performed to get the SAP logon ticket from SAP Enterprise Portal
- Preconfiguration of the MI AWT client for initial rollout
- Usage of logoff-hook
- The ABAP Synchronization Service shall be used instead of the MI Sync Servlet.

Further basic conditions:


Note: SSL enablement of SAP MI client and SAP Enterprise Portal is out of scope of this document.
3.1 Enablement of Single Sign-On @ SAP Enterprise Portal and Web AS

1. The Enterprise Portal server and the MI server component (running on Web AS 6.40) have to be configured accordingly to support Single Sign-On (see Figure 1). The Portal Platform Security Guide provides a detailed description how to do that: https://service.sap.com/securityguide
3.2 Enablement of Scenario 1

Prepare the SAP Enterprise Portal to issue the SAP logon ticket on request of the SAP MI client component. A convenient way to do this is to locate a simple HTML-page in a folder of the SAP Enterprise Portal that is directly accessible via an appropriate URL (at least for the group of users who are working with SAP Mobile Infrastructure). In the following steps description this folder is created as a sub-folder of the public documents folder. The default authentication scheme of the SAP Enterprise Portal to access the HTML-page in this context is Basic Authentication. Hence, there are no efforts e.g. to change the authentication scheme, because it is already the desired one.

Preparation at SAP Enterprise Portal

2. Create a simple HTML document on your local machine.

3. Logon to the SAP Enterprise Portal and go to the public documents folder. You must have the required permissions to create sub-folders there and to upload the simple HTML document. In case of permission questions contact your portal administrator.
4. Create a sub-folder in the public documents folder and upload the simple HTML page from your local machine.
5. Take the URL to access this page. This is the Target URL for SAP Mobile Infrastructure to request the SAP logon ticket.

Note: If target URL is HTTP based, but you desire to requests SAP logon tickets via HTTPS, you can simply replace HTTP by HTTPS and the HTTP port by the HTTPS port in the target URL. Independent of HTTP and HTTPS you have to extend the hostname to the full qualified domain name if this is not yet the case. This is important for the correct cookie handling later on.
6. Test the URL with full qualified domain name in your browser and perform the Basic Authentication. The dummy page should be displayed.
Configuration of the MI Client properties

7. In our scenario the MI JSP client must be correctly preconfigured before it is deployed to the mobile devices. The Preconfiguration of SAP MI client section of the Installation Guide describes the steps to be performed. The Installation Guide is located on the SAP Service Marketplace.

8. Take the uncompressed setup according to the Installation Guide and modify the MobileEngine.config file as described in the next steps.

9. Open the MobileEngine.config file with a text editor.

10. Enter the appropriate values of the required parameters, save the MobileEngine.config file and prepare the setup for distribution according to the installation guide.

   The values lighted in blue are example values in the context of the described scenario 1 and have to be adjusted in an implementation project.

   MobileEngine.Sync.Gateway.Host=pwdf2798.wdf.sap.corp
   MobileEngine.Sync.Gateway.Port=44350
   MobileEngine.Sync.Gateway.System=MI4
   MobileEngine.Sync.Client=000
   MobileEngine.Sync.Language=EN
   MobileEngine.Sync.Gateway.Service=/sap/bc/MJC/mi_host
   MI.Sync.ProtocolVersion=251600
   MobileEngine.UM.SingleUserMode=true
   MobileEngine.UM.SAPLogonTicketSupport=true
MobileEngine.UM.SAPLogonTicketRequestTimeout=60
MobileEngine.Runtime.Host=localhost.wdf.sap.corp
MobileEngine.UM.SAPLogonTicketBackgroundRequest=true
MobileEngine.UM.SAPLogonTicketWaitingRefresh=3
Virtual domain requirement

11. Enter the value of the MobileEngine.Runtime.Host parameter into the hosts file of Windows, so that it can be resolved to 127.0.0.1.

12. Contact your network experts to ensure that the resolving of the MobileEngine.Runtime.Host parameter is not prevented by automatic proxy scripts.

13. Additionally, it can be discussed whether an appropriate DNS entry to resolve MobileEngine.Runtime.Host parameter to 127.0.0.1 is an option. This would make step 11 above obsolete.
Test your SSO Configuration

14. Install the pre-configured setup and start the SAP MI client.

Because there is no user yet registered, an initial user authentication is immediately performed.

Therefore the user has to log on with the SAP Enterprise Portal credentials.
15. If the user authentication was successful and all (pre-) configurations were made correctly, the MI homepage should be displayed.

If you synchronize now, the already available SAP logon ticket is used to get the Device ID.

A restart of the MI client would lead you directly to the MI homepage with local authentication. If you press the synchronize-button a ticket request is performed again before the synchronization starts.
3.3 Enablement of Scenario 2

Preparation at SAP Enterprise Portal
The same as described in scenario 1.

