**System Landscape Directory**

**Last Modified: Juni 14, 2023**

[1 Introduction 2](#_Toc137661226)

[1.1 Displaying Systems and Testing Connections 2](#_Toc137661227)

[1.2 Creating Systems 2](#_Toc137661228)

[1.3 Upgrading Systems 2](#_Toc137661229)

[1.4 Editing Systems in SLD 3](#_Toc137661230)

[1.5 Deleting and Copying Systems 3](#_Toc137661231)

[1.6 Entering System Type Property Values 3](#_Toc137661232)

[1.7 Exporting SLD Systems 3](#_Toc137661233)

[1.8 Importing SLD Systems 4](#_Toc137661234)

[1.9 Creating Categories and Assigning Systems 5](#_Toc137661235)

[2 SAP Business One 5](#_Toc137661236)

[2.1 Configuring SAP Business One in SLD 5](#_Toc137661237)

[2.1.1 Defining Common Fields 6](#_Toc137661238)

[2.1.2 OIDC Registration 6](#_Toc137661239)

[2.1.2.1 Access Token Sync Scenario 7](#_Toc137661240)

[2.1.3 Connecting to SAP Business One DI API 7](#_Toc137661241)

[2.1.4 Connecting to Service Layer of SAP Business One 9](#_Toc137661242)

[2.1.5 Connecting to SAP Business One Using JDBC 9](#_Toc137661243)

[2.2 Using a Proxy Group for the DI Adapter 10](#_Toc137661244)

[2.2.1 Providing More Proxy Instances in the Operating System 10](#_Toc137661245)

[2.2.2 Defining Proxy Groups in DI Adapter 10](#_Toc137661246)

[3 SAP ERP 12](#_Toc137661247)

[3.1 Configuring the RFCA Connection 12](#_Toc137661248)

[3.2 Configuring the RFCP Connection 13](#_Toc137661249)

[3.3 Providing SNC Parameters for Secure RFC Communication 14](#_Toc137661250)

[4 File System 16](#_Toc137661251)

[4.1 Configuring File Inbound 16](#_Toc137661252)

[4.2 Configuring File Outbound 17](#_Toc137661253)

[5 HTTP System 18](#_Toc137661254)

[5.1 Configuring HTTP Outbound (HTTA) 18](#_Toc137661255)

[5.2 Configuring HTTP Inbound (HTTP) 19](#_Toc137661256)

[6 Web Service 20](#_Toc137661257)

[6.1 Configuring the WSAS and WSAN Connections 20](#_Toc137661258)

[6.2 Configuring the WSAR Connection 21](#_Toc137661259)

[7 Connecting to Databases 22](#_Toc137661260)

[8 FTP System 23](#_Toc137661261)

[8.1 Configuring FTP Outbound 23](#_Toc137661262)

[8.2 Configuring FTP Inbound 24](#_Toc137661263)

[9 E-Mail System 25](#_Toc137661264)

[9.1 Sending E-Mails 25](#_Toc137661265)

[9.2 Receiving E-Mails 26](#_Toc137661266)

[10 Scheduler 26](#_Toc137661267)

[11 Displaying and Enhancing System Type Properties 27](#_Toc137661268)

[Copyrights, Trademarks, and Disclaimers 29](#_Toc137661269)

# 1 Introduction

The System Landscape Directory (SLD) is the central place to administer all systems and their connections of your system landscape that you want to connect with each other.

Each SLD system has a system type (SysType), and for each system type, you define parameters and connectivity options. For some scenario packages, SLD entries are delivered. You can identify systems delivered by SAP by the sap string that is part of the system identifier.

**Example**

An SAP Business One system has the following connectivity options:

* B1DI Connecting to SAP Business One through the SAP Business One DI API
* B1SL Connection to SAP Business One through Service Layer
* JDBC Connecting to SAP Business One database

## 1.1 Displaying Systems and Testing Connections

**Procedure**

1. To display technical connection parameters, choose SLD and click a system in the navigation area.
2. To test the connection, click Test Connection in each connectivity section.

## 1.2 Creating Systems

**Procedure**

1. To add a system to SLD, choose SLD, select the B1i Server entry or a category, right-click to open the context menu and select Create System.
2. In the System Type field, select a system type (SysType).
3. In the *System Name* field, enter a unique name and click Create.

**Results**

You are in edit mode.

## 1.3 Upgrading Systems

**Procedure**

1. To upgrade a system type to a higher version, choose SLD, select the system in the navigation area, right-click and select *Upgrade System*.
2. In the *Upgrade to System Type* field, select the system type and click Upgrade.

**Results**

The upgrade does not have impact on active scenario packages. The connection parameters of the system are unchanged.

## 1.4 Editing Systems in SLD

**Procedure**

1. To change system parameters, choose SLD, and click the system in the navigation area.
2. Click Edit, change the parameters and click Save.

## 1.5 Deleting and Copying Systems

**Procedure**

1. To delete a system from SLD, choose SLD, select the system in the navigation area, right-click to open the context menu and select Delete.
2. To copy a system entry, select Copy from the context menu. SLD creates a copy\_<system-name> entry.
3. Rename the system copy and change parameters accordingly.

## 1.6 Entering System Type Property Values

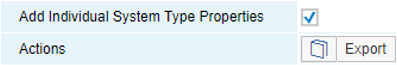
With system type properties, you can define a role for a system type.

**Procedure**

1. To enter values for system type properties, choose SLD, select the system in the navigation area and click Properties.
2. Enter or select values and click Save.

## 1.7 Exporting SLD Systems

With the export function, you can export all systems from SLD. The function creates the iae\_sld\_exporter.zip file. You have the option to add individual system type property definitions and values to the export.



**Procedure**

1. To export all systems from SDL, select B1i Server in the navigation area, right-click to open the context menu and select Export.
2. To add individual system type property definitions and values, select the checkbox.
3. To export all SLD systems, click Export.

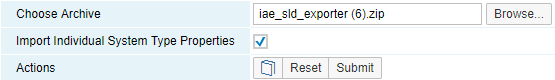
The SLD creates the iae\_sld\_exporter.zip file.

**Result**

You can import the file to another SLD.

