Duet for Microsoft Office and SAP; SAP Installation Guide

Version 1.00

September 2006

Table of Contents

Introduction

Duet^{TM} for Microsoft$^{®}$ Office and SAP$^{®}$ allows your employees to easily access SAP business processes and enterprise information through Microsoft Office environments.

> **Note**: Make sure that you have installed the Duet Metadata Service, and the Request Handler Service from Microsoft®, before you begin to prepare the environments in which you deploy Duet components from SAP.
>
> Find documentation for installing the Duet Metadata Service, and the Request Handler Service from Microsoft in the installation package: *…\Microsoft\Documentation*, or at *https://connect.microsoft.com/default.aspx*

This guide provides information for deploying the Duet components delivered by SAP. It contains the following sections:

- Setting Up the Duet System Landscape

  This section provides a high level description of the system landscape for running Duet to help you plan your implementation.

  In addition, it provides an overview of the installation and configuration tasks that you must perform.

- Deploying Duet Components

  There are three main chapters that describe the procedures for deploying Duet components: Duet server, Duet Add-On, and Duet business applications.

- Configuring the Duet System Landscape

  This section describes the configuration tasks you need to carry out in each Duet environment before running Duet applications in Microsoft Office Outlook.

  In addition, you will find explanation for performing post installation tasks in each of the three environments.

- Troubleshooting

  This section provides explanation for solving the problems you may encounter during the installation and configuration of the Duet components.

Setting Up the Duet System Landscape

This section provides information for preparing the hosts for the Duet components from SAP, in three separate environments.

In addition, there is a high level description of the system landscape for running Duet to help you plan your implementation.

Note: We recommend that you set up the Duet landscape in two stages:

- A testing landscape in which you successfully deploy, test, and run Duet.
- A productive landscape in which you perform extended configurations before making Duet available for wide use in your organization.

Duet Technical System Landscape

The technical system landscape describes the three environments in which you deploy and run Duet components: Duet server, Duet Add-On and mySAP™ ERP system, Duet business applications.

The configuration of some Duet components is dependent on the availability of other Duet environments. For this reason, you must deploy and configure Duet environments in the following sequence:

1. Deploy and configure the Duet server environment.
2. Deploy and configure the Duet Add-On components in your existing mySAP ERP system landscape.
3. Install and configure the Duet business applications for client computers.

For detailed information about the Duet technical system landscape, see the *Duet for Microsoft Office and SAP; SAP Master Guide* in Service Marketplace at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

Summary of Installation Tasks and Configuration Activities

The following overview of the Duet system landscape summarizes the installation flow, and configuration activities you must carry out in the three different environments: Duet server, Duet Add-On and mySAP™ ERP system, Duet business applications.

Tasks	Activity
1. Deploying and configuring the Duet server components	
a. Pre-installation configuration of the host of the Duet server. For detailed information, see "*Pre-Installation Requirements of the Duet Server*" on page 11.	i. Install SAP NetWeaver '04 Web Application Server Java 6.40 SP17, or higher. ii. Set up the SAP User Management Engine (UME) to connect to the Microsoft Active Directory® directory service. iii.Configure the authentication mechanism for use in the Duet landscape. iv. Gather the information you will need to provide during installation. v. Configure the host for the installation program and copy the installation package to the local drive.
b. Deploying Duet server components For detailed information, see "*Deploying the Duet Server Components*" on page 16.	• Follow the instructions in the SAPinst installation tool.
c. Post installation configurations. For detailed information, see "*Post Installation Configurations*" on page 22.	i. Import Kerberos configuration files into the SAP Web AS Java system. ii. Configure the properties of the SAP Web AS Java system. iii. Configure Active Directory data source file in the SAP Web AS Java system. iv. Configure the login module stack in the SAP Web AS Java system. v. Configure the host of the Duet Server as the ticket issuing system.

Tasks	Activity
2. Deploying the Duet Add-On components	
a. Pre-installation configuration of the host of the Duet Add-On. For detailed information, see "*Pre-Installation Requirements of the Duet Server*" on page 31.	i. Set up the SAP User Management Engine (UME) to connect to your user storage: either mySAP ERP system user store, or Microsoft Active Directory service. ii. Obtain a system user ID in mySAP ERP system, and define that same user ID in the UME of the SAP Web AS Java system. iii. Gather information that you will need during the installation. iv. Verify that the host computers for both Duet server and Duet Add-On have the same date and time.
b. Deploying Duet Add-On components For detailed information, see "*Deploying the Duet Add-On Components*" on page 36.	• Follow the procedures provided in the SAPinst installation tool.
3. Installing and configuring the Duet Business Applications components	
a. Pre-installation configuration For detailed information, see "*Pre-Installation Requirements for the Duet Business Applications*" on page 38.	i. Create new folders using the names, *DuetMetadata*, and *DuetCode*. ii. Share the folders, and define permissions for the administrator user on the host of the Duet server. iii. Set security settings for the Request Handler service in the IIS on the host of the Duet Metadata Service.
b. Installing the Duet business applications For detailed information, see "*Installing the Duet Business Applications*" on page 40.	• Installing business applications

Tasks	Activity
4. Configure trust in the Duet system landscape	
For detailed information, see "*Installing the Duet Business Applications*" on page 38.	i. Configure trust between the Duet server environment and the Duet Add-On Environment. ii. Configure trust between the Duet Add-On environment and the mySAP ERP system Environment. iii. Configure trust between mySAP ERP system and the Duet Add-On Environment.
5. Configure the host of the Duet Add-On	
For detailed information, see "*Configuring the Duet Add-On Environment*" on page 43.	i. Set the size for messages in the SAP Web Application Server Java. ii. Map Duet business application roles to mySAP ERP roles. iii. Configure the Service Map. iv. Configure communication destinations for the Web services in the Duet environment. v. Configure RFC destinations. vi. Verify the security settings of the ESA services.
6. Configure the client for the Duet business applications	
For detailed information, see "*Configuring the Duet Business Applications Environment*" on page 56.	i. Configure client access to the resources for the business applications. ii. Manually publish the metadata for the business applications. iii. Configure the Authorization Manager (AzMan). iv. Configure client computer for Duet business applications. v. Create the distribution package for installation the Duet business applications.

Deploying the Duet Server

This section describes the deployment of the Duet server components.

> **Note**: Make sure that you have installed the Duet Metadata Service, and the Request Handler Service from Microsoft® in a separate host, before you begin to prepare the environments in which you deploy Duet components from SAP.
>
> Find documentation for installing the Duet Metadata Service, and the Request Handler Service from Microsoft in the installation package: *...\Microsoft\Documentation*, or at *https://connect.microsoft.com/default.aspx*

Pre-Installation Requirements of the Duet Server

Prior to setting up the Duet server, you must assess your existing system landscape. Doing so allows you to project what is needed to accommodate future expansions, as well the security requirements for the landscape.

Hardware and Software Requirements

The table below lists the requirements. The host computer must meet the following:

Requirement Type	**Requirement**
Hardware Requirements	• Disk Space: Minimum 2GB free space, (includes space required during install) • RAM: Minimum 1GB physical memory; 2-4GB recommended • Processor: Pentium 4, 3.2GHz 2MB cache, or higher recommended
Software Requirements	• Microsoft Windows Server™ 2003, SP1 or higher • SAP NetWeaver® '04 Web Application Server Java 6.40 SP17, or higher

You must prepare the host in which you intend to deploy the Duet server before you start the installation.

- Make sure that you have an administrator user with which you perform the pre-installation configurations in the local computer.

Preparation Workflow

The following is the sequence of the tasks in the preparation stage. You will find detailed explanation for carrying out each task in the sections after this list:

1. Install SAP NetWeaver '04 Web Application Server Java 6.40 SP17, or higher.
2. Set up the SAP User Management Engine (UME) to connect to the Microsoft Active Directory® directory service.
3. Configure the authentication mechanism for use in the Duet landscape.
4. Gather the information you will need to provide during installation.
5. Configure the host for the installation program and copy the installation package to the local drive.

   Note: You can delete the installation package from your local drive once you finish installing all the Java components for Duet.

The following sections describe the procedures for performing each of the tasks in the workflow for preparing the host of the Duet server.

Installing SAP NetWeaver '04 Web Application Server Java

You must install SAP NetWeaver '04 Web Application Server Java 6.40 SP17, or higher. It provides the SAP Web Application Server Java system (SAP Web AS Java system) on top of which the Duet server runs.

You can download SAP Web AS Java system from the SAP Software Distribution Center on the SAP Service Marketplace at: *service.sap.com/swdc*

In addition, download and install the latest patch release for SAP Web AS Java 6.40 SP17.

Find the installation guide for SAP Web AS Java system in SAP Service Marketplace at: *service.sap.com/instguides→ Installation & Upgrade Guides→ SAP NetWeaver→ Release 04*

Setting Up the SAP User Management Engine to Connect to the Active Directory

After installing the SAP Web AS Java system, you must configure the User Management Engine (UME) of SAP Web AS Java system to connect to the user storage in the Microsoft Active Directory service in the Duet landscape. By so doing, you enable UME to support the hierarchy of users and groups in the Active Directory service.

You configure the UME to use the Active Directory service from the Duet server host.

The UME provides you with a configuration file from the UME LDAP Configuration tool, with which you configure the UME to use the Active Directory service.

To configure the UME to use Active Directory:

1. Start the *Config Tool* using the file: *<SAPJ2EEEngine_installation>\j2ee\configtool\configtool.bat*
2. In the *Config Tool* window, choose *UME Directory Server → LDAP data*.
3. Select the configuration file *dataSourceConfiguration_ads_readonly_db.xml* (or the Active Directory service write file), from the list of available XML files.
4. Specify the following:
    - Name or IP address of the Active Directory service
    - Port number for the Active Directory service
    - User name and user password for logging onto the Active Directory service. The format is *DOMAIN\USER*. For example, *USAP_IN\guptau*
    - Paths to the users and groups data stored in the Active Directory service. We recommend that you test both the connection and authentication.
5. Choose *Apply Changes* in the toolbar.
6. Restart the SAP Web AS Java system.

For more information about configuring UME to support a directory service, go to the SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver '04s → SAP NetWeaver Library→ Administrator's Guide → Technical Operations Manual for SAP NetWeaver → General Administration Tasks → Security and User Administration → User Administration and Identity Management*

> **Note**: Where the user ID in the Windows account of a user, differs from the user ID in the user store used by mySAP ERP, you should map user data in the UME to enable users to access all systems.
>
> Do not perform user mapping where the user ID for users are the same in Windows and in mySAP ERP system. Passwords do not have to be the same.

For more information, see the section "*Configuring User Mapping Data in the User Management Engine*" in the *Duet for Microsoft Office and SAP; SAP Administration Guide* on Service Market Place at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

Configuring the Authentication Mechanism for Use in Duet

You enable authenticated users to access Duet data and SAP systems using their Windows account.

You must configure the Duet server to work with one of the following authentication mechanisms:

- Kerberos authentication using Simple and Protected GSSAPI Negotiation (SPNego) protocol.

  Note: Using Kerberos authentication is an alternative to using X.509 client certificates.

- X.509 client certificates

  Note: Using X.509 client certificates for authentication is an alternative to using Kerberos.

  For more information, go to the *Duet for Microsoft Office and SAP; SAP Administration Guide* on Service Market Place at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

The following section describes how to implement Kerberos authentication in the Duet, as this is the Integrated Windows Authentication for use in the Duet landscape.

Configuring Kerberos Authentication for Use in Duet

Duet supports the use of Simple and Protected GSSAPI Negotiation (SPNego) protocol and Kerberos authentication for use with Windows clients.

The protocol allows for a negotiation between client computers and the host of the Duet server regarding the authentication mechanism to use.

You must configure the Duet server to access a Kerberos Key Distribution Center.

Configuring Kerberos Key Distribution Center

The key distribution center (KDC) is a service that implements Kerberos authentication. It contains a copy of every encryption key associated with every principal.

For Kerberos authentication, the SAP Web AS Java system on which Duet server runs, is known to the KDC as a service by its Service Principal Name (SPN). Using the SPN, SAP Web AS Java system can initiate actions in the KDC.

Defining the Key Distribution Center

The following is the sequence of the tasks to carry out in the domain controller, to implement Kerberos authentication in Duet:

- Create a service user for the SAP Web AS Java system in which you intend to run Duet server.
- Create a keytab file.
- Register service principal names (SPN).