Configuration of the MI Client properties

1. Perform steps 7, 8 and 9 similar to scenario 1 with the difference that this time the *Preconfiguring on Windows Mobile Platform* section of the Installation Guide must be referred.

2. Enter the appropriate values of the required parameters, save the MobileEngine.config file and prepare the setup for distribution according to the installation guide.

   The values lighted in blue are example values in the context of the described scenario 2 and have to be adjusted in an implementation project.

   Note: It is mandatory to escape (via backslash) the equal sign in values in MobileEngine.config file, e.g. `login_submit=on`.

   ```
   MobileEngine.Sync.Gateway.Host=pwdf2798.wdf.sap.corp
   MobileEngine.Sync.Gateway.Port=50500
   MobileEngine.Sync.Gateway.System=MI4
   MobileEngine.Sync.Client=000
   MobileEngine.Sync.Language=EN
   MobileEngine.Sync.Gateway.Service= /sap/bc/MJC/mi_host
   MI.Sync.ProtocolVersion=251600
   MobileEngine.UM.SingleUserMode=true
   MobileEngine.UM.SAPLogonTicketSupport=true
   MobileEngine.UM.SAPLogonTicketRequestURL=http://pwdf3037.wdf.sap.corp:50000/irj/go/km/docs/documents/Public%20Documents/SAP%20Mobile%20Infrastructure/TicketRequest.html
   MobileEngine.UM.SAPLogonTicketRequestTimeout=30
   MobileEngine.UM.ExternalAuthUserParameter=j_user
   MobileEngine.UM.ExternalAuthPasswordParameter=j_password
   MobileEngine.UM.ExternalAuthAdditionalParameters=login_submit=on
   ```
Test your SSO Configuration

3. Install the JVM and the pre-configured cab-file and start the SAP MI client.

Because there is no user yet registered, an initial user authentication is immediately performed.

Therefore the user has to log on with the SAP Enterprise Portal credentials.

4. If the user authentication was successful and all (pre-) configurations were made correctly, the MI homepage should be displayed.

Now you can check that no Device ID was yet received.

If you synchronize now, the already available SAP logon ticket is used to get the Device ID.

A restart of the MI client would lead you directly to the MI homepage with local authentication. If you press the synchronize-button a ticket request is performed again before the synchronization starts.
4 Appendix

4.1 Work URL Exceptions on Windows Mobile 2003 (SE)

For JSP clients running on Windows Mobile platform consider the following: The domain name of the Enterprise Portal server must be entered in the Network Settings of the mobile device.

Start → Settings → Tab: Connections → Connections → Tab: Advanced → Select Networks → Exceptions

Example: Portal server is running on pwdf2798.wdf.sap.corp

4.2 SSO by different MI installation users sharing a Windows 32 device (MI2.5 SP 19 and above/MI7.0 SPS 10 and above)

In Single Sign On scenario, when users share a Windows 32 device but each user has own MI installation, one user can launch the other’s MI Client as well as view, modify, and synchronize its data. To prevent one from accessing MI Client and data of the other user, following parameter should be set, provided that the MI Client user name is the same as the Windows system user name,

MobileEngine.UM.AuthenticateMIUserWithSystemUser

Possible values: true, false
Default: false

If this parameter is set to a value, true, MI Client will authenticate MI user with the Windows system user in addition to normal authentication process. The MI Client can be launched only if the Windows System user name is same as MI Client user name. This parameter should be used only in Single Sign On scenario.
4.3 Anonymous Logon on MI AWT Client
(MI2.5 SP 20 and above/MI7.0 SPS 12 and above)

Even if the SAP Logon Ticket issuing system is configured for Anonymous Logon in Single Sign On scenario, MI AWT Client users are prompted to enter their user credentials. To solve this problem, following parameter should be set then start/restart the MI Client.

**MobileEngine.UM.ExternalAuthRequired**

Possible values: true, false  
Default: true

If this parameter is set to a value, false, the users are required to provide their portal credentials.  
This parameter should be used only in Single Sign On scenario.

4.4 References

The links in this section lead to further information about topics around Single Sign-On integration. In particular further details about SAP Logon Tickets in general are explained as well as information about central user administration that may be helpful considering that several systems are involved.

- General information about SAP Logon Tickets that is SAP Mobile Infrastructure independent (e.g. security measures when using SAP Logon Tickets):  
http://help.sap.com/saphelp_nw04/helpdata/en/13/991a3a0792a622e10000000a114084/frameset.htm

- Central user administration information:  
  - E-book: Central User Administration with the SAP Web AS  
    http://service.sap.com/security → Education and Workshops