## 1.8 Importing SLD Systems

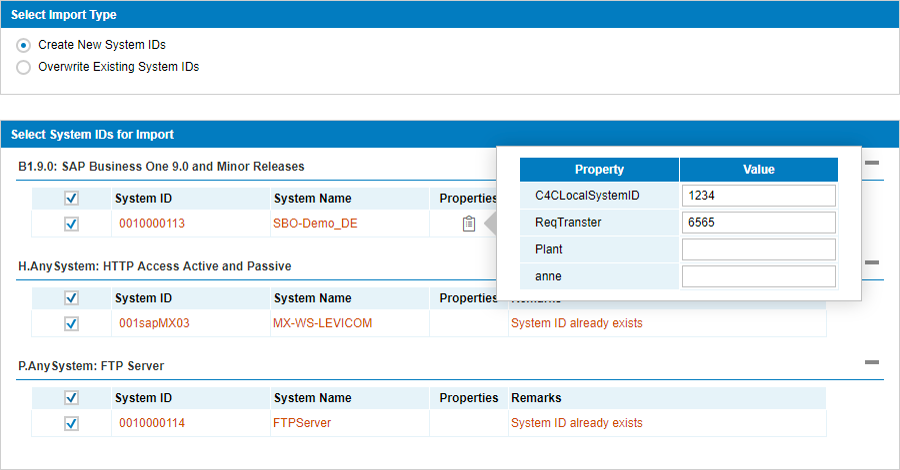
You can only import SLD systems exported from another SLD with the SLD export function.



**Procedure**

1. To import SLD systems exported from another SLD, select B1i Server in the navigation area, right-click to open the context menu, select Import, and choose the archive.
2. To import individual system type property definitions and values, select the checkbox.
3. To start import, click Submit.

The integration framework displays the import preview:



The SLD displays the systems available in the import archive grouped by system type. For each system type, the SLD displays the system ID, name, system type properties and some remarks.

1. You can deselect system types or dedicated systems to exclude them from import.
2. For import, click Create new System IDs to create new system IDs or select Overwrite Existing SystemIDs to overwrite already existing system IDs.

If you select the option to overwrite existing system IDs, consider system IDs used in activate scenarios. For SAP Business One systems, check and adjust the event sender setup.

1. The SLD encrypts passwords depending on the machine. If you import systems into an SLD running on another machine, open the new system entries and enter the passwords.

## 1.9 Creating Categories and Assigning Systems

Using categories, you can group your SLD systems.

**Procedure**

1. To create a category, select the B1i Server entry in the navigation area, right-click to open the context menu and select Create Category.
2. In the Category Name field, enter the category and click Create.

The SLD adds the category to the navigation area. Categories appear in alphabetical order.

1. To assign a system to a category, select the system in the navigation area and drag and drop it to a category.
2. To change the assignment of a system to a category, select the system in the navigation area, right-click to open the context menu, select Change Category and select the new category.
3. To remove a system from a category, select the B1i Server entry in the Change Category user interface.
4. You can only delete categories that have no systems assigned.

# 2 SAP Business One

## 2.1 Configuring SAP Business One in SLD

A system type is available for each SAP Business One (B1) major release:

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| B1.2004 | Connection to an SAP Business One 2004 system |
| B1.2005 | Connection to an SAP Business One 2005 system |
| B1.2007 | Connection to an SAP Business One 2007system |
| B1.8.8 | Connection to an SAP Business One 8.8 system |
| B1.9.0 | Connection to an SAP Business One 9.0 system  (Available in the integration framework for SAP Business One and in SAP Business One 9.0 integration for SAP NetWeaver) |
| B1.10.0 | Connection to an SAP Business One 10.0 system  (Available in the integration framework for SAP Business One and in SAP Business One 9.0 integration for SAP NetWeaver) |
| B1.Generic | Connection to a generic SAP Business One system where the version information is not relevant. |

note.gif NOTE

Note that the version provided in SLD is valid for the major and all minor releases.

To define, for example, an SAP Business One 9.3 system, select the B1 9.0 version.

You have the option to interact with SAP Business One using the SAP Business One DI API, the service layer of SAP Business One or directly connecting to the database using JDBC for read access.

### 2.1.1 Defining Common Fields

Common fields are relevant for all connectivity types. If you change a value, the SLD changes it for all connectivity types and additionally in the JDBC URL.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| b1Server | Enter the IP address or logical name of the SAP Business One server. To enter an instance, use the following pattern: <IP address or logical name>\<instance name>  To connect to SAP HANA 2.0, enter the information in the following way:  <tenant database>@<ip address or logical name>:<port>  note.gif NOTE  The string must be identical with the string in the EventSender setup for the SAP Business One system. If you use, for example, a logical name in the EventSender, enter the logical name here. The value comparison is case-sensitive.  If you use the *associatedSrvIP* parameter for a HTTP (section 4.4) or a Web service system (section 4.5) to associate an incoming call to an SAP Business One system, ensure that both parameters are identical. |
| Company | Enter the technical name of the company database (instance) of SAP Business One |
| companyId | The company ID is automatically generated by the sap.B1oidcSync scenario after the OIDC setting is registered. See 2.1.2.1 Access Token Sync Scenario below.  note.gif NOTE  If you choose not to use the OIDC option, keep this field empty. |
| accessToken | The access token is automatically generated by the sap.B1oidcSync scenario after the OIDC setting is registered. See 2.1.2.1 Access Token Sync Scenario below.  note.gif NOTE  If you choose not to use the OIDC option, keep this field empty. |

### 2.1.2 OIDC Registration

OpenID Connect (OIDC) 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User, based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User. With OpenID Connect, you can easily and securely log in and connect to B1 DIAPI and the Service Layer without a username and password. It is a key technology for enabling secure and seamless authentication.

note.gif NOTE

OIDC is only available for two system types: *B1 10.0* and *B1 Generic*.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| SLDServer | Enter the SAP Business One SLD server information. Enter the IP address or the host name, followed by a colon and the port number. The default port number of the SAP Business One SLD server is 40000.  note.gif NOTE  You must use the same attribute, IP address or host name, as you used in the SLD server login configuration. |
| SLDLoginUserAccount | Enter the user of theSAP Business One SLD server login |
| SLDLoginPassword | Enter the password of theSAP Business One SLD server login |
| LinkToIntegrationFramework | Enter an accessible link of the Integration Framework |
| ComponentName | Enter a unique component name |
| CertificatePassword | Enter the user-defined password for the creating certificate |

Choose the *Register* button and all other data will be populated automatically, including the component ID:

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| ComponentID | Enter the componet ID if you already have one from the same SLD server.  If you leave this field empty, you will get a new component ID from the SLD server, to be used for all company databases on this server. |
| ClientID | Displays the client ID |
| TokenEndpoint | Displays the link of the token endpoint |
| ServiceUnitID | Displays the service unit ID |
| Certificate | Displays the certificate |

note.gif NOTE

If you have several company databases on the same SLD server, use the same component ID to register all of the company databases.

