Administration Guide Groupware

SAP Enterprise Portal SP1

Copyright

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Typographic Conventions

Type Style	Description
Example text	Words or characters that appear on the screen. These include field names, screen titles, pushbuttons as well as menu names, paths and options.
	Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, titles of graphics and tables.
EXAMPLE TEXT	Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example, SELECT and INCLUDE.
Example text	Screen output. This includes file and directory names and their paths, messages, source code, names of variables and parameters as well as names of installation, upgrade and database tools.
EXAMPLE TEXT	Keys on the keyboard, for example, function keys (such as F2) or the ENTER key.
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. Pointed brackets indicate that you replace these words and characters with appropriate entries.

Contents

Groupware

Purpose

The sections below contain background, installation, administration, and configuration information on Groupware for SAP Enterprise Portal 6.0.

Once you have carried out the relevant steps explained in this documentation, you will be able to launch the groupware functions from various places within your portal.

The iViews *Appointments, Availability,* and *My Appointments* combine to form the calendar. The calendar is only available in a collaboration room created using the *Calendar* template. *My* Appointments can also be assigned to a page outside of a room environment, as can *Send E-Mail.* These iViews can be found under *Content Administration* → *Portal Content* → *Content Provided by SAP* → *Collaboration iViews.*

Groupware Framework

What is the Groupware Framework?

Various Java standards are emerging in the area of electronic mailing and scheduling. At the moment, the lack of an established standard necessitates the usage of vendor-specific tools or libraries for integrating a particular groupware application. For example, Microsoft Collaborative Data Object is required in order to connect to the Microsoft Exchange server, while Lotus Domino toolkit is required in order to connect to the Lotus Domino server.

The Groupware framework provides an abstraction of the groupware APIs across different vendors, thereby bringing in a standard for integration with SAP Enterprise Portal.

Architecture

The Groupware framework provides an abstraction of different groupware applications and provides the necessary APIs for integration with SAP Enterprise Portal. Different groupware applications such as Microsoft Exchange Server or Lotus Domino Server can be integrated by implementing a set of APIs called the transports.

The figure below depicts the Groupware architecture.
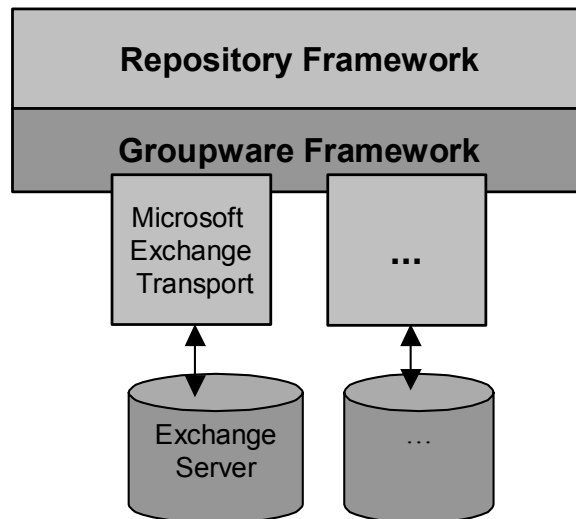
Transports

Connectivity to the groupware system is implemented and configured as a transport. The transport implements the necessary API for data extraction and submission to the groupware system by using the vendor-specific libraries.

> SAP ships Microsoft Exchange transport out-of-the-box. You need to develop and deploy new transports in order to integrate other groupware applications such as Novell Groupwise.

Systems

The credentials for the transports are maintained using systems. For more information, see *Creating a System.*

Features

The Groupware framework allows the quick development and deployment of reliable, secure, scalable, and manageable transports. It is written entirely in Java programming language, which allows portability and multi-platform support.

Functions

The Groupware framework supports the functions listed below. However, the functions actually available depend on the transport deployed and its capabilities. For more information, see the *Features* section of the appropriate transport documentation.

E-mail

- Sending e-mails using SMTP servers
- Saving sent e-mails on groupware servers that support IMAP
- Sending e-mails in HTML format
- Sending e-mails with attachments

Scheduling

- Creating non-recurring appointments
- Sending non-recurring meeting requests
- Reading appointments
- Modifying appointments
- Deleting appointments
- Modifying/deleting current instances of recurring appointments
- Sending meeting requests with attachments
- Scheduling online meetings

Creating a System

Use

A system allows you to maintain the credentials for a transport.

Procedure

To create a system, proceed as follows:

Starting from the top-level navigation bar, navigate to *System Administrator* → *System Configuration* → *System* → *Portal Content* → *Content Provided By SAP.*

Choose *Collaboration* → *New From Portal Archive* → *System.*

Select *com.sap.netweaver.col.appl.gw* and then choose *Next*.

Select a server (for example, *Microsoft_Exchange_Server*) and then choose *Next*.

Enter the system name and ID (for example, `Exchange` or `Lotus`), and then choose *Next* and then *Finish*.

Call up *System Aliases* for this system using the *Edit* dropdown box in the top right-hand side of the iView, and create a new alias according to the system you are using (Exchange or Lotus).

Installing and Configuring E-Mail Connectivity

Purpose

This documentation contains technical information on e-mail connectivity.

E-Mail Integration in SAP Enterprise Portal 6.0

The sending of e-mails is integrated into SAP Enterprise Portal 6.0 using the SAP J2EE Javamail implementation. This implementation can send e-mails using any SMTP protocol supported groupware server.

> You use the native Web clients delivered by the groupware vendor to read e-mails and other tasks.

Implementing the Transport

Purpose

The table below contains all prerequisites for implementing the transport for e-mail connectivity.

Transport Checklist

Number	Prerequisite	Comments
1.	You have configured the SMTP server appropriately.	If you want to allow users to send e-mails outside the company domain using the portal, this server must be configured to relay e-mails outside the domain.
2.	The groupware server supports IMAP protocol.	**Optional.** Messages sent from the portal can be stored on the groupware server only if the server supports IMAP protocol. If the groupware server does not support IMAP protocol, users cannot save copies of their messages in the *sent messages* folder.
3.	All users have valid e-mail addresses in the portal LDAP.	Every portal user must have a valid e-mail address. E-mail messages cannot be sent for users without an e-mail address.

Configuration Steps

The following sections contain information on configuring e-mail connectivity:

- *Creating an E-Mail Transport*
- *Configuring the E-Mailing Service*

Creating an E-Mail Transport

Purpose

The e-mail transport defines the SMTP server and other configurations required for sending e-mails.

Process Flow

You carry out Groupware configuration steps in the configuration iView.

To configure an e-mail transport, choose *Collaboration Administration* → *Collaboration Content* → *Configure Groupware Transport* → *Mail Transport* from the top-level navigation bar. Create a new instance of the transport by choosing *New* and update the instance created with appropriate values as described in the table below.

Attribute	Description	Comments
Name	Instance name of the transport. You cannot edit this attribute. It is automatically filled when a new instance is created.	`Javamail Transport`
SMTP server	Address of the SMTP server for sending e-mails.	`mysmtp.sap.corp`
System alias name	Alias that you defined for the groupware server in the system configuration. For more information, see *Creating a System*.	`Exchange, Lotus`
Sent messages folder	**Optional** parameter. Specify the folder on the server where the sent e-mail is to be stored.	*Sent Items* on the Microsoft Exchange server or *Sent* on the Lotus Domino server. If this value is not specified, users are unable to save e-mails sent from the portal
Transport class name	You cannot edit this attribute. It is automatically filled when a new instance is created.	

When you have finished creating your entries, restart the SAP J2EE engine.

Configuring the E-Mailing Service

Purpose

The e-mailing service provides the activation mechanism for sending e-mails.