For more information, go to the SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 → English→ SAP Library → SAP NetWeaver → Security → User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms → Using Kerberos Authentication for Single Sign-On → Key Distribution Center Configuration*

> **Note**: Add an *SPN* for the physical host name, and each *DNS* alias of the reverse proxy or application level gateway, if you enable access to SAP Web AS Java through an application gateway.
>
> For example, in a cluster with a load balancer, where all the server nodes are accessible through a single URL such as: *http://loadbalancer.mycompany.com*, you must add a new SPN for *HTTP/loadbalancer.mycompany.com.* (You do so using the command, *setspn*.

Gathering Information for the Installation

Gather information about the required components. During installation, SAPinst will ask you for specific data about the following:

- SAP Web Application Server Java system (SAP Web AS Java system), which is part of the SAP NetWeaver '04 Web Application Server Java 6.40 SP17.
  - Host name
  - Administrator credentials
  - The HTTP/HTTPS port numbers
  - The URL address
  - Message Server port number
- Identify the intended host of the Duet Add-On and gather information about the SAP Web Application Server Java system (SAP J2EE) on it.
- Host name and port number of the load balancing mechanism in the system landscape, if available.

Configuring the Host Computer for the Installation Program

You deploy both Duet Server and Duet Add-On component using SAPinst, a proprietary SAP installation tool.

Requirements

- Hard disk space: a minimum of 50 MB. In addition, you need between 60-200 MB free space for the SAPinst executables

To prepare the host for SAPinst:

1. Install JDK version 1.4.2_06, or higher.
2. Define JAVA_HOME in the environment variable.
3. Include %JAVA_HOME%\bin in the system path of the environment variable.

Pre-installation Checklist

The following is a checklist to help you verify that you have performed all the required pre-installation configuration tasks:

Check (√)	Task
	Install SAP NetWeaver '04 Web Application Server Java 6.40 SP17, or higher.
	Set up the SAP User Management Engine (UME) to connect to the Microsoft Active Directory® directory service.
	Configure the authentication mechanism for use in the Duet landscape.
	Gather the information you will need to provide during installation.
	Configure the host for the installation program.

Deploying the Duet Server Components

Before you install the Duet server, make sure that you have prepared the host for the Duet server.

> **Note**: The following describes the procedure for installing Duet server components in a testing environment. For your productive environment, we recommend that you configure the Duet environment to use Secure Socket Layer (SSL).

To deploy Duet server using SAPInst:

4. Double click *sapinst.exe* in the following path to start SAPinst: *\\SAPINST\NT\I386*

   SAPinst GUI starts automatically by displaying the *Select Duet Components* screen.

5. In the *Select Duet Components* screen, you can select one of the following:

   - Duet Server

     Consists of the Java components to install for the Duet server.

     Select this option to deploy the Duet server components.

   - Duet Add-On

     Consists of the Java components to install in the same system landscape as mySAP ERP system.

     Select this option to deploy the Duet Add-On components in mySAP ERP system landscape.

     Note: Although you can install the Duet Add-On components in the same host as the Duet server, we recommend that you deploy the Duet Add-On components in a separate host.

   - Duet Role Synchronization Agent

     This is optional, use only if you are running an SAP NetWeaver® Portal in your landscape.

     The role synchronization agent enables you to use portal roles for Duet users across the Duet system landscape.

6. Select *Duet Server*, and choose *Next*. The *Specify Details of the Duet Server Host* screen displays.
   Enter the following:

Property	**Explanation**
Central Instance Host Name	Enter the name of the host computer, or the IP address.
Message Server HTTP Port	Enter the Message server port for the J2EE engine. The default Message server port number is 8101. To obtain the Message Server port number: 1. Start the Visual Administrator. 2. Choose *Cluster* → *Server 0* → *Services*. 3. Choose *Message Info*. 4. Right click *Start Service* in the toolbar. 5. Select *Parameters* tab. The value for the property *ms/http_port* is the port number.
User	Enter the administrator user ID for the J2EE engine on which you want to deploy the Duet server. The default is *Administrator*.
Password	Enter the password for the administrator of the J2EE engine.

7. Choose *Next*. The *Specify Details of the Software Deployment Manager* screen displays.
   Enter the following details for the SDM:

Property	**Explanation**
SDM Host	Enter the host name of the computer in which you are deploying the Duet server.
Port	Enter the port number of the Software Deployment Manager (SDM). The default is *50018*.
Password	Enter the password for SDM.
Settings for the SCAs/SDAs	Choose *Update any version of the SCAs/SDAs*. The following are the options: • Update only the old versions of the SCAs/SDAs. This is the default option. Select this option to install all the archives and to replace components older than the ones you wish to deploy. • Update same or older versions of the SCAs/SDAs Select this option to update only deployed version of the component which have the same version as, or are older than the ones you wish to deploy. • Update any version of the SCAs/SDAs Select this option to update the deployed component, regardless of its version.

8. Choose *Next*. The *Specify Details of the Load Balancing Mechanism-Duet Server* screen displays.
   Enter the details of the load balancing mechanism in the Duet server environment:

Property	**Explanation**
Load Balancer Host Name	Enter host name of the load balancing mechanism in the landscape in which you are deploying the Duet server. **Note**: Do not use the IP Address. Where there is no load balancing mechanism, enter the host name of the J2EE central instance. For example: *myhost.*

Domain name	Enter the domain name of the load balancing mechanism in the landscape in which you are deploying the Duet server. **Note**: Where there is no load balancing mechanism, enter the domain name of the J2EE central instance.
Load Balancer HTTP Port	Enter the port number or the load balancing mechanism. **Note**: Where there is no load balancing mechanism, enter the HTTP port number of the J2EE central instance. The default is *50000*.
Load Balancer HTTPs Port	Enter the port number or the load balancing mechanism. **Note**: Where there is no load balancing mechanism, enter the HTTPS port name of the J2EE central instance. The default is *50001*. Where you do not use a custom HTTPS port in the load balancing mechanism, enter the HTTP port.

9. Choose *Next*, and select the default language in which content from Duet should be displayed to the end user. The default is *English*.

   Note: This is the language used for displaying content to the end user, if the user's language in Microsoft® Office is not supported in Duet.

10. Choose *Next*. The *Specify Security Settings* screen displays. The following are options:

    - **Use SSL**: Select this option to use SSL encryption for all URL connections. Choose *Next*. The *Configure Security Settings* screen displays. The following are the options:

        - **Kerberos and SAP Logon Ticket**: Select this option to configure SSL encryption for use in the Kerberos authentication method.

        - **X509 Client Certificate:** Select this option to configure SSL encryption for use with X509 client certificate in the authentication process. This is the default option.

      Note: Before you use the option, *Use SSL*, make sure that you have configured the use of SSL on both the Duet server and Duet Add-On hosts.

      For more information, see the section "*Configuring the Use of SSL and Secure Network Communication*," in the *Duet for Microsoft Office and SAP; Duet SAP*

Administration Guide on Service Market Place at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

- **Don't use SSL**: Select this option so that SSL is not implemented for URL connections. This is the default option.

  Note: If you select this option, Kerberos and SAP Logon Ticket authentication is automatically selected as the authentication method and the *Configure Security Settings* screen does not display.

11. Choose *Next,* and enter the following:

Property	**Explanation**
Host	Enter the name or the IP address of the host computer in which you are installing the Duet server.
IIS HTTP Port	Enter the http port number of the Internet Information Service (IIS). The default is *80*.
IIS HTTPS Port	Enter the https port number of the Internet Information Service (IIS). The default is *443*.
Duet Write Service Port	Enter the port number of the Duet Write Service. The default is *8082*.

12. Choose *Next*. The *SAP Duet Java Master Add-On* screen displays.

    Enter the details for the host in which you intend to deploy the Duet Add-On:

Property	**Explanation**
Central Instance Host Name	Enter the name of the host computer.
Message Server HTTP Port	Enter the Message Server port for the J2EE engine. The default port is *8101*.
User	Enter the administrator user name for the J2EE engine. The default is *Administrator*.
Password	Enter the password for administrator user of the J2EE engine.

13. Choose *Next*. The *Specify Details of the Load Balancing Mechanism-Duet Add-On* screen displays.

14. Enter the details of the load balancing mechanism for the host in which you intend to deploy the Duet Add-On:

Property	**Explanation**
Load Balancer Host Name	Enter host name of the load balancing mechanism in the landscape in which you are deploying the Duet Add-On. **Note**: Do not use the IP Address. Where there is no load balancing mechanism, enter the host name of the J2EE central instance. For example: *myhost*
Domain name	Enter the domain name of the load balancing mechanism in the landscape in which you are deploying the Duet server. **Note**: Where there is no load balancing mechanism, enter the domain name of the J2EE central instance.
Load Balancer HTTP Port	Enter the port number or the load balancing mechanism. **Note**: Where there is no load balancing mechanism, enter the HTTP port number of the J2EE central instance. The default is *50000*.
Load Balancer HTTPs Port	Enter the port number or the load balancing mechanism. **Note**: Where there is no load balancing mechanism, enter the HTTPS port name of the J2EE central instance. The default is *50001*. Where you do not use a custom HTTPS port in the load balancing mechanism, enter the HTTP port.

15. Choose *Next*, and then choose *Start* in the summary screen to start deploying the Duet server components.

    After you have entered all the required input parameters, SAPinst starts the installation and displays the progress of the installation.

    When the installation has successfully completed, the screen, *Finished successfully* is displayed.

    The *Finished successfully* screen provides the location of the log files of SAPInst, usually in the SAPInst folder: *...\program files\sapinst_instdir*

    The file *sapinst.log* holds the log of the last installation, or the current one if SAPinst is still running.

    Note: When an error occurs during installation, you can view the contents of the log file directly from SAPInst by selecting *View Log*.

Post Installation Configurations

After deploying the Duet server components, you need to configure it. The following is the sequence of the configuration tasks in the Duet server environment:

- Define the host of the ticket issuing system, and configure the ticket issuing system in the environment of the Duet server.

The following sections describe the post-installation configuration tasks.

Configuring the Duet Server Host for Kerberos

This section provides the flow for configuring Kerberos authentication for use in the host of the Duet server. For each task in the flow, there is a reference to the detailed configuration information available on the SAP Help Portal.

The SAP Web AS Java system on which the Duet server runs must be configured to authenticate clients' request, using the *SPNegoLoginModule* and the JDK Kerberos implementation.

For detailed information, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 → English→* SAP Library → SAP NetWeaver → Security → *User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms →Using Kerberos Authentication for Single Sign-On*

Requirement

- Make sure that you have a Key Distribution Center service. See "*Configuring Kerberos Authentication for Use in Duet*," on page 14, for more information.

The following sections provide an example for configuring the SAP Web AS Java system to use Kerberos:

1. Import Kerberos configuration files into the SAP Web AS Java system.
2. Configure the properties of the SAP Web AS Java system
3. Configure active directory data source file in the SAP Web AS Java system.
4. Configure the login module stack in the SAP Web AS Java system.
5. Configure the host of the Duet Server as the ticket issuing system.

Importing Kerberos Configuration Files

You import the *keytab* file, into the host of the SAP Web AS Java system, and create a configuration file using the name, *krb5.conf*.

For more information, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 →→ English→* SAP Library → SAP NetWeaver → Security → *User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms →Using Kerberos Authentication for Single Sign-On → J2EE Engine Configuration for Kerberos*

To import the keytab file:

- Copy the keytab file from the Kerberos KDC to the file system of the SAP Web AS Java system. For example, *C:\usr\sap\<instance*.

  Note: Make sure you locate the *keytab file* in a secure location. In a cluster, you can copy the file to a mounted (shared) directory.

To create and edit a configuration file:

1. Open a text editor and enter the following:

```
[domain_realm]

      <DNS_domain_pattern> = <Kerberos_Realm_in_upper_case>

 [libdefaults]

      default_keytab_name = <keytab_filename_with_full_path>

      default_realm = <Kerberos_Realm_in_upper_case>

      dns_lookup_kdc = true

      default_tgs_enctypes=des-cbc-md5;des-cbc-crc

      default_tkt_enctypes=des-cbc-md5;des-cbc-crc

 [logging]

 [realms]

      <Kerberos_Realm_in_upper_case> = {

             admin_server = <KDC_ip_or_host_name>

             kdc = <KDC_ip_or_host_name>}
```

Using the names in the examples from the section “*Configuring Kerberos Key Distribution Center*”, the values for the properties in this example configuration file are as follows:

```
[domain_realm]

   sap.mend = DUET-ENV.SAP.MEND

[libdefaults]

   default_keytab_name = C:\usr\sap\<instance>\<keytab-file-name>

   default_realm = DUET-ENV.SAP.MEND
   dns_lookup_kdc = true

   default_tgs_enctypes = des-cbc-md5;des-cbc-crc

   default_tkt_enctypes = des-cbc-md5;des-cbc-crc

[logging]

[realms]

   DUET-ENV.SAP.MEND = {

      admin_server = exchangedirectory.sap.mend

      kdc = exchangedirectory.sap.mend   }
```

Caution: Enter the exact names and verify the white spaces after the equal sign (=), to prevent bottlenecks during the authentication phase.