#### 2.1.2.1 Access Token Sync Scenario

Once the component ID is populated in the OIDC fields, go to *SCENARIOS* 🡪 *Control* and activate the *sap.B1oidcSync* scenario. Select the checkbox next to the *sap.B1oidcSync* scenario, and then in the *Scenario Setup Result* window, choose the *Activate* button. This scenario will synchronize the access token and the company ID.  
  
The default time trigger for this access token synchronization is 5 minutes. If you would like to change this time interval, you can choose the *Setup* button for the *sap.B1oidcSync* scenario. In the *Scenario Package Setup* window, choose the time setting icon, and in the *Scenario Setup – Timer Settings* window, you can set the time intervals.

note.gif NOTE

When B1i is installed or upgraded, the *sap.B1oidcSync* scenario is deactivated by default, so if you choose to use the OIDC registration, you need to manually activate the scenario as described above.

### 2.1.3 Connecting to SAP Business One DI API

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| b1Server | SLD displays the name you provided in the *Common Fields* section. |
| licenseServer | Enter information about the license service of SAP Business One. Enter the IP address; followed by a colon and the port number where the license service is available, usually this is the 30000 port. Ensure that the service and a license are available. If you leave the field empty, the integration framework adds the information obtained through the sldServer setting. |
| sldServer | Enter the SAP Business One SLD server information. Enter the IP address or logical name, followed by a colon and the port. The default port of the SAP Business One SLD server is 40000. |
| Company | SLD displays the name you provided in the *Common Fields* section. |
| dbType | Select the database system, that SAP Business One uses, either a Microsoft SQL Server version or SAP HANA. |
| dbUser | Enter the user for accessing the company database using the database connection. |
| dbPassword | Enter the password for database login. |
| Username, password | Enter the user name of the technical user that retrieves and posts integration data in SAP Business One. The default user is B1i. It must be available in the SAP Business One company.  The B1i user needs to be assigned the indirect access license B1iINDIRECT\_MSS and the user license B1i.  This user may not perform normal operations in the SAP Business One system. The integration framework filters messages based on this specific user to avoid endless loops of messages.  For more information about how to configure the B1 inbound filter, see the *Configuring the B1 Event Filter* section |
| language | Select the language for SAP Business One login. If you leave the field empty, the integration framework uses the SAP Business One default language setting. |
| isTrust | Select, if you want a trusted connection to SAP Business One. If you set the value to true, the integration framework uses the Microsoft Windows trusted database logon instead of the *dbUser* and *dbPassword* values. We recommend selecting false and providing *dbUser* and *dbPassword* entries. |
| jcoPath | You can centrally provide the Jco path in the DI proxy property file for each SAP Business One server. We recommend the approach as it is less error prone. If you follow the approach, leave the field empty.  The DI API version must be exactly the same version as your SAP Business One application. |
| diProxyhost | Enter the IP address or logical name of the server where the DI proxy runs.  The integration framework provides the technical DI adapter, consisting of the DI adapter control part and the DI adapter proxy part. The DI adapter runs locally on the SAP Business One server. The control part runs on the integration server. |
| diProxyport | Enter the port where the DI proxy listens. 2099 is the default port. If this port is occupied on the SAP Business One server, you can use any port. Make sure to also define the port number in the configuration file for the DI proxy. |
| proxyHost | Enter the IP address of a HTTP proxy server, if a proxy server is required in your network for connecting to the SAP Business One server. Leave the field empty, if a proxy is not required. |
| proxyPort | Enter the port number, if a proxy is required. Leave the field empty, if a proxy is not required. |

### 2.1.4 Connecting to Service Layer of SAP Business One

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| b1Server | SLD displays the name you provided in the *Common Fields* section. |
| Company | SLD displays the name you provided in the *Common Fields* section. |
| destProtocol | Select http or https. |
| destHost | Enter the name or IP address of the machine where the service layer is installed. |
| destPort | Enter the port of the machine where the service layer is installed. The default port is 50000. |
| destPath | Enter the destination path. The default path is /b1s/v1. |
| User | Enter the SAP Business One user name for accessing the service layer. |
| Password | Enter the SAP Business One password for accessing the service layer. |
| truststoreURI | To enable https, enter the path and name of the truststore in the BizStore. If the destination host requires https, and you do not provide information in this parameter, the integration framework uses the truststore provided by the Java runtime environment. We do not recommend adding certificates to the truststore of the Java runtime environment, because each upgrade overwrites the truststore and your certificates are no longer available.  If you have defined the http transport protocol, the integration framework ignores this parameter.  To import a certificate to a truststore in the BizStore, see *Operations, Part 2*, section *Creating Keystores and Truststores in the BizStore* |
| readTimeout | Sets the read timeout to a specific timeout in seconds. The read timeout is the timeout for waiting to obtain data from the API. If left empty, the adapter waits indefinitely.  The default value is 300 seconds. |

### 2.1.5 Connecting to SAP Business One Using JDBC

Connect to the SAP Business One company database using JDBC.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| driver | The database vendor provides the specification of the JDBC driver.  This is an example for the Microsoft SQL Server: com.microsoft.sqlserver.jdbc.SQLServerDriver. |
| url | Enter the JDBC URL.  This is an example for the SQL Server 2008 on localhost, dbName=DatabaseName: jdbc:sqlserver://ipaddress:1433;integratedSecurity=false;databaseName=DBNAME;selectMethod=cursor  Note that if you change the *b1Server* and *company* fields in the *Common Fields* section, the integration framework adjusts the URL accordingly. |
| Username | Enter the user name for database access. The user must have according rights for the required operations. Use in the same user name as in the *DIAPI* section in the *dbUser* field. |
| Password | Enter the password for database access. Use the same password as in the *DIAPI* section in the *dbPassword* field. |

## 2.2 Using a Proxy Group for the DI Adapter

The DI adapter allows defining multiple proxy groups in global adapter configuration properties. Using multiple proxies allows load balancing during request processing. Requests can come from IPO steps that are independent of each other. If you process a step using a certain proxy, it uses the proxy during complete step processing.

### 2.2.1 Providing More Proxy Instances in the Operating System

**Procedure**

1. To enable another configuration set for a second instance, copy the *DIProxy* folder and paste it.

The system creates the *DIProxy – Copy* folder.