Prerequisites

You have already created an e-mail transport. For more information, see *Creating an E-Mail Transport.*

Process Flow

To configure the e-mailing service, choose *Collaboration Administration* → *Collaboration Content* → *Configure Groupware Mailing Service* → *Mailing Service* from the configuration iView. You then edit the default instance created and update the attributes appropriately as described in the table below.

Attribute	Value	Description
Name	E-mailing service	Name of the service
Active	Checked	Specifies if the service is active

Now save your entries and restart the SAP J2EE engine.

E-Mail Connectivity Troubleshooting

The table below contains error messages and appropriate action.

Error number	Solution
GW-MAIL-001	Internal use
GW-MAIL-002	Retry the operation as indicated in the message
GW-MAIL-003	Internal use
GW-MAIL-004	The e-mail address specified could not be parsed. Check whether the e-mail address entered is in a valid format.
GW-MAIL-005	Internal use
GW-MAIL-006	The SMTP server was not specified when you created the e-mail transport. Update the SMTP server attribute in the configuration.
GW-MAIL-007	Internal use
GW-MAIL-008	The *Sent* e-mails folder attribute was not specified when you created the e-mail transport. This folder is required if the sent e-mails are to be stored on the e-mail server. The mail server must support IMAP protocol
GW-MAIL-009	Internal use
GW-MAIL-010	Either the SMTP server specified does not support the SMTP protocol or the e-mail server specified for saving the sent e-mails does not support IMAP protocol. Check and update the relevant attribute with the appropriate value.
GW-MAIL-011	This is an error response from your SMTP server. It indicates that your e-mail server is not configured to allow you to send e-mails using it. Check the configuration and setup of your SMTP server.
GW-MAIL-012	The user credentials specified for the e-mail server indicated by the system alias are not correct for the logged-on user. Specify the correct user credentials for the e-mail server. For more information, see *Mapping Your User* in the *SAP Enterprise Portal User Guide*.
GW-MAIL-013	The current user does not have an e-mail address specified in the LDAP configured for the portal. Update the LDAP with the e-mail address for the user.
GW-MAIL-014	An e-mail can be sent only if the *To* or the *Cc* field contains a valid e-mail address. Enter the name or e-mail address of the recipient in the *To* or *Cc* field.
GW-MAIL-015	Internal use
GW-MAIL-016	Internal use
GW-MAIL-017	Internal use

GW-MAIL-018	The e-mail server user credentials specified for the e-mail server indicated by the system alias are not correct for the logged-on user. Specify the correct e-mail server using user mapping. For more information, see *Mapping Your User* in the *SAP Enterprise Portal User Guide*.

Always restart the SAP J2EE engine after making configuration changes.

Installing and Configuring Calendar Connectivity

Purpose

The Groupware framework provides an abstraction for the Calendar APIs of different vendors. Depending on the groupware system used in your organization, you have to configure the appropriate transport in order to integrate scheduling functionality in your portal.

Implementation Considerations

For more information, see *Installing and Configuring Microsoft Exchange Connectivity* and *Integrating Lotus Domino Using iNotes*.

Integration

SAP provides out-of-the-box integration for Microsoft Exchange and Lotus Notes.

Features

- Configuring multiple calendar repositories
- Merging scheduling information from multiple repositories for display

Installing and Configuring Microsoft Exchange Connectivity

Purpose

This documentation contains technical information on Microsoft Exchange connectivity.

Microsoft Exchange Server Integration in EP6.0

The Microsoft Exchange server (subsequently called the Exchange server) is integrated using the Microsoft Exchange server transport. This transport supports the integration of the scheduling and tasks capabilities of Exchange Server 5.5 SP4 and Exchange Server 2000 with SAP Enterprise Portal 6.0

The transport uses Microsoft Collaborative Data Objects 1.2.1 (subsequently called CDO) to access data from the Exchange server.

Features

Microsoft Exchange connectivity provides the following features:

Scheduling

- Creating non-recurring appointments
- Sending non-recurring meeting requests
- Reading appointments
- Modifying appointments
- Deleting appointments
- Modifying or deleting current instances of recurring appointments
- Sending attachments
- Scheduling online meetings

Constraints

- The exchange transport currently only supports items with the type 'appointment', and 'meeting request'. Other types, such as 'discussion', are not currently supported.
- Deleting or updating an instance of a recurring appointment affects only that particular instance.
- Calendar items in personal folders are not supported. Users can only view and modify items located on the Exchange server from the iViews.
- Public folders on the Exchange server are not supported.
- Calendar items are delivered as such if sent to recipients within the intranet. If the recipient is in a different domain than the sender, the format in which the items are delivered depends on the server responsible for sending the items in question.
- Users cannot access calendar information from multiple logins of the same user in the portal.

- Attachments are stored temporarily in the folder in which the MSX-A component is installed. Attachments are deleted as soon as the read, save, or send action is performed.

Microsoft Exchange Connectivity Architecture

Microsoft provides CDO for connecting to the Exchange server in order to post or retrieve information. However, CDO does not provide a user/password-based logon mechanism on Win32 platforms, and needs an NT user impersonation to gain access to the Exchange server.

The NT user impersonation is achieved using the *basic authentication* feature of Microsoft Internet Information Server (IIS).

Transport

The overall transport consists of the following two parts:

- Java part that runs on the portal server (MSX-J)

- Active Server Page and SapExchangeConnector.dll running on an IIS server with CDO and in the same domain as the Exchange server or in a trusting domain. The ASP and DLL are collectively called MSX-A.

Architecture and Deployment Requirements

The figure below illustrates architecture and deployment requirements.
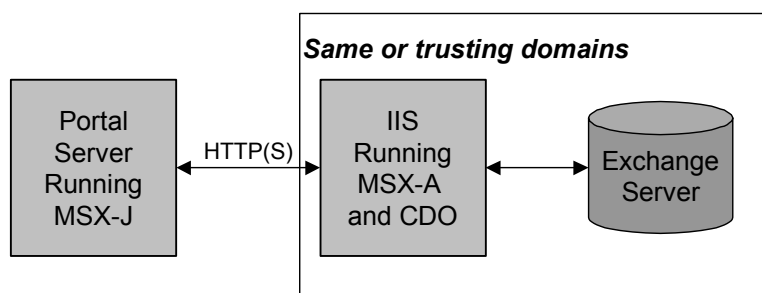
Process Flow

1. The MSX-J component makes an HTTP(S) request to the IIS. It passes user credentials using basic authentication.

2. The MSX-A component connects to the Exchange server and retrieves the relevant data.

3. The data is returned to the Java component as an XML stream.

Multiple Domain Considerations

Since the IIS uses *basic authentication* to impersonate the user, it necessitates that the IIS and the Exchange server reside in the same domain or in domains that have a trusting relationship established.