2. Save the file with the name, *krb5.conf*.

   Note: Users with operating system level permissions for running the SAP Web AS Java system can access these files.

Configuring Properties of the SAP Web AS Java System for Kerberos

You must configure the properties of the SAP Web AS Java system on which the Duet server runs for Kerberos authentication.

For more information, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 →→ English→* SAP Library → SAP NetWeaver → Security → *User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms →Using Kerberos Authentication for Single Sign-On → J2EE Engine Configuration for Kerberos →UME Configuration*

Requirements

- You have imported the keytab file into the host of the SAP Web AS Java system.
- You have created and configured the Kerberos configuration file, *krb5.conf*, in the host of the SAP Web AS Java system.
- Make sure that the SAP Web AS Java system has access to the files.

To configure the properties of the SAP Web AS Java system:

1. Start the *Config Tool* using the file: *<SAPJ2EEEngine_installation>\j2ee\configtool\configtool.bat*
2. Go to *cluster-data → instance_ID<name> → server_ID<name>*, select the *General* tab, add the following under *Java parameters*:
   - -Djavax.security.auth.useSubjectCredsOnly=*false*
   - -Djava.security.krb5.conf=*krb5.conf_with_complete_path*

Where *krb5.conf_with_complete_path* is the fully path to the configure file for Kerberos in the SAP Web AS Java system host. For example: *C:\usr\sap\<instance>*.

Depending on the JDK you are using, add the following:

JDK type	Property and value to add
SUN JDK	-Dsun.security.krb5.debug=true
IBM JDK	-Dcom.ibm.security.jgss.debug=all -Dcom.ibm.security.krb5.Krb5Debug=all

3. Restart the J2EE Engine.

   Note: For a cluster environment, repeat steps 1-3 for each Java instance for which you want to enable Kerberos authentication.

   For *krb5.conf_with_complete_path*, enter the location in the mounted (shared) directory.

Configuring the Active Directory Data Source in SAP Web AS Java System for Kerberos Authentication

You must configure the data source for the Active Directory service in the user management engine. Doing so allows you to use different modes for resolving the user account ID from the KPN.

For more information, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 → English→ SAP Library → SAP NetWeaver →* Security *→User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms →Using Kerberos Authentication for Single Sign-On → J2EE Engine Configuration for Kerberos →UME Configuration → Configuring ADS Data Source for Kerberos Authentication*

You configure the data source using the XML configuration file for active directory in the user management engine (UME). The following is the sequence:

- Download and edit the XML configuration file for the active directory to which the SAP Web AS Java system connects.

  See "*Setting Up the SAP User Management Engine to Connect to the Active Directory*" for the name of the data source configuration file.

- Edit the downloaded file by defining the value, *krb5principalname* in the attribute, *responsibleFor* in the data source configuration file.

- Map the value, *krb5principalname* to the physical attribute *userprincipalname* in the UME data source configuration file.

To edit the data source for active directory in the UME:

1. Start the *Config Tool* by executing *<SAPJ2EEEngine_installation>\j2ee\configtool\configtool.bat*
2. Click the icon, *Switch to configuration editor mode*.
3. Go to *cluster_data* → *server* → *persistent* → *com.sap.security.core.ume.service*, choose *Switch between view and edit mode* to switch to edit mode.
4. Select the configuration file you specified as the data source for the active directory, and choose Show the details of the selected node.
5. Choose *Download* and save the file to your local directory.
6. Open and edit the file in an editor.
7. In the section *<responsibleFor>*, define the value, *krb5principalname* in the name attribute.

```
<responsibleFor>
   ...
    <principal type="user">
      <nameSpaces>
        <nameSpace name="com.sap.security.core.usermanagement">
          <attributes>
            <attribute name="firstname" populateInitially="true"/>
            ...
            <attribute name="krb5principalname"/>
          </attributes>
       </namespace>
      </namespaces>
    </principal>
   ...
 </responsibleFor>
```

8. Map the already defined attributes to physical attributes:

```
<attributeMapping>
  <principals>
    <principal type="account">
      <nameSpaces>
       ...
      </nameSpaces>
    </principal>
    <principal type="user">
      <nameSpaces>
        <nameSpace name="com.sap.security.core.usermanagement">
          <attributes>
            <attribute name="firstname">
              <physicalAttribute name="givenname"/>
            </attribute>
            ...
            <attribute name="krb5principalname">
```

```
             <physicalAttribute name="userprincipalname"/>
           </attribute>
         </attributes>
      </namespace>
    </namespaces>
  </principal>
</attributeMapping>
```

9. Create a new node in the configuration tree for the edited file as follows:
   a. Select the node *com.sap.security.core.ume.service*.
   b. Click the icon *Create* a node below the selected node.
   c. Select the type *File-entry*.
   d. Choose *Upload* and select the file from your local directory.
   e. Enter the name for the entry. For example, *dataSourceConfiguration_ads_readonly_db_with_krb5new.xml*. By default, the name of the uploaded file is used.
   f. Choose *Create*.
   g. Choose *Close* window. The new node appears in the configuration tree.

   Note: For UME to use the new configuration file, you have to change the value of the *property ume.persistence.data_source_configuration* to the name of the new configuration file. See "*Editing UME Properties and Configuration Files for a Directory Service*" above for information on how to edit UME properties.

10. Restart the nodes in the cluster for the changes to take effect.

Configuring Login Module Stacks for Kerberos Authentication

You must configure login modules in UME for Kerberos authentication.

For more information, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 → English→* SAP Library → SAP NetWeaver → Security →*User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms → Using Kerberos Authentication for Single Sign-On → J2EE Engine Configuration for Kerberos → UME Configuration → Configuring Non-ADS Data Sources for Kerberos Authentication → Configuring Login Module Stacks for Kerberos Authentication*

To configure login modules in UME:

1. Start the *Visual Admin* using: *<SAPJ2EEEngine_installation>\j2ee\admin\go.bat*
2. Go to *Cluster tab → Server → Services → Security Provider.*
3. From *Policy Configurations*, change to edit mode (pencil icon), click *Add* and enter a name of the new configuration. For example, *Kerberos*.
4. Choose *Add New*, and enter select each login module.

5. Choose *Modify* to change the *Flag* and add the following properties under *Options*:

Login Modules	**Flag**	**Options**	**Value**
EvaluateTicketLoginModule	SUFFICIENT	ume.configuration.active	true
SPNegoLoginModule	REQUISITE	com.sap.spnego.jgss.name	<KPN>
		com.sap.spnego.uid.resolution.mode	simple
		com.sap.spnego.creds_in_thread	true
CreateTicketLoginModule	OPTIONAL	ume.configuration.active	true

Where the <KPN> value for the option, *com.sap.spnego.jgss.name* is the host specified for the service user.

> **Note**: The value for KPN is case sensitive, so make sure that you specify the value as it exists in the keytab file.

For example: *host/duetserver.sap.mend@DUET-ENV.SAP.MEND*

The property, *com.sap.spnego.creds_in_thread* has the value *true* if you are using Sun's JDK.

If you are using the Sun JDK, do the following:

1. Start the *Visual Admin* using: *<SAPJ2EEEngine_installation>\j2ee\admin\go.bat*
2. From *Cluster tab → Server → Services → Security Provider, c*hoose the *User Management* tab, and select *Manage Security* Stores. If it is disabled click the Edit icon.

   Make sure the UME User Store is selected as the user store.
3. Choose *Add Login Module* to add the following login modules:
   - name *Krb5LoginModule* and class name *com.sun.security.auth.module.Krb5LoginModule*
   - name *MappingModule* and class name *com.sap.security.core.server.jaas.SPNegoMappingLoginModule*
4. From *Policy Configurations* under the component, click *Add* and enter a name of the new configuration, *com.sun.security.jgss.accept.*
5. Choose *Add New*, and enter the following:

6. For each login module choose it and click *Modify* to change the Flag and add the properties under *Options*.

Login modules	**Flag**	**Options**	**Values**
Krb5LoginModule	REQUISITE	debug	true
		doNotPrompt	true
		keyTab	<keytab_filename_with_full_path>
		principal	<KPN>
		storeKey	true
		useKeyTab	true
		useTicketCache	true
MappingModule	OPTIONAL	com.sap.spnego.uid.resolution.attr	krb5principalname

Where *keytab_filename_with_full_path,* is the full path to the location where the *keytab* file is stored. For example: *C:\usr\sap\<instance>\<keytab_filename>*.

And the <KPN> value for the option, *principal* is the host specified for the service user.

> **Note**: The value for KPN is case sensitive, so make sure that you specify the value as it exists in the *keytab* file.

For example: *host/duetserver.sap.mend@DUET-ENV.SAP.MEND*

Configuring the Host of the Duet Server as the Ticket Issuing System

After configuring the login modules, you must configure the host of the Duet server as the ticket issuing system.

To configure the Duet server as the ticket issuing system:

1. Start the Visual Admin Using: *<SAPJ2EEngine_installation>\j2ee\admin\go.bat*
2. Go to *Cluster Tab → Server → Services → Security Provider,* and under *Runtime* in Policy Configuration, click *sap.com/xapps~osp~server~deployer*osp_TicketIssuer*
3. From *Authentication Template*, choose the new policy configuration which you created. For example, Kerberos. This must contain the following login modules: *EvaluateTicketLoginModule*, *SPNegoLoginModule* and *CreateTicketLoginModule*.

   If you cannot see the newly created policy configuration, close and reopen the Visual Admin Console.
4. Select *Security Roles* tab in the right hand panel.
5. Select *RoleAuthenticated*, and from *Groups* in the right hand pane, select *Add*. The Choose User or Group window opens.
6. Click *Search* in window, and select *Authenticated Users*. The *Authenticated Users* are added under Groups.

Post-Installation Checklist

The following is a checklist to help you verify the post-installation configuration tasks:

Check (√)	Task
	Import Kerberos configuration files into the SAP Web AS Java system.
	Configure the properties of the SAP Web AS Java system
	Configure active directory data source file in the SAP Web AS Java system.
	Configure the login module stack in the SAP Web AS Java system.
	Configure the host of the Duet Server as the ticket issuing system.

Deploying the Duet Add-On

Deploy Duet Add-On components in a host which is in the same system landscape as mySAP ERP, and verify that the host meets the following software requirements:

- SAP NetWeaver '04 Web Application Server Java 6.40 SP17, or higher (SAP Web AS Java system)
- SAP GUI version 6.40 (SAP Logon)

You can install the Duet Add-On components in a single host, or in a cluster. In a cluster, the host in which you deploy the Duet Add-On components for the first time becomes the Master Duet Add-On, with the metadata repository. All other instances of the Duet Add-On installation must interface with the Master Duet Add-On.

See "*Deploying Additional Duet Add-On Hosts in the Duet System Landscape*" on page 37, for detailed information about installing additional Duet Add-On host.

Pre-Installation Requirements for the Duet Add-On Host

You must prepare each host computer in which you want to deploy the Duet Add-On components.

Preparation Workflow

The following is the workflow for the pre-installation configurations tasks:

1. You have administration privileges on the computer in which you intend to perform the pre-installation tasks.
2. Set up the SAP User Management Engine (UME) to connect to your user storage: either mySAP ERP system user store, or Microsoft Active Directory service.
3. Obtain a system user ID in mySAP ERP system, and define that same user ID in the UME of the SAP Web AS Java system.
4. Gather information that you will need during the installation.
5. Verify that the host computers for both Duet server and Duet Add-On have the same date and time.

Setting Up User Management Engine to Connect to mySAP ERP User Store

Where users have the same user ID in both mySAP ERP system and Windows, you can connect the UME in the Duet Add-On host to your Active Directory service, or to the mySAP ERP user management. The passwords do not have to be the same.

See “Setting Up the SAP User Management Engine to Connect to the Active Directory” on page 13, for more information.