1. Rename the folder to DIProxy2.
2. In the *…\DIProxy2* folder, open the service.ini file and change the following entries:

* ServiceName=SAPB1iDIProxy2
* DisplayName=SAP Business One DI Proxy 2 Service

1. In the *…\DIProxy2* folder, open the diproxyserver.properties file.
2. Change the HTTPS\_PORT parameter to 2098, if port 2098 is available on your machine.

HTTPS\_PORT=2098

1. Choose *Start*, richt click *Command Prompt* and choose the *Run as administrator* option.
2. To run 32-bit DI proxy: run service.exe with the -install” parameter in the *…\DIProxy2* folder.
3. To run 64-bit DI proxy: Refer to SAP Note 1955107 for a detailed description of required settings and then run service64.exe with the -install parameter in the *…\DIProxy2* folder.
4. Start the *SAP Business One DI Proxy 2 Service Monitor* service.
5. In SLD, change the *diProxyport* value for a reasonable number of companies to 2098.
6. For more instances, repeat the procedure above accordingly.

### 2.2.2 Defining Proxy Groups in DI Adapter

**Procedure**

1. In the integration framework, choose Tools → Control Center → Configuration → Global Adapter Config.
2. In the Global Adapter Configuration Properties user interface, for the B1DI adapter, click the Edit Global Configuration Properties link.
3. For the diProxyGroupList property, define the proxy groups in the following way:

[<groupname1> <hostname1> :<port1>,<port2>][<groupname2> <hostname2> :<port1>,<port2>]

* <groupname1,2> are the proxy group names
* <hostname1,2> are the host names or IP addresses of the proxies
* <port1,2> are the port numbers

1. In SLD in the *diProxyhost* field, enter the proxy group definition you want to use and leave the diProxyport field empty

**Example**

You want use the following proxy groups:

* alpha and beta
* Each group ast wo proxies

[alpha abc:2099 def:3701][beta 1.2.3.4:2099,3000]

* In the *diProxyhost* field, enter [alpha]
* Leave the *diProxyport* field empty

# 3 SAP ERP

To connect to to SAP ERP, the following system types are available:

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| R3.46C | Connection to an SAP ERP system 4.6 C |
| R3.47.100 | Connection to an SAP ERP system 4.7 100 |
| R3.47.200 | Connection to an SAP ERP system 4.7 200 |
| ECC6.0 | Connection to an SAP ERP system ECC 6.0 |
| S/4HANA on Premise | Connection to an SAP S/4HANA on premise system |

For SAP ERP systems, there is an active RFCA (remote function call) connection available to callfunctions using RFC and a passive RFCP connection to receive incoming IDocs.

The integration framework is an RFC server and in passive mode. To send data from an SAP ERP system, configure ALE in SAP ERP. In ALE, define the integration framework server as a logical system.

Using the RFCA adapter, you can call any remote-enabled function in SAP ERP, typically developed in ABAP. You must enable the function to allow remote calls.

For more recent versions of SAP ERP systems ECC, there are additional sections for Web service connections. For more information about how to configure Web services, see the *Web Service* section

## 3.1 Configuring the RFCA Connection

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| applicationServer | Enter the host name or IP address of the SAP ERP application server, for example, iwdf9349.wdf.sap.corp.  To receive this information, contact your SAP ERP administrator. |
| client | Enter the three-digit numerical key to uniquely identify the client in your SAP ERP to which you want to connect. You can find the client identifier in the MANDAN field. |
| user | Enter the name of the user that connects to SAP ERP at runtime to post the interface objects, such as IDocs. |
| password | Enter the password for the SAP ERP runtime user. Note that older ERP systems typically support uppercase passwords only. Very often this is handled transparent as the ERP user interfaces and the RFC connectors perform an automatic transformation to uppercase. This can be the reason why the test connection fails. |
| language | Enter the two-digit language key in ISO code format. Enter, for example, EN for English or DE for German. Refer to your SAP ERP system for the language key table. |
| systemNumber | Enter the two-digit number that identifies the SAP ERP system. This is the instance number you find in the login properties of the SAP ERP system. |
| maxConnections | Define the maximum allowed connections between SAP ERP and the integration framework. |
| gatewayHost | Enter the hostname or IP address of the SAP ERP gateway host, for example, iwdf9349.wdf.sap.corp.  To check the gateway host in SAP ERP, call the smgw transaction and choose Goto → Parameters → Display. |
| gatewayServiceNumber | Enter the number of the gateway service. By default the system compiles the number with the pattern sapgw<*systemNumber*>.  To check the gateway host in SAP ERP, call the smgw transaction and choose Goto → Parameters → Display. |
| senderPartner | The sender partner is the identifier under which the integration framework is defined in SAP ERP system. This identifier is called *logical system*.  Prerequisite is that you have created a *Logical System* for the integration framework in the SAP ERP system. To create a logical system, call /nSALE transaction, navigation path IDoc Interface/Application Link Enabling → Basic Settings → Logical Systems → Define Logical System. |
| senderPort | Sender port. Typically this is also the *logical system*. |
| recieverPartner | The receiver partner is the identifier under which the client (MANDAN) of the SAP ERP system is defined in SAP ERP. This identifier is called *logical system*.  Prerequisite is that you have created and assigned a *logical system* for the client of the SAP ERP system. To create a *logical system* in SAP ERP, call the /nSALE transaction, navigation path IDoc Interface/Application Link Enabling → Basic Settings → Logical Systems → Define Logical System.  To assign the logical system to the client of the SAP ERP system, call the nSALE transaction, IDoc Interface/Application Link Enabling → Basic Settings → Logical Systems → Assign Logical System to Client. |
| recieverPort | Enter the port number of the RFC destination for SAP ERP.  Apart from using the port key, which is for example A000000009, you can access the port using the name of the RFC destination for your SAP ERP client in the SAP ERP system.  To check the port key for the RFC destination, use the WE21 transaction in SAP ERP. In the *Ports* section, expand *Transactional RFC* and identify the port by the description for the logical system. |

## 3.2 Configuring the RFCP Connection

**Procedure**

1. For the following fields, refer to the previous section:

* applicationServer
* client
* user
* password
* language
* systemNumber
* maxConnection
* gatewayHost
* gatewayServiceNumber

1. Enter the following values:

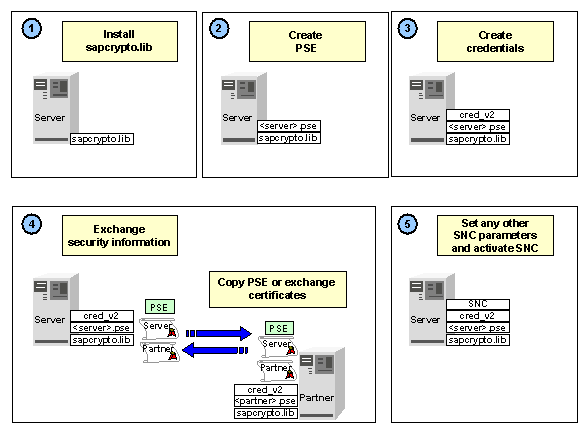
| **Parameter** | **Description** |
| --- | --- |
| programID | The Program Identifier is the Program ID, specified in the RFC destination definition in the SAP ERP system. Prerequisite is that you have created an RFC destination definition for the integration framework. To create the destination in SAP ERP, call the /nSM59. transaction. Select the TCP/IP protocol. |
| unicode | If the ERP client supports Unicode, select true. |

## 3.3 Providing SNC Parameters for Secure RFC Communication

To enable SNC, provide additional entries for the *RFCA* and *RFCP* sections.