There are the following possible scenarios for this:

- **The portal server and the Exchange server are in the same domain or in trusting domains**

You do not need a separate box for the IIS in this scenario. You can install the IIS in the same box as the portal server.
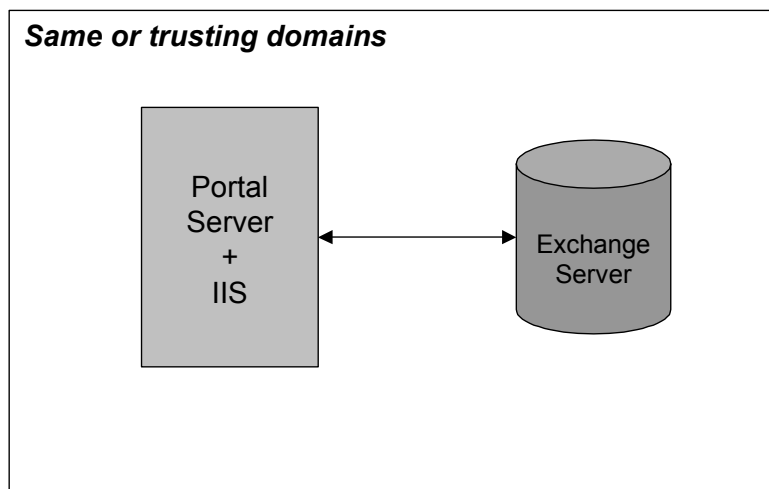
- **The portal server and the Exchange server are in different, non-trusting domains**

You need a separate box for the IIS in this scenario. You have to install the IIS in the same domain as the Exchange server.

```
┌─────────────────────────────────────────────────────────────────┐
│  Same or trusting domains                                         │
│                                                                   │
│  ┌──────────────┐            ┌──────────────┐      ╔══════════╗   │
│  │  Portal      │            │    IIS       │      ║          ║   │
│  │  Server      │  HTTP(S)   │  Running     │      ║ Exchange ║   │
│  │  Running     │ ───────►   │   MSX-A      │ ◄──► ║ Server   ║   │
│  │  MSX-J       │            │  and CDO     │      ║          ║   │
│  │  component   │            │              │      ╚══════════╝   │
│  └──────────────┘            └──────────────┘                     │
│                                                                   │
└─────────────────────────────────────────────────────────────────┘
```
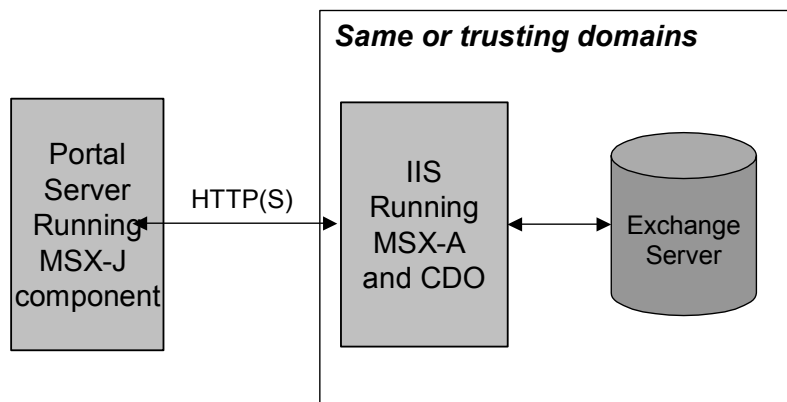
- **There are multiple exchange servers in different geographical regions or in
  different trusting or non-trusting domains**

If you have a system landscape with multiple servers in different geographical locations such
as Germany, India, USA and so on, or if you have multiple servers in non-trusting domains
irrespective of the geographical locations, you need at least one IIS for each domain or
geographical location. The portal server can be located in any domain or geographical
location.

The figure below illustrates the landscape.

```
┌─────────────────────┐   ┌──────────────────────────────┐
│ Server in USA       │   │ Same or trusting domains in  │
│                     │   │ Germany                      │
│  ┌──────────────┐   │   │  ┌──────────┐    ╔══════════╗│
│  │  Portal      │   │   │  │   IIS    │    ║          ║│
│  │  Server      │   │   │  │ Running  │    ║ Exchange ║│
│  │  Running     │◄──┼HTTP(S)│MSX-A and│◄──►║ Server   ║│
│  │  MSX-J       │   │   │  │  CDO     │    ║          ║│
│  │  component   │   │   │  └──────────┘    ╚══════════╝│
│  └──────────────┘   │   └──────────────────────────────┘
└─────────────────────┘
          │ HTTP(S)
          ▼
┌──────────────────────────────────────┐
│ Same or trusting domains in India    │
│                                      │
│  ┌──────────────┐    ╔══════════╗    │
│  │    IIS       │    ║          ║    │
│  │  Running     │    ║ Exchange ║    │
│  │  MSX-A and   │◄──►║ Server   ║    │
│  │  CDO         │    ║          ║    │
│  └──────────────┘    ╚══════════╝    │
└──────────────────────────────────────┘
```
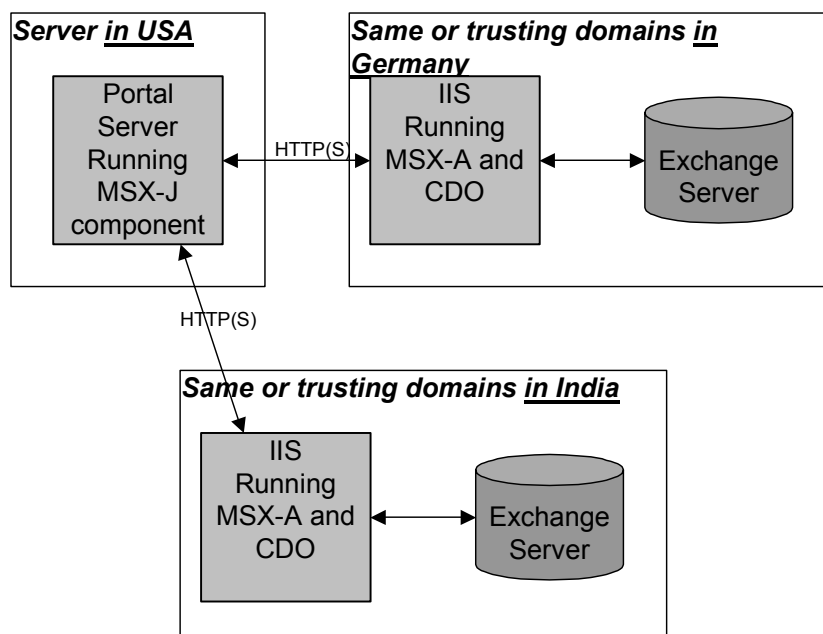
- **Exchange server with Outlook Web Access 5.5 SP4 (OWA)**

If you are running OWA for Exchange Server 5.5 SP4, you do not need an additional server for the IIS. You can install the MSX-A component on the OWA server and configure the portal server accordingly.
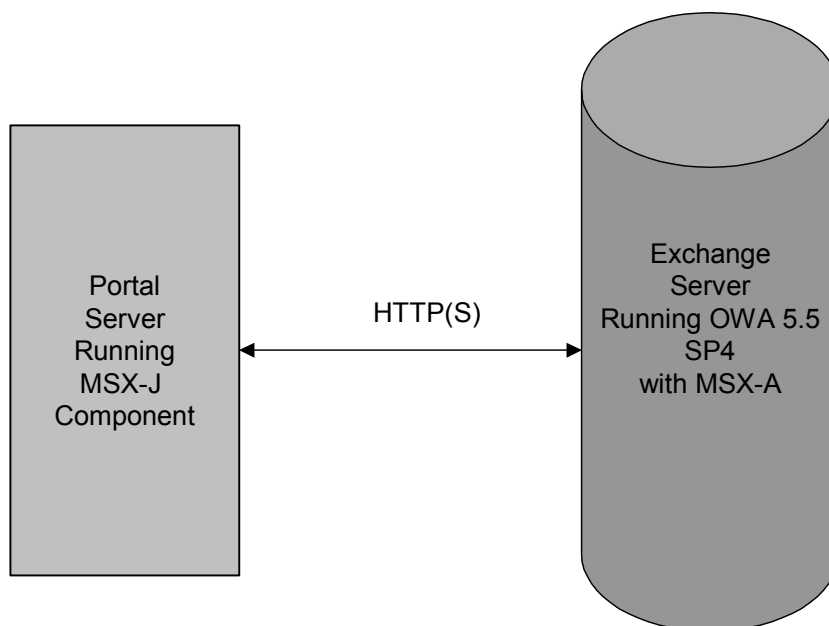
Implementing the Transport

Purpose

The table below contains all prerequisites for implementing the transport for Microsoft Exchange connectivity.