> **Note**: If users do not have the same user ID in Windows and mySAP ERP, then connect the UME in the Duet Add-On host to mySAP ERP user management, and then configure user mapping data using the User management engine in the Duet server host.
>
> For more information on user mapping data configuration, see the section “*Configuring User Mapping Data in the User Management Engine*” in the *Duet for Microsoft Office and SAP; Duet SAP Administration Guide* on Service Market Place at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

Connecting User Management Engine to mySAP ERP User Store

You must set up the User Management Engine in the host of the Duet Add-On to connect to mySAP ERP user management of the SAP Web AS ABAP. Doing so enables Duet to access user data of the SAP Web AS ABAP.

Using the SAP Web AS ABAP as your data source for user management data has the following advantages:

- Users of mySAP ERP system are visible as users in the UME.
- Roles of mySAP ERP system are visible as groups in the UME.

The UME provides you with a configuration file from the UME LDAP Configuration tool. Using the UME LDAP Configuration tool, you configure the UME to use the user management data.

To configure the UME to use mySAP ERP UME:

1. Start the Config Tool using the file: *<SAPJ2EEEngine_installation>\j2ee\configtool\configtool.bat*
2. In the *Config Tool* window, select the icon *Switch to configuration editor mode*.
3. Select *cluster_data → server→ cfg→ services→ Propertysheet com.sap.security.core.ume.service*
4. Select the icon *Switch between view and edit mode.*
5. Double click on *Propertysheet com.sap.security.core.ume.service*
6. Edit the following properties according to your SAP® R/3® system:

   Note: Where you are not using a message server (no load balancing), but one application server, enter values only for *ume.r3.connection.master.ashost* and *ume.r3.connection.master.sysnr.*

Properties	**Values**
ume.persistence.data_source_configuration	Specify the data source, *dataSourceConfiguration_r3.xml*

ume.r3.connection.master.msghost	Specify the Message Server host address. For example, *server01.company.com*
ume.r3.connection.master.msserv	Specify port number.
ume.r3.connection.master.r3name	Specify the system ID (SID) of mySAP ERP system to connect to. For example, *Bon.*
ume.r3.connection.master.sysnr	Specify the system number of mySAP ERP system to connect to. For example, *00.*
ume.r3.connection.master.user	Specify the user name in mySAP ERP. For example, *007Bo.* This is the SAP JSF (communication user). Make sure that this user has the following: Profile = `T_BE111319 (Profile for the role SAP_BC_JSF_COMMUNICATION_RO)` Role = `SAP_BC_JSF_COMMUNICATION_RO` For more information, go to the SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 → English→ SAP Library → SAP NetWeaver → Security →Network and Transport Layer Security → Transport Layer Security on the SAP J2EE Engine → Configuring SNC (SAP J2EE Engine (ABAP Engine) → Configuring SNC Between the UME and an ABAP-Based System → Requirements for Communication User SAPJSF_<SID> in ABAP Systems* **Caution**: Do not use this communication user for other purposes.
Ume.r3.connection.master.passwd	Specify user password in mySAP ERP.
ume.r3.connection.master.client	Specify the client number of mySAP ERP. For example, *007.*
ume.r3.connection.master.group	Specify the group for mySAP ERP. For example, *Public.*
ume.r3.connection.master.lang	Specify the language used in mySAP ERP. For example, *en.*
Ume.r3.connection.master.ashost	Specify the Application server host address. For example, *server02.company.com*

7. Click *Switch to configuration editor* mode and select *UME LDAP DATA.*

8. Select the configuration file, *dataSourceConfiguration_r3.xml.*

   Note: Where the users IDs in the SAP system are not the same as the user IDs in the Active Directory server, you must configure user mapping.

   If you need to configure user mapping data, skip the following step 9. Where you do not need to configure user mapping perform the following procedures in step 9.

9. Enable the use of assertion ticket between mySAP ERP and Duet Add-On environment:
   a. Go to *cluster data* → *Global server configurations* → *services*, choose *com.sap.security.core.ume.service*, and change the following UME configuration property: *login.ticket_portalid*
   b. Enter the value *yes* in *Value* at the bottom of the screen. The default value is *auto*.
   c. Choose *Set*.
   d. Choose Apply changes.

10. Restart the cluster.

Defining Existing System User ID in UME

You must obtain the ID of an existing system user in mySAP ERP system, and define administrator rights for it in the User Management Engine (UME) in the Duet Add-On host.

The system user must have the following authorizations for budget monitoring and reporting in mySAP ERP:

- For cost centers: K_REPO_CCA and K_CCA
- For internal orders: K_REPO_OPA and K_ORDER
- For profit centers: K_PCA

See SAP note numbers **15211** and **103818** for information about these authorizations**.** In addition, you need the basic authorizations for executing RFCs. This is S_RFC.

```
RFC_TYPE = FUGR,

RFC_NAME = FPB_MON_VAR_RFC, FPB_RULE_VAR_RFC, FPB_MON_LINE_RFC and
FPB_RULE_LIN_RFC
```

Later, you specify this administrator user ID when deploying the Duet Add-On components.

To define administrator rights for the system user ID using the User Administration Console:

1. Log on to the SAP Web AS Java system using: http://*<Java_Addon_Hostname>:<J2EE_HTTP_port>/useradmin*
2. Click *User Management*. The *User Management Admin Console* opens.

3. Click *Groups*, and search for all groups using the wild card string.
4. Select *Administrators* from the search result and click the icon *Assign Users to*.
5. Click the plus (+) icon to search for the system user ID from mySAP ERP.
6. Select it and click *Select*, and then *Continue*.
7. Log off and close the browser.

   Note: The passwords do not have to be the same.

Gathering Information for Installation

You must gather information about the SAP Web AS Java system in which you want to deploy the Duet Add-On. Later, you need to provide the information during deployment of the Duet Add-On components.

Gather the following about the SAP Web AS Java system:

- Host name of the SAP Web AS Java system.
- Administrator credentials for logging onto the SAP Web AS Java system.
- The URL and HTTP port number of the SAP Web AS Java system.
- Host name and port number of the load balancing mechanism in the system landscape, if there is one.

Pre-installation Checklist

The following is a checklist to help you verify that you have performed all the required pre-installation configuration tasks:

Check (√)	Task
	Set up the SAP User Management Engine (UME) to connect to your user storage: either mySAP ERP system user store, or Microsoft Active Directory service.
	Obtain a system user ID in mySAP ERP system, and define that same user ID in the UME of the SAP Web AS Java system.
	Gather information that you will need during the installation.
	Verify that the host of both Duet server and Duet Add-On have the same date and time.

Deploying the Duet Add-On Components

You must deploy the Duet Add-On components using SAPInst from the same host as the Duet server. On installing the Duet Add-On components, you deploy the components for communicating with mySAP ERP, in addition to the metadata repository for Duet business applications.

> **Note**: The following describes the procedure for installing Duet Add-On components in a testing environment. For your productive environment, we recommend that you configure the Duet environment to use SSL and https.

The following sections provide information for deploying the Duet Add-On components.

To deploy the Duet Add-On using SAPInst:

1. Double click *sapinst.exe*, in the following path to start SAPinst: *…\SAPINST\NT\I386*

   SAPinst GUI starts automatically by displaying the *Select Duet Components* screen.

2. Select the *Duet Add-On*, and click *Next*. The *Specify Details of the Duet Add-On Host* screen displays.
3. Enter the following:

Property	**Explanation**
Central Instance Host Name	Enter the host name of the computer. For example: *Duet001*.
Message Server Port	Enter the *Message Server* port for the J2EE engine. The default Message server port for J2EE is *8101*.
User	Enter the administrator user name for the J2EE engine. The default name is *Administrator*.
Password	Enter the password for the administrator user of the J2EE engine.

4. Click *Next*, the *Specify Details of the Software Deployment Manager* screen displays.
5. Enter the following details for the SDM:

Property	**Explanation**
SDM Host	Enter the host name of the computer in which you are installing the Duet Add-On components. For example: *Duet001*.
Port	Enter the port number of the Soft Deployment Manager (SDM). The default is *50018*.
Password	Enter the password for SDM.
Settings for the	Choose Update any version of the SCAs/SDAs. The

SCAs/SDAs	following are the options: Update only the old versions of the SCAs/SDAs Update same or older versions of the SCAs/SDAs Update any version of the SCAs/SDAs

6. Click *Next*, and enter the J2EE administrator user ID and password.

   Note: You created this administrator user ID in the SAP Web AS Java system during the preparation stage. Make sure that the same user ID exists as a system user in mySAP ERP system.

7. Click *Next*. The *Specify Details of the Duet Server* screen displays.
8. Enter the host name, Message Server HTTP port number, the port number, and the administrator logon details of the SAP Web AS Java system on which the Duet server runs.

   Note: Make sure that the Duet server is running when you perform this step.

   After you have entered all required input parameters, SAPInst starts the installation and displays the progress of the installation.

   When the installation has successfully completed, the screen *Finished successfully* is displayed. The *Finished successfully* screen provides the location of the log files of SAPInst.

Deploying Additional Duet Add-On Hosts in the Duet System Landscape

You can add and configure additional Duet Add-On hosts in the Duet system landscape. The following is the sequence for adding an additional Duet Add-On host:

The following is a checklist to help you verify the post-installation configuration tasks:

1. Prepare the host, and then deploy the Duet Add-On components from the Duet server host, using SAPInst.

   See the section “*Pre-Installation Requirements for the Duet Add-On Host*” on page 31.

2. Deploy the Duet Add-On components. For more information, see the section “Deploying the Duet Add-On Components” 36.
3. Perform all post-installation configuration tasks. See the section “*Configuring the Duet Add-On Environment*” on page 43.

Installing the Duet Business Applications

To make Duet business applications available for use in Microsoft Office Outlook® 2003, you must install, configure and distribute them to client computers.

Pre-Installation Requirements for the Duet Business Applications

You must prepare the environment for the Duet business applications, to make business applications available for use in Microsoft Office Outlook® 2003.

Requirements

- You have permissions in the local computer to perform the installation.
- You have installed the Duet Metadata Service and the Request Handler.

  The Duet Metadata Service and the Request Handler components can be installed from the following folder in the installation CD: …*\Microsoft\Installation\Duet Server.*

  You can find the installation guide and other documentation for the Duet Metadata Service and Request Handler Service, in the installation CD: *…\Microsoft\Documentation*

The following is the workflow for preparing the environment for Duet business applications:

1. Create new folders using the names, *DuetMetadata*, and *DuetCode*. Share the folders, and define permissions for the administrator user on the host of the Duet server.
2. Set security settings for the Request Handler service in the IIS on the host of the Duet Metadata Service.

Creating New Folders in the Duet Metadata Service Host

You must create two new folders, using the names, *DuetMetadata* and *DuetCode* in the Duet Metadata Service host.

The installer program will ask for these paths during installation of the Duet server. The folder, *DuetMetadata* will store the metadata for the Duet business applications, and the folder, *DuetCode* will contain the resources (DLL files, graphic files, and the Duet help) for the business applications.

In addition, you must enable sharing of the folders, and define specific permissions for working in them. Permissions in the folder, *DuetCode* must allow writing, and reading, as the installer configures the Duet server to do the following:

- Write into the folder, ...\DuetCode.
- Enable clients to read from the same folder, ...\DuetCode.

To create, share and define permissions for the new folders:

1. From the root folder of the host of the Duet Metadata Service, create two new folders using the name *DuetMetadata*, and *DuetCode*. For example, C:\
2. Perform the following for each of the folders you have created:
   a. Right click the folder and select *Sharing and Security,* and click *Share this folder* to share it.
   b. Click *Permissions* and add the user ID that runs SAP services on the host of the Duet server. For example, *SAPService<Instance>*.

      Note: You can verify the user ID using the Task Manager in the Duet server. Find the java process, and then find the user that is running that process.
   c. Define the following permissions:
      - Full Control
      - Change
      - Read
   d. Select the *Security* tab and add all Duet users (usually use the *Domain Users* group).
   e. Define read permissions for the users.
   f. Click *OK*.

Security Settings for Request Handler Service

You must configure access to the Duet business applications through the Internet Information Service (IIS), in the same host as the Duet Metadata Service. By so doing, you enable the Duet Metadata Service to access assemblies and metadata for the Duet business applications.

Requirement

- Make sure that the Duet Metadata Service and the Request Handler Service have been installed.

To configure the Request Handler service in the IIS:

1. From the *Start menu → Settings → Control Panel → Administrative tools → Internet Information Services Manager.*
2. Expand the node in the left hand pane, and click Web Sites.

3. Select *Web Sites → Default Web Site → RequestHandler.*
4. From the right hand panel, select *RequestHandler.asmx*.
5. Right-click *RequestHandler.asmx*, select *Properties.*
6. Select the *File Security* tab, and select *Edit* under *Authenticated access control*.
7. Select *Basic authentication* under *Authenticated access control*.