**Prerequisites**

* The RFC destination in SAP ERP was enabled with SNC.
* The SAP ERP administrator provided you with the SAP ERP server certificate as a \*.pse file.
* You downloaded the SAP Cryptographic Library from SAP Service Marketplace, choosing support.sap.com → Support Packages and Patches → A-Z Index → S → SAPCRYPTOLIB → SAPCRYPTOLIB <choose a version>.
* You configured the SAP Cryptographic Library, and you have the RFC certificate available to enable trust between the SAP ERP and the integration framework server.
* For more information, see help.sap.com → SAP NetWeaver → SAP NetWeaver 7.5 → Application Help → SAP NetWeaver Library: Function Oriented View → Security → Network and Transport Layer Security → Transport Layer Security on SAP NetWeaver AS for ABAP → Using the SAP Cryptographic Library for SNC → Configuring the Use of the SAP Cryptographic Library for SNC



Find a detailed step-by-step decription in the *Administrator’s Guide for SAP Business One integration for SAP NetWeaver 9.0*.

**Procedure**

1. To enter values, click Display SNC.

In the RFCA and RFCP sections, the SLD provides a set of parameters that is only relevant, if you want to secure the RFC connection using SNC (Secure Network Communication).

1. Provide the following values:

| **Parameter Name** | **Description** | **Required/ Optional** | **Values** |
| --- | --- | --- | --- |
| SNC\_MODE | SNC mode | Required | 0=disabled  1=activated  The default is 0. |
| SNC\_QOP | Quality of protection, protection level | Required | This parameter defines the quality of protection level.  The following options are available:  1: Authentication only  2: Integrity protection  3: Privacy protection (default)  8: Use the value from snc/data\_protection/use on the application server  9: Use the value from snc/data\_protection/max on the application server  Use the same level as the SAP ERP administrator. |
| SNC\_MYNAME | SNC name of the user sending the RFC | Optinal | String  Enter the SNC name of the user sending messages using RFC.  Since we use the same PSE as SAP ERP, this parameter is identical with the value of SNC\_PARTNERNAME. |
| SNC\_PARTNERNAME | SNC name of the communication partner | Required | String  Enter the SNC name of your communication partner.  Since we use the same PSE as SAP ERP, this parameter is identical with the value of SNC\_MYNAME. |
| SNC\_LIB | Path and name of the library that provides the security service. | Required | String  Enter the path and name of your local SNC library, for example, C:\Program Files (x86)\SAP\SAP Business One integration for SAP NetWeaver\secudir\sapcrypto.dll. |

# 4 File System

To connect to a file system, the F.AnySystem system type is available

The integration framework interacts with the file system using separate inbound and outbound directories. The directories must exist in the file system, and the technical user the integration framework uses at runtime, must have full access rights to the directories.

## 4.1 Configuring File Inbound

**Procedure**

Enter the following values in the FILI section:

| **Parameter** | **Description** |
| --- | --- |
| filePattern | To define the inbound file pattern, enter the complete path to the directory and the file specification. The integration framework supports Microsoft Windows UNC (Universal Naming Convention) names.  The directory that you define must be available in the file system. The user for directory access must have the necessary rights in the file system. Use the asterisk (\*), to define multiple files. |
| Encoding | Select the required character encoding from the list. The default is ISO-8859-1.  Character encoding is necessary to apply the technical representation of the characters according to the country or system-specific needs.  The following entries are available: ISO 8859-1, ISO 8859-2, ISO 8859-3, ISO 8859-4, ISO 8859-5, ISO 8859-6, ISO 8859-7, ISO 8859-8, ISO 8859-9, ISO 8859-11, ISO 8859-13, ISO 8859-14, ISO 8859-15, ISO 8859-16, US-ASCII, EBCDIC, Shift-JIS, EUC-JP, ISO-2022, GB2312, EUC-KR, Big5, Unicode UTF-7, Unicode UTF-8, Unicode UTF-16, ISO-10646-UCS2, ISO-10646-UCS4. |
| Delimiter | Enter the delimiter that separates the fields in the file. Usually, this is a comma or semicolon.  This entry is mandatory for DSV (delimiter separated value) files. |
| WrapChar | Define the field wrappers. The field wrapper is optional and only necessary to avoid that a field delimiter character inside a value is misinterpreted as a field delimiter. |
| PayloadType | Define the inbound format or formats supported in file inbound of the selected system:   * automatic detection   The integration framework detects the payload type by the file extension. (xml*→* XML, csv*→* DSV, txt*→* OFFSET).  Define the filePattern in the following way: … .\*.   * xml file   The integration framework interprets any incoming document as an XML document, independent of the file extension.   * dsv file   The integration framework interprets any incoming document as an delimiter-separated value document, independent of the file extension.   * txt file   The integration framework interprets any incoming document as a fixed length file, independent of the file extension. A fixed length file requires an offset definition per field, all lines have the same structure. It is mandatory that you define the field transformation in the XML document in the base directory of the scenario step. Additionally, define the name of the control document in the inbound specification.   * regex file:   The integration framework interprets any document as a text file interpreted by regular expressions, independent of the file extension. It is mandatory that you define the field transformation in an XML document in the base directory of the scenario step. Additionally, define the name of the control document in the inbound specification. |
| LineBreak | Depending on the operating system that you run, the line break commands are different. Select the line break command:   * 1 CRLF (Windows) * 2 LF (Linux) * 3 CR (Mac OS) |