You need to have fulfilled all of the prerequisites listed in the table. If you have not done so, refer to the information in the *Comments* column and proceed accordingly.

Transport Checklist

Number	Prerequisite	Comments
1	You have installed and configured Microsoft Collaborative Data Objects 1.2.1. CDO is installed with Microsoft Outlook or the Exchange server with Active Server components.	For more information on installing and configuring CDO. See **http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cdo/html/_olemsg_overview_of_cdo.asp?frame=true**
2	If you are using CDO installed with Outlook, Outlook is the default e-mail client.	To check this, start Outlook using a command prompt with the parameter /checkclient, for example, C:\Program Files\Microsoft Office\Office\Outlook.exe /checkclient. You can also check whether Outlook is the default e-mail client by checking the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail.
3	If you are using CDO installed with Outlook, Outlook is configured to access Corporate/Workgroup.	To check this, start Outlook and choose *Tools* → *Options*. On the *Mail Services* tab, choose *Reconfigure Mail Support* and follow the instructions that appear.
4	If you need all portal users to access the exchange server using the portal, all users have *Logon Locally* permissions on the server on which the MSX-A component is running.	This is necessary due to the IIS *basic authentication* requirement. For more information, launch the following URL on an IIS: **http://localhost:80/iishelp/iis/htm/core/iiauths.htm#enablebasic**
5	You have specified a directory in which temporary .mmp files are to be created.	Using CDO to access information from the Exchange server creates temporary .mmp files. For more information, see Note **498521**.

6	If the MSX-A component is installed on the portal server, the Exchange server and the portal server are in the same domain or in trusting domains.	
7	You have configured the SAP J2EE engine with the appropriate proxy settings for accessing your IIS.	For more information, see the documentation on installing and configuring SAP J2EE.
8	You are running IIS 5.0 or above.	
9	If the MSX-A component is installed on the portal server, the Web site or virtual directory is different than the one hosting the portal.	For more information, see Note **491129**.
10	If the machine hosting the MSX-A component is a domain controller, *basic authentication* is set and all users have *Logon Locally* permissions.	For more information, see **http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ comsrv2k/htm/cs_mmc_authentication_nzyi.asp.**

It is not currently possible to use the German version of the CDO and Outlook.

Installation Steps

Use

This section gives an overview of the steps that you carry out in order to set up the Exchange server transport for Microsoft Exchange connectivity.

Installing the MSX-A Components

Use

The sections below describe the steps that you have to carry out in order to set up the MSX-A components for the Exchange server transport. You have to carry out these steps for every IIS that accesses the Exchange server or the Outlook Web Access 5.5 SP4 server in the system landscape.

For more information on multiple IIS and domain considerations, see *Microsoft Exchange Connectivity Architecture.*

Procedure

1. Locate the MSX-A components shipped with the Exchange transport. The components can be found at <irj>\root\portalapps\com.sap.netweaver.coll.appl.gw\external\exchange.

2. Locate an IIS that is in the same domain as the Exchange server or in a trusting domain.

3. Create a folder on the IIS, for example, c:\SAPExchangeTransport.

4. Copy the MSX-A components to the folder you just created.

5. Register the DLL by using the command `regsrvr32` in the command prompt, for example, `c:\winnt\system32\regsvr32.exe c:\SAPExchangeTransport\ SapExchangeConnector.dll.`

6. Create a new IIS Web site (see *Creating and Configuring an IIS Web Site*) or if you are using Outlook Web Access 5.5 SP4, create a virtual directory (see *Configuring Microsoft Outlook Web Access 5.5 SP4*).

Creating and Configuring an IIS Web Site

Procedure

1. Open the Internet Service Manager.

2. Create a new Web site with the name *SAPExchange* and make a note of the port on which this site is running.

3. Set the permissions to *Execute*.

4. Select the directory you just created as the home directory, for example, `c:\SAPExchangeTransport.`

5. Open the properties dialog box for the new Web site, and choose the *Directory security* tab.

6. Deselect all *Authentication* modes.

7. Select *Basic Authentication*.

8. Confirm with *OK*.

Result

Now see *Testing the MSX-A Setup*.

Configuring Microsoft Outlook Web Access 5.5 SP4

Use

Configure the system so that Groupware can access calendar information from the Outlook Web Access server.

Procedure

1. Open the Internet Service Manager and locate the OWA Web site.

2. Create a new virtual directory with the name *SAPExchange* beneath this Web site.

3. Set the permissions to *Execute*.

4. Select the directory you just created as the home directory, for example, `c:\SAPExchangeTransport.`

5. Open the properties dialog box for the new Web site, and choose the *Directory security* tab.

6. Deselect all *Authentication* modes.

7. Select *Basic Authentication*.

8. Confirm with *OK.*

Result

Now see *Testing the MSX-A Setup*.

Testing the MSX-A Setup

Use

The domain considerations already mentioned increase the complexity of testing the connectivity setup. Since most of these issues arise in the setup and configuration of the MSX-A component, a separate test application is shipped with the connectivity. This test application allows you to check that the setup is correct.

Procedure

1. Carry out the steps below to check that the setup is correct.

3. Locate `SAPPXchText.exe.` This is shipped with the Exchange transport. The components can be found at <irj>\root\portalapps\com.sap.netweaver.coll.appl.gw\external\exchange.

4. Copy the executable file to the machine to which the MSX-A component has been deployed.

5. Test the CDO version.

   i. Launch the executable file on the machine on which MSX-A was deployed.

   ii. Choose *Test → CDO Version.*

   iii. You should receive a success message. If you receive an error message, follow the instructions given.

6. Test data retrieval.

   iv. Launch the executable file on the machine on which MSX-A was deployed.

   v. Choose *Test → Data Retrieval*.

   vi. Fill in the necessary fields. Mandatory fields are indicated by a red asterisk (*). Click on the question mark (?) next to each field for more information.

   vii. You should receive a success message. If you receive an error message, follow the instructions given.

   For quick access to Microsoft Knowledge Base and SAP Support, choose *Tools → Quick Links.*

Configuration Steps

The following sections contain information on configuring Microsoft Exchange connectivity:

- *Creating an Exchange Transport*
- *Configuring the Calendar Repository Manager*

Creating an Exchange Transport

Purpose

You create an Exchange transport so that data can be retrieved from the Microsoft Exchange server*.*

Process Flow

You carry out Groupware configuration steps in the configuration iView.

To configure an Exchange transport, choose *Collaboration Administration* → *Collaboration Content* → *Configure Groupware Transport* → *Exchange Transport* from the top-level navigation bar. Create a new instance of the transport by choosing *New,* and then update the instance created with appropriate values as described in the table below.

Attribute	Description	Example
Name	Instance name of the transport. It is automatically filled when a new instance is created.	`Exchange Transport`
System alias name	Alias that you defined for the Exchange server in the system configuration. For more information, see *Creating a System.*	`Exchange`
Default server	Default Exchange server to be used for this IIS.	`myexchange.sap.corp`
Domain	Domain in which the user account is located.	`SLIIT`
IIS server	IIS setup in the same or trusted domain as the default server, on which the MSX-A components are installed.	`myiis.sap.corp`

Exchange server	The name or name pattern of the Exchange server that is to be accessed by the IIS mentioned above.	If the IIS server accesses only one Exchange server, specify the name of that server. This may be the same as the default server. Select "=" as the pattern. For example, `myexchange.sap.corp` If the IIS accesses multiple Exchange servers, the Exchange servers must follow a naming convention. For example, `myexchange01.sap.corp, myexchange02.sap.corp, myexchange03.sap.corp.` In this case, specify `myexchange` as the Exchange server name and select the pattern "*" for the Pattern attribute
Pattern	Select the pattern that corresponds to the Exchange server entry specified above.	
Port	IIS port on which the MSX-A components are installed.	`1080`
Virtual path	Virtual path on the IIS under which the MSX-A components are installed.	`/calendar`
Protocol	Protocol for connecting to the IIS.	`HTTP` for use **without** SSL, `HTTPS` for use **with** SSL.
Transport class name	You cannot edit this attribute. It is automatically filled when a new instance is created.	