   Note: Make sure that the option, *Enable anonymous access* is not selected.

Pre-installation Checklist

The following is a checklist to help you verify that you have performed all the required pre-installation configuration tasks:

Check (√)	Task
	Create the folders, *DuetMetadata*, and *DuetCode*.
	Share the folders, and define permissions for the administrator user on the host of the Duet server.

Installing the Duet Business Applications

The Duet business applications are integrated into Microsoft Office Outlook® 2003 for information workers.

Requirements

- You have an administrator user, with which you perform the installation.
- You have installed the Duet Metadata Service and the Request Handler.

  The Duet Metadata Service and the Request Handler components can be installed from the following installation folder: *...\Microsoft\Installation\*

  You can find the installation guides and other documentation for the Duet Metadata Service, Request Handler and Duet client components, on the installation folder: *...\Microsoft\Documentation*
- You have configured English (United States) as the default language setting for your system.
- You have created the folders *DuetMetadata*, and *DuetCode*.

  Make sure that you share these folders and define permissions for the Windows administrator user ID with which you installed SAP Web AS Java system on the Duet Add-On host.

Loading Metadata for Duet Business Applications

You install the Duet business applications in both the Duet Add-On host and the Duet server environments.

The business applications are provided as zipped files, containing assemblies (DLL and Java files), XML files, XIN files, and DIN files.

You install the Duet business applications using a browser-based application, called *Application Installer*.

- Open the Application Installer in each host (Duet Add-On, and Duet server), using the URL: *http://<host_name>:<port>/webdynpro/dispatcher/sap.com /xapps~osp~fw~appinst~ui~webdynpro/AppInstUiApp*

Where you have installed the Duet Add-On components in more than one host, you install the business applications in the following sequence.

1. From the Master Duet Add-On host, open the Application Installer, and install only the file *ApplicationsFramework.zip*, by entering the following:

Property	**Description**
SDM Password	Enter the SDM password.
Port	Enter the SDM port. The default port number is 50018.
SAP Master Add-On	Select the checkbox.
Upload File	Choose browse to select the file, *ApplicationsFramework.zip*.

2. Then, you install the file *DuetBusinessApplications.zip*, by entering the following:

Property	**Description**
SDM Password	Enter the SDM password.
Port	Enter the SDM port. The default port number is 50018.
SAP Master Add-On	Select the checkbox.
Upload File	Choose browse to select the file, *DuetBusinessApplications.zip*.

3. From each Duet Add-On host, open the Application Installer, and install the file DuetBusinessApplications.zip, by entering the following:

Property	**Description**
SDM Password	Enter the SDM password.
Port	Enter the SDM port. The default port number is 50018.
SAP Master Add-On	Do not select the checkbox.

Upload File	Choose browse to select the file, *DuetBusinessApplications.zip*.

4. From the Duet server host, open the Application Installer, and install the file *DuetBusinessApplications.zip*, by entering the following:

Property	**Description**
SDM Password	Enter the SDM password.
Port	Enter the SDM port. The default port number is 50018.
Upload File	Choose browse to select the file, *DuetBusinessApplications.zip*. **Note**: If the Duet server and Duet Add-on components are in the same host, load the file *DuetBusinessApplications.zip*, once and select the checkbox.

After loading the Duet business applications, the installation program places data and other resources for the business applications in the Duet Metadata Service host, in the following folders:

- DuetMetadata: the metadata for the installed business applications.
- DuetCode: the resources for the installed business applications.

Configuring the Duet Add-On Environment

After setting up the Duet Add-On environment successfully, you must configure the following:

1. Set the size for messages in the SAP Web Application Server Java.
2. Map Duet business application roles to mySAP ERP roles.
3. Configure communication channels for the Duet Add-On
4. Configure RFC destinations.
5. Verify the security settings of the ESA services.

The following sections provide the procedures for the above configuration tasks.

Setting the Size for Messages in the SAP Web Application Server Java

You must configure the SAP Web AS Java system, on which the Duet Add-On runs, to process large messages.

To set the size for messages:

1. Start the Visual Admin Console using the file, *go.bat* in the path: *<AddonServer_SAPJ2EE Engine_installation>\j2ee\admin\*
2. In the login window, specify the administrator user and password and choose *Connect*.
3. Go to *Cluster → Server → Services → JMS Provider*
4. Select the *Properties* tab, and enter the following:
   - clientConsumerBuffer = *524288*
   - clientMemorySize = *52428800*
   - sizeLimitInMasterQueue = *3145728*

6. Select *Save* to save the changes.

7. Restart the *JMS Provider* as follows:
   a. From the *Admin Console* window, select *Service*.
   b. Right click *JMS Provider,* and select *Stop*. Then right click again and select *Start,* after the process has stopped.

Note: The property values specified in the above procedures are suggested values where the virtual machine's heap size is 1GB for the SAP Web AS Java system.

Consider the effect and demands of all other J2EE components and applications running on the virtual machine when changing the total heap size.

Settings for Queues in the JMS Provider Service

1. Start the *Offline Configuration editor* using the file, *offlinecfgeditor.bat* in the path: *<AddonServer_SAPJ2EE Engine_installation>\j2ee\configtool*
2. Go to *Configurations → JMS provider →DEFAULT→…→Queues → ItemsQueues*.
3. Switch to edit mode and set the following property value:
   `deliveryAttemptsLimited = false`
4. Restart the cluster of the Duet Add-On for the change to take effect.

Configuring Communication Channels for Duet Add-On

The following section provides information for configuring communication channels for the Web service proxies in the Duet Add-On host to the following:

- Duet Metadata Service host
- SAP system

Define Connection Settings to the Duet Metadata Service Host

You must configure communication channels for the Web service proxy, Authorization Manager (AzMan) service, by defining permissions for the administrator user that runs Windows services used by components from SAP.

Using a browser–based application, you define the details for logging on to Authorization Manager (AzMan).

To define the settings for connecting to the Authorization Manager:

1. Open the Duet Administration Control Panel using the following URL:

   http://<Duet_Host>:<Duet_Port>//webdynpro/dispatcher/sap.com/xapps~osp~fw~admin~launchpad~webdynpro/AdminLaunchpadApp

2. Choose *Connect Duet Server to the Duet Metadata Service* and enter the following:

Property	**Description**
Host	Specify the name of the host of the Duet Metadata service. By default, the name of the host of the Duet Metadata Service displays.
Port	Specify the port number assigned to the Duet Metadata Service in the IIS. By default, the port number displays.
User	Enter the user name for logging onto Authorization Manager service, in the same host as the Duet Metadata Service.

	The user name is the user that runs SAP services in Windows. The user name is in the format *DOMAIN\user_name*. For example, *duetcorp\SAPAgent*
Password	Enter password of the user with which to logon to Authorization Manager.

3. Choose *Apply*.

   The application attempts to connect to the AzMan service. If it fails, an appropriate error message is displayed.

4. Choose *Finish*, when *Automatic background processing* completes. When the connection succeeds, a message is displayed.

Define Duet Configuration Details

Using a browser–based application *Duet Configuration Details,* you define the settings for configuring communication connections between the Item Handler service in the Duet Add-On host, and the Request Handler service in the Duet Metadata Service host.

Using the settings you specify, the *Duet Configuration Details* application attempts to connect to the Request Handler service in the same host as the Duet Metadata Service.

To define the settings for connecting to the Request Handler:

1. Open the Duet Administration Control Panel using the following URL:

http://<AddOn_Host>:<AddOn_Port>/webdynpro/dispatcher/sap.com/xapps~osp~fw~addon~config~ui~webdynpro/AddonConfigUIApp

2. Choose *Duet Connection Configuration Details*.
3. Enter the following:

Property	Description
Host	Specify the name of the host of the Duet Metadata service. By default, the name of the host of the Duet Metadata Service displays.
Port	Specify the port number assigned to the Duet Metadata Service in the IIS. By default, a port number is displays.
User	Enter the user name you provided during installation of the Request Handler component. The user name is in the format DOMAIN\user_name. For example, *duet.corp\SAPAgent.*
Password	Enter password of the user you provided during installation of the Request Handler component.

4. Choose *Apply*.

   The application attempts to connect to the connection to the Request Handler service. If it fails, an appropriate error message is displayed.

5. Choose *Finish*, when *Automatic background processing* complete.

   Note: Later, you configure trust between the Duet server and the Duet Add-On host using this screen.

Define RFC Destinations

Using a browser–based application *Duet Configuration Details,* you define the settings for configuring communication connections between the specific Duet Add-On host and the specific SAP system.

To define the settings for connecting to an SAP system:

1. Open the Duet Administration Control Panel using the following URL:

http://<AddOn_Host>:<AddOn_Port>/webdynpro/dispatcher/sap.com/xapps~osp~fw~addon~config~ui~webdynpro/AddonConfigUIApp

2. Choose *SAP System Connection Configuration Details.* Enter the following:

Property	**Description**
RFC destination	Select the RFC destination you want to configure. For example, *OSP/AB5/003*.
User	Enter the system user ID for connecting to the SAP system. See "*Defining Existing System User ID in UME*" on page 34.
Password	Enter the password of the system user for logging onto the SAP system.

3. Choose Apply.

   The application attempts to connect to the specified system. A message displays.

   Note: Later, you configure trust between the Duet Add-On host and the SAP system using this screen.

Post-Installation Checklist

The following is a checklist to help you verify the post-installation configuration tasks:

Check (√)	**Task**
	Setting the size for messages in the SAP Web Application Server Java
	Configure communication channels for the Duet Add-On
	Define connection settings to the Duet Metadata Service host
	Define Duet configuration details
	Define RFC destinations

Configuring the Duet System Landscape

This section describes the post installation configuration to be performed across the Duet system landscape.

Configuring Trust in the Duet Add-On Environment

This section provides information for configuring the Duet components to trust and accept the logon tickets issued by the ticket issuing mechanism.

The following is the sequence for configuring trust in the environments.

1. Configure trust between the each Duet Add-On host and Duet server host, using a browser-based application.
2. Issue a certificate in each specific mySAP ERP environment and import it into the specific Duet Add-On host to which it connects.
3. Configure trust between each specific Duet Add-On host, and the specific mySAP ERP system to which it needs to connect, using a browser-based application.
4. Issue and import a certificate issued from each Duet Add-On into mySAP ERP system.

Configure Trust between Each Duet Add-On Host and the Duet Server

You configure trust between each Duet Add-On and the Duet server using a browser-based application. The application imports and configures a certificate issued in the Duet server host to the Duet Add-On host. This process enables single sign-on between the Duet server host and Duet Add-On host.

To configure trust between a Duet Add-On host and the Duet server host:

1. Open the browser-based application using the URL: *http://<AddOn_Host>:<AddOn_Port>/webdynpro/dispatcher/sap.com /xapps~osp~fw~addon~config~ui~webdynpro/AddonConfigUIApp*
2. Choose *Duet Connection Configuration Details.*

   Note: You configured the communication channel between the Item Handler service and the Request Handler service using this screen.

3. Under *Trust*, enter the following:

Property	Description
System ID	Enter the System ID (SID) of the SAP Java WAS (J2EE system) where the Duet Server is deployed.
Client	Enter the client of the SAP Java WAS (J2EE system) where the Duet Server is deployed (the default client is 000). You can check your client ID using the *Offline Configuration editor*, *offlinecfgeditor.bat* in the path: *<AddonServer_SAPJ2EE Engine_installation>\j2ee\configtool*.

4. Choose Apply. A message displays.

   A certificate from the Duet server host is automatically imported and configured for use in the Duet Add-On host.

Configure Trust between Each Duet Add-On Host and mySAP ERP System

You need to enable single sign-on between each specific Duet Add-On host and the specific mySAP ERP system to which it connects.

The following is the workflow for configuring trust between an SAP system and the Duet Add-On:

1. Issue a certificate in mySAP ERP system. Later you import this certificate to the Duet Add-On environment.
2. Import the certificate from mySAP ERP system to the Duet Add-On host.
3. Configure the certificate in the Duet Add-On host

Issuing a Certificate in mySAP ERP System

You must configure the SAP system you have prepared for Duet, to issue a certificate for use in the Duet Add-On host.

Later, you import the certificate into Duet Add-On host.

To issue and export the certificate from the SAP Web AS ABAP system:

1. Log on to the SAP system, and in the system command line enter the transaction *STRUST*.
2. Select the *Personal Security Environment* (*PSE*) that is used for logon tickets (per default, this is the System PSE).