## 4.2 Configuring File Outbound

**Procedure**

Enter the following values in the FILO section:

| **Parameter** | **Description** |
| --- | --- |
| filePattern | To define the outbound file pattern, enter the complete path and the file specification. The integration framework supports Microsoft Windows UNC (Universal Naming Convention) names. The directory must be available in the file system. The user for directory access must have the required rights in the file system.  For more information about using special characters and variables, see the table below. |

For file patterns, you can use the following special characters and variables:

| **Character/**  **Variable** | **Description** |
| --- | --- |
| ? | To introduce numbering in the file directory use ?.  If you enter for example data????.xml, the integration framework creates an outbound file called data0000.xml, if the directory is empty. If a file, following this naming convention, already exists in the outbound directory, the next generated file name is data<last number>+1.xml. If data0000.xml already exists in the directory, the next file in the directory is data0001.xml. |
| [vbiu] | This is a placeholder for a value you can define in scenario package processing. If you use the value, add the b1im\_filename attribute directly in the outbound payload. [This applies to Integration Framework Version 1 only]  <xsl:template name="transform">  <xsl:attribute name="b1im\_filename">myName</xsl:attribute>  ...  </xsl:template> |
| [TID] | Transaction ID [This applies to Integration Framework Version 1 only] |
| [TS] | To add a timestamp to the file name, use the variable. This gives you another possibility to define unique file names. |
| [yyyy] | Adds the year in four digits to the file name |
| [yy] | Adds the year in two digits to the file name |
| [mm] | Adds the month to the file name |
| [dd] | Adds the day to the file name |
| [hour] | Adds the hour to the file name |
| [min] | Adds the minute to the file name |
| [sec] | Adds the second to the file name |

You can combine variables, for example, file[TS]??.[hour][min].txt

# 5 HTTP System

To connect to a system using http or https, the H.AnySystem system type is available

If the destination application requires it, you can authenticate with the user name and password at the destination host using http. Using https, you can additionally authenticate using an X.509 client certificate.

H.AnySystem supports the POX (Plain Old XML) standard supporting HTTP calls with any type of incoming and outgoing XML message.

## 5.1 Configuring HTTP Outbound (HTTA)

In the HTTA section, you configure connection parameters for outgoing HTTP calls to another system.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| destProtocol | To specify the protocol for communication, enter http or https. |
| destHost | Specify the destination host system that receives calls. Enter the IP address or the logical name for the receiver system. |
| destPort | Specify the port and service to be called on the destination host. An empty value defaults to the protocol-specific default. |
| destPath | Destination resource that consists of the remaining destination path and the document name. Do not enter query parameters or fragment identifiers. |
| query | Enter the query strings, separated by semicolon. Do not add ?. |
| proxyHost | If you use a proxy server to connect to the integration framework server, enter the IP address. Leave the field empty if you do not use a proxy. |
| proxyPort | If you use a proxy server to connect to the integration framework server, enter the port number. Leave the field empty if you do not use a proxy. |
| method | Enter the HTTP method. The integration framework supports POST, GET, PUT, DELETE, and TRACE. If you want to set up a standard scenario to handover data using HTTP, use the POST method. |
| authentication | * To enable authentication using user name and password, enter basic. * If you must authenticate at the destination host using an X.509 client certificate, enter x509. * Leave the field empty, if a login is not required by the system. |
| user | Enter the user name for authentication.  To authenticate at the destination host with an X.509 client certificate using https, you can provide the alias here. |
| password | Enter the password for authentication.  To authenticate at the destination host with an X.509 client certificate using https, enter the password for keystore access here. |
| user2query | If the user must be available as a query parameter, this property holds the parameter name. |
| password2query | If the password must be available as a query parameter, this property holds the parameter name. |
| trustStoreURI | To enable https, enter the path and name of the truststore in the BizStore. If the destination host requires https, and you do not provide information in this parameter, the integration framework uses the truststore provided by the Java runtime environment. We do not recommend adding certificates to the truststore of the Java runtime environment, because each upgrade overwrites the truststore and your certificates are no longer available.  If you have defined the http transport protocol, the integration framework ignores this parameter.If you have defined the http transport protocol, the integration framework ignores this parameter. |
| keyStoreURI | To enable the integration framework server to authenticate at the destination host using an X.509 client certificate (private key), enter the path and name of the keystore in the BizStore. Provide the password for keystore access in the *password* field above.  If the destination host requires https and client authentication with an X.509 certificate , and you do not provide information in this parameter, the integration framework accesses the keystore provided by the Java runtime environment. If you have defined the http transport protocol, the integration framework ignores this parameter.  For more information about the keystore and truststore in the BizStore, see *Creating Keystores and Truststores in the BizStore* |
| tlsVersion | Enter the required version of the TLS protocol, if the host does not accept the JRE standard setting. |
| readTimeout | Sets the read timeout to a specific timeout in seconds. The read timeout is the timeout for waiting to obtain data from the API. If left empty, the adapter waits indefinitely.  The default value is 300 seconds. |

## 5.2 Configuring HTTP Inbound (HTTP)

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| associatedSrvIP | If an incoming HTTP call is associated to an SAP Business One system, use the parameter to define the relevant association details. The parameter depends on the scenario package you want to set up with this SLD entry. For the *sap.B1Mobile* scenario package, the parameter is b1Server/company, for the *sap.Xcelsius* scenario package, the parameter is the b1server. The parameter has to be the same as in SLD entry for SAP Business One for this parameter. |

# 6 Web Service

To call a Web service or to provide a Web service, use the W.AnySystem system type.

If the destination system requires it, you can authenticate with the user name and password at the destination host using http. Using https, you can additionally authenticate using an X.509 client certificate.

The following sections are available:

* WSAN (active connectivity), for outgoing one-way, asynchronous communication, client, consumer. To use the Web service type, enter parameters in the *WSAN* section.
* WSAS (active connectivity), for outgoing request-response, synchronous communication, client, consumer. To use the Web service type, enter parameters in the *WSAS* section
* WSAO (passive connectivity) for incoming one-way, asynchronous communication, service, provider. The passive Web service type does not require any parameters.
* WSAR (passive connectivity) for incoming request-response, synchronous communication, service, provider