If you have a distributed Exchange server landscape, create an entry for each IIS server. When you have finished creating your entries, restart the SAP J2EE engine.

Configuring the Calendar Repository Manager

Purpose

The calendar repository manager provides the option of selecting the required groupware transports from a set of deployed transports.

Process Flow

To configure the calendar repository manager, choose *Collaboration Administration* → *Collaboration Content* → *Configure Groupware Calendar RM* → *Calendar Repository* from the configuration iView. You then edit the default instance created and update the attributes appropriately as described in the table below.

Attribute	Value	Description
Description	`Calendar Repository Manager`	Repository manager description
Prefix	`/calendar`	Repository prefix
Default transport	`Select Exchange`	Specifies that the Exchange transport is the default transport
Transports	`Select Exchange server`	

Now save your entries and restart the SAP J2EE engine.

Microsoft Exchange Connectivity Troubleshooting

The table below contains error messages and appropriate action.

Error number	Solution
GW-EXC-001	The configured IIS could not be reached. Check the following: • Can the IIS be reached from the portal server? • Is the SAP J2EE engine configured for proxy access and is the IIS listed under nonProxyHosts? Use the test application described in *Testing the MSX-A Setup* to check the configuration.
GW-EXC-002	An error occurred while retrieving the protocol information. Check the Exchange transports created.
GW-EXC-003	Either the IIS was not reached or the IIS did not recognize the user. Test the connection for the specified user using the test application described in *Testing the MSX-A Setup.*
GW-EXC-004	The protocol specified when you created an Exchange transport is incorrect. Check the specification and specify a protocol that IIS supports. Only HTTP and HTTPS protocols are supported. For more information, see *Creating an Exchange Transport*.
GW-EXC-005	Check and configure the transports described in *Creating an Exchange Transport*.
GW-EXC-006	Internal use
GW-EXC-007	The port to connect to the IIS was not specified when you created an Exchange transport. Check the port on which the virtual folder exists on the IIS and update the transport accordingly.
GW-EXC-008	The URL constructed from the information specified when you created an Exchange transport resulted in an error. Use the test application as described in *Testing the MSX-A Setup* to check the settings and update the configuration of the Exchange transport accordingly.

GW-EXC-009	The IIS or the Exchange server specified when you created an Exchange transport is either incorrect or cannot be reached.
	Use the test application as described in *Testing the MSX-A Setup* to check the settings and update the configuration of the Exchange transport accordingly.
GW-EXC-010	The user credentials specified in user mapping are not correct for the user currently logged on. Check and update the user credentials. The following are valid formats for usernames:
	1. `username`
	2. `domain\username`
	3. `domain\username\mailboxalias`
	`username` means WINNT username and `domain` means the domain in which the above username is recognized.
	`mailboxalias` means the alias of the mailbox on the Exchange server, if the alias is not the same as the username.
	For more information, see *User Mapping* in the *SAP Enterprise Portal User Guide*.
GW-EXC-011	Internal use
GW-EXC-012	Internal use
GW-EXC-013	The Groupware manager has not been initialized for this transport. Check for errors logged during the startup of the portal.
GW-EXC-014	The virtual path specified when you created an Exchange transport is not correct or the MSX-A components have not been deployed.
	Check if the MSX-A components have been deployed properly as described in *Installing the MSX-A Components*.
	Check the validity of virtual path using the test application as described in *Testing the MSX-A Setup* and update the configuration.
GW-EXC-015	The name of the IIS was not configured when you created an Exchange transport. Update the IIS name for the appropriate transport instance.
GW-EXC-016	Internal use

GW-EXC-017	Microsoft Collaboration Data Object threw an exception. Use the test application as described in *Testing the MSX-A Setup* to determine the CDO exception. Search on MSDN (http://msdn.microsoft.com) for known solutions and take the necessary action as recommended by Microsoft.
GW-EXC-018	The IIS service is not running on the server mentioned in the IIS attribute. Check the attribute and start the IIS service on the IIS.
GW-EXC-019	The e-mail address specified in the LDAP mapped for the portal is invalid or was not recognized by the Exchange server. Check and correct the e-mail address.
GW-EXC-020	The configuration for this transport was not initialized. Restart the SAP J2EE engine. Check for any error messages logged during startup and take any necessary action.

If availability information for newly created Exchange users is not available, make sure that the users have logged in using the Outlook client at least once. For more information, see point #5 under **http://support.microsoft.com/default.aspx?scid=kb;EN-US;q179639.**

Make sure that you restart the SAP J2EE engine after making any configuration changes.

Integrating MS Exchange Using Outlook Web Access

Purpose

The sections below explain how to integrate the Microsoft Exchange server in SAP Enterprise Portal 6.0 using native Microsoft clients.

Integration

Administrators can enable this access by

- Creating an iView to display contents using Microsoft Outlook Thick Client for Exchange 5.5 and Exchange 2000 (see *Displaying Contents Using Thick Client*)

- Creating an iView to display contents using Outlook Web Access for Exchange 5.5 and Exchange 2000 (see *Displaying Contents Using Outlook Web Access*)

Features

Integrating Microsoft Exchange allows users to access their Microsoft Outlook e-mail, task, and calendar information from the portal.

Displaying Contents Using Thick Client

Use

Microsoft Outloook Thick Client for Exchange 5.5 and Exchange 2000 allows users to display Microsoft Exchange data in an iView in SAP Enterprise Portal.

Integration

The Outlook Thick Client iView connects to the Exchange server using the Outlook installation on the desktop of the user and displays the user's e-mail. calendar, and task data. This allows users to view and reply to e-mails.

This iView uses only HTML and JavaScript.

Prerequisites

- Users have installed Microsoft Outlook 2000 on their desktop

- You have installed Microsoft Exchange 5.5 SP4 or Microsoft Exchange 2000

- There is a connection between the machine being used to access the portal and the relevant Exchange server

- The Active-X control has been installed and configured appropriately (see *Installing and Configuring the Active-X Control*)

> The ActiveX control precludes the need for users to log on to the Exchange server in order to view Outlook information. However, as this method uses the Outlook installation on the user's desktop for authentication and to retrieve information from the Exchange server, it only works on desktops where the user's Outlook profile is active.

Installing and Configuring the Active-X Control

Use

The steps below explain how to download the Active-X control and configure your system so that you can access Microsoft Outlook data using Thick Client.

Procedure

1. Create an HTML page for displaying Outlook data within a browser.
   You do this using a standard HTML editor such as Microsoft Frontpage.

2. Add the following code for the Active-X control:

```
<object ID="ViewCtl1" classid="CLSID:0006F063-0000-0000-C000-
000000000046"  codebase="../outlctlx.CAB#ver=9,0,3024"
width="100%" height="100%" id="Messages">
<param NAME="View" VALUE>
<param NAME="Folder" value="Inbox">
<param NAME="Namespace" VALUE="MAPI">
<param NAME="Restriction" VALUE=" = ''">
<param NAME="DeferUpdate" VALUE="0">
</object>
```

This HTML page is to display the contents of the inbox from the Outlook client.