   The server’s public-key certificate appears in the upper section of the screen. The Distinguished Name appears in the Own. cert. field.
3. Double-click the *Distinguished Name*. The certificate appears in the lower section of the screen.

4. Choose *Certificate → Export*. The *Export Certificate* dialog appears.
5. Save the certificate to a file. Use *DER* encoding or base 64, and the extension *.crt. For example, *abapaddon.crt*.

Import the Certificate from mySAP ERP into the Duet Add-On Host

You need to configure the Duet Add-On host to accept assertion logon tickets issued from mySAP ERP system.

You perform this task in the Duet Add-On environment.

To import the certificate from the SAP Web AS ABAP system:

1. Start the Visual Admin Console, using the file, *go.bat*, located in the path: *<SAPJ2EEEngine_installation>\j2ee\admin\>*
2. In the *Visual Admin* window, choose *Server→Services →Key Storage*.
3. From the *Runtime* tab, choose *Ticket Keystore* view, and then select *Load to import* the certificate from the certificate file. For example, *abapaddon.crt*.

   Note: Specify the pathname of the certificate file you saved in the host of mySAP ERP. You can map a drive to the host of mySAP ERP from the Duet Add-On host.

   The certificate is stored in the selected view as a CERTIFICATE entry.

To configure trust between a Duet Add-On host and a specific mySAP ERP system:

1. From the Duet Add-On host, open the browser-based application using the URL: *http://<AddOn_Host>:<AddOn_Port>/webdynpro/dispatcher/sap.com /xapps~osp~fw~addon~config~ui~webdynpro/AddonConfigUIApp*
2. Choose *SAP System Connection Configuration Details.*

   Note: You configured the RFC destination using this screen.
3. Under *Trust*, enter the following:

Property	**Description**
SAP System Certificate	Select the certificate you imported into the Duet Add-On host. For example, *abapaddon.crt.*
SAP system	Select the system ID of the SAP system from which you imported the certificate.

4. Choose *Apply*, to configure trust and the *EvaluateAssertionTicketLoginModule*. A message displays.

Issuing and Importing a Certificate from Duet Add-On into mySAP ERP System

To enable single sign-on between each Duet Add-On host and the specific mySAP ERP system to which it connects, you must create and configure a certificate in the Duet Add-On host. Later you import this certificate into the SAP system.

Issue a Certificate from the Duet Add-On Host

The following is the workflow for configuring the certificate:

- Change the public key for the certificate in the SAP Web AS Java system
- Replace Public Key-Certificate
- Export the certificate from the SAP Web AS Java

Changing the Public Key of the New Certificate

Note: If you do not have an Add-In installation, skip the following steps.

1. Start the *Config Tool* using the file: *<SAPJ2EEEngine_installation>\j2ee\configtool\configtool.bat*
2. From the left pane, choose *cluster data → Global server configuration → Services → com.sap.security.core.ume.service*
3. From the list of UME properties in the right hand pane, select *login.ticket_client*.
4. From *Value* at the bottom of the pane, replace the value by entering a three digit number. For example, *120*.
5. Select *Set* and select *Save*.
6. Restart the nodes in the cluster for the changes to take effect.

For detailed information for configuring logon tickets, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 → SAP Library → SAP NetWeaver→ Security → User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms → Using Logon Tickets for Single Sign-On → Configuring the Use of Logon Tickets → Specifying the J2EE Engine Client to Use for Logon Tickets*

Replacing the Public Key-Certificate

1. Start the *Visual Admin Console* using the file, *go.bat*, located in the path: *<SAPJ2EEEngine_installation>\j2ee\admin\>*
2. From Visual Admin window, choose *Server → Services→ Key Storage*.
3. From the *Runtime* tab, select *TicketKeystore*.
4. Rename the *SAPLogonTicketKeypair* and *SAPLogonTicketKeypair-cert* entries. For example, *OLD_SAPLogonTicketKeypair.crt*.

5. From Entry, select *Create*. The *Key and Certificate Generation* dialog appears.
6. Enter the *Common Name* (CN) under *Subject Properties*.
7. The *Common Name* should be unique, so we recommend that you create one that consists of:
   - Abbreviation of country/city (this can be anything)
   - The same three digit number you entered for the log-client. For example, IL120
8. In the *Entry Name*, enter *SAPLogonTicketKeypair*.

   Do not enter a different name. SAP Web AS Java uses this name to sign logon tickets.
9. Select *Store certificate* and select *DSA* as the algorithm to use.
10. Choose *Generate*. Now you are ready to export the certificate for use in the SAP Web AS ABAP.

For more information on configuring logon tickets, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 → SAP Library → SAP NetWeaver→ Security → User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms → Using Logon Tickets for Single Sign-On → Configuring the Use of Logon Tickets → Replacing the Public-Key Certificate to Use for Logon Tickets*

Exporting a Certificate from the Duet Add-On Host

To export the certificate using the Key Storage Service:

1. Start the Visual Admin Console, using the file, *go.bat*, located in the path: *<SAPJ2EEEngine_installation>\j2ee\admin\>*
2. From *Visual Admin* window, choose → *Server* → *Services*→ *Key Storage*.
3. From the *Runtime* tab, choose *TicketKeystore* view, and then choose *SAPLogonTicketKeypair*-cert *Entry*.
4. Select *Export* to export the certificate by saving it to a file.
5. Specify a filename. Use the file type *X.509 Certificate* with the extension *.crt* and choose *OK*. For example, *JavaddonCert.crt*.

   Note: Write down the path and the name of the certificate file you saved, as you will have to import it into your existing mySAP ERP system.

Importing the Certificate from the Duet Add-On Host into the SAP System

You need to configure your SAP system to accept logon tickets using the certificate issued by the Duet Add-On host.

You perform this task in mySAP ERP environment.

To import the certificate into the SAP system:

1. Logon to the specific mySAP ERP system.
2. Enter the transaction */nstrustSSO2*. The Trust Manager for Single Sign-On screen displays.
3. Select *System PSE* (for logon tickets).
4. Select *Import Certificate.*
5. Browse to locate the certificate from the Duet Add-On host. For example, *javaddon.cert.*
6. Click *Add to certificate list* in *Certificate* pane.
7. Click *Add to ACL*, and specify the following:
   - Common Name: Enter the system ID for the Duet Add-On host
   - Client: Enter the same three digit number that you specified for the client. For example, *120*. See step 4, under “Changing the Public Key of the New Certificate”.
8. Choose *Save*.

For more information on configuring logon tickets, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 →* SAP Library → SAP NetWeaver→ *Security → User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms → Using Logon Tickets for Single Sign-On → Configuring the Use of Logon Tickets → Configuring SAP Web AS ABAP to Accept Logon Tickets from the J2E*

Configure Trust between the Duet Server Host and mySAP ERP System

You need to enable the Role management Web service in mySAP ERP system to call other services in the Duet server.

Find detailed information for configuring the role management Web service in mySAP ERP system in the *Duet for Microsoft Office and SAP; Duet SAP Administration Guide* on Service Market Place at:
s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

The following is the workflow for configuring trust between an SAP system and the Duet server:

1. Issue a certificate in mySAP ERP system. Later you import this certificate to the Duet server environment.
2. Import the certificate from mySAP ERP system to the Duet server host.

Issuing a Certificate in mySAP ERP System

You must configure the SAP system you have prepared for Duet, to issue a certificate for use in the Duet server host.

Later, you import the certificate into Duet server host.

To issue and export the certificate from the SAP Web AS ABAP system:

1. Log on to the SAP system, and in the system command line enter the transaction *STRUST*.
2. Select the *Personal Security Environment* (*PSE*) that is used for logon tickets (per default, this is the System PSE).

   The server's public-key certificate appears in the upper section of the screen. The Distinguished Name appears in the Own. cert. field.
3. Double-click the *Distinguished Name*. The certificate appears in the lower section of the screen.
4. Choose *Certificate → Export*. The *Export Certificate* dialog appears.
5. Save the certificate to a file. Use *DER* encoding or base 64, and the extension *.crt. For example, *abapduetserver.crt*.

Import the Certificate from mySAP ERP into the Duet Server Host

You need to configure the Duet server host to accept assertion logon tickets issued from mySAP ERP system.

You perform this task in the Duet server environment.

To import the certificate from the SAP Web AS ABAP system:

1. Start the Visual Admin Console, using the file, *go.bat*, located in the path: *<SAPJ2EEngine_installation>\j2ee\admin\>*
2. In the *Visual Admin* window, choose *Server→ Services →Key Storage*.
3. From the *Runtime* tab, choose *Ticket Keystore* view, and then select *Load to import* the certificate from the certificate file. For example, *abapduetserver.crt*.

   Note: Specify the pathname of the certificate file you saved in the host of mySAP ERP. You can map a drive to the host of mySAP REP from the Duet server host.

   The certificate is stored in the selected view as a CERTIFICATE entry.
4. Maintain the logon ticket access control list in the options for the login module *EvaluateAssertionTicketLoginModule*:
   a. Go to Visual Admin → Services → Security Provider →User Management.
   b. Choose *Manage Security Stores*.
   c. Make sure the UME User Store is selected as the user store.

d. Select the *EvaluateAssertionTicketLoginModule* entry and choose *View* / *Change Properties*.

e. Under *Options*, enter the following for the host that issued the logon ticket to be accepted by the Duet server:

Name	**Value**
trustedsys1	Enter the system ID of the mySAP ERP system and the client number. The following is the format: <*SID*>, <*Client*> For example: *ABC*,*005* Where the system ID is ABC and the client number is *005*. **Note**: Add the value, *trustedsys<x>,* for each SAP system. Where <x> is a number to help differentiate between the options. For example, to configure the Duet server to trust three SAP systems, add the value three times, one for each SAP system: *trustedsys2, trustedsys3, trustedsys4.*
trustediss1	Enter the Distinguished Name of the issuer of the ticket-issuing system's public-key certificate. The following is the format: *<Issuer's_Distinguished_Name>* For example: *CN=ABC,OU=OSP,O=SAP Web AS* **Note**: Add the value, *trustediss<x>,* for each SAP system. Where <x> is a number to help differentiate between the two options. For example, to configure the Duet Add-on to trust three SAP systems, add the value three times, one for each SAP system: *trustediss2 ,trustediss3, trustediss4.*

trusteddn1	Enter the Distinguished Name of the ticket-issuing system. The following is the format: *<System's_Distinguished_Name>* If the ticket-issuing system uses a self-signed certificate, then these two Distinguished Names are identical. Also, the corresponding public-key certificate must exist in the *SAPLogonTicket keystore* view entry. For example: *CN=ABC,OU=OSP,O=SAP Web AS* **Note**: Add the value *trusteddn<x>,* for each SAP system. Where <x> is a number to help differentiate between the two options. For example, to configure the Duet Add-on to trust three SAP systems, add the value three times, one for each SAP system: *trusteddn2, trusteddn3, trusteddn4*.
ume.configuration.active	true

For more information on configuring logon tickets, go to SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 2004 → SAP Library → SAP NetWeaver→Security → User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms → Using Logon Tickets for Single Sign-On → Configuring the Use of Logon Tickets → Configuring the J2EE Engine to Accept Logon Tickets*.

Trust Configuration Checklist

The following is a checklist to help you verify the trust configuration tasks:

Check (√)	**Task**
	Configure trust between each Duet Add-On host and the Duet server.
	Issue and import a certificate from the SAP system into the Duet Add-On host.
	Configure trust between each Duet Add-On host and the specific SAP system to which it connects.
	Issue a certificate from the Duet Add-On. Later, you import it into the SAP system to which it connects.
	Configure Trust between the Duet server host and mySAP ERP System

Configuring the Duet Business Applications Environment

You must configure the environment for running the Duet business applications. The following is the sequence of the configuration tasks:

1. Configure client access to the resources for the business applications.
2. Manually publish the metadata for the business applications.
3. Configure the Authorization Manager (AzMan).
4. Configure client computer for Duet business applications.
5. Create the distribution package for installation the Duet business applications.

Configuring Access to Duet Business Applications Resources

You can configure access to the resources for running Duet business applications, by sharing the folder …*\DuetCode*, in the Duet Metadata Service host.

Client computers can access the resources for business applications using one of the following:

- Directly from the file system of the Duet Metadata Service host.
- Through a URL address

After installing the Duet business applications, you must configure the "*Service Provider category,*" using the Duet System Management tool, to allow clients to read from the shared folder.