## 6.1 Configuring the WSAS and WSAN Connections

The *WSAS* and *WSAN* sections require the same parameters. WSAS supports an outgoing solicit/response call. WSAN supports an outgoing notification.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| destProtocol | To specify the protocol for communication, enter http or https. |
| destHost | Specify the destination host system that receives calls. Enter the IP address or the symbolic name for the receiver system. |
| destPort | Specify the port or service called on the destination host. An empty value defaults to the protocol-specific default. |
| destPath | Enter the destination resource consisting of the remaining destination path and the document name. Do not use query parameters or fragment identifiers. |
| query | Enter the query strings, separated by semicolon. |
| proxyHost | If you use a proxy server to connect to the integration framework server, enter the IP address. Leave the field empty if you do not use a proxy. |
| proxyPort | If you use a proxy server to connect to the integration framework server, enter the port number. Leave the field empty if you do not use a proxy. |
| authentication | * To enable authentication using user name and password, enter basic. * If you must authenticate at the destination host using an X.509 client certificate, enter x509. * Leave the field empty, if no login is required by the system. |
| user | Enter the user name for authentication.  To authenticate at the destination host with an X.509 client certificate using https, you can provide the alias here. |
| password | Enter the password for authentication.  To authenticate at the destination host with an X.509 client certificate using https, enter the password for keystore access here. |
| trustStoreURI | To enable https, enter the path and name of the truststore in the BizStore. If the destination host requires https, and you do not provide information in this parameter, the integration framework uses the truststore provided by the Java runtime environment. We do not recommend adding certificates to the truststore of the Java runtime environment, because each upgrade overwrites the truststore and your certificates are no longer available.  If you have defined the http transport protocol, the integration framework ignores this parameter. If you have defined the http transport protocol, the integration framework ignores this parameter. |
| keyStoreURI | To enable the integration framework server to authenticate at the destination host using an X.509 client certificate (private key), enter the path and name of the keystore in the BizStore. Provide the password for keystore access in the *password* field above.  If the destination host requires https and client authentication with an X.509 certificate , and you do not provide information in this parameter, the integration framework accesses the keystore provided by the Java runtime environment. If you have defined the http transport protocol, the integration framework ignores this parameter.  For more information about the keystore and truststore in the BizStore, see section *Creating Keystores and Truststores in the BizStore* |
| readTimeout | Sets the read timeout to a specific timeout in seconds. The read timeout is the timeout for waiting to obtain data from the API. If left empty, the adapter waits indefinitely.  The default value is 300 seconds. |

## 6.2 Configuring the WSAR Connection

The WSAR connection supports supports an incoming request call that requires a response. The WSAO connection supports incoming one way calls and does not require parameters in SLD.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| associatedSrvIP | If an incoming HTTP call is associated with a particular SAP Business One system, specify the relevant association details using the parameter. The parameter depends on the scenario package you want to set up with this SLD entry. For the *sap.B1Mobile* scenario package, the parameter is b1Server/company, for the *sap.Xcelsius* scenario package, the parameter is the b1server. The name you enter here must be identical with the name you enter in SLD for the SAP Business One system. |

# 7 Connecting to Databases

To connect to a database, the J.AnySystem system type is available. The integration framework enables you to interact with any database system that provides access using JDBC.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| driver | The database vendor provides the specification of the JDBC driver.  This is an example for SQL Server 2005 and 2008: com.microsoft.sqlserver.jdbc.SQLServerDriver |
| url | Specify the JDBC URL.  Example for SQL Server 2008 on localhost, dbName=DatabaseName: jdbc:sqlserver://ipaddress:1433;integratedSecurity=false;databaseName=DBNAME;selectMethod=cursor |
| username | Enter the user name for database access. The user must have all necessary rights for operations. |
| password | Enter the password for database access. |

# 8 FTP System

Currently, the integration framework does not support the File Transfer Protocol (FTP) for inbound and outbound channels.

If you want to retrieve data using FTP, define a scenario step that uses timer-triggered inbound and perform the FTP call directly in the process flow using the *Download File fron FTP Server* atom.

If you want to send data to an FTP outbound system, define a scenario package using VOID outbound and hand over the data using FTP directly in the process flow using the *Write File to FTP Server* atom.

To connect to an FTP server, use the P.AnySystem system type.

## 8.1 Configuring FTP Outbound

To send files to an FTP server, use the FTPO section.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| ftpServer | Enter the FTP server address or server name. |
| protocol | Select the protocol you want to use. You have the following options:   * FTP   FTP protocol without encryption.   * FTP over SSH   This is the Secure File Transfer Protocol (SFTP) option.   * FTP over SSL explicit   This is the FTPS option. It secures the control and the data connection. |
| ftpPort | Enter the port number. The default is the standard port for the FTP server (21). |
| username | To logon to the FTP server, enter the user name. |
| password | To logon to the FTP server, enter the password. |
| filePattern | Enter the file pattern and target directory on the FTP server for the file you want to save or delete on the FTP server. For the target directory, you can enter an absolute or relative path. When providing the path, comply with the rules of the FTP server operating system.  If you want to create a file, you can add the following to the file pattern:   * Use the ? character to add a counter to the file name. For example, when using **myfile??.txt**, the integration framework checks the file pattern in the FTP target directory and provides myfile02.txt on the FTP server, if myfile01.txt already exists. * [TS] adds the timestamp to the file name. * [yyyy] adds the current year in four digits format to the file name * [yy] adds the current year in two digits format to the file name * [mm] adds the current month to the file name * [dd] adds the current day to the file name * [hour] adds the current hour to the file name * [min] adds the current minute to the file name * [sec] adds the current second to the file name |
| proxyHost | Enter the proxy Host IP address or name. |
| proxyPort | Enter the proxy port. |
| proxyUser | Enter the user name to access the proxy. |
| proxyPassword | Enter the password to access the proxy. |
| proxyType | Select the type. You have the following options:   * NOPROXY   Select to directly connect to the FTP server without using a proxy.   * HTTP   Select to indicate an HTTP proxy   * SOCKS4   Select to indicate a SOCKS proxy using version 4   * SOCKS5   Select to indicate a SOCKS proxy using version 5 |
| ssl\_trustStoreURI | Enter the path and name of the truststore in the BizStore. If the destination host requires a secure connection, and you do not provide information in this parameter, the integration framework uses the truststore provided by the Java runtime environment. We do not recommend adding certificates to the truststore of the Java runtime environment, because each upgrade overwrites the truststore and your certificates are no longer available.  If you have defined the http transport protocol, the integration framework ignores this parameter. If you have defined the FTP transport protocol, the integration framework ignores this parameter. |
| ssl\_trustStorePassword | Enter the password for the truststore. |