3. Create controls for viewing the calendar and inbox. You do this using VB script.

```
<script language=vbscript>
    Sub ViewCalendar()
     ViewCtl1.Folder = "Calendar"
    End Sub

    Sub ViewInbox()
     ViewCtl1.Folder = "Inbox"
    End Sub
</script>
```

4. Add the controls to the HTML page for navigation. For the image files, create the icons using a picture editor or download icons from **http://dgl.microsoft.com/default.asp.**

```
<span class="MenuItem" id="spanMessages1" style="WIDTH: 97px;
HEIGHT: 22px" onclick="ViewCalendar()">
<img SRC="calendar.gif">Calendar</span>

<span class="MenuItem" id="spanMessages1" style="WIDTH: 97px;
HEIGHT: 22px" onclick="ViewInbox()">
```

```
<img SRC="inbox.gif">Inbox</span>
```

5. Create a folder on the server on which the Internet Information Service is running under Inetpub (for example, c:/Inetpub/wwwroot/Outlook) and add the HTML file and the images.

6. Download the Active-X control from **http://activex.microsoft.com/activex/controls/office/outlctlx.cab - ver=9,0,3203** and place it in the above folder.

7. Create a virtual directory under the default website (for example, Outlook_Portal) and point it to the folder containing the files.

8. Launch the HTML in your web browser. The Outlook control is loaded in the browser and displays the inbox for the profile configured on the machine.

> You can also add controls for viewing other Outlook folders such as Drafts, Public Folders, and Tasks.

Result

You can now create a Web-based iView using the URL for the HTML file as described in *Creating Web-based URL iViews* in the *SAP Enterprise Portal Administration Guide.*

Displaying Contents Using Outlook Web Access

Use

Users who find the restrictions of using Microsoft Thick Client unacceptable can use Outlook Web Access iViews to display Microsoft Outlook data in the portal.

Integration

For information on configuring Outlook Web Access, see *Configuring Outlook Web Access.* If using Microsoft Exchange 5.5, you have to make certain configuration changes in order for the logon procedure in the portal to function properly. These changes are not required for Exchange 2000.

Prerequisites

- You have installed Microsoft Exchange 5.5 SP4 or above with Outlook Web Access

- You have not yet customized Outlook Web Access.
  If you have customized Outlook Web Access, you need to map certain parts of this document to your setup. Consult your Outlook Web Access customization team for more information.

  > Since logging on to Outlook Web Access is independent of logging on to the portal, the normal restrictions associated with the timeout of the Outlook Web Access session apply. Once the user closes the portal session, either by logging out of the portal or by closing the browser, the Outlook Web Access session also expires.

Configuring Outlook Web Access 5.5

Use

Configure the system so that you can create an iView for the Outlook Web Access client.

Single sign-on is not possible with Outlook Web Access on Microsoft Exchange 5.5. This uses a logon.asp page for user identification before the user can log on to Web Access. The page with user information persistence is root.asp. This page redirects to logon.asp every time the user starts a new session.

This redirection process replaces the browser session and the user is logged out of the portal session.

If you are using Exchange 2000, this issue does not exist and the following changes are not required.

Procedure

1. Locate the file `<outlook-web-access-server-root>\WEBDATA\USA\LIB\session.inc`

2. Open this file and locate the method *CheckSession2*

3. Replace the following line of code

   `CheckSession2 = CheckSession3(bstrRedirectURL,"top",-1)`

   with new code so that that the FRAME gets replaced with logon.asp instead of the entire browser window

   CheckSession2 = CheckSession3(bstrRedirectURL,"**self**",-1)

   The contents of this section will change based on your customization. Contact your Outlook Web Access customization team for relevant information. Backup the file before saving the modifications.

Result

You can now create an iView for displaying Microsoft Exchange information using Outlook Web Access.

Creating an iView for Outlook Web Access

Purpose

Once you have configured Outlook Web Access, you have to create a corresponding iView.

Prerequisites

You have already configured Outlook Web Access (see *Configuring Outlook Web Access*).

Process Flow

You create a Web-based iView as described *Creating Web-based URL iViews* in the *SAP Enterprise Portal Administration Guide*.

Use the relevant URL format to do this:

- For Microsoft Exchange 5.5, *http://<server name>:<port>/exchange/root.asp*

This is important because the default page is **logon.asp**.

- For Microsoft Exchange 2000, *http://<server name>:<port>/exchange*

> If you have multiple Outlook Web Access servers, you need to create one iView for each Outlook Web Access server. Users can select the appropriate iView using the portal personalization.

Result

You can now add this iView to a page in your portal, and add the page to a workset and role. When users log on to the portal and go to the page where this iView is located, they are presented with the logon page for Outlook Web Access. The logon process is identical to that for the standard Outlook Web Access logon.

Installing and Configuring Lotus Domino Connectivity

Purpose

Application integration to Lotus Domino Server has not yet been made available. The following sections describe the integration of Lotus iNotes in Enterprise Portal 6.0.

Integrating Lotus Domino Using iNotes

Purpose

The sections below explain how to integrate Lotus Domino into SAP Enterprise Portal 6.0 using iNotes.

Integration

- You need to have configured Lotus Domino 5.0.8 or above for iNotes access. This document does **not** address the configuration required for iNotes. For more information on deployment and configuration, see *iNotes Web Access* on the *IBM iSeries Server.*

- WebMailRedirect
  Users have to specify the URL of their e-mail databases to access their e-mail files. This is quite inconvenient and difficult to remember for users especially if the design includes having a multi-level of subdirectories to divide users by department or organization unit.
  However, Domino WebMailRedirect provides an advanced front portal for redirecting users to their e-mail files. Domino URLs are often hard to manage or remember, and with this the administrator needs to point users to the root URL.

Web Mail Redirect v6.41 is available for download from
http://www-10.lotus.com/ldd/sandbox.nsf/ecc552f1ab6e46e4852568a90055c4cd/f4b19c0c3327df5385256a8f0063bdf4?OpenDocument&Highlight=0,redirect.
This tool is provided free of charge by IBM-Lotus.

For more information on configuring WebMailRedirect, see Chapter 4 of *iNotes Web Access* on the *IBM iSeries Server.*

For detailed installation information, see
https://quickplaceuk.lotus.com/QuickPlace/webmailredirect/Main.nsf/h_Toc/664b1ea875ff827480256a29005ac1d7/?OpenDocument.

Features

iNotes is the Web client for Lotus Domino as opposed to the Notes client. iNotes can be accessed using a Web browser and offers basic functions for accessing mail, calendar and task information.

For more information on iNotes, see the PDF under http://www-10.lotus.com/ldd/sandbox.nsf/ecc552f1ab6e46e4852568a90055c4cd/21f02fa3e9647d1a85256a72006a5a4e?OpenDocument&Highlight=0,iNotes.

Now see *Creating an iView for iNotes.*

Creating an iView for iNotes

Purpose

Once you have configured Lotus Domino 5.0.8 or above for iNotes, you need to create iViews to display the InBox, Calendar, Notebook, and ToDo folders in the portal. This integration is based on WebMailRedirect.

Prerequisites

You have configured Lotus Domino 5.0.8 or above for iNotes access.

Process Flow

The steps below describe the creation of a Calendar iView.

1. Download WebMailRedirect from http://www-10.lotus.com/ldd/sandbox.nsf/ecc552f1ab6e46e4852568a90055c4cd/f4b19c0c3327df5385256a8f0063bdf4?OpenDocument&Highlight=0,redirect.

2. Copy the database template found in the download to your Lotus Domino data directory, for example, `c:\lotus\domino\data`.