See the section "*Configuring and Editing Properties of Duet Components*" in the *Duet for Microsoft Office and SAP; Duet SAP Administration Guide* on Service Market Place at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

Configuring Client Access to the Resources for Duet Business Applications through URL

To configure clients to access the resources for business applications using URL:

1. From the file system of the host of the Duet Metadata Service host, select the folder,*\DuetCode*.
2. Right click the selected folder, and select *Properties*.
3. Select the tab, *Web Sharing*, and select *Share this folder*.

4. Select *Edit Properties*, and under *Access permissions*, select the following:
    - Directory browsing
    - Read
5. Click *OK* twice to the close the *Edit*, and the *Properties* dialog boxes.

Publishing the Metadata for Duet Business Applications

You manually publish the metadata for the Duet business applications from the Duet Metadata Service host.

To publish metadata, you use the metadata publishing tool in the folder: *C:\Inetpub\DuetServiceProvider\bin*

To publish the metadata for the Duet business applications:

1. From the Duet Metadata Service host, find the XML file *DuetMetadata.xml*, in the folder: *C:\Duetmetadata*
2. At the command line, change directory to folder: *C:\Inetpub\DuetServiceProvider\bin*
3. Type the following:

    Microsoft.Duet.Tools.DeployMetadata.exe copyftos C:\Duetmetadata\DuetMetadata.xml

Configuring the Authorization Manager

Configure the Authorization Manager (AzMan) for Duet. Configuring AzMan consists of the following:

- Configure Authentication for AzMan Service through IIS
- Define in AzMan, permissions for the Windows administrator user that runs Windows services installed for SAP.
- Synchronize the roles between Duet business applications and mySAP ERP systems.

Configuring Authentication for AzMan Service through IIS

You must configure the AzMan service to use basic authentication in the Internet Information Server (IIS), on the Duet Metadata Service host.

To configure basic authentication for AzMan service:

1. From the *Start menu → Settings → Control Panel → Administrative tools → Internet Information Services*. The *Internet Information Services* window opens.
2. Under *Internet Information Services*, expand the computer host name and click *Web Sites*.

3. Right-click *Duet AzMan Service* and select *Properties*.
4. Select *Directory Security* tab, and choose *Edit* in the *Authentication and access control* panel.
    - Do not select *Enable anonymous access.* Make sure that this option is not selected.
    - Select *Basic authentication* under *Authenticated access*.
5. Choose *OK*.

Defining Permissions for the Administrator User in the Authorization Manager

After configuring authentication for the AzMan service in the Duet Metadata Service host, you must define permissions for the administrator user that runs SAP services, in the Authority Manager (AzMan).

To define permissions for the administrator user:

1. From the *Start* menu, select *Run*, and then type *AzMan.msc*.
2. Right-click *Authorization Manager*, and select *Open Authorization Store*.
3. For the authorization store type, click XML file, and type the full path to the Information Bridge authorization store, *Microsoft.InformationBridge.Roles.xml*.

    For example, *C:\Inetpub\azRoles\Microsoft.InformationBridge.Roles.xml*.
4. Click *OK*, and expand *Microsoft.InformationBridge.Roles.xml file → Microsoft Information Bridge Framework Metadata Service → Role Assignments → Administrators*
5. Right-click the role administrators and assign the administrator user that runs SAP services in Windows. For example, *SAPService<SID>*.

    Note: You can assign the entire Administrators Group if the user is part of this group.

Define and Map Roles from mySAP ERP to Roles in Business Applications

Mapping the default roles of the Duet business applications to roles in mySAP ERP involves the following:

- Obtain the details of the roles in mySAP ERP system.
- Map the default roles of the Duet business applications, and the roles in mySAP ERP.

Gathering Information about Roles

The table below describes the roles in mySAP ERP system:

Role	**Explanation**
mySAP ERP system	Obtain the roles from the specific mySAP ERP system. The administrator of mySAP ERP created the relevant roles. ERP roles in Duet have the following format: *ERPname.ClientID.Role* For example: *OSS.201.EMP*

You map the default roles of the Duet business applications to roles in mySAP ERP using the *Define SAP System* wizard available in the *Duet Administration Control Panel*.

In addition, you can connect a single Duet Add-On host to several SAP systems using the wizard.

To define and map roles between business applications and mySAP ERP:

1. Start the *Duet Administration Control Panel* using the following URL: *http://<Duet Server Host Name>:<J2EE HTTP PORT> /webdynpro/dispatcher/sap.com/xapps~osp~fw~admin~launchpad~webdynpro /AdminLaunchpadApp*

   Where *<Duet Server Host Name>:<J2EE HTTP PORT>* refers to the host name of the Duet Server and the port number of the J2EE engine.
2. Enter the administrator credentials for the SAP J2EE on which the Duet server runs.
3. From the *Duet Administration Control Panel*, select *Define SAP System.*
4. In the *Connection Details* screen, enter the connection settings to a specific SAP system (this is the SAP system you intend to enable for Duet):

Property	**Description**
System Name	Specify the system ID of the mySAP ERP system to connect to.
Client	Specify the client number to connect to.
Host	Specify the host name of the SAP system. For example, *duetsys.sap.com*
Port	Specify the port number of the SAP system you want to connect to.
Number	Specify the system number in the SAP system to connect to. For example, *77*.
Loading balancing	You can choose *Yes* or *No*. Choose *Yes*, and enter the settings for the Message server. Choose *No*, if there is no Message server in the SAP system landscape.

Message Server Host	Specify the host name of the SAP system. For example, *U9Cmain.duet.sap.com*.
Message Server Port	Specify the port number of the Message server you want to connect to.
Logon Group	Specify the group and server to logon to.

5. Choose *Next*, the *Map Role* screen displays:

Property	**Description**
System Name	Specify the system ID of the mySAP ERP system to connect to.
Role Name	Specify the name of the role in the SAP system.
Synchronized	Select *Synchronized*. **Note**: Always select Synchronized to enable synchronization between the roles from the SAP system and the business application roles.

   Specify the name of the role in the SAP system, and choose *Add Role*. The table on the left displays a list of the specified roles in the SAP system.

   Note: You can add several roles that exist in the SAP system one after the other.

6. Select an SAP system role from the table on the left, and from the table on the right, select the default business application roles to map to the selected SAP system role.

   Note: You can select several business applications roles, and enable role synchronization for them.

   The following is an example of the mapped roles between the business applications and the roles from the specified mySAP ERP system.

Mapped ERP or Portal Roles	**Application role**
QEF.801.ZMANAGER_SELF_SERVICE	BudgetMonitoring.Manager
QEF.801.ZMANAGER_SELF_SERVICE	TeamManagement.Manager
QEF.801.ZESS	ALL.USERS
QEF.801.ZMANAGER_SELF_SERVICE	ALL.USERS

7. Choose *Next*, the Business Applications screen displays.
8. Select the Duet business applications with their roles mapped to the roles in mySAP ERP system.

   Note: Make sure that you install the appropriate support package required by the selected business applications in mySAP ERP system.

9. Choose *Finish*.

10. Choose *Define Add-On*, and enter the following:

Property	Description
Host	Specify the host name of the SAP Web AS Java system on top of which the Duet Add-On runs. For example, *il9duet.sap.com*
Port	Specify the http port number of the SAP Web AS Java system on which the Duet server runs. For example, *50000*.
SSL Port	Specify the SSL (https) port number of the SAP Web AS Java system on which the Duet server runs. For example, *50004*.
Host	Specify the host name of the SAP Web AS ABAP system. The host name is the same if you do not have SAP Web AS ABAP system installed. For example, *il9duet.sap.com*
Port	Specify the http port number of the SAP Web AS ABAP system. The port number is the same if you do not have SAP Web AS ABAP system installed. For example, *50004*.

11. From the list of SAP system IDs, select the SAP system you want the Duet Add-On to connect to, and choose *Apply*.
12. Repeat step 10 and 11 to connect several SAP systems to the Duet Add-On.

Synchronizing Roles between Duet Business Applications and mySAP ERP

1. Start the Duet Administration Control Panel using the following URL:

   http://<Duet Server Host Name>:<J2EE HTTP PORT>/webdynpro/dispatcher/sap.com/xapps~osp~fw~admin~launchpad~webdynpro/AdminLaunchpadApp

   Where *<Duet Server Host Name>:<J2EE HTTP PORT>* refers to the host name of the Duet Server and the port number of the J2EE engine.
2. Enter the administrator credentials for the SAP J2EE on which the Duet server runs.
3. From the *Duet Administration Control Panel → Duet System Management*, select *Role Management*.
4. Click *Activate ERP Role Synchronization* to automate the configuration of roles between Duet business applications and mySAP ERP system.

   Note: If users do not have the same user ID in Windows and mySAP ERP, you must configure user mapping data in the Duet Server environment before activating Role Synchronization.

5. Choose *Copy Role Assignments to AzMan* to copy the assigned roles in the UME in the same host as the Duet server to the Authorization Manager (AzMan) in the Duet Metadata host.

For more information on user mapping data configuration, see the section "*Configuring User Mapping Data in the User Management Engine*" in the *Duet for Microsoft Office and SAP; Duet SAP Administration Guide* on Service Market Place at: *service.sap.com/instguides → SAP xApps → Duet → Duet 1.0*

Configuring the Client Computer

The following is the workflow for configuring the Duet Metadata Service host for the Duet business applications:

1. Install the Duet client components from Microsoft.

   You can find documentation for Duet components from Microsoft, in the installation folder: *...\Microsoft\Documentation*
   Note: Make sure that you configure the URL for the *DuetReadService* components, during the client setup.

2. Configure authentication for clients.

Requirement

- You have an existing Exchange Mail Profile.
- You have adjusted daylight saving in the Time Zone for the clients, where daylight saving is applicable.

Installing the Duet Client Components from Microsoft

You can find documentation for installing Duet client components from Microsoft, in the installation folder: *...\Microsoft\Documentation.*

Configuring Client Authentication to Use Kerberos

Authentication of clients' request using Kerberos protocol involves the client, the J2EE Engine and the Kerberos KDC.

To enable authentication of a client request to the SAP Web AS Java using Kerberos, you must configure the client.

For more information about configuring clients to use Kerberos authentication, go to the SAP Help Portal at: *help.sap.com → Documentation → SAP NetWeaver → SAP Library → SAP NetWeaver → Security → User Authentication and Single Sign-On → Authentication on the J2EE Engine → Configuring Authentication Mechanisms → Using Kerberos Authentication for Single Sign-On → J2EE Engine Configuration → Configuring the UME → Configuring the UME when Using Non-ADS Data Sources*

→ *SPNegoLoginModule Configuration Options →Accessing J2EE Engine with Kerberos Authentication*.

Settings of Duet Business Applications

You must configure mySAP ERP system to work with Duet.

- Make sure that you install in mySAP ERP system, the required support packages for configuring Duet.
- From the specific mySAP ERP environment, set and optionally customize the default settings for the business applications.

For more information, see the section "*Configuring mySAP ERP for Duet Business Applications*" in the *Duet for Microsoft Office and SAP; Duet SAP Administration Guide* on Service Market Place at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet1.0*

Post-Installation Checklist

The following is a checklist to help you verify the post-installation configuration tasks:

Check (√)	**Task**
	Configure Access to Duet Business Applications Resources
	Configure Client Access to the Resources for Duet Business Applications through URL
	Publish the Metadata for Duet Business Applications
	Configure the Authorization Manager
	Configure the Client Computer
	Install the Duet Client Components from Microsoft
	Configure Client Authentication to Use Kerberos
	Settings for Duet Business Applications in SAP system

Troubleshooting

This section describes some tips for working around problems that sometimes occur during or after installation.

Domain Name

During installation of the Duet server, the installer requires the Domain Name (DNS).

- To get the DNS (on Windows and UNIX), use the following at the command line: *nslookup IP_ADDRESS*

  Where IP_ADDRESS is the IP address of the computer for which you want the DNS name.
- Alternatively, on Windows only use: *Ipconfig IP_ADDRESS*
  The command usually returns the DNS suffix.

Using Host Name to Reference Shared Folders

Problem

You are prompted to provide a user and a password if you attempt to access the shared folders for Duet using the fully qualified domain name.

Cause

Some systems are configured such that you can connect to them using host name, and not the Fully Qualified Domain Name (FQDN).

The following is an example of a FQDN: *\\duethost01.msft.sap.mendocino*

Solution

Change the FQDN to the host name. Using the example above, the host name will be: *\\duethost01*, and not *\\duethost01.msft.sap.mendocino*.