## 8.2 Configuring FTP Inbound

To poll files from an FTP server, use the FTPP section.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| ftpServer | Enter the FTP server address or server name. |
| protocol | Select the protocol you want to use. You have the following options:   * FTP   FTP protocol without encryption.   * FTP over SSH   This is the Secure File Transfer Protocol (SFTP) option.   * FTP over SSL explicit   This is the FTPS option. It secures the control and the data connection. |
| ftpPort | Enter the port number. The default is the standard port for the FTP server (21). |
| username | To logon to the FTP server, enter the user name. |
| password | To logon to the FTP server, enter the password. |
| filePattern | To download a single file, provide the file pattern, extension and the target directory on the FTP server for the file you want to retrieve from the FTP server. For the source directory, you can provide an absolute or relative path. When providing the path, comply to the rules of the FTP server operating system. To retrieve a list of files, provide the path to the directory. You can use the \* and ? wildcard characters. |
| proxyHost | Enter the proxy Host IP address or name. |
| proxyPort | Enter the proxy port. |
| proxyUser | Enter the user name to access the proxy. |
| proxyPassword | Enter the password to access the proxy. |
| proxyType | Select the type. You have the following options:   * NOPROXY   Select to directly connect to the FTP server without using a proxy.   * HTTP   Select to indicate an HTTP proxy   * SOCKS4   Select to indicate a SOCKS proxy using version 4   * SOCKS5   Select to indicate a SOCKS proxy using version 5 |
| ssl\_trustStoreURI | Enter the path and name of the truststore in the BizStore. If the destination host requires a secure connection, and you do not provide information in this parameter, the integration framework uses the truststore provided by the Java runtime environment. We do not recommend adding certificates to the truststore of the Java runtime environment, because each upgrade overwrites the truststore and your certificates are no longer available.  If you have defined the http transport protocol, the integration framework ignores this parameter. If you have defined the FTP transport protocol, the integration framework ignores this parameter. |
| ssl\_trustStorePassword | Enter the password for the truststore. |

# 9 E-Mail System

The integration framework currently does not support connecting to an e-mail server in inbound and outbound channels. If you want to trigger a scenario step by an incoming e-mail, define a scenario step that uses timer-triggered inbound and use the *Receive Email* atom directly in the process flow.

If you want to address an e-mail system in the outbound phase, define a scenario step using VOID outbound and hand over the data using the *Send Email* atom directly in the process flow.

To connect to an e-mail server, the E.AnySystem system type is available.

## 9.1 Sending E-Mails

**Procedure**

Enter the following values in the SMPT section:

| **Parameter** | **Description** |
| --- | --- |
| protocol | To define the protocol for communication, you have the following options:   * SMTP (default) * SMTPS (SMTP is secured on the transport layer using SSL), or * TLS.   To enable SMTPS, use the keytool to make the certificate available in the SAP JVM keystore. |
| smtpHost | Enter the address of the e-mail server host. |
| smtpPort | Enter the port of the e-mail server host. |
| username | Enter the user name to access the e-mail server. |
| password | Enter the password to access the e-mail server. |
| trustedHost | You can add the name of the e-mail server to the list of trusted hosts. If the e-mail server requires a certificate for a secure connection, you do not need to import the certificate to the Java keystore. To add the name of the e-mail server to the list of trusted hosts, select true.  If the e-mail server requires a secure connection and you set the value to false, import the certificate to the Java keystore using the keytool program. The default value is false. |

## 9.2 Receiving E-Mails

**Procedure**

Enter the following values in the MAIR section:

| **Parameter** | **Description** |
| --- | --- |
| Protocol | You have the following options:   * POP3 (Post Office Protocol Version 3) to download e-mails from an e-mail server * IMAP (Internet Message Access Protocol) to access e-mails in a folder of an e-mail server |
| Host | Enter the host name or IP address of the e-mail server. |
| Port | Enter the port of the e-mail server.   * For IMAP, the standard port is 143. The standard port for a secure connection is 993. * For POP3, the standard port is 110. The standard port for a secure connection is 995. |
| User | Enter the user name to access the e-mail server. |
| Password | Enter the password to access the e-mail server. |
| UseSSL | To enable a secure connection to the e-mail server using Secure Socket Layer (SSL), select true. The adapter supports the SSL connection without checking the certificate. |

# 10 Scheduler

To trigger scenario steps by a timer, enter values for the T.AnySystem system type.

**Procedure**

Enter the following values:

| **Parameter** | **Description** |
| --- | --- |
| minute | Set the value for the *minute* part of the time. Use \* or a list of elements separated by comma. An element is either a number in the range of 0 to 59 or two numbers in the range separated by a hyphen. This is an inclusive range. Enter, for example, \* or 5 or 0,30, or 0-59 |
| hour | Set the value for the *hour* part of the time. Use \* or a list of elements separated by comma. An element is either a number in the range 0 to 23 or two numbers in the range separated by a hyphen. This is an inclusive range. |
| day | Set the value for the *day* part of the date. Use \* or a list of elements separated by comma. An element is either a number in the range 1 to 31 or two numbers in the range separated by a hyphen. This is an inclusive range. |
| month | Set the value for the *month* part of the date. Use \* or a list of elements separated by comma. An element is either a number in the range 1 to 12 or two numbers in the range separated by a hyphen: This is an inclusive range. |
| dow | Day of week  Set the value for the *day of the week*. Use \* or a list of elements separated by commas. An element is either a number in the range 0 to 6 (Sunday = 0) or two numbers in the range separated by a hyphen. This is an inclusive range. |
| year | Set the value for the *year* part of the date. Use \* or a list of elements separated by comma. An element is either a number, specifying a year, for example, 2015, or two numbers in the range separated by a hyphen. This is an inclusive range. |

**Example**

The following entry in the minute field triggers the step every ten minutes:

0,10,20,30,40,50

# 11 Displaying and Enhancing System Type Properties

SAP delivers properties for system types. You can use system type properties as filter criteria, and you can add individual properties to the system types.

**Procedure**

1. To add properties to system types, choose *SLD*, select the B1i Server entry, right-click to open the context menu and select SysType Properties.

The SLD displays property names and default values for system type properties that SAP delivers. You cannot change or delete properties delivered by SAP.

1. To add system type properties for a system type, scroll down to the system type and click Add.

The SLD adds an entry at the end of the property list.

1. To enter property details, click Details.
2. In the Name field, enter the property name.
3. In the Default Value field, you can enter a default value
4. In the Description field, enter a description for the property.
5. To define a list of values for selection, enter the values is the following way in the Enumeration field:

Value1\*Value2\*Value3\*

1. To delete a property, click Delete.

# Copyrights, Trademarks, and Disclaimers

© Copyright 2023 SAP SE. All rights reserved.

The current version of the copyrights, trademarks, and disclaimers at <https://www.sap.com/about/legal/copyright.html> is valid for this document.