3. Rename the database template to `wmr_calendar.nsf`.

4. Open the `wmr_calendar.nsf` database for configuration.

5. Set the following values by selecting the appropriate screen in the configuration form.

Option	Value
Please select the Redirection type	Select `MailServer`
Please enter a valid domain for the mailserver	Enter a valid domain, for example, `sap.com`
Please enter the time in seconds before the user is redirected	Enter `0`
Enable Personal Profiles	Select `No`
Enable Global Profiles	Select `iNotes – Calendar Portal`

6. Modify the ACL settings as prompted by the tool by clicking the *Auto set ACL settings* button.

7. Choose *Save & Exit*.

8. The calendar can now be launched using the URL
http://<server_hostname>:<port>/wmr_calendar.nsf, for example,
http://lotusserver:1080/wmr_calendar.nsf.

9. Create a Web-based iView using the above URL as described in *Creating Web-based URL iViews* in the *SAP Enterprise Portal Administration Guide*.

To create iViews for the InBox, Notebook and ToDo folders, carry out the steps mentioned above in each case, selecting the appropriate value for *Enable Global Profiles* in the WebMailRedirect configuration. One instance of the WebMailRedirect database is required for each of the above configurations.

Accessing iNotes Data in the Portal

The iViews you created as described in *Creating an iView for iNotes* can be placed in any page in your portal and can be accessed by making the page part of a workset within a role. When users access the page on which one of these iViews has been placed, they are presented with a dialog box asking for their user ID and password.

Once this information has been provided, the iView redirects the URL to the .nsf file that contains the relevant user data. As long as the user remains in the portal session, the iNotes session is also valid, even if the user navigates away from this iView. However, once the user logs off from the portal session, the iNotes session is also terminated.

In the above scenario, the user has to log on to the iNotes session in addition to the portal login. However, it is possible to automatically access the Domino server using a SSO ticket.

For more information, see the sections under *Ticket Verifier for Lotus Domino.*

Ticket Verifier for Lotus Domino

Purpose

The sections below outline the Ticket Verifier solution for Lotus Domino. This solution enables single sign-on so that users no longer need to log on separately to the Lotus Domino server.

Ticket Verifier Architecture

This section describes the architecture of the Ticket Verifier for Lotus Domino connectivity.

Logical Components

The solution comprises the following logical components:

- SAP Enterprise Portal 5.0/6.0

- Lotus Domino Server R5/R6

- Ticket Verifier for Lotus Domino

- Security certificate(s) keystore

- The figure below depicts the architecture of this solution.
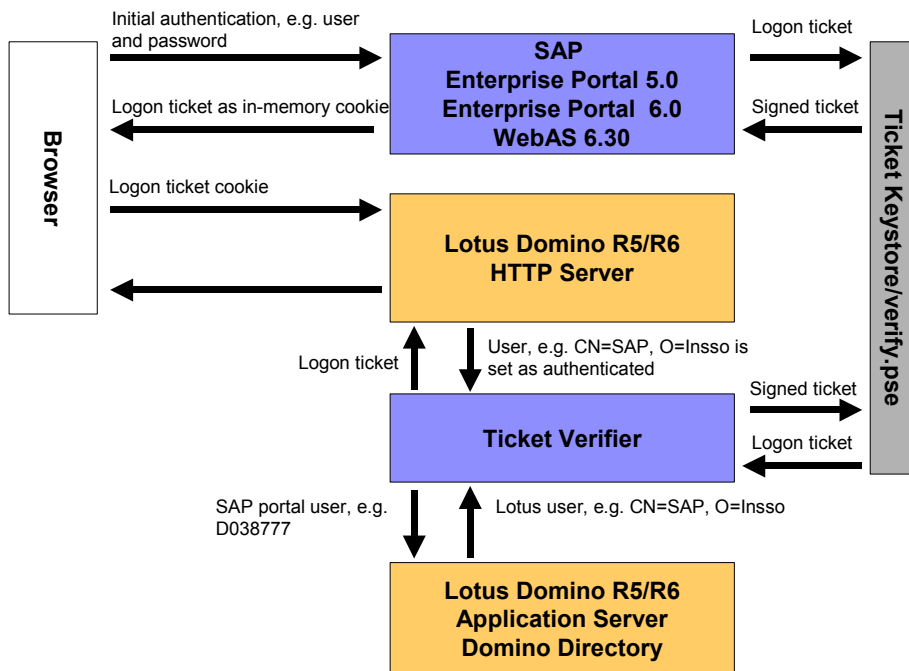
Single-sign-on information is carried in the SAP logon ticket that is stored as an encrypted cookie in the Web browser. SAP logon tickets can be described as pieces of information used for user authentication and single sign-on with SAP systems.

The logon ticket is issued to users when they log on to an SAP system that is configured to create tickets (for example, the SAP Web Application Server or Enterprise Portal).

The Ticket Verifier reads the cookie, obtains the SAP logon ticket, and performs a user look-up with the SAP user stored in the logon ticket in the Domino directory (public name and address book). Finally, the Ticket Verifier logs the SAP user on to Lotus Domino using the full canonical name. There is no need for a Lotus Domino password.

If there is **no** SAP logon ticket cookie in the HTTP request header, the Ticket Verifier passes the authentication request back to the Lotus Domino server and access to Lotus Domino resources remains unchanged. The Ticket Verifier is triggered only by the existence of an SAP logon ticket cookie in an HTTP request that requires authentication.

Ticket Verifier Process Flow

Purpose

This section depicts the process flow for the Ticket Verifier for Lotus Domino.

The function of the Ticket Verifier is to receive Lotus Domino Web server authentication requests and to handle these requests so that authentication at the Domino server is bypassed.

The Ticket Verifier replaces the Lotus Domino authentication mechanism to enable single sign-on for SAP Enterprise Portal users.

Process Flow

When sent an HTTP request for an access-protected Lotus Notes database or URL, the Ticket Verifier proceeds as follows:

1. Parses the HTTP request header
2. Extracts the SAP logon ticket cookie from the request header
3. Decrypts the cookie in question using SAP Enterprise Portal's `verify.pse` keystore
4. Verifies the validity of the SAP logon ticket (expiration and so on)
5. Retrieves the SAP username stored in the ticket
6. Performs a look-up in the Lotus Domino directory (`names.nsf`) for the SAP username
7. Logs on the matching domino user (if a match is found) using the full canonical name
8. Continues processing the requested URL

Involved Lotus Domino Applications

Typically, a Lotus Notes application is a Lotus Notes database that is stored and runs on a Lotus Domino server. However, a Lotus Notes application can also be comprised of several Lotus Notes databases . A Lotus Notes database carries the suffix `.nsf,` which stands for Notes Storage Facility.

A Lotus Notes database can be accessed using a Web browser if implemented and configured for Web access. This is typically the case for Lotus Notes R5 databases. In this case, you can use the Ticket Verifier for Lotus Domino to enable single sign-on for accessing any Lotus Notes database using the Web browser (HTTP).

Other Lotus Domino Products

Lotus ships other products based on the Lotus Domino server as well. These include:

- Lotus Sametime for instant messaging and application sharing

- Lotus Quickplace for self-serviced collaborative team rooms on the Web

- Lotus Discovery Server for knowledge management

- Lotus Domino Extended Search for searching and indexing various data sources

The Ticket Verifier for Lotus Domino supports Sametime 2.5 and Sametime 3.0.

Ticket Verifier Technical Components

The technical components of this solution consist of two parts:

- Runtime components (executed during operation)

- Security components (for information shared between SAP Enterprise Portal and Lotus Domino to safeguard security

Runtime Components

The runtime environment of the Ticket Verifier consists of a Microsoft Windows DLL. The table below contains the libraries that are required.

Library	Filename	Description
Ticket Verifier for Lotus Domino R5/R6	`ds_ticket.dll`	Implementation of the Ticket Verifier for Lotus Domino
SAP Seculib	`sapsecu.dll`	Functions for working with the `verify.pse` key store (public key infrastructure)
mySAP.com-SSO	`wpsso_v3.dll`	Implementation of `mySAP.com` logon ticket handling functions

> The server that runs the Ticket Verifier for Lotus Domino has to run all these libraries. The Ticket Verifier is registered on the Lotus Domino server and the other libraries are placed on the file system of the operating system.