Language Settings in Client Computers

Verify that you can view the date of a file by selecting the properties of the file in the client computer in which you are running Duet business applications.

If you cannot read the date of the selected, you must configure the regional settings of the computer:

1. From *Start* → *Setting* → *Control panel* → *Regional and Language Options*
2. Select any language other than English (United States) and click *OK*.
3. Open *Regional* and *Language Options*, again.
4. Select *English* (*United States*), and click *OK*.

   Make sure that you view the properties of any file you select.

Personalization Error

From the Microsoft Office Outlook, the user may get the following error: `InitializePersonalization Failed`.

Cause

One of the Duet business application metadata files was not deployed to the metadata repository.

Solution

Make sure that you deploy the appropriate Duet business application metadata file, *Default Personalized Data*, into the metadata repository.

Communication Destinations on Duet Add-On

The following error may occur after you test the connection for communication destinations in the Duet Add-On environment: *401 error message*

Solution

1. From the Duet Metadata Service host, open IIS.
2. Expand the host name, and select *Web Site* → *Default Web Site* → *RequestHandler*
3. Right-click *RequestHandler*, and select *Properties*.
4. Select *Directory Security* tab and click *Edit*
    - Make sure that the checkbox *Enable anonymous access* is not selected
    - Make sure that the checkbox *Integrated windows authentication* under *Authenticated access control* is selected.
5. Choose *OK*.
6. From the right hand panel, select *RequestHandler.asmx*
7. Right-click *RequestHandler.asmx* , select *Properties*
8. Select the *File Security* tab and click *Edit*
    - Make sure that the checkbox *Enable anonymous access* is not selected
    - Make sure that the checkbox *basic authentication* under *Authenticated access control* is selected.

SAPinst Aborts during Deployment

SAPinst aborts during deployment of Duet Add-On, and an error message displays.

When you check the log file, *sapinst_dev.log,* it indicates that: *The stub cannot be established*

The following exception is shown in the log file:

```
Caught exception during application startup from SAP J2EE Engine's deploy
service:

java.rmi.RemoteException: Error occurred while starting application
sap.com/xapps/osp/common/enterpriseapp and wait.

Reason: Clusterwide exception: server ID
609155950:com.sap.engine.services.jmsconnector.exceptions.BaseDeploymentE
xception: Naming error.

Caused by:
com.sap.engine.services.jndi.persistent.exceptions.NamingException:
Exception while trying to get InitialContext. [Root exception is
com.sap.engine.services.security.exceptions.BaseLoginException: Cannot
create new RemoteLoginContext instance.]
Caused by:
com.sap.engine.services.rmi_p4.exception.P4BaseConnectionException: The
stub cannot establish connection.
```

Problem:

The problem is that you may be having two SAP Web AS Java Systems (one for the Duet Server and the other for Duet Add-On) with the same brokerId.

Verify as follows:

1. First, open the *Visual Admin* on the Duet server host.
2. Under *Server → Services → P4 provider → Property Tab*
3. Write down the broker ID.
4. Do the same on the Duet Add-On host and compare the broker IDs.

   If the ID is the same for the two J2EE servers, follow the steps in the solution section. The problem is that you may be having two SAP Web AS Java Systems (one for Duet server and the other for Duet Add-On) with the same brokerId.

Solution

1. Stop the J2EE cluster to change the broker id.
2. Use the offline config tool (*offlinecfgeditor.bat*) to delete the following entries:
   - - P4_Persistent
   - - P4_PersistentObject

- cluster_data'server'IDxxxxxxx'services'Propertysheet p4 (for every server ID if the cluster has more than one).

3. After, start the cluster to regenerate the entries with a new broker ID.

Loading Duet Business Applications

Sometimes, after loading two or more Duet business applications, any attempt to load an additional business application produces the following error message:

"*Insufficient system resources exist to complete the requested service*."

Cause

J2EE is holding some of the file handles.

Solution

Make sure that you restart the host in which you are loading the Duet business applications.

Duet Business Applications Resources Fail to Display in Microsoft Office Outlook.

When the resources such as, graphics and icons do not display in the Action Pane in which a business application is running, do the following.

Verify

Open the Event Viewer, and choose Applications in the left panel. Look for the following error:

```
Microsoft.Solutions.InformationWorker.Common.EnterpriseInstrumentation
.Schema.ErrorMessageEvent

{
  String Message =
   Microsoft.InformationBridge.Framework.Interfaces.UIException --->
   Microsoft.InformationBridge.Framework.ExecutionEngine.EngineException:
   The MetadataScope InformationBridge is not available. It might be
   incorrectly defined or you might not have permission to access it.
```

For detailed information about using the Event Viewer in the client, see the Duet™ for Microsoft® Office and SAP®; SAP Operations Guide in Service Market Place at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

Solution

Verify the following:

- If the Request Handler Service is installed on the same host as the Duet Metadata Service, if not install the Request Handler Service.
- If the Request Handler Service is properly installed on the same host as the Duet Metadata Service. If not uninstall and install it.

- If the Request Handler Service is using a different port other than that used by the client. Using the Duet Settings Manager, check that the port defined for the client is the same as the port specified for the Request Handler Service.
- That the host name, or port number of the Duet Metadata Service is defined in the Duet Settings Manager in the client. If not, open the Duet Settings Manager and set the host and the port number of the Duet Metadata Service host.
- You published the metadata for the business applications to the Duet Metadata Service.

The User is Not Authenticated in Microsoft Office Outlook

Where an end user is not authenticated, you get the following error in the Event Viewer on the client:

```
Authentication ticket request failed: The remote server returned an
error: (401) Unauthorized.
```

For detailed information about using the Event Viewer in the client, see the Duet for Microsoft Office and SAP; SAP Operations Guide in Service Market Place at: s*ervice.sap.com/instguides → SAP xApps → Duet→ Duet 1.0*

Solution

Verify the following:

- That the user has been authenticated both on the client and on the Duet server using Kerberos protocol, or X.590 client certificates and SSL.
- That the local time on the client is the same as that of the network.
  a. From *Start* → *Run*, type *cmd*.
  b. At the command prompt type *net time*.
  c. If your local time is different from that of the network time, type *net time /set* to fix it.
- That the proxy is not manually set in your Web browser.
  a. Open *Internet Explorer*, and choose *Tools* → *Internet Options.*
  b. Click *Connections Tab* and select *LAN Settings*.
  c. Make sure that *Automatically detect settings* is checked.

Clients Cannot Get Metadata and Access Duet Read Service

In some cases where you have Microsoft Internet Information Service (IIS) and SAP Web AS Java system running in the same computer, you are prompted for your user credentials several times when you attempt to call the URL: *http://duet_server:<ReadServicePort>/DuetReadService.asmx*

In this case, the client running Duet cannot get metadata and access the Duet Read Service.

Solution

Go to: *http://support.microsoft.com/?id=871179*, and follow the instructions in the section, WORKAROUND.

Failed to Run Duet Administration Control Panel in the Browser

When any of the administration tools, including the Duet Administration Control Panel fail to run in the browser, you get errors similar to the following:.

```
Application error occurred during request processing.
com.sap.tc.webdynpro.services.sal.api.WDDispatcherException: Requested
deployable object 'sap.com/xapps~osp~fw~systemadmin~ui~webdynpro' and
application 'SystemAdminUiFrameworkApp2' are not deployed on the server.
Please check the used URL.

Exception id: [0050569F0AF20047000000BF00000D100004136E89C5D0AD]
```

Solution

- Verify that you loading the Duet Administration Control and the administration tools on the host of the Duet server, as some of the applications exist only on the Duet Server, or only on the Duet Add-On host.
- Verify that the applications that run the administration tools have been deployed.
- If you encounter this error after restarting the J2EE server, it may be that the J2EE engine loads the applications for the administration tools before loading the WebDynpro engine on which the applications tools run.
  a. Log on to the Visual Admin: *<SAPJ2EEEngine_installation>\j2ee\admin\go.bat*
  b. Go to *cluster tab → Server → Services → Deploy Service*.
  c. Choose *Applications*, and verify that all the applications starting with, *sap.com/xapps~osp*, have been checked. If any application has not been selected, select it.
  d. Select *Start Application*.

Duet Durable Message Driven Bean Errors

When you receive Message Driven Bean (MDB) errors in the Log Viewer on either the Duet server or the Duet Add-On, they are caused by a problem in the J2EE engine.

Cause

After redeploying archive files, and you attempt to restart, the old MDB still exists in the J2EE engine leading to exceptions, that start with:

```
Caught exception during application startup from SAP J2EE Engine's deploy
service.
```

Solution

See SAP note number **910959**; it describes how to solve the problem.

SAPInst Error

SAPInst may produce errors about non-existing destinations, and non-existing MDB, and non-existing WebDynpro.

You can see these errors in the SAPInst summary file, which is usually located in:
C:\Program Files\sapinst_instdir\summary.html

Solution

Check if you specified the correct value in SAPInst for the host of the Duet server. If this is not correct, you must remove the incomplete installation and reinstall Duet server again.

Errors When Running the Application Installer

You may receive errors that start with any of the following exceptions while running the Applications Installer:

- *IOException: Invalid permission*

  Probably, you did not create the following folders: *DuetMetadata* and *DuetCode* on the host of the Duet Metadata Service.

  Verify that you have created these folders. See "*Creating New Folders in the Duet Metadata Service Host*" on page 38.

- *No template is found*

  Probably, you failed to install the files in the specified sequence. See "*Loading Metadata for Duet Business Applications*" on page 41.

- *IOException: Directory not found*

  Probably, you failed to define the *DLL Write path*, or you did not specify the host name of the Duet Metadata Service component from Microsoft using the Duet System Management tool.

  See "*Creating New Folders in the Duet Metadata Service Host*" on page 38.

- *Insufficient system resources*

  Restart the SAP Web AS Java system on which the Duet server runs.

Errors During Installation of the Request Handler Service

During the installation of the Request Handler Service, you may get the following error:

```
The designated account credentials could not be authenticated.
```

Solution

Make sure that you have specified the correct port number of the Microsoft Exchange Server. The default port is 1080. For example: *metadataservice.duet.sap.microsoft:1080*.

Internet Explorer Fails to Request a New Kerberos Token on Windows XP SP2

The Internet Explorer browser sends NTLM token after Kerberos token expiration. The browser must request a new Kerberos token but fails to get it due to Microsoft bug for Windows XP SP2 workstation.

Solution

Read SAP Note number 934138, as it provides more explanation and what to do.

Testing Connections Between Duet Add-On and mySAP ERP System

After deploying the Duet Add-On components in the same environment as mySAP ERP, you can perform some basic tests to check your connectivity to the specific mySAP ERP system.

Requirements

- You have performed all the required post installation configurations in the Duet Add-On environment.
- You have prepared the specific mySAP ERP system for use with Duet.
- You have an ABAP user ID and password.

There are two tests for checking connectivity between the Duet Add-On and mySAP ERP system:

- Test the connections of the ESA services deployed on Duet Add-On to mySAP ERP.
- Test the connections of JCO from Duet Add-On to mySAP ERP.

Testing Connections of ESA Services to mySAP ERP System

You test connections of the ESA services to mySAP ERP from the host of the Duet Add-On, using the Visual Admin Console of the SAP Web AS Java system.

To test the connections of the ESA services to mySAP ERP:

1. Using the ABAP user ID and password, log on to the *Visual Admin*: *<SAPJ2EEEngine_installation>\j2ee\admin\go.bat*
2. Go to *Cluster Tab → Server → Services → Destinations*
3. Under *Runtime,* select Web service. A list of all the Web Services destinations in the SAP Web AS Java system displays.
4. Select a Web service proxy and choose the correct authentication method.

   Note: In case of basic authentication, you must provide the user name and password.
5. Click Save and Test. If the message shows HTTP response 500, the test is successful.

Testing Connections of JCO to mySAP ERP System

You test connections of the JCO to mySAP ERP from the host of the Duet Add-On, using the Visual Admin Console of the SAP Web AS Java system.

To test JCO connections to mySAP ERP system:

1. Using the ABAP user ID and password, log on to the *Visual Admin*: *<SAPJ2EEEngine_installation>\j2ee\admin\go.bat*
2. Go to *Cluster Tab → Server → Services → Destinations*
3. Under *Runtime,* select *RFC* and select the RFC destinations that do not contain the word TICKET as a suffix. For example, *OSP/OSS/001*.
4. Choose the correct authentication method:

   Note: In case of basic authentication, you must provide the user name and password.
5. Click *Save* and *Test*. The message, "*Successfully connected system <SYS name> as user <user ID>*" displays.