Security Components

The security of the Ticket Verifier solution is based on a public key infrastructure (PKI) and a trust relationship.

The trust relationship between SAP Enterprise Portal and Lotus Domino is established by copying the SAP Enterprise Portal certificate(s) from the portal to Lotus Domino.

Security is achieved through digitally signing the credentials of the portal user.

The Ticket Verifier has to have access to SAP Enterprise portal's PKI certificate/keystore that is stored in a file called `verify.pse`. As mentioned before, the Ticket Verifier does not affect Lotus Domino ACLs and user privileges.

Lotus Domino Server Configurations

Lotus Domino Server can be installed in different server configurations. The usage of the Ticket Verifier in different configurations is described below.

Domino Server Clusters

A Lotus Domino server cluster is a Domino application server-based feature and does not affect the Domino HTTP Server configuration. Accessing a Lotus Domino server using HTTP triggers the Ticket Verifier. You can install the Ticket Verifier on any cluster node that runs the HTTP task.

Domino Internet Cluster Manager (ICM)

ICM allows you to use Domino clusters to provide fail-over and workload balancing to HTTP clients (Internet browsers) when they access Domino Web servers.

You can run the ICM on any server that uses the Domino Release 5 Enterprise Server license. You install and configure Domino clusters as normal, and then you configure the ICM. The ICM always uses its local copy of the Domino Directory. Therefore, the ICM must be in the same Domino DNS domain as the cluster.

The ICM acts as an intermediary between HTTP clients and the Domino Web servers in a cluster. When Domino Web servers run in a cluster, they generate URLs that direct HTTP client requests to the ICM. When the ICM receives a client request, it redirects the client to the most available server that contains a replica of the requested database.

This leads to the following scenarios:

- If the ICM is inside the cluster, the Ticket Verifier has to be installed on the ICM and on all cluster member nodes. This is because the ICM also serves HTTP requests.

- If the ICM is outside the cluster, Ticket Verifier has to be installed on all cluster member nodes, but not on the ICM. This is because the ICM only carries out the HTTP redirecting, and is not involved in the authentication and/or serving of HTTP requests.

Domino Server Web Single Sign-On Configuration

The Ticket Verifier does not affect a Domino Server Web SSO configuration, since the Ticket Verifier only handles authentication requests where an SAP logon ticket is sent using a cookie in the HTTP request. You can run the Ticket Verifier and a Domino Server Web SSO configuration on the same machine.

Lotus Domino Directory and Users

The Ticket Verifier performs single sign-on against the Lotus Domino Directory (previously known as the Public Name&Address book). The SAP logon ticket carries an SAP portal username. The Ticket Verifier performs a Domino directory look-up operation to retrieve the canonical name of the corresponding Lotus Domino user to log on. This leads to the following possible scenarios:

- Domino Directory usernames match portal usernames
  In the case of a single match of each portal username with a Lotus Domino user ID, the Ticket Verifier works for all users without any modification.

- Domino Directory usernames differ from portal usernames
  In this case username mapping is required on Domino side (name aliases). Since Lotus Domino is able to carry several different usernames (aliases) for a particular Lotus Domino user (for example, for the user Michael Sambeth it might carry "Michael Sambeth/dev/sap" as well as "MSambeth" and "Michael K. Sambeth"), all you have to do is to add the SAP username to the Lotus Domino Person Record. The SAP username is then changed to the corresponding Lotus Domino canonical name when the Domino Directory look-up operation takes place.

Lotus Domino Web Server API (DSAPI)

The Domino Web Server Application Programming Interface (DSAPI) is a C API that allows you to write your own extensions to the Domino Web Server. DSAPI extensions, or filters, are notified whenever a particular event occurs during the processing of a request.

There are currently two events for which a filter can be written, for user authentication in particular. The Ticket Verifier for Lotus Domino binds itself to the user authentication requests and serves to authenticate a user.

Implementing the Ticket Verifier

Purpose

The table below contains all prerequisites for implementing the Ticket Verifier.

You need to have fulfilled all of the prerequisites listed in the table. If you have not done so, refer to the information in the *Comments* column and proceed accordingly.

Checklist

Number	Prerequisite	Comments
1.	You are running Lotus Domino R5, Release 5.0.6a or higher or Lotus Domino R6	
2.	Lotus Domino is running on the Domino Application server or in Domino Enterprise server mode	Lotus ships its Domino server in three different types: • Domino Mail Server • Domino Application Server • Domino Enterprise Server The Ticket Verifier has been successfully tested on Domino Application Server and Domino Enterprise Server.
3.	The Domino server runs the HTTP task	The Ticket Verifier for Lotus Domino is a Web server DSAPI filter developed for the Lotus Domino HTTP server. It runs only with the Domino HTTP server.
4.	The SAP Enterprise Portal hostname and the Domino Web server hostname have to carry the same internet domain suffix	The Ticket Verifier solution is based on browser cookies. The cookie-handling is domain-dependent and the browser only attaches the corresponding cookies to an HTTP request for a particular domain.

Installing the Ticket Verifier

Purpose

To successfully run the Ticket Verifier for Lotus Domino R5, you have to perform the following steps on every Lotus Domino server to be accessed from the portal.

Process Flow

1. Locate the components in the table below and copy them to the respective recommended target directories on the Lotus Domino server.

File	Version	Description	Location	Recommended Target Directory
`ds_ticket.dll`	1.4.0.0	Implementation of the Ticket Verifier for Lotus Domino version 1.4	`<SAP_J2EE>\cluster\server\ services\servlet_jsp\work\ jspTemp\irj\root\portalapps\ com.sap.netweaver. coll.appl.gw\external\lotus`	Any directory, for example, `c:\winnt\ system32`
`sapsecu.dll`	5.4.24.0	Functions for working with the `verify.pse` keystore (public key infrastructure)	Download from SAPSERV using FTP. For more information, see SAP Note **442401**.	Any directory mentioned in the PATH environment variable, for example, `c:\winnt\ system32`
`wpsso_v3.dll`	6200.93.0.0	Implementation of `mySAP.com` logon ticket handling functions	Download from SAPSERV using FTP. For more information, see SAP Note **442401**.	Any directory mentioned in the PATH environment variable, for example, `c:\winnt\ system32`
`verify.pse`		PKI keystore	`<SAP_J2EE>\ume`	Any directory, for example, `c:\lotus\ domino\sap`.

2. Using the Lotus Administrator client, update the Domino server document, section *Internet Protocols - HTTP - DSAPI* with the path and file name of the `ds_ticket.dll` < file, for example, `c:\winnt\system32\ds_ticket.dll`. If there are already DSAPI filter(s) listed, press enter at the end of the list and add the Ticket Verifier in a new line.

3. Update the `notes.ini` file with the variable `MySapPsePath` with the SAP Enterprise Portal PKI keystore path and file name.
   `MySapPsePath= c:\lotus\domino\sap\verify.pse`
   If you do not set this `notes.ini` variable, the Ticket Verifier looks for the file `c:\lotus\domino\verify.pse` by default.
   You can check `notes.ini` variables by typing the "SHOW CONFIGURATION" command in the server console, for example, `show configuration MySapPsePath`.

4. Restart the Lotus Domino server for the settings to take effect.

The Ticket Verifier redirects to the standard Lotus Domino authentication mechanism (for example, basic authentication or session login form) in the following scenarios:

- If there are two or more matches of a portal username in the Domino Directory. In this case there will be a log message on the server console and in the server log file as well.

- If user mapping is not successful, for instance, if the portal username cannot be found in the Domino Directory.